

# Documentation

## OpenScape Office V3

Feature Description

A31003-P1030-F100-12-7618

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standards and are certified by an external certification company.

Copyright © Siemens Enterprise Communications GmbH & Co. KG 04/2012  
Hofmannstr. 51, D-80200 München

Siemens Enterprise Communications GmbH & Co. KG is a Trademark Licensee of Siemens AG

Reference No.: A31003-P1030-F100-12-7618

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.

OpenScope, OpenStage and HiPath are registered trademarks of Siemens Enterprise Communications GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

# Contents

<b>1 Introduction and Important Notes</b>	<b>15</b>
1.1 About this Documentation	15
1.1.1 Documentation and Target Groups	15
1.1.2 Structure	17
1.1.3 Types of Topics	20
1.1.4 Display Conventions	20
1.2 Safety Information and Warnings	21
1.2.1 Warnings: Danger	22
1.2.2 Warnings: Warning	23
1.2.3 Warnings: Caution	24
1.2.4 Warnings: Note	24
1.3 Important Notes	25
1.3.1 Emergencies	25
1.3.2 Intended Use	26
1.3.3 Correct Disposal and Recycling	26
1.3.4 Installation Standards and Guidelines	27
1.3.4.1 Connecting OpenScape Office MX to the Power Supply Circuit	27
1.3.4.2 Connecting OpenScape Office LX and OpenScape Office HX to the Power Supply Circuit	27
1.3.4.3 Shielded Cabling for LAN, WAN and DMZ Connections of OpenScape Office MX	28
1.3.4.4 Marks (MX)	29
1.3.5 Notes on Electromagnetic and Radio Frequency Interference (MX)	29
1.3.6 Data Protection and Data Security	29
1.3.7 Technical Regulations and Conformity (MX)	30
1.3.7.1 CE Conformity	30
1.3.7.2 Conformity with US and Canadian Standards	31
1.3.7.3 Conformity with International Standards	31
1.3.8 Operating Conditions	31
1.3.8.1 Operating Conditions for OpenScape Office MX	31
1.3.8.2 Operating Conditions for OpenScape Office LX and OpenScape Office HX	32
<b>2 System Overview and Scenarios</b>	<b>33</b>
2.1 System Overview	33
2.1.1 OpenScape Office LX	35
2.1.2 OpenScape Office MX	35
2.1.3 OpenScape Office HX	37
2.1.4 Communications Clients, Mobility Clients and Contact Center Clients	38
2.1.5 Supported Phones	40
2.1.6 Infrastructure Components	42
2.1.7 Open Interfaces	42
2.1.8 Recommended and Certified Applications	42
2.1.9 Additional Links	43
2.2 Sample Scenarios	43
2.2.1 Sample Scenario for OpenScape Office LX	43
2.2.2 Sample Scenario for OpenScape Office MX	44
2.2.3 Sample Scenario for OpenScape Office HX	45
<b>3 Hardware and Installation of OpenScape Office MX</b>	<b>47</b>
3.1 OpenScape Office MX System Box	47

Contents

- 3.1.1 Motherboard ..... 48
- 3.1.2 Slot and Access Designations ..... 53
- 3.2 Gateway Modules ..... 55
  - 3.2.1 Not for U.S. and Canada: Gateway Module GMS ..... 56
  - 3.2.2 Not for U.S. and Canada: Gateway Module GMSA ..... 57
  - 3.2.3 Not for U.S. and Canada: Gateway Module GME ..... 59
  - 3.2.4 For U.S. and Canada only: Gateway Module GMT ..... 61
  - 3.2.5 Gateway Module GMAA ..... 62
  - 3.2.6 Gateway Module GMAL ..... 64
- 3.3 Installation ..... 65
  - 3.3.1 Prerequisites for Installation ..... 66
  - 3.3.2 Preparatory Steps ..... 68
  - 3.3.3 Installation Methods ..... 68
  - 3.3.4 Protective Grounding ..... 68
  - 3.3.5 Trunk connection ..... 69
  - 3.3.6 Integration in the LAN Infrastructure ..... 69
  - 3.3.7 Connecting ISDN Phones and Analog Phones and Devices ..... 70
  - 3.3.8 Closing Activities ..... 70
- 3.4 Multibox Systems ..... 70
  - 3.4.1 Details on Multibox Systems ..... 70
  - 3.4.2 Configuring a Multibox System ..... 71
- 4 Administration Concept ..... 72**
  - 4.1 Web Based Management ..... 72
    - 4.1.1 Prerequisites for OpenScope Office Assistant ..... 72
    - 4.1.2 OpenScope Office Assistant ..... 72
    - 4.1.3 User Administration of OpenScope Office Assistant ..... 74
    - 4.1.4 Online Help ..... 75
  - 4.2 Wizards (LX/MX) ..... 75
    - 4.2.1 Wizards – **Basic Installation (LX/MX)** ..... 75
    - 4.2.2 Wizards – **Network / Internet (LX/MX)** ..... 75
    - 4.2.3 Wizards – **Telephones / Subscribers (LX/MX)** ..... 76
    - 4.2.4 Wizards – **Central Telephony (LX/MX)** ..... 76
    - 4.2.5 Wizards – **User Telephony (LX/MX)** ..... 77
    - 4.2.6 Wizards – **UC Suite** ..... 77
  - 4.3 Expert mode ..... 78
    - 4.3.1 Expert Mode - **Maintenance > Configuration (LX/MX)** ..... 78
    - 4.3.2 Expert Mode - **Maintenance > Software Image (LX/MX)** ..... 79
    - 4.3.3 Expert Mode - **Maintenance > Traces (LX/MX)** ..... 79
    - 4.3.4 Expert Mode - **Maintenance > Events (LX/MX)** ..... 80
    - 4.3.5 Expert Mode - **Maintenance > SNMP (LX/MX)** ..... 80
    - 4.3.6 Expert Mode - **Maintenance > Admin Log (LX/MX)** ..... 80
    - 4.3.7 Expert Mode - **Maintenance > Actions (LX/MX)** ..... 80
    - 4.3.8 Expert Mode - **Maintenance > Platform Diagnostics (LX/MX)** ..... 81
    - 4.3.9 Expert Mode - **Maintenance > Application Diagnostics (LX/MX)** ..... 81
    - 4.3.10 Experten-Modus – **Telephony > Basic Settings (LX/MX)** ..... 81
    - 4.3.11 Expert Mode – **Telephony > Security (MX)** ..... 82
    - 4.3.12 Expert Mode – **Telephony > Network Interfaces (MX)** ..... 83
    - 4.3.13 Expert Mode – **Telephony > Routing (MX)** ..... 83
    - 4.3.14 Expert Mode – **Telephony Voice > Voice Gateway (LX/MX)** ..... 83
    - 4.3.15 Experten-Modus – **Telephony > Stations (LX/MX)** ..... 84
    - 4.3.16 Expert Mode – **Telephony > Incoming Calls (LX/MX)** ..... 84

- 4.3.17 Expert Mode – **Telephony > Trunks/Routing (LX/MX)** ..... 85
- 4.3.18 Experten-Modus – **Telephony > Classes of Service (LX/MX)** ..... 85
- 4.3.19 Expert Mode – **Telephony > Auxiliary Equipment (LX/MX)** ..... 86
- 4.3.20 Experten-Modus – **Telephony > Payload (LX/MX)** ..... 86
- 4.3.21 Experten-Modus – **Telephony > Statistics (LX/MX)** ..... 86
- 4.3.22 Expert Mode – **Applications > UC Suite** ..... 87
- 4.3.23 Expert mode – **Applications > Web Services (LX/MX)** ..... 89
- 4.4 Service Center ..... 89
  - 4.4.1 Service Center - **Download Center** ..... 90
  - 4.4.2 Service Center – **Inventory** ..... 90
  - 4.4.3 Service Center – **Software Update** ..... 91
  - 4.4.4 Service Center – **E-mail Forwarding** ..... 91
  - 4.4.5 Service Center – **Remote Access (LX/MX)** ..... 91
  - 4.4.6 Service Center – **Restart / Reload** ..... 91
  - 4.4.7 Service Center – **Diagnostics > Status (LX/MX)** ..... 91
  - 4.4.8 Service Center – **Diagnostics > Event Viewer (LX/MX)** ..... 91
  - 4.4.9 Service Center – **Diagnostics > Trace** ..... 92
- 5 Connection to Service Provider (LX/MX) ..... 93**
  - 5.1 Internet Access (MX) ..... 93
    - 5.1.1 Internet Access via an External Internet Router (MX) ..... 94
    - 5.1.2 Internet Access via an Internet Modem (MX) ..... 95
    - 5.1.3 WAN Port (MX) ..... 96
    - 5.1.4 NAT (MX) ..... 96
    - 5.1.5 DNS, Domain Name Service (MX) ..... 97
    - 5.1.6 Gateway DNS Functionality (MX) ..... 97
    - 5.1.7 DNS Zones (MX) ..... 98
    - 5.1.8 DynDNS (MX) ..... 98
    - 5.1.9 IP Routing (MX) ..... 99
    - 5.1.10 IP Mapping (MX) ..... 100
  - 5.2 IP Telephony (Voice over IP, VoIP) ..... 100
    - 5.2.1 ITSP Requirements (LX/MX) ..... 101
    - 5.2.2 Internet Telephony via a Station Connection (LX/MX) ..... 102
    - 5.2.3 Internet Telephony via a Point-to-Point Connection (LX/MX) ..... 102
    - 5.2.4 STUN (Simple Traversal of UDP through NAT (LX/MX) ..... 102
  - 5.3 Outside Line (MX) ..... 103
    - 5.3.1 Trunks (MX) ..... 103
    - 5.3.2 Routes (MX) ..... 105
    - 5.3.3 Prioritization for Exchange Line Seizure (LX/MX) ..... 107
    - 5.3.4 Dial Tone Monitoring ..... 107
- 6 Subscribers/Stations ..... 109**
  - 6.1 Dial Plan ..... 109
    - 6.1.1 Default Dial Plan for OpenScope Office LX/MX ..... 111
    - 6.1.2 Individual Dial Plan for OpenScope Office LX/MX ..... 111
  - 6.2 IP Stations and LAN Telephony (LX/MX) ..... 112
    - 6.2.1 IP Stations ..... 112
    - 6.2.2 LAN Telephony Requirements (LX/MX) ..... 113
    - 6.2.3 IP Addresses (LX/MX) ..... 113
    - 6.2.4 DHCP, Dynamic Host Configuration Protocol (LX/MX) ..... 114
    - 6.2.5 IP Protocols (LX/MX) ..... 115
    - 6.2.6 Audio Codecs (LX/MX) ..... 116
    - 6.2.7 RTP Payload for Telephony Tones According to RFC2833 (LX/MX) ..... 117

## Contents

6.2.8	Quality of Service (LX/MX)	117
6.2.9	CorNet-IP Security (LX/MX)	118
6.2.10	Key Programming (LX/MX)	119
6.3	ISDN Stations and Analog Stations	120
6.3.1	ISDN Stations (LX/MX)	120
6.3.2	Analog Stations (LX/MX)	121
6.4	Users of the UC Suite	122
6.5	Virtual Stations	122
6.5.1	Virtual Stations for Mobility Entry	123
6.5.2	Virtual stations for call forwarding	123
6.6	Station and User Profiles	123
6.7	Configuring Stations	123
6.7.1	Configuring Stations Using Wizards (LX/MX)	124
6.7.2	Configuring Stations in Expert Mode (LX/MX)	126
6.7.3	Configuring Users of the UC Suite	128
6.7.4	Exporting Subscriber Data	130
6.8	Configuring Station and User Profiles	131
6.8.1	Configuring Station Profiles (LX/MX)	131
6.8.2	Configuring the User Profiles of UC Clients	132
<b>7</b>	<b>Licensing</b>	<b>134</b>
7.1	Licensing Procedure	134
7.1.1	License Server (Central License Server, CLS)	134
7.1.2	Grace Period	135
7.1.3	MAC Address	135
7.1.4	Advanced Locking ID (LX)	135
7.1.5	Licensing Process using OpenScope Office MX as an Example	136
7.2	Licenses	136
7.2.1	Basic Licenses	137
7.2.2	Extension Licenses	138
7.2.3	Licenses for Multimedia Contact Center	140
7.2.4	Evaluation Licenses	141
7.2.5	Upgrade Licenses	142
7.3	Activating and Updating Licenses	142
7.3.1	Activating Licenses (MX/LX)	143
7.3.2	Updating a License (MX/LX)	144
7.4	Licensing in an Internetwork	145
7.4.1	Licensing Process in the Internetwork	147
7.5	License Information in OpenScopeOffice Assistant	147
7.5.1	License Information without a Network (Standalone)	148
7.5.2	License Information in an Internetwork	148
<b>8</b>	<b>Unified Communications</b>	<b>149</b>
8.1	UC Clients	149
8.1.1	myPortal for Desktop	150
8.1.2	myPortal for Outlook	150
8.1.3	myPortal for Zimbra	151
8.1.4	myPortal for OpenStage	151
8.1.5	Fax Printer	152
8.1.6	myAttendant	152
8.1.7	Prerequisites for UC PC Clients	152
8.1.8	Prerequisites for myPortal for Zimbra	155
8.1.9	Prerequisites for myPortal for OpenStage	156

- 8.1.10 Silent installation/Uninstallation for UC PC Clients . . . . . 157
- 8.1.11 Automatic Updates . . . . . 157
- 8.2 Presence Status and CallMe Service . . . . . 158
  - 8.2.1 Presence Status . . . . . 158
  - 8.2.2 CallMe Service . . . . . 161
  - 8.2.3 Status-based call forwarding . . . . . 162
  - 8.2.4 Rule-Based Call Forwarding . . . . . 163
- 8.3 Directories and Journal . . . . . 164
  - 8.3.1 Directories . . . . . 164
  - 8.3.2 Internal Directory . . . . . 166
  - 8.3.3 External directory . . . . . 167
  - 8.3.4 External Offline Directory (LDAP) . . . . . 168
  - 8.3.5 System Directory . . . . . 169
  - 8.3.6 Departments . . . . . 169
  - 8.3.7 OpenScape Office Directory Service . . . . . 170
  - 8.3.8 Favorites List . . . . . 173
  - 8.3.9 Journal . . . . . 174
- 8.4 Calls . . . . . 175
  - 8.4.1 Call Number Formats . . . . . 176
  - 8.4.2 Desktop Dialer . . . . . 176
  - 8.4.3 Screen pops . . . . . 177
  - 8.4.4 Record calls . . . . . 177
- 8.5 Conferences . . . . . 178
  - 8.5.1 Conference Management (LX/MX) . . . . . 178
  - 8.5.2 Ad-hoc Conference (LX/MX) . . . . . 182
  - 8.5.3 Scheduled Conference (LX/MX) . . . . . 183
  - 8.5.4 Permanent Conference (LX/MX) . . . . . 185
  - 8.5.5 Open Conference (LX/MX) . . . . . 186
  - 8.5.6 Web Collaboration Integration . . . . . 187
- 8.6 Voice and Fax Messages . . . . . 188
  - 8.6.1 Voicemail Box . . . . . 188
  - 8.6.2 Voicemail Announcements . . . . . 190
  - 8.6.3 Phone Menu of the Voicemail Box . . . . . 192
  - 8.6.4 Fax box . . . . . 193
  - 8.6.5 Sending Fax Messages with Fax Printer . . . . . 194
  - 8.6.6 Notification Service for Messages . . . . . 195
  - 8.6.7 Sending E-mails . . . . . 196
  - 8.6.8 SMS Template . . . . . 197
  - 8.6.9 Fax over IP (T.38 Fax) (LX/MX) . . . . . 197
- 8.7 Instant Messaging . . . . . 199
  - 8.7.1 Instant Messaging . . . . . 199
- 8.8 AutoAttendant . . . . . 200
  - 8.8.1 Central AutoAttendant . . . . . 200
  - 8.8.2 Personal AutoAttendant . . . . . 200
  - 8.8.3 Announcements for the AutoAttendant . . . . . 201
  - 8.8.4 Profiles for the AutoAttendant . . . . . 203
- 8.9 Attendant Console Functions . . . . . 204
  - 8.9.1 Subscriber Management . . . . . 204
  - 8.9.2 Message Center . . . . . 204
- 9 Functions at the Telephone (LX/MX) . . . . . 206**
- 9.1 Making Calls (LX/MX) . . . . . 206

Contents

- 9.1.1 Digit Dialing . . . . . 206
- 9.1.2 En-Bloc Dialing . . . . . 206
- 9.1.3 End-of-Dialing Recognition . . . . . 207
- 9.1.4 Editing the Telephone Number . . . . . 207
- 9.1.5 Redialing . . . . . 207
- 9.1.6 System Speed Dialing . . . . . 208
- 9.1.7 Individual Speed Dialing (ISD). . . . . 210
- 9.1.8 Direct station select . . . . . 211
- 9.1.9 Speaker Calls / Direct Answering . . . . . 211
- 9.1.10 Associated Dialing . . . . . 212
- 9.1.11 Trunk Queuing . . . . . 212
- 9.1.12 Private Trunk . . . . . 213
- 9.2 Call Signaling, Calling Line ID (LX/MX). . . . . 213
  - 9.2.1 Different Call Signaling . . . . . 214
  - 9.2.2 Calling Line Identification Presentation (CLIP) . . . . . 214
  - 9.2.3 Calling Line Identification Restriction (CLIR) . . . . . 215
  - 9.2.4 Connected Line Identification Presentation (COLP) . . . . . 216
  - 9.2.5 Connected Line Identification Restriction (COLR) . . . . . 216
  - 9.2.6 CLIP No Screening (Transmission of Customer-Specific Phone Number Information) . . . . . 217
  - 9.2.7 CLIP for Analog Telephones . . . . . 217
  - 9.2.8 Ringer Cutoff . . . . . 218
  - 9.2.9 Translating Station Numbers to Names for System Speed Dialing . . . . . 218
- 9.3 Functions During a Call (LX/MX). . . . . 218
  - 9.3.1 Placing a call on hold . . . . . 218
  - 9.3.2 Parking . . . . . 219
  - 9.3.3 Consultation . . . . . 220
  - 9.3.4 Alternate (Toggle/Connect) . . . . . 220
  - 9.3.5 Transfer . . . . . 220
  - 9.3.6 Automatic Recall . . . . . 221
  - 9.3.7 Call Monitoring (Selected Countries Only) . . . . . 222
- 9.4 Controlling Availability (LX/MX). . . . . 223
  - 9.4.1 Call Forwarding on Busy . . . . . 223
  - 9.4.2 Call Forwarding—No Answer (CFNA) With a Timeout (Fixed Call Forwarding) . . . . . 223
  - 9.4.3 Call Forwarding (CF) . . . . . 224
  - 9.4.4 Call Forwarding After Timeout . . . . . 226
  - 9.4.5 External Call Forwarding - No Answer (Not for U.S.) . . . . . 227
  - 9.4.6 Ringing Assignment / Call Allocation . . . . . 227
  - 9.4.7 Rejecting Calls . . . . . 227
  - 9.4.8 Deferring a Call . . . . . 228
  - 9.4.9 Do Not Disturb . . . . . 228
- 9.5 Optimizing Communication (LX/MX). . . . . 229
  - 9.5.1 Callback . . . . . 229
  - 9.5.2 Call waiting . . . . . 230
  - 9.5.3 Override . . . . . 231
  - 9.5.4 Advisory Messages . . . . . 232
  - 9.5.5 Message Texts . . . . . 232
  - 9.5.6 Associated Services . . . . . 233
  - 9.5.7 Reset activated features . . . . . 233
  - 9.5.8 Procedures . . . . . 234
- 10 Working in a Team (Groups) (LX/MX) . . . . . 236**
  - 10.1 Call Pickup Group, Group Call and Hunt Group (LX/MX) . . . . . 236



- 10.1.1 Call pickup group ..... 236
- 10.1.2 Group Call..... 237
- 10.1.3 Hunt Group..... 241
- 10.1.4 Configuring Call Pickup Groups, Group Calls and Hunt Groups using Wizards ..... 243
- 10.1.5 Configuring Call Pickup Groups, Group Calls and Hunt Groups using Expert Mode ..... 244
- 10.2 Team Configuration / Team Group and Executive/Secretary or Top Group (LX/MX) ..... 244
  - 10.2.1 Team Configuration / Team Group ..... 245
  - 10.2.2 Executive/Secretary or Top Group ..... 248
  - 10.2.3 Configuring Team Configurations / Team Groups and Executive/Secretary Functions / Top Groups using Wizards ..... 252
  - 10.2.4 Configuring Team configurations / Team groups and Executive/Secretary functions / Top groups using Expert mode ..... 252
- 10.3 Basic MULAP and Executive MULAP (LX/MX) ..... 253
  - 10.3.1 Basic MULAP ..... 253
  - 10.3.2 Executive MULAP ..... 255
  - 10.3.3 Configuring Basic MULAPs and Executive MULAPs ..... 257
- 10.4 Voicemail Group and Fax Box Group (LX/MX) ..... 258
  - 10.4.1 Voicemail Group ..... 258
  - 10.4.2 Fax Box Group ..... 258
  - 10.4.3 Configuring Voicemail Box Groups and Fax Box Groups ..... 259
- 10.5 Speaker Call for Groups (LX/MX) ..... 259
  - 10.5.1 Internal Paging ..... 259
  - 10.5.2 Transfer to Group from Announcement ..... 260
- 10.6 UCD (Uniform Call Distribution) (LX/MX) ..... 260
  - 10.6.1 Call Distribution / UCD Group ..... 261
  - 10.6.2 UCD Agents ..... 262
  - 10.6.3 Wrap up ..... 263
  - 10.6.4 Call Prioritization ..... 264
  - 10.6.5 Accepting UCD Calls Automatically ..... 265
  - 10.6.6 UCD queue ..... 265
  - 10.6.7 UCD Overflow ..... 266
  - 10.6.8 UCD Night Service ..... 266
  - 10.6.9 Announcements / Music on Hold for UCD ..... 267
  - 10.6.10 Transfer to UCD Groups..... 267
  - 10.6.11 Releasing UCD from Analog Lines ..... 268
- 11 Call Routing..... 269**
  - 11.1 Toll and Call Restrictions (LX/MX)..... 269
    - 11.1.1 Selective Seizure of Exchange Lines (LX/MX)..... 269
    - 11.1.2 Classes of Service, Toll Restriction (LX/MX) ..... 269
    - 11.1.3 CON Groups (LX/MX)..... 271
      - 11.1.3.1 CON Groups (Traffic Restriction Groups) (LX/MX) ..... 271
      - 11.1.3.2 Assigning Speed-Dialing Numbers to CON Groups (LX/MX) ..... 272
  - 11.2 Night Service and Intercept (LX/MX) ..... 272
    - 11.2.1 Night Service (LX/MX) ..... 272
    - 11.2.2 Intercept ..... 273
  - 11.3 LCR (Least Cost Routing) (LX/MX) ..... 275
    - 11.3.1 LCR Functionality (LX/MX)..... 275
    - 11.3.2 LCR Dial Plan (LX/MX)..... 277
    - 11.3.3 LCR Routing Tables (LX/MX)..... 279
    - 11.3.4 LCR Class of Service (COS) (LX/MX) ..... 279
    - 11.3.5 LCR Outdial Rules (LX/MX) ..... 280

## Contents

11.3.6	Network Carriers (LX/MX)	282
11.4	Emergency Calls (LX/MX)	283
11.4.1	Hotline after Timeout / Hotline (LX/MX)	284
11.4.2	Trunk Release for Emergency Call (LX/MX)	285
11.4.3	For U.S. and Canada only: E911 Emergency Call Service (LX/MX)	285
11.4.4	Emergency Calls in Combination with Mobile Logon	286
11.4.4.1	Configuring the Emergency Scenario	286
<b>12</b>	<b>Multimedia Contact Center</b>	<b>290</b>
12.1	Contact Center Clients	290
12.1.1	myAgent	291
12.1.2	Prerequisites for myAgent	292
12.1.3	myReports	294
12.1.4	Prerequisites for myReports	296
12.1.5	Notes on Using myAgent and UC Clients Simultaneously	298
12.2	Agents	299
12.2.1	Agent Functions Independent of the Authorization Level	299
12.2.2	Preferred Agents	301
12.2.3	Agents in multiple queues	301
12.2.4	Contact Center Breaks	301
12.3	Queues and Schedules	301
12.3.1	Queues	301
12.3.2	Schedules	303
12.3.3	Wrap up	309
12.3.4	Grade of Service	310
12.3.5	Wallboard	310
12.3.6	Agent Callback	310
12.4	VIP service	311
12.4.1	VIP Caller Priority	311
12.4.2	VIP Call List	311
12.5	Fallback solution	312
12.6	Configuring the Contact Center	314
12.6.1	Example of an OpenScope Office MX Contact Center Configuration	315
12.6.2	Example of an OpenScope Office HX Contact Center Configuration	317
12.6.3	Configuration Procedure	326
12.7	Notes on Using the Contact Center	326
12.7.1	Using the Contact Center in a Communication System with IP Trunks and Outside Line	326
12.7.2	Restrictions on Operating the Contact Center	327
12.8	Notes on the Use of DECT Telephones (HiPath Cordless Office)	329
12.9	Reports	330
12.9.1	Predefined Report Templates	332
12.9.2	Report Designer	332
<b>13</b>	<b>Mobility</b>	<b>333</b>
13.1	Integrated Mobility Solution	333
13.2	Mobility on the Road	334
13.2.1	myPortal for Mobile	334
13.2.1.1	Prerequisites for myPortal for Mobile	336
13.2.2	Mobility Entry (MX)	338
13.2.3	Comparison between myPortal for Mobile and Mobility Entry	340
13.2.4	Dependencies for myPortal for Mobile and Mobility Entry	342
13.2.5	One Number Service (LX/MX)	344
13.2.6	Dual-Mode Telephony (LX/MX)	345

- 13.2.7 Configuring myPortal for Mobile and Mobility Entry (LX/MX) . . . . . 345
- 13.2.8 Configuring myPortal for Mobile and Mobility Entry (HX/HiPath 3000). . . . . 346
- 13.2.9 DISA (MX). . . . . 347
- 13.3 Mobility in the Office (LX/MX) . . . . . 347
  - 13.3.1 IP Mobility / Desk Sharing (LX/MX) . . . . . 348
    - 13.3.1.1 Mobile Logon (LX/MX). . . . . 349
    - 13.3.1.2 Flex Call/Mobile PIN (LX/MX) . . . . . 349
  - 13.3.2 HiPath Cordless IP (LX/MX). . . . . 350
  - 13.3.3 WLAN Phones and Access Points (LX/MX) . . . . . 350
  - 13.3.4 WLAN Requirements (LX/MX) . . . . . 350
- 13.4 Mobility at Home (LX/MX) . . . . . 351
- 14 Security . . . . . 352**
- 14.1 VPN (Virtual Private Network) (MX) . . . . . 352
  - 14.1.1 LAN Requirements for a VPN (MX) . . . . . 354
  - 14.1.2 Connecting Teleworkers via a VPN . . . . . 356
  - 14.1.3 Networking Communication Systems via a VPN (MX) . . . . . 358
  - 14.1.4 VPN - Security Mechanisms (MX) . . . . . 358
  - 14.1.5 VPN - Certificates (MX) . . . . . 361
  - 14.1.6 VPN - Clients (MX) . . . . . 362
    - 14.1.6.1 NCP Client Settings (MX) . . . . . 363
    - 14.1.6.2 Microsoft Windows XP Client Settings (MX) . . . . . 365
  - 14.1.7 VPN Services (MX). . . . . 368
  - 14.1.8 VPN - Tunnel (MX) . . . . . 368
  - 14.1.9 VPN - Rules (MX) . . . . . 368
  - 14.1.10 PKI Servers (MX) . . . . . 368
  - 14.1.11 Upgrading a VPN Configuration from V3.2 to V3.3 (MX) . . . . . 368
- 14.2 Firewall (LX/MX) . . . . . 369
  - 14.2.1 Ports and Services (LX/MX). . . . . 370
    - 14.2.1.1 Port Administration and Port Forwarding (MX) . . . . . 371
    - 14.2.1.2 Opening Ports (MX). . . . . 371
  - 14.2.2 URL Blocker (MX). . . . . 371
  - 14.2.3 Expression Filter (Web Filter) (MX) . . . . . 372
  - 14.2.4 Intrusion Detection System (IDS) (MX). . . . . 372
  - 14.2.5 Services Administration (LX) . . . . . 373
- 14.3 MAC and IP Address Filtering (MX). . . . . 373
- 14.4 Secure Administration (MX). . . . . 374
  - 14.4.1 SSL (Secure Socket Layer) (MX) . . . . . 374
  - 14.4.2 Admin Log (MX) . . . . . 375
- 14.5 Security at the Phone. . . . . 375
  - 14.5.1 Central Lock Code, COS Changeover (LX/MX) . . . . . 375
  - 14.5.2 Individual Lock Code (Locking the Phone) (LX/MX). . . . . 375
- 14.6 Signaling and Payload Encryption (SPE) (LX/MX) . . . . . 376
- 14.7 Samba Share (LX/MX). . . . . 377
- 14.8 SIP Attack Protection . . . . . 378
- 15 Networking OpenScope Office . . . . . 379**
- 15.1 Network Plan . . . . . 379
  - 15.1.1 Homogeneous and Heterogeneous Networks . . . . . 380
  - 15.1.2 Single and Multi-Gateway. . . . . 380
  - 15.1.3 Removing a Node from the Internetwork . . . . . 381
- 15.2 Network-wide Features . . . . . 382
  - 15.2.1 Network-wide Features of UC Clients. . . . . 382

## Contents

15.2.2 Network-wide Voice Features	388
15.2.3 Central Intercept Position in the Internetwork (LX/MX)	389
15.3 Licensing an Internetwork	390
15.4 Networking Requirements	390
15.4.1 LAN Networking Requirements	391
15.4.2 WAN Networking Requirements	393
15.4.3 Dial Plan in the Network	395
15.5 Path Optimization (Path Replacement)	396
15.6 Networking Scenarios	397
15.6.1 General Information	397
15.6.2 Scenario 1: Networking Multiple OpenScope Office MX Systems	399
15.6.3 Configuring Scenario 1	401
15.6.4 Scenario 2: Networking Multiple OpenScope Office HX Systems	403
15.6.5 Configuring Scenario 2	406
15.6.6 Scenario 3: Networking of OpenScope Office LX and OpenScope Office MX (Single Gateway)	407
15.6.7 Configuring Scenario 3	410
15.6.8 Scenario 4: Networking Multiple OpenScope Office MX Systems with one OpenScope Office LX (Multi-Gateway)	414
15.6.9 Configuring Scenario 4	417
15.6.10 Scenario 5: Networking OpenScope Office LX/MX/HX and HiPath 3000	423
15.7 Synchronization Status in the Internetwork	425
15.7.1 Manual Synchronization in the Internetwork	426
15.8 Survivability (Only LX)	426
<b>16 Application Connectivity</b>	<b>428</b>
16.1 XMPP	428
16.2 Application Launcher	428
16.2.1 Prerequisites for Application Launcher	429
16.2.2 Profile with Configuration Data for Application Launcher	430
<b>17 Auxiliary Equipment</b>	<b>431</b>
17.1 Fax Devices and Fax Servers (MX)	431
17.2 Entrance Telephone and Door Opener (MX)	432
17.3 OpenStage Gate View	432
17.3.1 Legal Framework	432
17.3.2 Components	433
17.3.3 Function Overview	434
17.3.4 Menu	435
17.3.5 Initial Setup of OpenStage Gate View	436
17.3.6 OpenStage Gate View Video Recording	436
17.3.7 OpenStage Gate View User Management	437
17.3.8 OpenStage Gate View Server Administration	437
17.3.9 OpenStage Gate View Customizations	437
<b>18 Accounting (LX/MX)</b>	<b>439</b>
18.1 Call Detail Recording (LX/MX)	439
18.1.1 Call Detail Recording Central (LX/MX)	439
18.1.2 Enabling or Disabling Call Detail Recording (LX/MX)	444
18.1.3 Account Codes (LX/MX)	444
18.2 Display of Call Charges and Call Duration (LX/MX)	445
18.2.1 Advice of Charges at Station (LX/MX)	445
18.2.2 Call Duration Display on Telephone (LX/MX)	446
18.2.3 Call-Charge Display with Currency (not for U.S.) (LX/MX)	446

18.3 Cost Control (LX/MX) . . . . .	447
18.3.1 Expensive Connection Route Advisory (LX/MX) . . . . .	447
18.3.2 Toll Fraud Monitoring (LX/MX) . . . . .	448
18.4 Accounting Tools (LX/MX) . . . . .	448
18.4.1 Accounting Manager (LX/MX) . . . . .	448
18.4.2 Teledata Office (LX/MX) . . . . .	448
<b>19 Maintenance . . . . .</b>	<b>449</b>
19.1 Telephony Configuration . . . . .	449
19.1.1 Date and Time (LX/MX) . . . . .	449
19.1.2 SNTP (LX/MX) . . . . .	450
19.1.3 Telephone Logos . . . . .	450
19.1.4 Customized Display (LX/MX) . . . . .	450
19.1.5 Flexible Menus (LX/MX) . . . . .	451
19.1.6 Music on Hold (LX/MX) . . . . .	451
19.1.7 Music on Hold / Announcements Wizard (LX/MX) . . . . .	452
19.1.8 Announcements (LX/MX) . . . . .	452
19.1.9 User to User Signaling (LX/MX) . . . . .	452
19.1.10 Voice Channel Signaling Security (LX/MX) . . . . .	452
19.1.11 Time Parameters (LX/MX) . . . . .	453
19.1.12 Controlling Centrex Features (LX/MX) . . . . .	453
19.2 Backup and Restore . . . . .	453
19.2.1 Backup Sets . . . . .	454
19.2.2 Backup Media . . . . .	454
19.2.3 Immediate Backup . . . . .	455
19.2.4 Scheduled Backup . . . . .	456
19.2.5 Restore . . . . .	456
19.3 Updates and Upgrades . . . . .	456
19.3.1 Using an Internal Web Server . . . . .	458
19.3.2 Updating OpenScape Office . . . . .	458
19.3.3 Updating System Telephones . . . . .	458
19.3.4 Software Status . . . . .	459
19.3.5 Upgrading from OpenScape Office V2 LX/MX to OpenScape Office V3 LX/MX . . . . .	459
19.3.6 Upgrading from OpenScape Office HX V2 to OpenScape Office V3 HX . . . . .	460
19.3.7 Upgrading UC Clients from V2 to V3 . . . . .	462
19.4 Restart, Reload, Shutdown, Factory Reset . . . . .	462
19.4.1 Restarting OpenScape Office . . . . .	462
19.4.2 Reloading OpenScape Office . . . . .	462
19.4.3 Restarting the UC Suite . . . . .	463
19.4.4 Restarting the Web Services . . . . .	463
19.4.5 Shutting Down the OpenScape Office MX Communication System . . . . .	463
19.4.6 Factory Reset of the OpenScape Office MX Communication System . . . . .	464
19.4.7 System Behavior after Pressing the On/Off Switch (MX) . . . . .	464
19.4.8 System Behavior after Unlocking the Module Release Latch of the Motherboard (MX) . . . . .	465
19.4.9 System Behavior after Initiating a Reset via the Reset Switch (MX) . . . . .	466
19.4.10 System Behavior after Initiating a Reload via the Reset Switch (MX) . . . . .	468
19.5 Inventory Management . . . . .	469
19.5.1 System Status (LX/MX) . . . . .	469
19.5.2 Inventory . . . . .	475
19.5.3 Hardware Configuration (MX) . . . . .	476
19.6 Automatic Actions (LX/MX) . . . . .	476
19.6.1 Garbage Collection Automatic Action . . . . .	477

Contents

- 19.6.2 DLS Notification Automatic Action ..... 477
- 19.7 Monitoring and Maintenance of OpenScope Office ..... 477
  - 19.7.1 Checking the Network Connection (MX) ..... 477
  - 19.7.2 SNMP (Simple Network Management Protocol) (LX/MX) ..... 478
  - 19.7.3 Manual Actions ..... 479
  - 19.7.4 Traces (LX/MX) ..... 481
  - 19.7.5 Events (LX/MX) ..... 490
  - 19.7.6 Configuration Data for Diagnostics ..... 491
- 19.8 Monitoring and Maintaining the UC Suite ..... 492
  - 19.8.1 Logging ..... 492
  - 19.8.2 Notification ..... 493
  - 19.8.3 Maintenance ..... 494
- 19.9 Remote Services ..... 494
  - 19.9.1 Remote Access (MX) ..... 494
  - 19.9.2 SSDP (Smart Services Delivery Platform) ..... 495
  - 19.9.3 Remote Service via VPN (MX) ..... 497
  - 19.9.4 PIN for Activating and Deactivating the Remote Service via VPN and the SSDP Service Plugin . . 497
  - 19.9.5 Online User ( LX/MX) ..... 497
- 20 Appendix ..... 499**
  - 20.1 Languages Supported ..... 499
  - 20.2 Supported Standards (LX/MX) ..... 500
  - 20.3 Configuration Limits and Capacities ..... 502
  - 20.4 Euro-ISDN Features (LX/MX) ..... 515
  - 20.5 Features of the UC Clients that can be used with SIP Telephones ..... 516
  - 20.6 SIP Features Supported by OpenScope Office ..... 517
  - 20.7 Codes for Activating and Deactivating Features (LX/MX) ..... 518
  - 20.8 IP Protocols and Port Numbers Used ..... 527
    - 20.8.1 IP Protocols and Port Numbers for Server Functions ..... 528
    - 20.8.2 IP Protocols and Port Numbers for Client Functions ..... 534
  - 20.9 Interface Ranges for Subscriber Lines (MX ) ..... 535
  - 20.10 Standards and Attenuation Values for Trunk Connections (MX ) ..... 537
  - 20.11 System Flags (LX/MX) ..... 540
  - 20.12 Station Flags (LX/MX) ..... 546
- 21 Glossary ..... 550**
  - 21.1 Glossary ..... 550
- Index ..... 566**

# 1 Introduction and Important Notes

This introduction provides you with an overview of the documentation structure. The introduction should assist you in finding information on selected topics faster. Before you begin with the installation and startup of the communication system, make sure that you have carefully read the safety information and warnings as well as the important notes.

---

**INFO:** The safety information and requirements inform you about the safety and other requirements to be observed. The important notes contain information on the emergency behavior, the standards and guidelines for the installation, and the radio frequency interference of the communication system. In addition, you will also find details on and the proper disposal and recycling of the communication system here.

---

## 1.1 About this Documentation

This document describes OpenScape Office.™.

This document describes the UC communication systems OpenScape Office LX and OpenScape Office MX as well as OpenScape Office HX and the UC Suite for the HiPath 3000 communication system. The headers of the features contain an identifier to show which feature applies to which system:

- Headers identified with (LX) describe features for OpenScape Office LX.
- Headers identified with (MX) describe features for OpenScape Office MX.
- Headers identified with (HX) describe features for OpenScape Office HX.
- Headers identified with (LX/MX) describe features for OpenScape Office LX and OpenScape Office MX.
- Headers without identifiers apply to all systems.

---

**INFO:** In this document, OpenScape Office LX and OpenScape Office MX are both referred to generically as the communication system.

---

### 1.1.1 Documentation and Target Groups

The documentation is intended for various target groups.

### **Administrator and Service Documentation**

- **OpenScape Office V3, Feature Description**  
This document describes all features and is intended for Sales and customers. This document is an extract from OpenScape Office V3, Administrator documentation .
- **OpenScape Office V3, Getting Started**  
This document is included with the communication system. It provides a quick overview of the initial installation of the communication system and is intended for administrators. This document is an extract from OpenScape Office V3, Administrator documentation .
- **OpenScape Office V3, OpenScape Office LX, Installation Guide**  
This document describes the installation of the OpenScape Office V3 LX communication system and is intended for administrators. This document is an extract from OpenScape Office V3, Administrator documentation .
- **OpenScape Office V3, OpenScape Office MX, Installation Guide**  
This document describes the installation of the OpenScape Office V3 MX communication system and is intended for administrators. This document is an extract from OpenScape Office V3, Administrator documentation .
- **OpenScape Office V3, OpenScape Office HX, Installation Guide**  
This document describes the installation of the UC Suite for HiPath 3000 and is intended for administrators. This document is an extract from OpenScape Office V3, Administrator documentation .
- **OpenScape Office V3, Linux, Installation Guide**  
This document describes the installation of Linux for OpenScape Office LX und OpenScape Office MX communication systems and is intended for administrators. This document is an extract from OpenScape Office V3, Administrator documentation .
- **OpenScape Office V3, Planning Guide**  
This document provides guidelines for the planning of OpenScape Office V3 MX and OpenScape Office V3 LX and is intended for project planners. This document is an extract from OpenScape Office V3, Administrator documentation .
- **OpenScape Office V3, Administrator documentation**  
This document provides a complete description of the hardware, installation, configuration, operation, features and administration and is intended for administrators. It includes all the contents of the documentation listed above. The Administrator documentation is available in the system as online help.

### **User Guides**

- **OpenScape Office V3, myPortal for Desktop, User Guide**  
This document describes the installation, configuration and operation of the integrated application myPortal for Desktop and is intended for the user.
- **OpenScape Office, myPortal for Outlook, User Guide**  
This document describes the installation, configuration and operation of the integrated application myPortal for Outlook and is intended for the user.



- **OpenScape Office V3, myPortal for Mobile/Tablet/Zimbra, User Guide**  
This document describes the configuration and operation of myPortal for Mobile and myPortal for Zimbra and is intended for the user.
- **OpenScape Office V3, myPortal for OpenStage, User Guide**  
This document describes the configuration and operation of myPortal for OpenStage and is intended for the user.
- **OpenScape Office V3, Fax Printer, User Guide**  
This document describes the installation, configuration and operation of the integrated application OpenScape Office Fax Printer and is intended for the user.
- **OpenScape Office V3, Application Launcher, User Guide**  
This document describes the installation, configuration and operation of Application Launcher and is intended for the user.
- **OpenScape Office V3, myAgent, User Guide**  
This document describes the installation, configuration and operation of the integrated application myAgent and is intended for the user.
- **OpenScape Office V3, myReports, User Guide**  
This document describes the installation, configuration and operation of the integrated application myReports and is intended for the user.
- **OpenScape Office V3, myAttendant, User Guide**  
This document describes the installation, configuration and operation of myAttendant and is intended for the user.

## 1.1.2 Structure

This section shows you how the content of this documentation is structured.

Section	Contents
Introduction and Important Notes	This introduction provides you with an overview of the documentation structure. The introduction should assist you in finding information on selected topics faster. Before you begin with the installation and startup of the communication system, make sure that you have carefully read the safety information and warnings as well as the important notes.
System Overview and Scenarios	The System Overview provides you with an introduction to the features of the communication system. The scenarios depict typical deployment scenarios for selected topics.
Hardware and Installation of OpenScape Office MX	The OpenScape Office MX communication system is a modular system that can be deployed as a one-box system (consisting of a single OpenScape Office MX system box) or as a multibox system (consisting of two or three OpenScape Office MX system boxes). Every OpenScape Office MX system box is equipped with a motherboard and provides three slots for installing optional gateway modules for the trunk and station connections.

**Introduction and Important Notes**  
About this Documentation

Section	Contents
Administration Concept	The administration of OpenScape Office is performed using web-based management (OpenScape Office Assistant). The user administration of the web-based management allows you to set up role-based administration.
Installing the Linux Server	This section describes the prerequisites and initial startup of the Linux server that is required to operate OpenScape Office LX and OpenScape Office HX.
Installing OpenScape Office LX	The initial installation of OpenScape Office LX with OpenScape Office Assistant is described here with the aid of a selected installation example.
Installing OpenScape Office MX	The initial installation of OpenScape Office MX with OpenScape Office Assistant is described here with the aid of a selected installation example.
Installing OpenScape Office HX	The initial installation of OpenScape Office Assistant is described here with the aid of a selected basic scenario.
Connection to Service Provider	The communication system supports different connections to service providers for Internet access and Internet telephony via an Internet Telephony Service Provider (ITSP, SIP Provider). OpenScape Office MX also provides access to outside lines via ISDN or analog connections through optional gateway modules.
Subscribers/Stations	A subscriber or station is a communication partner connected to the communication system. In general, every station (apart from virtual stations) is assigned a terminal. A terminal is, for example, a telephone, a PC or fax device. The subscribers can also be users of the OpenScape Office clients (e.g., users of myPortal for Outlook).
Licensing	Licensing is mandatory for the operation of OpenScape Office. Following the initial startup, the licensing must be completed within 30 days (called the Grace Period); otherwise, when this period expires, the system will only operate in restricted emergency mode.
Unified Communications	Unified Communications offers features such as the Presence status and CallMe, conferencing (not with OpenScape office HX), as well as voicemail and fax functionality in the myPortal for Desktop and myPortal for Outlook clients. myAttendant also provides Attendant Console functions.
Functions at the Telephone	The communication system offers a comprehensive set of telephony features extending from the usual features such as hold, toggle/connect and consultation hold, etc., through various call signaling mechanisms, down to call transfers, call deflections and call forwarding.

Section	Contents
Working in a Team (Groups)	Several features are provided by the communication system to enable and facilitate working in a team. Besides call pickup groups, group calls and hunt groups, this also includes groups with team and executive/secretary functions as well as voicemail box and fax box groups. The "UCD (Uniform Call Distribution)" feature enables incoming calls to be uniformly distributed to a group of users (UCD group).
Call Routing	The communication system offers Toll and Call Restrictions, a Night Service, powerful LCR (Least Cost Routing) capabilities and different options for making emergency calls.
Multimedia Contact Center	The OpenScape Office Contact Center is a powerful solution for the optimum distribution and handling of incoming calls, faxes and e-mails. Intelligent skills-based distribution ensures that callers are always connected to the best qualified agents, regardless of which contact medium is used. A number of convenient functions for handling and wrapping up calls, faxes and e-mails are offered to the Contact Center agents via the myAgent application. myReports provides a number of report templates for analyzing the Contact Center operations.
Mobility	OpenScape Office provides integrated mobility solutions for any business. This typically includes the integration of mobile phones/smartphones, the usage of Cordless and WLAN phones, etc., down to Desk Sharing and teleworking. Mobility includes Mobility on the road, Mobility in the office and Mobility at home.
Security	The term security includes not only the security in a data network with secure access by users (via a VPN and secure administration using SSL) and with restricted system access (through firewalls, IP and MAC address filtering and a DMZ), but also the security against unauthorized access at telephones (e.g., telephone locks).
Networking OpenScape Office	OpenScape Office enables the networking of OpenScape Office MX, OpenScape Office LX and OpenScape Office HX. In this network-wide unified communications solution, subscribers can now use features such as the presence status, voicemail, conferencing and much more in exactly the same way as was originally possible with only a single OpenScape Office communication system.
Auxiliary Equipment	Auxiliary equipment consists of external devices (such as a fax device or door opener) that are connected to the interfaces of the communication system. Using an IP-enabled camera, the video surveillance solution Gate View can be deployed.
Application Connectivity	Application connectivity is supported by the system, e.g., with XMPP and Application Launcher.

Section	Contents
Accounting	Accounting offers call detail recording, the display of call charges and call duration, as well as cost control and accounting tools.
Maintenance	OpenScope Office offers several maintenance options. This includes changing the telephony settings, backing up and restoring the configuration data, updating the software with updates and upgrades and restarting/reloading functions. In addition, appropriate functions to determine status and for monitoring and maintenance are available. Remote access to OpenScope Office is possible via different Remote Services.
Appendix	This appendix contains reference information such as the supported languages, standards, configuration limits and capacities, Euro-ISDN features, codes for enabling and disabling features, feature codes using DTMF and the IP protocols and port numbers used.

### 1.1.3 Types of Topics

The types of topics include concepts and operating instructions (tasks).

Type of topic	Contents	Title
Concept	Explains the "What".	without a verb, e.g., <i>Call Duration Display on Telephone.</i>
Operating instructions	Describe task-oriented application cases – i.e., the "How" – and assumes familiarity with the associated concepts.	Starts with "How to" followed by a verb, e.g., <i>How to Enable or Disable the Call Duration Display on a Telephone.</i>

### 1.1.4 Display Conventions

This documentation uses a variety of methods to present different types of information.

Purpose	Appearance	Example
User Interface Elements	Bold	Click <b>OK</b> .
Menu sequence	>	<b>File &gt; Exit</b>
Special emphasis	Bold	<b>Do not delete</b> Name.
Cross-reference text	Italics	You will find more information in the topic <i>Network</i> .

Purpose	Appearance	Example
Output	Monospace font, e.g., Courier	Command not found.
Input	Monospace font, e.g., Courier	Enter LOCAL as the file name.
Key combination	Monospace font, e.g., Courier	<Ctrl>+<Alt>+<Esc>
Work Steps and Substeps	Numbered and alphabetical lists	<ul style="list-style-type: none"> <li>• Configure the DSL telephony stations with the associated DID phone numbers.               <ul style="list-style-type: none"> <li>– Click <b>Add</b>.</li> <li>– Enter the name of the Internet telephony station under <b>Internet Telephony Station</b>.</li> </ul> </li> </ul>
Alternative Work Steps	Enumeration	<ul style="list-style-type: none"> <li>• If you want to output amounts, enable the check box <b>Display amounts instead of units</b>.</li> <li>• If you want to output units, clear the check box <b>Display amounts instead of units</b>.</li> </ul>

## 1.2 Safety Information and Warnings

Safety information and warnings indicate situations that can result in death, injury, property damage, and/or data loss.

Work on the communication system and devices should **only** be performed by personnel with proper qualifications.

Within the context of this safety information and these warnings, qualified personnel are people who are authorized to ground and label systems, devices, and trunks and put them into operation in compliance with the applicable safety regulations and standards.

Make sure you have read and noted the following safety information and warnings before installing and starting up the OpenScape Office LX or OpenScape Office MX communication system.

Make sure you also read carefully and follow all safety information and warnings printed on the communication system and devices.

Familiarize yourself with emergency numbers.

### Types of Safety Information and Warnings

This documentation uses the following levels for the different types of safety information and warning:



#### **DANGER**

Indicates an immediately dangerous situation that will cause death or serious injuries.

---



#### **WARNING**

Indicates a universally dangerous situation that can cause death or serious injuries.

---



#### **CAUTION**

Indicates a dangerous situation that can cause injuries.

---

---

**NOTICE:** Indicates situations that can cause property damage and/or data loss.

---

### Additional symbols for specifying the source of danger more exactly

The following symbol is generally not used in this documentation, but may appear on the devices or packaging.



ESD - electrostatically sensitive devices

---

#### **Related Topics**

- [Important Notes](#)

## 1.2.1 Warnings: Danger

"Danger" warnings indicate immediately dangerous situations that will cause death or serious injury.



## **DANGER**

### **Risk of electric shock from touching live conductors**

- Note: Voltages over 30 VAC (alternating current) or 60 VDC (direct current) are dangerous.
  - Only personnel with proper qualifications or qualified electricians should perform work on the low-voltage network (<1000 VAC), and all work must comply with the national/local requirements for electrical connections.
  - Opening the case of an OpenScape Office MX system box is forbidden! The case contains potentially dangerous circuits that are not protected. Opening the case invalidates the warranty. Siemens Enterprise Communications GmbH & Co. KG does not assume any liability for damage arising from the illicit opening of the case.
- 

## 1.2.2 Warnings: Warning

"Warnings" indicate universal dangerous situations that can cause death or serious injury.



## **WARNING**

### **Risk of electric shock from touching live conductors**

- When using the OpenScape Office MX communication system in countries with country-specific requirements (Finland, Canada, Norway, Sweden and the USA), each OpenScape Office MX system box must be grounded with a separate grounding wire. Before you start up the system and connect the phones and phone lines, connect the communication system with a permanent earthing conductor.
  - Only use systems, tools and equipment which are in perfect condition. Do not use equipment with visible damage.
  - Replace the power cable immediately if it appears to be damaged.
  - The communication system should only be operated with an outlet that has connected ground contacts.
  - During a thunderstorm, do not connect or disconnect communication lines and do not install or remove gateway modules.
  - Disconnect all power supply circuits if you do not require power for certain activities (for example, when changing cables). Disconnect all the communication system's power plugs and make sure that the communication system is not supplied by another power source (uninterrupted power supply unit, for instance).
-

### 1.2.3 Warnings: Caution

"Caution" warnings indicate a dangerous situation that can result in injury.



**CAUTION**

**Risk of explosion caused by the incorrect replacement of batteries**

The lithium battery should only be replaced with an identical battery or one recommended by the manufacturer.

---



**CAUTION**

**Risk of fire**

Only use communication lines with a conductor diameter of 0.4 mm (AWG 26) or more.

---



**CAUTION**

**General risk of injury or accidents in the workplace**

Install cables in such a way that they do not pose a risk of an accident (tripping), and cannot be damaged.

---

### 1.2.4 Warnings: Note

"Note" warnings are used to indicate situations that could result in property damage and/or data loss.

The following contains important information on how to avoid property damage and/or data loss:

- When transporting and sending components of the communication system (such as gateway modules, for example), please use appropriate packaging to ensure the protection of electrostatic sensitive devices (ESD).
- Use only original accessories. Failure to comply with this safety information may damage the system equipment or violate safety and EMC regulations.
- Sudden changes in temperature can result in condensing humidity. If the communication system is transported from a cold environment to warmer areas, for example, this could result in the condensation of humidity. Wait until the equipment has adjusted to the ambient temperature and is completely dry before starting it up.
- Connect all cables only to the specified connection points.



- Do not allow easily flammable materials to be stored in or near the room where the communication system is installed.
- If no emergency backup power supply is available or if no switchover to emergency analog phones is possible in the event of a power failure, then no emergency calls can be made via the communication system following a power failure.

## 1.3 Important Notes

These important notes contain information on the emergency behavior, intended use, and operating conditions of the communication system. In addition, you will find details on the standards and guidelines for the installation, the radio frequency interference of the OpenScape Office MX communication system, and its proper disposal and recycling.

---

### Related Topics

- [Safety Information and Warnings](#)

### 1.3.1 Emergencies

This section provides information on how to proceed in an emergency.

#### What To Do In An Emergency

- In the event of an accident, remain calm and controlled.
- Always switch off the power supply before you touch an accident victim.
- If you are not able to immediately switch off the power supply, only touch the victim with non-conductive materials (such as a wooden broom handle), and first of all try to isolate the victim from the power supply.

#### First Aid

- Be familiar with basic first aid procedures for electrical shock. A fundamental knowledge of the various resuscitation methods if the victim has stopped breathing or if the victim's heart is no longer beating, as well as first aid for treating burns, is absolutely necessary in such emergencies.
- If the victim is not breathing, immediately perform mouth-to-mouth or mouth-to-nose resuscitation.
- If you have appropriate training, immediately perform heart massage if the victim's heart is not beating.

#### Calling for Help

Immediately call an ambulance or an emergency physician. Provide the following information in the following sequence:

- Where did the accident happen?

- What happened?
- How many people were injured?
- What type of injuries?
- Wait for questions.

#### **Reporting Accidents**

- Immediately report all accidents, near accidents and potential sources of danger to your manager.
- Report all electrical shocks, no matter how small.

### **1.3.2 Intended Use**

The communication system may only be used as described in this documentation and only in conjunction with add-on devices and components recommended and approved by Siemens Enterprise Communications GmbH & Co. KG.

Prerequisites for the intended use of the communication system include correct transport, storage, assembly, startup, operation and maintenance of the system.

### **1.3.3 Correct Disposal and Recycling**

Please read the information on the correct disposal and recycling of electrical and electronic equipment and old batteries.



All electrical and electronic products should be disposed of separately from the municipal waste stream via designated collection facilities appointed by the government or the local authorities. The correct disposal and separate collection of your old appliance will help prevent potential negative consequences for the environment and human health. It is a precondition for reuse and recycling of used electrical and electronic equipment. For more detailed information about disposal of your old appliance, please contact your city office, waste disposal service, the shop where you purchased the product or your sales representative. The statements quoted above are only fully valid for equipment which is installed and sold in the countries of the European Union and is covered by the directive 2002/96/EC. Countries outside the European Union may have other regulations regarding the disposal of electrical and electronic equipment.



Old batteries that bear this logo are recyclable and must be included in the recycling process. Old batteries that are not recycled must be disposed of as hazardous waste in compliance with all regulations.

## 1.3.4 Installation Standards and Guidelines

This section provides information on the specifications you must comply with when connecting the communication system to the power supply circuit and when using shielded cabling for LAN, WAN and DMZ connectors.

### 1.3.4.1 Connecting OpenScape Office MX to the Power Supply Circuit

The OpenScape Office MX communication system has been approved for connection to TN-S power supply systems. They can also be connected to a TN-C-S power supply system in which the PEN conductor is divided into a ground wire and a neutral wire. TN-S and TN-C-S systems are defined in the IEC 364-3 standard.

Only qualified electricians should perform any work that may be required on the low-voltage network. These installation activities to connect the OpenScape Office MX communication system must be performed in compliance with IEC 60364-1 and IEC 60364-4-41 or any corresponding legal norms or national regulations (for example in the U.S. or Canada).

### 1.3.4.2 Connecting OpenScape Office LX and OpenScape Office HX to the Power Supply Circuit

For information regarding the connection of OpenScape Office LX and OpenScape Office HX to the power supply circuit, please refer to the manufacturer's documentation for the server PC and the other components.

Only qualified electricians should perform any work that may be required on the low-voltage network. These installation activities to connect the OpenScape Office MX and OpenScape Office HX must be performed in compliance with IEC 60364-1 and IEC 60364-4-41 or any corresponding legal norms or national regulations (for example in the U.S. or Canada).

### 1.3.4.3 Shielded Cabling for LAN, WAN and DMZ Connections of OpenScape Office MX

Compliance with CE requirements on electromagnetic compatibility in OpenScape Office MX communication systems and their LAN, WAN and DMZ connections is subject to the following conditions:

- The communication system may only be operated with shielded connection cables. This means that a shielded Category-5 (CAT.5) cable with a length of at least 3 m should be used between the shielded LAN, WAN and DMZ sockets of the communication system and the building installation port or the external active component port. The cable shield must be grounded at the building installation end or the external active component end (connection to the building's potential equalization terminal).
- A shielded Category-5 (CAT.5) cable should also be used for shorter connections with external active components (LAN switch or similar). However, the active component must feature a shielded LAN connection with a grounded shield connection (connection to the building's potential equalization terminal).
- The shield properties of the cable components should at least satisfy the requirements of the European standard EN 50173-1<sup>\*)</sup> "Information technology - Generic cabling systems" (and all references specified).<sup>\*\*\*)</sup>
- Building installations that are fitted with shielded symmetrical copper cables throughout in accordance with the Class-D requirements<sup>\*\*)</sup> of EN 50173-1 satisfy the above condition.<sup>\*\*\*)</sup>

\*) The European standard EN 50173-1 is derived from the international standard ISO/IEC 11801.

\*\* ) Class-D is reached, for instance, if Category-5 (CAT.5) components (cables, wall outlets, connection cables, etc.) are installed.

\*\*\* ) UTP cables (U.S. standard EIA/TIA 568 T) are the most widely used cables on the North American market; this has the following implications for the LAN connections in communication systems: The system may only be operated with shielded connection cables. This means that a shielded Category-5 (CAT.5) cable with a length of at least 3 m should be used between the shielded LAN, WAN and DMZ sockets of the communication system and the building installation port or the external active component port. The cable shield must be grounded at the building installation end or the external active component end (connection to the building's potential equalization terminal).

#### 1.3.4.4 Marks (MX)



This device complies with the EU guideline 1999/5/EEC as confirmed by the CE certificate.

#### 1.3.5 Notes on Electromagnetic and Radio Frequency Interference (MX)

Please note the information about the radio frequency interference of the OpenScape Office MX communication system.

- Not for U.S. and Canada  
OpenScape Office MX is a Class B (EN 55022) device.
- For U.S. and Canada only:  
OpenScape Office MX is a Class A (EN 55022) device. Class A equipment can cause radio frequency interference in residential areas. In such cases, the providers of the communication system are required to take appropriate counteractive measures.

#### 1.3.6 Data Protection and Data Security

Please note the details below with respect to protecting data and ensuring privacy.

This communication system processes and uses personal data for purposes such as call detail recording, displays, and customer data acquisition.

In Germany, the processing and use of such data is subject to various regulations, including those of the Federal Data Protection Law (Bundesdatenschutzgesetz, BDSG). For other countries, please follow the appropriate national laws.

The aim of data protection is to protect the rights of individuals from being adversely affected by use of their personal data.

In addition, the aim of data protection is to prevent the misuse of data when it is processed and to ensure that one's own interests and the interests of other parties which need to be protected are not affected.

---

**INFO:** The customer is responsible for ensuring that the communication system is installed, operated and maintained in accordance with all applicable labor laws and regulations and all laws and regulations relating to data protection, privacy and safe labor environment.

---

Employees of Siemens Enterprise Communications GmbH & Co. KG are bound to safeguard trade secrets and personal data under the terms of the company's work rules.

In order to ensure that the statutory requirements are consistently met during service – whether on-site or remote – you should always observe the following rules. You will not only protect the interests of your and our customers, you will also avoid personal consequences.

A conscientious and responsible approach helps protect data and ensure privacy:

- Ensure that only authorized persons have access to customer data.
- Take full advantage of password assignment options; never give passwords to an unauthorized person orally or in writing.
- Ensure that no unauthorized person is able to process (store, modify, transmit, disable, delete) or use customer data in any way.
- Prevent unauthorized persons from gaining access to storage media such as backup CDs or log printouts. This applies to service calls as well as to storage and transport.
- Ensure that storage media which are no longer required are completely destroyed. Ensure that no sensitive documents are left unprotected.
- Work closely with your customer contact; this promotes trust and reduces your workload.

### 1.3.7 Technical Regulations and Conformity (MX)

Details on how the OpenScape Office MX communication system meets conformity requirements can be found here.

#### 1.3.7.1 CE Conformity

CE certification is based on the R&TTE Directive 99/5/EEC.

	<b>Standards reference</b>
Safety	EN 60950-1
Electromagnetic Compatibility EMC	EN 55022: Class B (EMC, Emission ITE Residential Environment) EN 55024 (EMC, Immunity ITE Residential Environment) EN 61000-3-2: Class A (EMC, Harmonic Current Emissions)
Electromagnetic Field EMF	EN 50371 (EMF, General Public Human Field Exposure)

### 1.3.7.2 Conformity with US and Canadian Standards

	Standards reference
Safety USA	UL 60950-1
Safety Canada	CSA-C22.2 NO. 60950-1-03
EMC Emission	FCC Part 15 Subpart B Class A
Transmission: USA	FCC Part 68
Transmission: Canada	CS-03

### 1.3.7.3 Conformity with International Standards

	Standards reference
Safety	IEC 60950-1

## 1.3.8 Operating Conditions

Note the environmental and mechanical conditions for operating the communication system.

### 1.3.8.1 Operating Conditions for OpenScape Office MX

The environmental and mechanical conditions for operating the OpenScape Office MX communication system are specified.

#### Environmental Operating Conditions

Operating limits:

- Room temperature: + 5 to + 40 °C (41 to 104 °F)
- Absolute humidity: 1 to 25 g H<sub>2</sub>O/m<sup>3</sup>

- Relative humidity: 5 to 85%

---

**NOTICE:** Damage caused by local temperature increases  
Avoid exposing the communication system to direct sunlight and other sources of heat.

---

---

**NOTICE:** Damage caused by condensation due to humidity  
Avoid any condensation of humidity on or in the communication system before or during operation under all circumstances.  
The communication system must be completely dry before you put it into service.

---

### **Mechanical Operating Conditions**

The communication system is intended for stationary use.

### **1.3.8.2 Operating Conditions for OpenScape Office LX and OpenScape Office HX**

For details on the environmental and mechanical conditions for operating OpenScape Office LX and OpenScape Office HX, please also refer to the manufacturer documentation of the server PCs and the other components.



## 2 System Overview and Scenarios

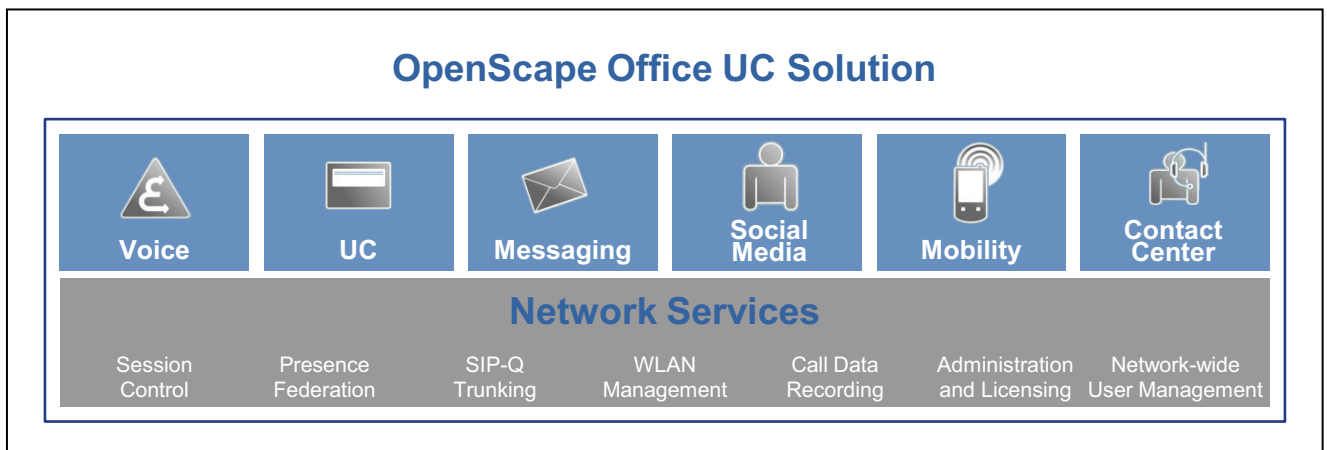
The System Overview provides you with an introduction to the features of the communication system. The scenarios depict typical deployment scenarios for selected topics.

### 2.1 System Overview

OpenScape Office is the world's first "All in One" Unified Communications (UC) solution for single and multi-site SMBs that uniquely unifies voice communications with presence, mobility and office applications providing unsurpassed business speed, agility and efficiency in a secure and reliable solution.

OpenScape Office offers:

- UCC Networking  
Network-wide UC features and functions (extended UC domain)
- Mobility  
UC Clients myPortal for Mobile and myPortal for OpenStage
- Software UC  
OpenScape Office LX/MX to support 500 users
- Virtualization for small and medium size enterprises  
OpenScape Office LX/HX Virtualization with VMware vSphere
- Social networks  
Google Chat Integration Presence Federation



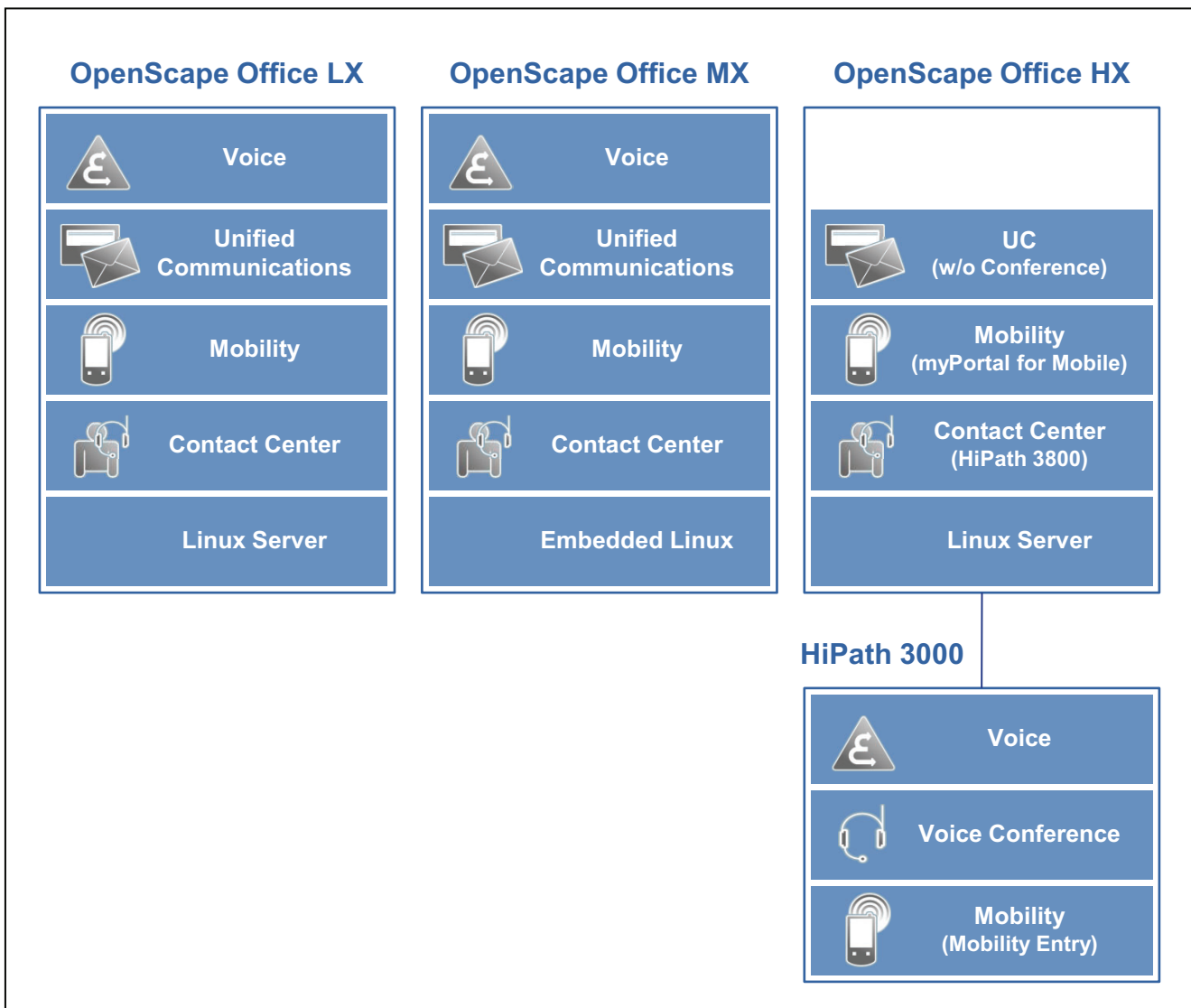
#### Scalability

OpenScape Office is available in the following variants:

- Software UC solution OpenScape Office LX
  - Supports up to 500 users

**System Overview and Scenarios**  
System Overview

- SW running on Linux OS & standard server HW:  
Virtualization opportunity with VMware vSphere  
Carrier connectivity via broadband (ITSP, SIP Trunking)
- All-in-one HW/SW UC platform OpenScape Office MX
  - Supports up to 150 users
  - All-in-one functionality comes pre-installed:  
Analog and ISDN Subscribers  
Carrier connectivity via broadband (ITSP), digital (ISDN) and analog lines
- Server-based UC solution OpenScape Office HX for HiPath 3000
  - Supports up to 500 users
  - UC software running on Linux OS & standard server hardware  
Virtualization opportunity with VMware vSphere
  - UC functions supported via OpenScape Office HX  
Voice functions supported via HiPath 3000



### Networking

OpenScape Office is networkable for customers:

- with multiple buildings on the company premises
- with distributed locations
- with migration from existing HiPath 3000

With OpenScape Office, networks with a maximum of 8 nodes and up to 1000 stations are supported.

### UC Clients, Mobility Clients and Contact Center Clients

OpenScape Office offers the following UC clients with an intuitive user interface:

- myPortal (UC User Portal)
  - myPortal for Desktop (UC Desktop Client)
  - myPortal for Outlook (UC Outlook Integration)
  - myPortal for Mobile/Tablet PC (Mobility Client for mobile phones and tablet PCs)
  - myPortal for OpenStage (UC improvements for OpenStage 60/80)
- myAttendant (UC Attendant Console)
- myAgent (Contact Center Client)
- myReports (Reports for Contact Center)

## 2.1.1 OpenScape Office LX

OpenScape Office HX is the software-based UC solution that is platform-independent and can be operated on a Linux server. OpenScape Office MX or HiPath 3000 can be used as a gateway to the Central Office.

	<b>OpenScape Office LX</b>
Installation variants	<ul style="list-style-type: none"> <li>• Linux server certified for SUSE Linux Enterprise 11</li> </ul>
Subscribers/Stations	<ul style="list-style-type: none"> <li>• Max. 500 stations</li> <li>• Max. 1000 stations through networking</li> <li>• Max. 200 stations for mobile phone integration</li> </ul>
Operating System	<ul style="list-style-type: none"> <li>• Linux</li> </ul>
Internet connection	<ul style="list-style-type: none"> <li>• 1 Internet Service Provider (ISP)</li> <li>• Four Internet Telephony Service Providers (ITSP)</li> </ul>

## 2.1.2 OpenScape Office MX

OpenScape Office MX is the all-in-one unified communications solution that offers not only modern VoIP (Voice over IP) features, but also the option of connecting ISDN and analog devices directly to the communication system.

	<b>OpenScape Office MX</b>
Installation variants	<ul style="list-style-type: none"> <li>• As a standalone unit (desktop operation) or 19" rack mount; space requirements in 19" rack for a system box = 1.5 rack units</li> <li>• Standalone communication system with max. 3 system boxes (multibox system)</li> </ul>
Subscribers/Stations	<ul style="list-style-type: none"> <li>• Max. 150 stations, of which 148 are freely configurable</li> <li>• Max. 50 stations per system box</li> <li>• Max. 1000 stations through networking</li> <li>• Max. 100 stations with mobile phone integration</li> </ul>
Gateway Modules	<ul style="list-style-type: none"> <li>• 3 slots per system box for the use of various gateway modules</li> <li>• Optional Gateway Modules <ul style="list-style-type: none"> <li>– GMS (not for U.S. and Canada) = Gateway module with four S<sub>0</sub> ports for the ISDN trunk connection or the ISDN station connection</li> <li>– GMSA (not for U.S. and Canada) = Gateway module with four S<sub>0</sub> ports for the ISDN trunk connection or ISDN station connection and four a/b interfaces for the analog station connection</li> <li>– GME (not for U.S. and Canada) = Gateway module with one S<sub>2M</sub> port for the ISDN Primary Rate Interface</li> <li>– GMT (for U.S. and Canada only) = Gateway module with one T1 interface for the ISDN Primary Rate Interface</li> <li>– GMAA = Gateway module with four a/b interfaces for the analog trunk connection and two a/b interfaces for the analog station connection</li> <li>– GMAL = Gateway module with eight a/b interfaces for the analog station connection</li> </ul> </li> </ul>
Standard interfaces (motherboard)	<ul style="list-style-type: none"> <li>• One motherboard per system box with powerful AMD Sempron CPU and 1 GB memory</li> <li>• Standard interfaces <ul style="list-style-type: none"> <li>– 4 Gigabit LAN ports, internal (virtual LAN support, Layer 3 Routing, 802.1p L2 QoS)</li> <li>– 1 Gigabit DMZ port (e.g., to securely integrate E-mail and Web servers in the customer network)</li> <li>– 1 Gigabit WAN port, external (e.g., for Internet access); Internet access with up to 50 Mbit/ sec)</li> <li>– 1 USB server</li> <li>– 1 USB Control</li> </ul> </li> </ul>
Operating System	<ul style="list-style-type: none"> <li>• Linux (embedded)</li> </ul>
Internet connection	<ul style="list-style-type: none"> <li>• 1 Internet Service Provider (ISP)</li> <li>• Four Internet Telephony Service Providers (ITSP)</li> </ul>

	<b>OpenScape Office MX</b>
Dimensions (mm)	<ul style="list-style-type: none"> <li>• Width = 440 mm</li> <li>• Height = 66.5 mm (3.36 in)</li> <li>• Depth = 350 mm</li> </ul>
Power supply	<p>The communication system is equipped for connection to the power supply.</p> <ul style="list-style-type: none"> <li>• Nominal input voltage: 110V to 240V, with a tolerance of (+/- 10%) -&gt; 99V to 264V</li> <li>• Nominal frequency: 50/60 Hz</li> </ul>
Current draw	Max. 4A at 99V
Power consumption	Depending on the configuration, from 80 W to a maximum of 250 W per system box (also depends on configuration)
Battery buffering	UPS for 110V to 240V, capacity: 4 Ah (at 110V) * desired hours; a UPS interface as with a PC is not present
Environmental Conditions	<ul style="list-style-type: none"> <li>• Operating conditions: +5 to +40 °C (41 to 104 °F)</li> <li>• Humidity: 5 to 85%</li> </ul>
Color	Metallic blue / Silver front

### 2.1.3 OpenScape Office HX

OpenScape Office HX is the server-based UC solution for HiPath 3000 that can be run on a Linux server. For voice communications, the features of the HiPath 3000 communication system are used.

Installation variants	<ul style="list-style-type: none"> <li>• Linux server certified for SUSE Linux Enterprise 11</li> </ul>
Subscribers/Stations	<ul style="list-style-type: none"> <li>• Max. 500 stations If every subscriber uses the fax box, the number of subscribers is reduced to 250, since a maximum of 500 phone numbers can be created.</li> <li>• Max. 1000 stations through networking</li> <li>• Max. 100 stations for mobile phone integration</li> </ul>
Operating System	<ul style="list-style-type: none"> <li>• Linux</li> </ul>
Supported communication systems	<ul style="list-style-type: none"> <li>• HiPath 3000 V9 and later</li> </ul>

## 2.1.4 Communications Clients, Mobility Clients and Contact Center Clients

With the Communications Clients myPortal and myAttendant, OpenScape Office provides access to unified communications via an intuitive user interface. The Mobility Clients (myPortal for Mobile/Tablet PC) offer access to UC on the move. The contact center clients myAgent and myReports provide access to the contact center functionality.

### Communications Clients

Client	Technical Data
myPortal for Desktop myPortal for Outlook myAttendant	<ul style="list-style-type: none"> <li>• Conferences (Ad-hoc, Scheduled, Permanent): OpenScape Office MX: max. 5 conferences with max. 16 participants, max. 20 conference channels OpenScape Office LX: max. 12 conferences with max. 16 participants, max. 40 conference channels</li> <li>• Presence status (Office, Meeting, Sick, Break, Out of the Office, Vacation, Lunch, Gone Home)</li> <li>• Messages (Voicemail and Fax Box)</li> <li>• Journal (Open, All, Missed, Answered, Internal, External, Inbound, Outbound, Scheduled)</li> <li>• Directories (Internal, External, Search)</li> <li>• Personal AutoAttendant</li> <li>• myAttendant: Up to 20 Attendant workplaces</li> </ul>
myPortal for Zimbra	myPortal for Zimbra integrates with the Zimbra e-mail program. The functionality is identical to myPortal for Mobile.
myPortal for OpenStage	myPortal for OpenStage can be used with the following telephones: <ul style="list-style-type: none"> <li>• OpenStage 60 V2 and later</li> <li>• OpenStage 80 V2 and later</li> </ul>

### Mobility Clients

Client	Technical Data
myPortal for Mobile myPortal for Tablet	<p>myPortal for Mobile is optimized for presentation on Apple's iPhone and can also be used with several other mobile phones. myPortal for Tablet is optimized for presentation on Apple's iPad and can also be used with several other tablet PCs. Depending on which device and operating system is used, the ease of use or function may be affected. The following requirements apply:</p> <ul style="list-style-type: none"> <li>• Touch screen (recommended for ease of use)</li> <li>• Min. display resolution of 240x320 pixels (myPortal for Mobile)</li> <li>• Min. display resolution of 800x480 pixels (myPortal for Tablet); a minimum resolution of 1024x600 pixels is recommended</li> <li>• Internet access</li> <li>• Web browser with JavaScript enabled</li> <li>• Support for the simultaneous transmission of voice and data through mobile phones and the mobile network</li> <li>• 3G data connection, for example, EDGE, UMTS, HSDPA (recommended for smooth service). GPRS can lead to slow page rendering.</li> <li>• Flat rate data plan (recommended for cost reasons), since data volumes of several 100 MB per month may be involved, depending on usage.</li> </ul>

### Contact Center Clients

Client	Technical Data
myAgent myReports	<ul style="list-style-type: none"> <li>• Agents MX one-box system: max. 10 agents MX multibox system, LX and HX: max. 64 agents</li> <li>• Calls per hour to the Contact Center One-box system: max. 200 calls per hour Multibox system: max. 500 calls per hour</li> <li>• Max. 50 queues/groups</li> <li>• Max. 64 supervisors The sum of agents and supervisors must not exceed a value of 64.</li> <li>• Max. 1 myReports</li> </ul>

**Application Launcher**

Client	Technical Data
Application Launcher	<ul style="list-style-type: none"> <li>• Looking up call-related information on a phone number in either the Directory Service or in system directories</li> <li>• Configurable screen pops for incoming calls with call-related information and buttons for user actions</li> <li>• Launching Windows applications or web applications for incoming and outgoing calls</li> <li>• Transfer of call-related information to applications (e.g., phone number, name of the caller, customer ID)</li> <li>• Max. 100 system connections</li> </ul>

**2.1.5 Supported Phones**

OpenScape Office LX / MX enables telephony and UC via IP phones. Both analog and ISDN telephones can be connected directly to OpenScape Office MX. OpenScape Office HX also enables UC via TDM, a/b, DECT and WLAN phones. Phone calls made with OpenScape Office HX always occur via the connected HiPath 3000.

**IP phones**

IP phones (HFA)	<ul style="list-style-type: none"> <li>• OpenStage HFA 15, 20 E, 20, 20 G, 40, 40 G, 60, 60 G, 80, 80 G, 80 E</li> <li>• optiPoint 410/420 are supported</li> </ul>
Key modules	<ul style="list-style-type: none"> <li>• OpenStage Key Module, only for OpenStage 15, 40, 60 and 80</li> <li>• OpenStage BLF 40 (Busy Lamp Field), only for OpenStage 40</li> </ul>
PC clients (HFA)	<ul style="list-style-type: none"> <li>• OpenScape Personal Edition (incl. video)</li> </ul>



SIP phones / AP adapter	<p>myPortal for Desktop, myPortal for Outlook and myAttendant can be used with SIP telephones that support RFC 3725.</p> <p>The following devices have already been certified:</p> <ul style="list-style-type: none"> <li>• OpenStage 15 S</li> <li>• Mediatrix 4102S (for connecting 2 analog phones or Fax devices)</li> <li>• AP 1120 S (for connecting 2 analog phones or Fax devices)</li> </ul> <p>The operation of other SIP devices must be certified within the framework of the HiPath Ready program.</p>
WLAN Phones	<p>The optiPoint WL2 professional can be optionally connected and operated via the following Access Points and Controllers:</p> <ul style="list-style-type: none"> <li>• Enterasys Wireless Access Point AP 2630 (wireless with internal antenna) and AP 2640 (wireless with external antenna). No more than six WL2 professionals can be connected to each access point (AP) and up to ten access points can be operated.</li> <li>• Enterasys Wireless Controller - Part No. C20 for larger configurations</li> </ul>
Dual-mode mobile phones	<p>Dual-mode mobile phones are differentiated on the SIP protocol level. The tested devices are:</p> <ul style="list-style-type: none"> <li>• Nokia E52, E75</li> <li>• Nokia N79, N85, N97</li> </ul>

**TDM telephones (HX via HiPath 3000)**

TDM telephones	<ul style="list-style-type: none"> <li>• OpenStage T 10 T, 15 T, 20 T, 30 T, 40 T, 60 T, 80 T</li> </ul> <p>optiPoint 500 is supported</p>
----------------	--

**DECT phones (LX/MX)**

HiPath Cordless IP (DECT phones)	<p>HiPath Cordless IP is a campus-wide mobility solution with the following mobile components:</p> <ul style="list-style-type: none"> <li>• Gigaset S3 professional</li> <li>• Gigaset S4 professional</li> <li>• Gigaset SL3 professional</li> <li>• Gigaset M2 professional</li> </ul> <p>DECT phones are integrated using SIP. The scope of features is correspondingly restricted.</p>
----------------------------------	--

**Analog and ISDN Stations (MX)**

Analog telephones	at OpenScape Office MX
ISDN devices	at OpenScape Office MX

**Add-on devices (MX)**

- Entrance telephone via ET-S adapter at OpenScape Office MX

**2.1.6 Infrastructure Components**

OpenScape Office supports the setup of a network infrastructure through the connection of additional infrastructure components.

- Enterasys switches (of the A2, B3 and D2 series) with and without Power over Ethernet (PoE)
- LAN switches from other vendors with or without Power over Ethernet (PoE)
- Routers (e.g., DSL router, VPN router)
- VPN Client (tested with Microsoft Standard Client and NCP Client)
- UPS (uninterrupted power supply unit)

---

**INFO:** More Information can be found under:  
<http://wiki.siemens-enterprise.com>

---

**2.1.7 Open Interfaces**

OpenScape Office provides open interfaces for the integration of external applications.

	LX	MX	HX
Physical Interfaces	LAN, USB, S <sub>0</sub> , S <sub>2M</sub> , a/b	LAN	LAN
Logical Interfaces	CSTA protocol, protocol for call detail records, SIP, DSS1	CSTA protocol, protocol for call detail records, SIP, DSS1	
API (Microsoft TAPI 2.1), Web Server Interface			
Interface for integrating web-based applications	http(s)	http(s)	http(s)

**2.1.8 Recommended and Certified Applications**

OpenScape Office can be optionally supplied with different applications that can be ordered and purchased separately. These are connected via LAN.

### OpenStage Gate View

OpenStage Gate View presents a camera image from the entrance area on an OpenStage phone (only OpenStage 60/80 HFA) or iPhone.

### Accounting (LX/MX)

- Standard Evaluation  
The Accounting Manager is supplied for the standard evaluation of call charge data.
- Professional Evaluation  
Teledata Office combines cost management in the telecommunications area with an analysis of the communication traffic.

### HiPath TAPI 120/170

The HiPath TAPI 120/170 service provider is installed on a Windows server as standardized interface software. For TAPI 120/170, an additional free CSTA license must be ordered.

HiPath TAPI 170 is supported for networking throughout the network, i.e., the external application is connected to a central network node.

### CallBridge IP

TAPI service provider for phoning with PCs under MS Windows operating systems via a LAN. CallBridge IP does not work in a VLAN configuration.

## 2.1.9 Additional Links

- Internet:  
<http://www.siemens-enterprise.com>
- Partner portal:  
<https://www.siemens-enterprise.com/seba/>
- Expert wiki for telephones, communication systems and UC:  
<http://wiki.siemens-enterprise.com>

## 2.2 Sample Scenarios

The sample scenarios describe the basic scenarios for the installation of OpenScape Office.

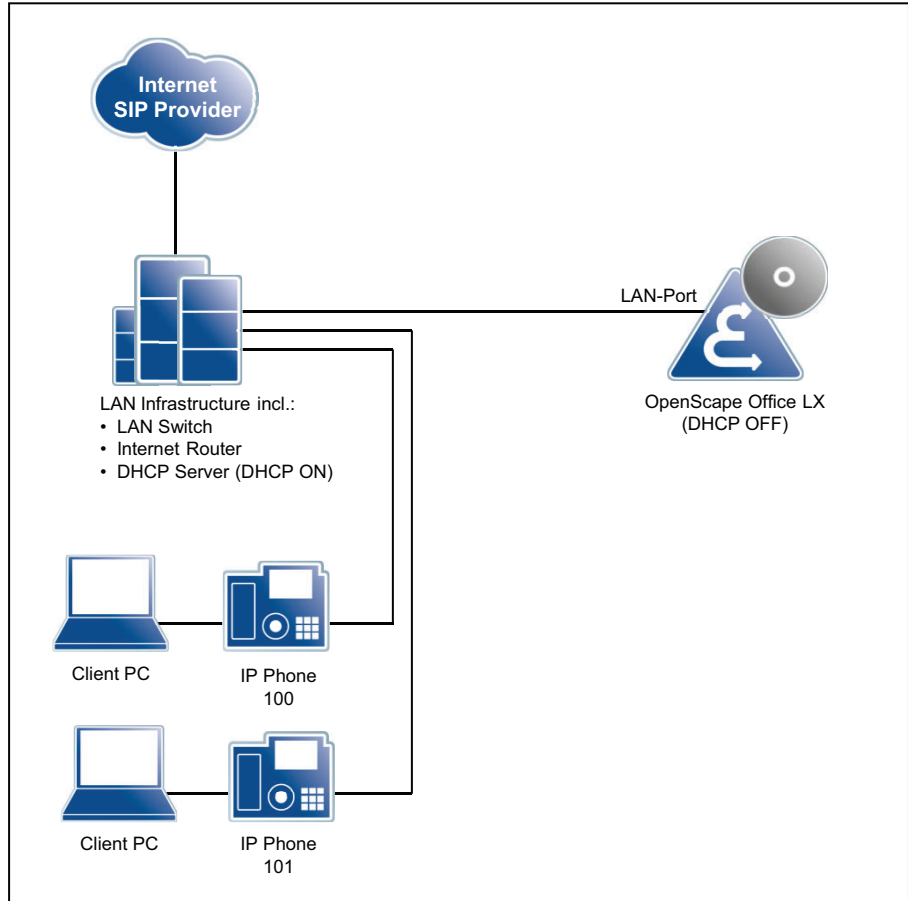
### 2.2.1 Sample Scenario for OpenScape Office LX

The sample scenario illustrates the standalone deployment of OpenScape Office LX.

In this scenario, OpenScape Office LX offers:

**System Overview and Scenarios**  
Sample Scenarios

- Trunk connection via an Internet Telephony Service Provider (SIP Provider)
- Internet access via an existing Internet router (e.g., DSL)
- IP phones (OpenStage)
- UC Clients (myPortal)

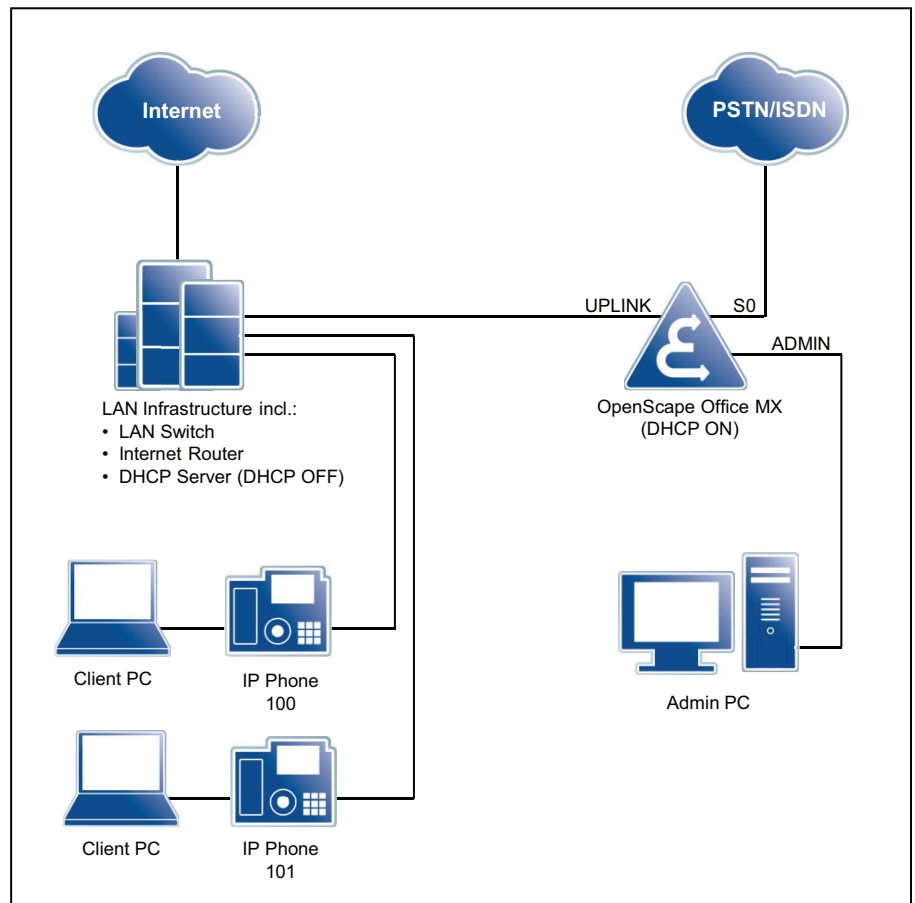


## 2.2.2 Sample Scenario for OpenScape Office MX

The sample scenario illustrates the stand-alone deployment of OpenScape Office MX.

In this scenario, OpenScape Office MX offers:

- Trunk connection to the public network (PTSN) via ISDN
- Internet access via an existing Internet router (e.g., DSL)
- IP phones (OpenStage)
- UC Clients (myPortal)



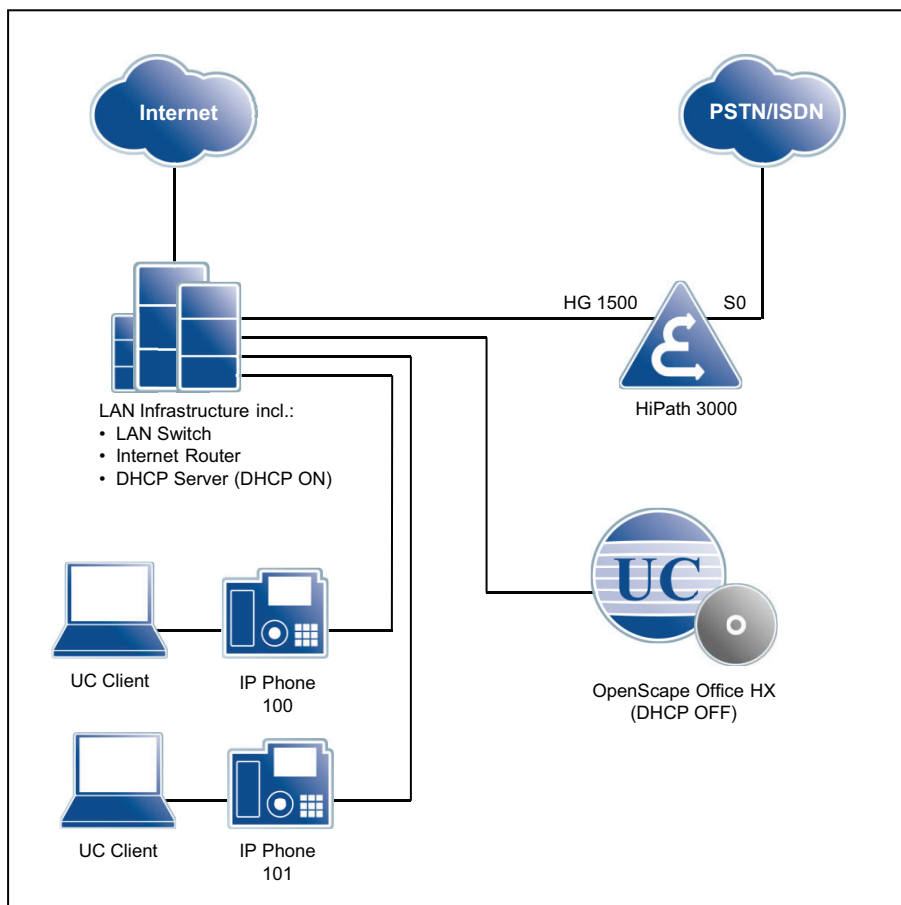
### 2.2.3 Sample Scenario for OpenScape Office HX

The sample scenario illustrates the deployment of OpenScape Office HX as a stand-alone unit with HiPath 3000.

In this scenario, OpenScape Office HX offers:

- Voice communications via HiPath 3000 and trunk connection to the public network (PTSN) via ISDN
- Internet access via HG 1500 through an existing Internet router (e.g., DSL)
- IP phones (OpenStage) at the HiPath 3000
- UC clients (myPortal) via OpenScape Office HX

**System Overview and Scenarios**  
Sample Scenarios



## 3 Hardware and Installation of OpenScape Office MX

The OpenScape Office MX communication system is a modular system that can be deployed as a one-box system (consisting of a single OpenScape Office MX system box) or as a multibox system (consisting of two or three OpenScape Office MX system boxes). Every OpenScape Office MX system box is equipped with a motherboard and provides three slots for installing optional gateway modules for the trunk and station connections.

OpenScape Office MX can be installed as a standalone unit (desktop mode) or in a 19" rack.

### 3.1 OpenScape Office MX System Box

Every OpenScape Office MX system box is equipped with a motherboard. The motherboard is the central processing unit of a system box. In addition, three slots are available for installing gateway modules.

The OpenScape Office MX communication system is based on a modular design and can comprise up to three OpenScape Office MX system boxes, depending on customer requirements.

A single-box system consists of a single OpenScape Office MX system box known as the central box.

Multibox systems consist of two or three OpenScape Office MX system boxes: one central box and one or two expansion boxes. The system boxes are interconnected using the LAN cable included in the delivery package for each system box.

In effect, the central box and expansion boxes consist of the same hardware, the OpenScape Office MX system box. The distinction between a central box and an expansion box is based purely on functionality. When configuring a multibox system with the OpenScape Office Assistant, one system box is assigned the function of the central box, another the function of expansion box 1 and, if present, a third the function of expansion box 2.



#### **WARNING**

##### **Risk of electric shock from touching live conductors**

When using the communication system in countries with country-specific requirements (Finland, Canada, Norway, Sweden and the USA), each OpenScape Office MX system box must be grounded with a separate grounding wire. Before you start up the system and connect the telephone lines, connect the OpenScape Office MX system box(es) with a permanent earthing conductor.

---

**Figure:** OpenScape Office MX System Box



### On/Off Switch

Switching the system off and on again by using the On/Off switch causes the system to be powered down and powered up again in an undefined state (analogous to the situation when switching a PC on and off with the PC switch). The system will be operational again after the startup.

---

**INFO:** An OpenScape Office MX system box may only be turned off with the On/Off switch in emergencies.

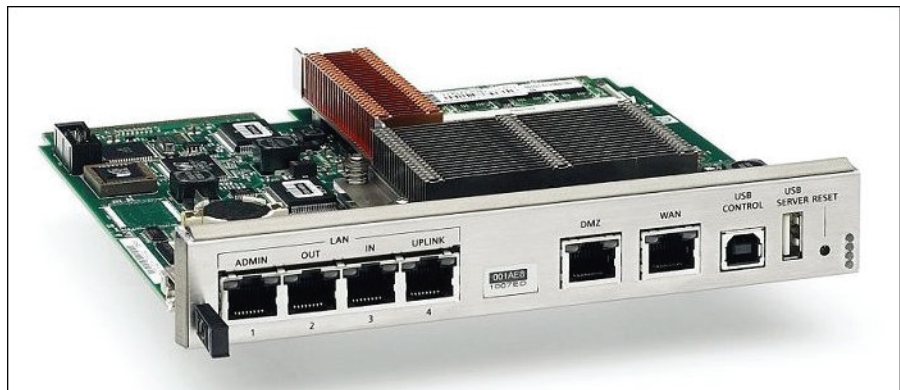
---

For more information, see [System Behavior after Pressing the On/Off Switch \(MX\)](#).

## 3.1.1 Motherboard

The motherboard is the central processing unit of an OpenScape Office MX system box.

**Figure:** OpenScape Office MX Motherboard



Every OpenScape Office MX system box is equipped with a motherboard (slot 1).

Multibox systems are subject to higher system loads due to the increased number of interfaces and stations. To ensure uniformly high performance, the system load is internally distributed to the motherboards of all multibox systems. This load balancing occurs automatically, depending on the system configuration.



Figure: Motherboard – Front View



**Connectors**

A motherboard provides the following ports (interfaces) in one-box and multibox systems:

- 4 x LAN (10/100/1000 Mbit/s):

Table: One-box system – LAN connections (interfaces)

LAN (10/100/1000 Mbit/s)	Motherboard in Central Box (CB)
LAN interface 1 (ADMIN)	For connecting a service PC to administer the communication system.
LAN interface 2 (OUT)	Cannot be used during operation of the communication system.
LAN interface 3 (IN)	
LAN interface 4 (UPLINK)	For linking into the LAN infrastructure of the customer, for connecting a WLAN Access Point, an additional LAN switch or the direct connection of an IP phone or PC client.

Table: Multibox system – LAN connections (interfaces)

LAN (10/100/1000 Mbit/s)	Motherboard in Central Box (CB)	Motherboard in Expansion box 1 (EB1)	Motherboard in Expansion Box 2 (EB2) (if present)
LAN interface 1 (ADMIN)	For connecting a service PC to administer the communication system.	Cannot be used during operation of the communication system.	

LAN (10/100/1000 Mbit/s)	Motherboard in Central Box (CB)	Motherboard in Expansion box 1 (EB1)	Motherboard in Expansion Box 2 (EB2) (if present)
LAN interface 2 (OUT)	For the connection to EB1.	<ul style="list-style-type: none"> <li>EB2 present: For the connection to EB2.</li> <li>Cannot be used during operation of the communication system.</li> </ul>	Cannot be used during operation of the communication system.
LAN interface 3 (IN)	Cannot be used during operation of the communication system.	For the connection to the CB.	For the connection to EB1.
LAN interface 4 (UPLINK)	For linking into the LAN infrastructure of the customer, for connecting a WLAN Access Point, an additional LAN switch or the direct connection of an IP phone or PC client.	Cannot be used during operation of the communication system.	

- 1 x DMZ (10/100/1000 Mbit/s), for "DMZ-like" (demilitarized zone) operation  
To connect E-mail servers and Web servers  
A demilitarized zone (DMZ), in conjunction with firewalls, represents a logically protected network segment which houses a company's publicly accessible services, such as its e-mail and web servers. In this way, the DMZ prevents external access to internal IT structures. With DMZ there are two physically separated firewalls. The term "DMZ-like" is used for OpenScape Office MX, since it has only one central firewall.
- 1 x WAN (10/100/1000 Mbit/s)  
To connect to an ITSP, for example, using DSL (PPPOE or PPTP protocol). The WAN can be connected to the DSL modem either directly or via a router.

---

**NOTICE:** The WAN port may only be used for the Internet access. If the WAN port is not used, it should be disabled.

---

**Table:** Assignment of the LAN, DMZ and WAN ports

RJ45 Jack, Pin	Signal	Notes
1	Tx +	Transmit +
2	Tx -	Transmit -
3	Rx +	Receive +
4	-	not used
5	-	not used

RJ45 Jack, Pin	Signal	Notes
6	Rx –	Receive –
7	–	not used
8	–	not used

**Table:** LEDs to display the status of the LAN, DMZ and WAN interfaces

LED	Status	Meaning
left	steady green light	link
	flashing	activity
right	steady green light	1000 Mbps
	steady orange light	100 Mbps
	off	10 Mbps

- 1 x USB Control (USB 1.1 Slave)  
To connect a PC for service and diagnostic purposes.
- 1 x USB Server (USB 2.0 Master)  
For connecting an external hard disk or USB stick for backups and software upgrades.

---

**INFO:** For multibox systems, only the USB server port of the central box can be used.

---

### Reset Switch

The motherboard's front panel features a Reset switch:

- Press reset switch < 10 sec.:  
The OpenScape Office MX system box performs a controlled restart (similar to pressing the Reset button on a PC). The system box will be operational again after the startup.

---

**INFO:** The Reset (Restart) switch should only be used in emergencies!

---

- Press Reset switch > 10 sec.:  
It causes the OpenScape Office MX system box to reload. The system box reverts to the initial (default) state following startup. All country and customer-specific settings are lost (system country code = Germany). Country- and customer-specific data backups can be reloaded once the basic settings have been configured.

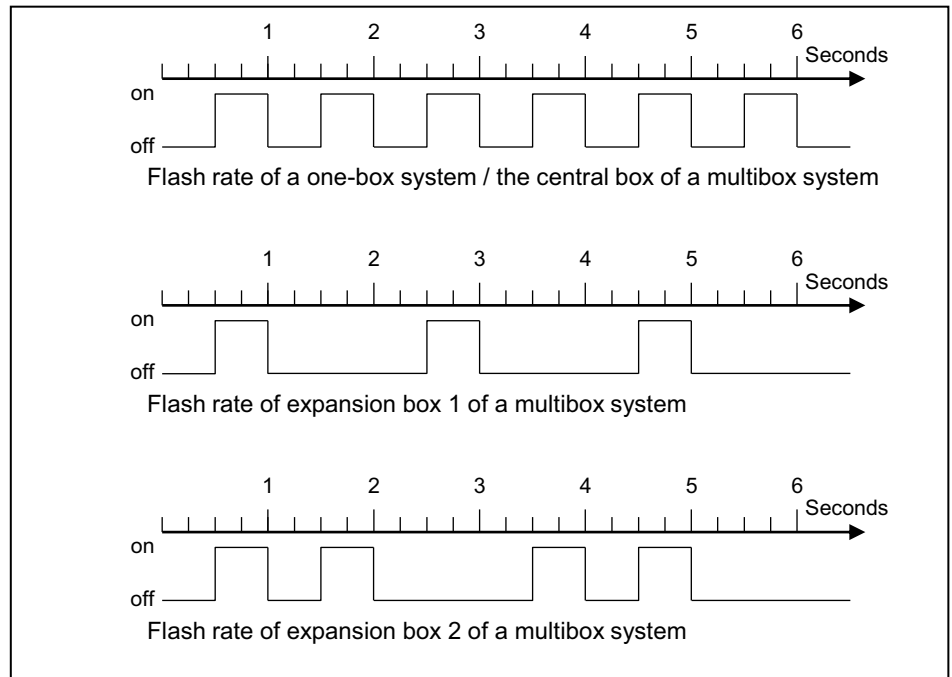
For more information on the function of the Reset switch, especially with respect to the differences in behavior for one-box and multibox systems, see [System Behavior after Initiating a Reset via the Reset Switch \(MX\)](#) and [System Behavior after Initiating a Reload via the Reset Switch \(MX\)](#).

## LEDs

The motherboard's front panel features four LEDs that indicate the operating states of the associated OpenScape Office MX system box:

- Green LED:
  - Flashing = normal operating state

**Figure:** Green LED – Flash Rates in Normal Operating State



- Off = On/Off switch at position "0"; power outage or error
- Red LED:
  - Off = normal operating state
  - Blinking = Error

Note: The brief flashing of the red LED after the system has been switched on or restarted signals a normal operating state during startup and does not indicate an error.
- Yellow LED:
  - On = the hard disk is being accessed
- Blue LED:
  - On = Operating state "Shutdown". Module release latch of the motherboard pulled out until the first resistance is felt.

### Module Release Latch

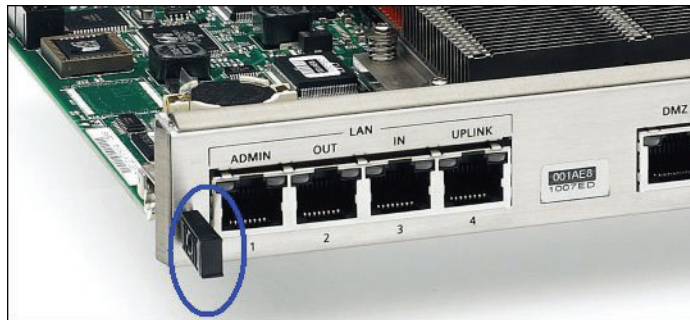
---

**NOTICE:** Damage to the motherboard through removal or insertion when the system box is active!

The motherboard can only be removed from a system box after the associated system box has been shut down gracefully and then turned off. The motherboard may only be inserted into a system box when the system box has been turned off.

---

**Figure:** Module release latch of the motherboard



Pulling out the module release latch of a motherboard results in a controlled shutdown of the associated OpenScape Office MX system box. All services are stopped, and the current data is backed up. You may only slide the module release latch until the first resistance is felt. On completing the shutdown, the blue LED of the motherboard lights up (operating state "Shutdown"). It is only at this point that you can safely switch off the system box and remove the motherboard.

To put the OpenScape Office MX system box back into service, the module release latch must be pressed in until it is arrested at the motherboard and it clicks into place. The On/Off switch must then be set to the position "I".

For more information, see [System Behavior after Unlocking the Module Release Latch of the Motherboard \(MX\)](#).

### 3.1.2 Slot and Access Designations

This section contains information on the slot designations in the OpenScape Office MX system box and the accesses (ports) available in the gateway modules.

### Slot Designations

Each OpenScape Office MX system box provides three slots (slots 2 through 4) for installing gateway modules (GM). The motherboard of the system box is always installed in one slot (slot 1).

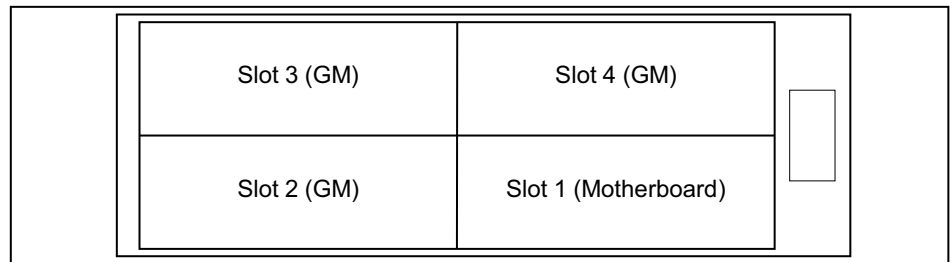
---

**NOTICE:** Protection against radio frequency interference and overheating

To ensure adequate protection and the dissipation of heat, the system box should not be operated with an open slot. Slots in which no gateway modules are installed must be closed with slot covers.

---

**Figure:** OpenScape Office MX system box – Slot numbering



### Access Designations

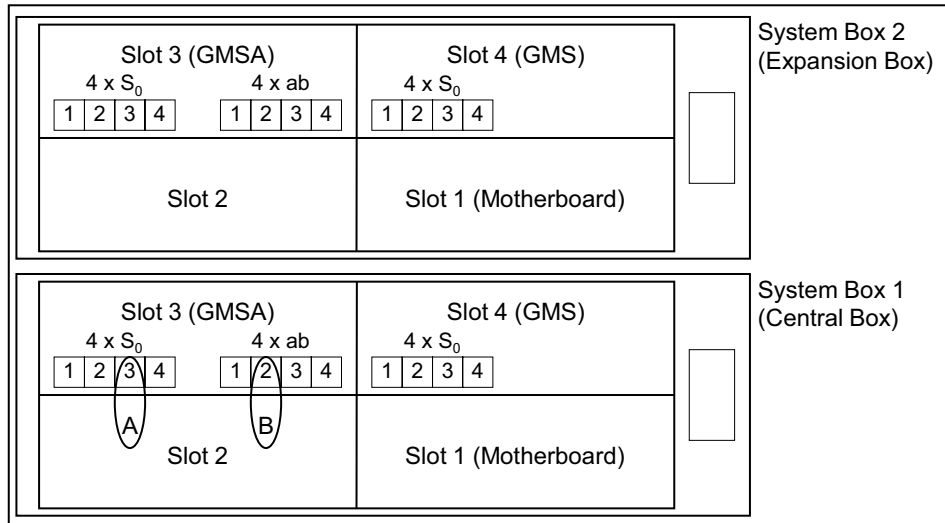
The accesses available in the gateway modules are identified as follows in OpenScape Office Assistant:

OpenScape Office MX system box no. – Slot no. – Interface type – Access no.

- OpenScape Office MX system box no.: indicates the system box containing the relevant access.
- Slot no.: indicates the slot containing the relevant access.
- Interface type: indicates the relevant access type.
- Access no.: indicates the number of the relevant access.

Example of a communication system consisting of two OpenScape Office MX system boxes:

**Figure:** Example of a Multibox system



- Access identified as A: 1–3–S<sub>0</sub>–3 = system box 1 – Slot 3 – S<sub>0</sub> port – Access 3
- Access identified as B: 1–3–a/b–2 = system box 1 – Slot 3 – a/b interface – Access 2

## 3.2 Gateway Modules

Gateway modules provide interfaces for the trunk and station connections.

Each OpenScape Office MX system box provides three slots (slots 2 through 4) for the custom installation of gateway modules (GM).

### Types

The following gateway modules can be used:

- GMS (not for U.S. and Canada) = Gateway module with four S<sub>0</sub> ports for the ISDN trunk connection or the ISDN station connection
- GMSA (not for U.S. and Canada) = Gateway module with four S<sub>0</sub> ports for the ISDN trunk connection or ISDN station connection and four a/b interfaces for the analog station connection
- GME (not for U.S. and Canada) = Gateway module with one S<sub>2M</sub> port for the ISDN Primary Rate Interface
- GMT (for U.S. and Canada only) = Gateway module with one T1 interface for the ISDN Primary Rate Interface
- GMAA = Gateway module with four a/b interfaces for the analog trunk connection and two a/b interfaces for the analog station connection
- GMAL = Gateway module with eight a/b interfaces for the analog station connection

## LEDs

The gateway modules described feature a front panel with two LEDs that indicate the relevant module's operating states:

- Green LED:  
Flashing = normal operating state  
Off = On/Off switch at position "0"; power outage or error  
On (briefly): startup phase
- Red LED:  
Off = normal operating state  
Blinking = Error

---

**NOTICE:** If a gateway module signals an error (red LED flashing), the problem can often be resolved by simply removing and then reinserting the gateway module. Note that the gateway module should not be reinserted into the slot of the system box until at least 150 seconds have passed. Otherwise, problems may arise when starting up the gateway module.

---

As can be seen in the following figure, only the upper two recesses are equipped with LEDs. The bottom two recesses have no function.

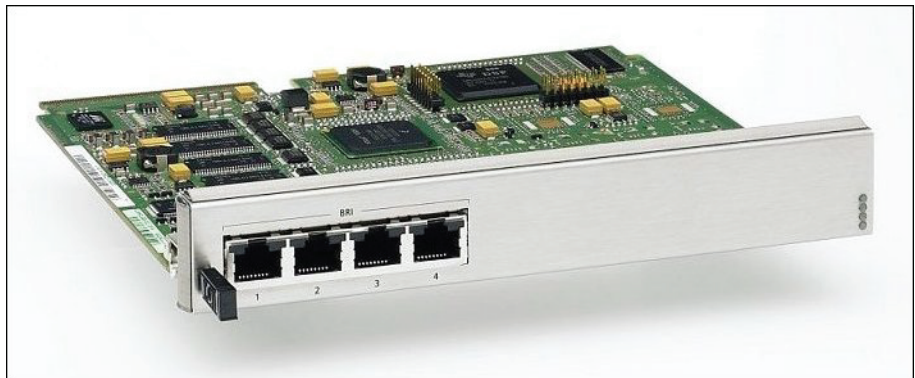
**Figure:** LEDs in gateway modules



### 3.2.1 Not for U.S. and Canada: Gateway Module GMS

The Gateway Module GMS provides four S<sub>0</sub> ports (BRI 1 - 4) for the ISDN system connection (ISDN trunk) or the ISDN station connection.

**Figure:** Gateway Module GMS







**WARNING**

**Risk of electric shock from touching live conductors**

When using the communication system in countries with country-specific requirements (Finland, Canada, Norway, Sweden and the USA), each OpenScape Office MX system box must be grounded with a separate grounding wire. Before you start up the system and connect the telephone lines, connect the OpenScape Office MX system box(es) with a permanent earthing conductor.

**Figure:** GMS – Front Panel



The RJ45 jacks on the S<sub>0</sub> ports each have four wires. ISDN trunk lines can be directly connected (1:1 cable). For ISDN phones, the Receive and Transmit lines must be swapped in each case.

The delivery package of the gateway module includes four S<sub>0</sub> cables for the ISDN trunk connection.

**INFO:** Lines for connecting ISDN phones may only exit the building via an external upstream device that guarantees primary overvoltage protection.

**Table:** GMS – Assignment of the S<sub>0</sub> connections (BRI 1 - 4)

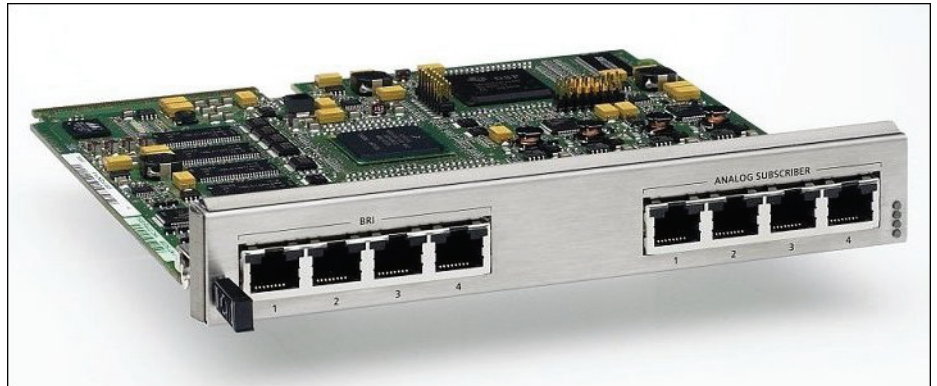
RJ45 Jack, Pin	Signal	Notes
1	–	not used
2	–	not used
3	Ta	Transmit +
4	Ra	Receive +
5	Rb	Receive –
6	Tb	Transmit –
7	–	not used
8	–	not used

### 3.2.2 Not for U.S. and Canada: Gateway Module GMSA

The Gateway Module GMSA provides four S<sub>0</sub> ports (BRI 1 - 4) for the ISDN system connection (ISDN trunk) or the ISDN station connection and four a/b interfaces (ANALOG SUBSCRIBER 1 - 4) for the analog station connection.

The a/b interfaces for the analog station connection support the CLIP feature.

**Figure:** Gateway Module GMSA



#### **WARNING**

##### **Risk of electric shock from touching live conductors**

When using the communication system in countries with country-specific requirements (Finland, Canada, Norway, Sweden and the USA), each OpenScape Office MX system box must be grounded with a separate grounding wire. Before you start up the system and connect the telephone lines, connect the OpenScape Office MX system box(es) with a permanent earthing conductor.

The delivery package of the gateway module includes four S<sub>0</sub> cables for the ISDN trunk connection.

**Figure:** GMSA – Front Panel



- S<sub>0</sub> ports  
The RJ45 jacks each have four wires. ISDN trunk lines can be directly connected (1:1 cable). For ISDN phones, the Receive and Transmit lines must be swapped in each case.

**INFO:** Lines for connecting ISDN phones may only exit the building via an external upstream device that guarantees primary overvoltage protection.

**Table:** GMSA – Assignment of the S<sub>0</sub> connections (BRI 1 - 4)

RJ45 Jack, Pin	Signal	Notes
1	–	not used
2	–	not used
3	Ta	Transmit +
4	Ra	Receive +
5	Rb	Receive –
6	Tb	Transmit –
7	–	not used
8	–	not used

- a/b interfaces  
The RJ45 jacks each have two wires.

---

**INFO:** Lines for connecting analog devices (e.g., phones or fax machines) must not leave the building.

---

The a/b interfaces supply a ring voltage of 45 V<sub>eff</sub>. Malfunctions can occur depending on the phones connected.  
If a higher ring voltage is required, the GMAL gateway module must be used. The a/b interfaces of this gateway module supply a ring voltage of 70 V<sub>eff</sub>.

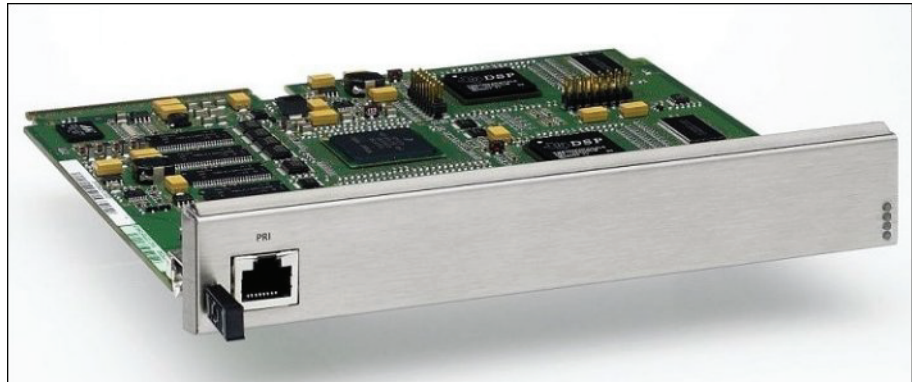
**Table:** GMSA – Assignment of the a/b connections (ANALOG SUBSCRIBER 1 - 4)

RJ45 Jack, Pin	Signal	Notes
1	–	not used
2	–	not used
3	–	not used
4	a	
5	b	
6	–	not used
7	–	not used
8	–	not used

### 3.2.3 Not for U.S. and Canada: Gateway Module GME

The Gateway module GME provides one S<sub>2M</sub> port for the ISDN Primary Rate Interface.

**Figure:** Gateway Module GME



**WARNING**

**Risk of electric shock from touching live conductors**

When using the communication system in countries with country-specific requirements (Finland, Canada, Norway, Sweden and the USA), each OpenScape Office MX system box must be grounded with a separate grounding wire. Before you start up the system and connect the telephone lines, connect the OpenScape Office MX system box(es) with a permanent earthing conductor.

**INFO:** A maximum of eight GME gateway modules may be used in a multibox system consisting of three system boxes.

The delivery package of the gateway module includes a patch cable for the ISDN Primary Rate Interface.

**Figure:** GME – Front Panel



A Primary Rate Interface features 30 bidirectional bearer channels (B-channels), each with 64 Kbps, a signaling channel (D-channel) with 64 Kbps, and a synchronization channel with 64 Kbps = 2048 Kbps gross bandwidth. This connection is mainly used by companies with high telephone traffic volumes to connect the communication system to the ISDN trunk.

**Table:** GME – Assignment of the S<sub>2M</sub> Connection (PRI)

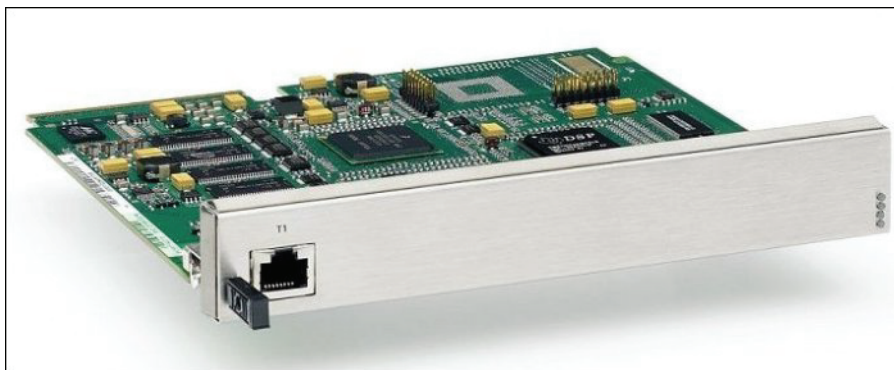
RJ45 Jack, Pin	Signal	Notes
1	Rb	B-wire, Receive
2	Ra	A-wire, Receive
3	–	not used

RJ45 Jack, Pin	Signal	Notes
4	Tb	B-wire, Transmit
5	Ta	B-wire, Transmit
6	–	not used
7	–	not used
8	–	not used

### 3.2.4 For U.S. and Canada only: Gateway Module GMT

The Gateway Module GMT provides one T1 interface for the ISDN Primary Rate Interface.

Figure: Gateway Module GMT



#### WARNING

##### Risk of electric shock from touching live conductors

When using the communication system in countries with country-specific requirements (Finland, Canada, Norway, Sweden and the USA), each OpenScape Office MX system box must be grounded with a separate grounding wire. Before you start up the system and connect the telephone lines, connect the OpenScape Office MX system box(es) with a permanent earthing conductor.

Figure: GMT – Front Panel



A Primary Rate Interface connection features 24 bidirectional bearer channels (B-channels), each with up to 64 Kbps per channel and a gross bandwidth of 1544 Kbps. This connection is mainly used by companies with high telephone traffic volumes to connect the communication system to the ISDN trunk.

The delivery package of the gateway module includes a T1 cable for the ISDN Primary Rate Interface.

---

**INFO:** The DSX-1 interface (T1 interface) in OpenScape Office MX must not be directly connected to the PSTN (Public Switched Telephone Network). A Channel Service Unit (CSU) must be installed between the communication system and the digital trunk connection. The CSU must be approved according to FCC Part 68 and satisfy the ANSI directive T1.403. The CSU provides the following features for OpenScape Office MX: Isolation and overvoltage protection of the communication system, diagnostic options in the event of a malfunction (such as signal loopback, application of test signals and test patterns), line-up of the output signal in compliance with the line lengths specified by the network provider.

---

**Table:** GMT – Assignment of the T1 Connection (T1)

RJ45 Jack, Pin	Signal	Notes
1	Rb	B-wire, Receive
2	Ra	A-wire, Receive
3	–	not used
4	Tb	B-wire, Transmit
5	Ta	B-wire, Transmit
6	–	not used
7	–	not used
8	–	not used

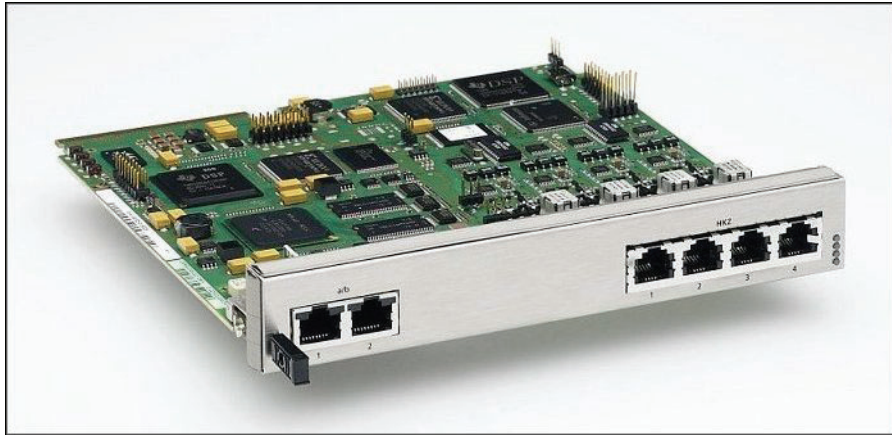
### 3.2.5 Gateway Module GMAA

The Gateway Module GMAA provides two a/b interfaces for the analog station connection (ANALOG SUBSCRIBER 1 - 4) and two a/b interfaces for the analog trunk connection (ANALOG TRUNK 1 - 2).

The a/b interfaces for the analog trunk connection support call detail recording with 12 kHz and 16 kHz pulses. The selection occurs automatically on setting the language of the communication system.

The a/b interfaces for the analog trunk connection and the analog station connection support the CLIP feature.

Figure: Gateway Module GMAA



**WARNING**

**Risk of electric shock from touching live conductors**

When using the communication system in countries with country-specific requirements (Finland, Canada, Norway, Sweden and the USA), each OpenScape Office MX system box must be grounded with a separate grounding wire. Before you start up the system and connect the telephone lines, connect the OpenScape Office MX system box(es) with a permanent earthing conductor.

Figure: GMAA – Front Panel



- a/b interfaces for the analog station connection  
The RJ45 jacks each have two wires.

---

**INFO:** Lines for connecting analog devices (e.g., phones or fax machines) must not leave the building.

---

The a/b interfaces supply a ring voltage of 45 V<sub>eff</sub>. Malfunctions can occur depending on the phones connected.

If a higher ring voltage is required, the GMAL gateway module must be used. The a/b interfaces of this gateway module supply a ring voltage of 70 V<sub>eff</sub>.

- a/b interfaces for the analog trunk connection  
The RJ45 jacks each have two wires. OpenScape Office MX supports analog trunk connections with ground-start and loop-start signaling.

---

**INFO:** The installation regulations in the U.S. and Canada require analog trunks to be connected using approved protectors as per UL 497A or CSA C22.2 No. 226.

---

**Table:** GMAA – Assignment of the a/b interfaces (ANALOG SUBSCRIBER 1 - 2, ANALOG TRUNK 1 - 4)

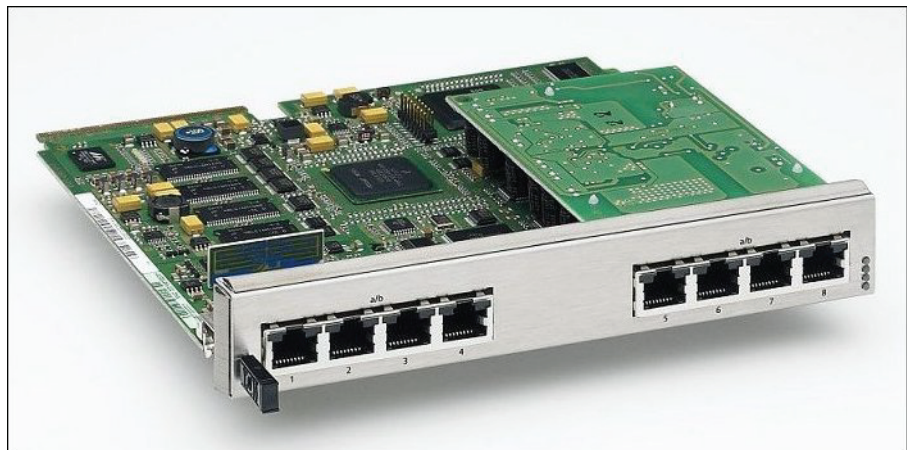
RJ45 Jack, Pin	Signal	Notes
1	–	not used
2	–	not used
3	–	not used
4	a	
5	b	
6	–	not used
7	–	not used
8	–	not used

### 3.2.6 Gateway Module GMAL

The Gateway Module GMAL provides eight a/b interfaces (ANALOG SUBSCRIBER 1 - 8) for the analog station connection.

The a/b interfaces for the analog station connection support the CLIP feature.

**Figure:** Gateway Module GMAL





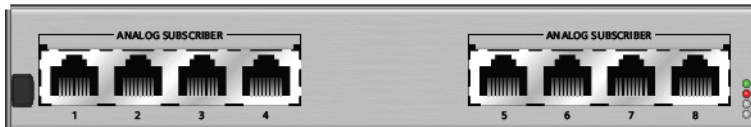


**WARNING**

**Risk of electric shock from touching live conductors**

When using the communication system in countries with country-specific requirements (Finland, Canada, Norway, Sweden and the USA), each OpenScape Office MX system box must be grounded with a separate grounding wire. Before you start up the system and connect the telephone lines, connect the OpenScape Office MX system box(es) with a permanent earthing conductor.

**Figure:** GMAL – Front Panel



The RJ45 jacks on the a/b (T/R) interfaces each have two wires. The a/b interfaces supply a ring voltage of 70 V<sub>eff</sub>.

**INFO:** Lines for connecting analog devices (e.g., phones or fax machines) must not leave the building.

**Table:** GMAL – Assignment of the a/b connections (ANALOG SUBSCRIBER 1 - 8)

RJ45 Jack, Pin	Signal	Notes
1	–	not used
2	–	not used
3	–	not used
4	a	
5	b	
6	–	not used
7	–	not used
8	–	not used

### 3.3 Installation

Before the OpenScape Office MX communication system can be set up and started for the first time, the hardware installation must be completed.

Install the hardware of the OpenScape Office MX communication system as described below.

Make sure that you have carefully read and noted the details provided under [Safety Information and Warnings](#) and under [Important Notes](#) before you begin with the installation.

- Preparatory Steps:
  - Unpacking the components
  - Attaching the plastic cover
  - For U.S. and Canada only: Setting ground start for analog trunk connection
  - Installing gateway modules
- Selecting the type of installation
- Providing protective grounding for the communication system
- Setting up one or more trunk connections of the communication system
- Integration in the LAN Infrastructure
- Connecting ISDN Phones and Analog Phones and Devices
- Closing Activities:
  - Performing a visual inspection

### 3.3.1 Prerequisites for Installation

To install the OpenScape Office MX communication system, you will need some specific tools and resources. Certain requirements must be observed when selecting the installation site. Note that there are also some specific requirements regarding the power supply when using the communication system in the United States and Canada.

#### Tools and Resources

The following tools and resources are required:

- TORX screwdriver, size T10
- TORX screwdriver, size T25, for the screws at the ground wire connection of an OpenScape Office MX system box.
- For 19-inch rack mount only: Special cabinet screws, which are not included in the delivery package of the communication system are needed to attach the communication system to the 19" rack. You will need a suitable screwdriver for these screws.
- Digital multimeter for measuring voltage. To check ground connections, if protective grounding is required for the system.

## Prerequisites for Selecting the Installation Site

---



### WARNING

#### Risk of electric shock from touching live conductors

When using the communication system in countries with country-specific requirements (Finland, Canada, Norway, Sweden and the USA), each OpenScape Office MX system box must be grounded with a separate grounding wire. Before you start up the system and connect the telephone lines, connect the OpenScape Office MX system box(es) with a permanent earthing conductor.

---

The OpenScape Office MX communication system can be installed as a standalone unit or in a 19" rack.

The following aspects should be considered when selecting the installation site of the communication system:

- To guarantee sufficient ventilation for the communication system, you must observe the following guidelines:
  - Standalone installation: A minimum clearance of 10 cm (4 in.) must be maintained to the right and left of the case.
  - 19" rack mount: The intake air temperature (i.e., the temperature of the air sucked in by the fan) of an OpenScape Office MX system box must not exceed a maximum of 40 °C (104 °F).
- Do not expose the communication system to direct sources of heat (for example, direct sunlight, radiators, etc.).
- Do not expose the communication system to extremely dusty environments.
- Avoid contact with chemicals.
- Avoid all condensation of humidity on or in the communication system during operation. The communication system must be completely dry before you put it into service.
- Note the environmental and mechanical conditions for operating the communication system (see [Operating Conditions](#)).
- The power cable connector must be readily accessible on every OpenScape Office MX system box for quick disconnection from the power source at any time.

#### For U.S. and Canada only: Prerequisites for Connecting the Power Supply

The power supply for the communication system must meet the following requirements:

- Electrical Connection Specifications:

Nominal voltage	Nominal voltage range		Nominal frequency range		Terminal box configuration
	from	To	from	To	
120 V AC/60 Hz	110 V AC	130 V AC	47 Hz	63 Hz	NEMA 5-15, 2-pin, 3-wire, grounded

- The power source must not be more than 2 m (6 ft.) away from the communication system.
- The power source must supply a voltage of 120 V AC (single-phase, protected) at 47-63 Hz.
- A local electric circuit must be used.
- We recommend an overvoltage arrestor between the AC power and the communication system.

### 3.3.2 Preparatory Steps

Before the actual installation, some preparatory steps such as unpacking the supplied components, attaching the plastic cover and installing gateway modules must be performed.

### 3.3.3 Protective Grounding

The protective grounding provides a secure connection to the ground potential to protect against dangerously high touch voltages in the event of a malfunction.

The OpenScape Office MX communication system is a Class 1 device and may only be connected to grounded sockets on the power supply circuit. Only then can a proper protective grounding of the communication system be guaranteed.

In accordance with country-specific requirements, a separate, permanently connected protective earthing conductor provides an additional protective grounding for the communication system and the connected telecommunications network. The additional protective grounding can be basically installed even if this is not mandated by national installation regulations.



---

## WARNING

### Risk of electric shock from touching live conductors

- When using the communication system in countries with country-specific requirements (Finland, Canada, Norway, Sweden and the USA), each OpenScape Office MX system box must be grounded with a separate grounding wire.
- Make sure that the ground wire is protected and strain-relieved (minimum conductor cross section = 12 AWG/2.5 mm<sup>2</sup>). A minimum conductor cross section of 10 AWG/4 mm<sup>2</sup> is needed to block the effects of external factors if the ground wire cannot be protected.

---

**NOTICE:** The protective grounding is highly recommended even in countries where this is not mandatory. To optimize the interference resistance of the communication system, the protective grounding should always be provided.

---

## 3.3.4 Trunk connection

The OpenScape Office MX communication system offers different options for trunk connections and thus for access to the public communication network.

You can select the trunk connection or connections required for your communication system from the following options:

- ISDN point-to-point connection via S<sub>0</sub> interface (not for U.S. and Canada)
- ISDN point-to-multipoint connection via S<sub>0</sub> interface (not for U.S. and Canada)
- ISDN Primary Rate Interface via the S<sub>2M</sub> Interface (not for U.S. and Canada)
- ISDN Primary Rate Interface via the T1 interface (not for U.S. and Canada)
- Analog trunk connections

## 3.3.5 Integration in the LAN Infrastructure

The integration of OpenScape Office MX in an internal customer network depends on the LAN infrastructure being used.

An internal customer network with an Internet router (DSL router) is already available in the basic scenario. Internet access is configured in the external Internet router. OpenScape Office MX is connected to the existing customer network via a LAN switch. The IP phones, PC clients, WLAN Access Points, etc.

are integrated in the internal customer network via one or more LAN switches and obtain their IP addresses dynamically from the DHCP server of the communication system.

### 3.3.6 Connecting ISDN Phones and Analog Phones and Devices

The OpenScope Office MX communication system offers numerous options for connecting ISDN phones and analog phones and devices.

Select the connection options required for your telephones and other devices:

- Direct connection of ISDN phones (not for U.S. and Canada)
- Connection of ISDN phones via the S<sub>0</sub> bus (not for U.S. and Canada)
- Connection of analog phones and devices

### 3.3.7 Closing Activities

To finish the installation, a visual inspection must be performed to check all connected cables and to verify the separate protective grounding of all the OpenScope Office MX system boxes. In addition, the local power supply should be tested with a digital multimeter.

## 3.4 Multibox Systems

Multibox systems consist of two or three OpenScope Office MX system boxes: one central box and one or two expansion boxes. A multibox system offers more slots for gateway modules than a one-box system and thus supports higher station configurations.

Maximum station configurations in one-box and multibox systems:

- One-box system = maximum 50 stations
- Multibox system consisting of two system boxes = maximum 100 stations
- Multibox system consisting of three system boxes = maximum 150 stations

### 3.4.1 Details on Multibox Systems

The central box and expansion boxes of a multibox system consist of the same hardware, the OpenScope Office MX system box. The distinction between a central box and an expansion box is based purely on functionality. When configuring a multibox system with the OpenScope Office Assistant, one system box is assigned the function of the central box, another the function of expansion box 1 and, if present, a third the function of expansion box 2.

A multibox system has a central database and is administered centrally.

Due to the increased number of system interfaces and subscribers, the system load is higher. To ensure uniformly high performance, the system load is internally distributed to the motherboards of all multibox systems. This load balancing occurs automatically, depending on the system configuration.

---

**INFO:** When a multibox system is updated, only the central box is supplied with the software image. Since the expansion boxes load the new software from the central box, they do not require any new image files.

After deconfiguring a multibox system, the individual system boxes must be individually updated to the latest software status.

---

### 3.4.2 Configuring a Multibox System

This section provides information on the procedures for configuring multibox systems including, for example, the initial configuration of a multibox system, the reconfiguration of a one-box system to a multibox system and the deconfiguration of a multibox system.

---

**INFO:** A three-box system cannot be directly downgraded to a two-box system!

---

The customized data of the three-box system can no longer be used. The entire administration of the two-box system must be repeated from the start.

## 4 Administration Concept

The administration of OpenScape Office is performed using web-based management (OpenScape Office Assistant). The user administration of the web-based management allows you to set up role-based administration.

### 4.1 Web Based Management

Web based management occurs using OpenScape Office Assistant.

#### 4.1.1 Prerequisites for OpenScape Office Assistant

In order to use OpenScape Office Assistant, the administration PC must have the appropriate software installed.

Supported Web browsers:

- Microsoft Internet Explorer 7 (Windows XP, Windows 2003 and Windows Vista)
- Microsoft Internet Explorer Version 8 in compatibility mode (Windows XP, Windows 2003, Windows Vista and Windows 7)
- Microsoft Internet Explorer Version 9 in compatibility mode (Windows Vista and Windows 7)
- Mozilla Firefox 4 (Windows XP, Windows 2003, Windows Vista, Windows 7 and Linux)

In addition, Java Edition 6 (1.6.x) must be installed.

#### 4.1.2 OpenScape Office Assistant

OpenScape Office Assistant is the web-based application for the administration of the system.

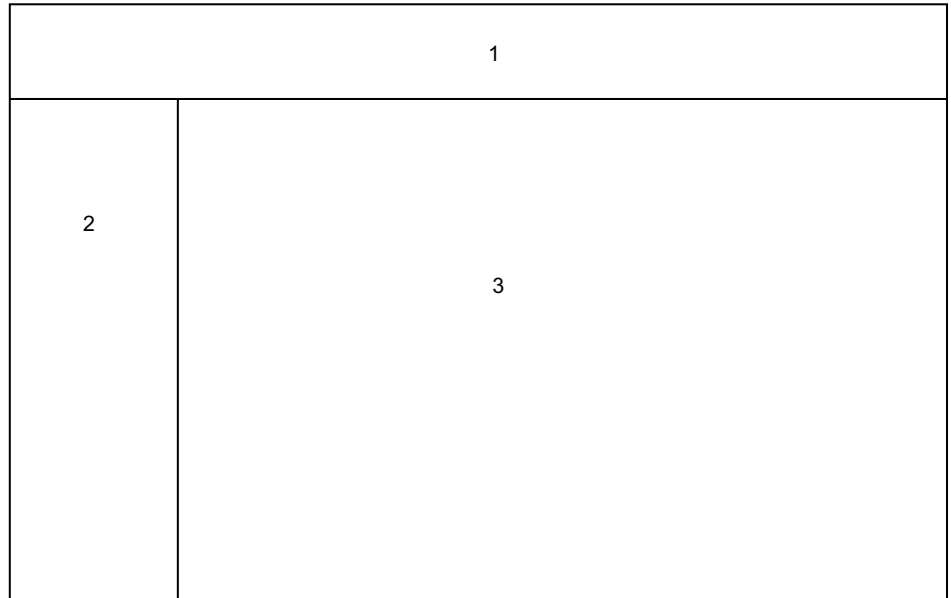
##### Language of the User Interface

You can select one of the following languages at login:

- German
- English
- French
- Italian
- Dutch (The online help is only available in English)
- Portuguese
- Spanish



## User Interface Elements



- **Navigation bar (1)**  
The navigation is the primary navigation aid and always shows the same links to main task centers, i.e., **Home**, **Administrators**, **Setup (LX/MX)**, **Expert Mode**, **Data Backup**, **License Management (LX/MX)** and **Service Center**. When you click on one of these task centers, the associated navigation tree opens in the navigation area, and the home page of the task center appears in the workspace.
- **Navigation area (2)**  
The navigation area is the secondary aid and contains the navigation tree with the menu items of the selected task center. The name of the selected task center is displayed at the top of the navigation tree with expandable and collapsible menu groups and menu items below it. Different menu items are displayed in the menu groups, depending on the situation. Clicking on a menu item displays the associated page in the workspace.
- **Workspace (3)**  
The workspace is where administration tasks are performed. It is usually opened in a separate window. The number and selection of messages and actions displayed depends on the menu item selected in the navigation tree. In Expert Mode, the menu tree is displayed on the left in the workspace.

### Navigating in the Menu Tree

The menu tree is a graphical interface component in the Expert Mode of OpenScope Office Assistant. The menu tree contains expandable and collapsible folders. These folders (e.g., **Basic Settings**) may, in turn, include further folders (e.g., **Call Charges**) and elements (e.g., **Call Charges - Output Format**).

You can navigate in the menu tree by double-clicking on a folder (which toggles its expanded or collapsed state).

### Automatic Logout After Timeout

You are automatically logged off after 30 minutes of inactivity. You must log back on to continue working with OpenScape Office Assistant. If you make some changes and then take a break, to be on the safe side, you should reload the page before making any further changes so that no changes are lost due the automatic logout.

---

### Related Topics

- [Backup and Restore](#)
- [Licensing](#)

## 4.1.3 User Administration of OpenScape Office Assistant

You can configure and manage up to 16 administrators for OpenScape Office Assistant. Every administrator is assigned a user profile that specifies the scope of his or her authorization.

The users of OpenScape Office Assistant are also referred to as administrators.

The default administrator is administrator@system with the default password "administrator" and has the user profile **Advanced**. This password must be changed on logging in for the first time. The password for an administrator must consist of at least 8 characters and a maximum of 128 characters, of which at least one character must be a digit. In addition to letters and digits, a password may include the following characters: !"#%&'()\*+,-./:;<=>@[ ]^\_`{|}~

### User profiles

OpenScape Office Assistant supports three permanently defined user profiles with different authorizations for administrators with different levels of technical expertise and tasks.

User profile	Know-how	Class of Service
<b>Basic</b> (not for OpenScape Office HX)	No knowledge of configuring the system	certain wizards, e.g., for <b>Key Programming, Music on Hold / Announcements</b> .
<b>Advanced</b>	Trained users	All wizards
<b>Expert</b>	Trained service technicians	All wizards and additional service functions in Expert Mode

The Advanced and Expert user profiles are authorized to change the user names and passwords of other administrators.

## 4.1.4 Online Help

The integrated online help describes key concepts and operating instructions.

### Navigation

The buttons in the online help provide the following functions:

- **Contents**  
provides you with an overview of the structure
- **Index**  
provides direct access to a topic using keywords
- **Search**  
allows you to do a full-text search and selectively find all relevant topics

## 4.2 Wizards (LX/MX)

Wizards make it easy to install and configure the system. Only selected wizards are available to customer administrators (with the **Basic** profile).

### 4.2.1 Wizards – Basic Installation (LX/MX)

The wizards under **Basic Installation** support the simple basic installation.

Menu item in the navigation area	Wizards	Customer administrator
<b>Basic Installation</b>	<b>Multibox System</b>	-
	<b>Initial installation</b>	-
	<b>Basic Installation</b>	-
	<b>Licensing</b>	-
	<b>Networking Configuration</b>	-

### 4.2.2 Wizards – Network / Internet (LX/MX)

The wizards under **Network / Internet** support the simple configuration of networks and the Internet access.

Menu item in the navigation area	Wizards	Customer administrator
Network / Internet	Network Configuration Internet Configuration VPN Configuration	- - -

### 4.2.3 Wizards – Telephones / Subscribers (LX/MX)

The wizards under **Telephones / Subscribers** support the simple configuration of phones and subscribers.

Menu item in the navigation area	Wizards	Customer administrator
Telephones / Subscribers	IP Telephones ISDN devices Analog Terminals Key programming	- - - x

### 4.2.4 Wizards – Central Telephony (LX/MX)

The wizards under **Central Telephony** support the simple configuration of central telephony features.

Menu item in the navigation area	Wizards	Customer administrator
Central Telephony	CO Trunk ISDN / Analog	-
	Internet Telephony	-
	Voicemail	-
	Directory / Speed Dialing	x
	Call Detail Recording	x
	Music on Hold / Announcements	x
	Entrance Telephone (Door Opener)	-

#### 4.2.5 Wizards – User Telephony (LX/MX)

The wizards under **User Telephony** support the simple configuration of user telephony features.

Menu item in the navigation area	Wizards	Customer administrator
User Telephony	Class of Service	-
	Station Name and Release	x
	Group call / Hunt group	-
	Call Forwarding	-
	Call pickup	-
	Team Configuration	-
	Mobile Phone Integration	-
	Executive / Secretary	-
	UCD	-
	Attendant Console	-
Station Profiles	-	

#### 4.2.6 Wizards – UC Suite

The wizards under **OpenScape Office** support the simple configuration of the UC Suite.

Menu item in the navigation area	Wizards	Customer administrator
OpenScape Office	<b>Departments</b> <b>Recorder</b> <b>User Directory</b> <b>Contact Center</b> <b>File Upload</b> <b>External directory</b> <b>Fax Headlines</b> <b>Groups</b> <b>Conferencing</b> <b>External Providers Config</b> <b>Profiles</b> <b>Templates</b> <b>Schedules</b>	- - - - - - - - - - - - -

### 4.3 Expert mode

Expert mode provides the administrator with several menus and functions to configure and maintain the system.

#### 4.3.1 Expert Mode - Maintenance > Configuration (LX/MX)

Under **Configuration** you will find a group of functions to load Music on Hold (MoH), display the hardware configuration or manage a multi-box system, for example.

The following functions can be accessed by the service technician under **Configuration** in Expert mode:

Menu tree	see
<b>Music on Hold</b>	• <a href="#">Music on Hold (LX/MX)</a>
<b>Slot Modules</b>	• <a href="#">Hardware Configuration (MX)</a>
<b>Multibox System</b>	• <a href="#">Configuring a Multibox System</a>
<b>Port Administration</b>	• <a href="#">Port Administration and Port Forwarding (MX)</a>

### 4.3.2 Expert Mode - Maintenance > Software Image (LX/MX)

The functions for refreshing the gateway software and the phone images are grouped together under **Software image**.

The following functions can be accessed by the service technician under **Software Image** in Expert mode

- **Gateway Software**
- **Phone Images**
- **Phone Images via Internet**
- **Phone Logo Images**

Information on updating the software can be found under [Updating OpenScape Office](#).

### 4.3.3 Expert Mode - Maintenance > Traces (LX/MX)

Trace functions are grouped together under **Traces**. The administrator can start and stop traces and change the trace settings.

---

**INFO:** Traces should only be activated by experienced service technicians and only following consultation with Back-Level Support. Activating traces can have a negative impact on system performance.

---

The following functions can be accessed by the service technician under **Traces** in Expert mode:

- **Trace Format Configuration**
- **Trace output interface**
- **Trace log**
- **Digital Loopback**
- **customer trace log**
- **M5T Syslog Trace**
- **M5T Trace Components**
- **Secure Trace**
- **Call Monitoring**
- **H.323 Stack Trace**
- **Trace Profiles**
- **Trace Components**

Information on **Traces** can be found under [Traces \(LX/MX\)](#).

#### 4.3.4 Expert Mode - Maintenance > Events (LX/MX)

The functions for displaying and controlling events are grouped together under **Events**. These include event configuration, for instance, and e-mail settings.

The following functions can be accessed by the service technician under **Events** in Expert mode:

- **Event Configuration**
- **Event Log**
- **E-mail**
- **Reaction Table**
- **Diagnosis Logs**

Information on **Events** can be found under [Events \(LX/MX\)](#).

#### 4.3.5 Expert Mode - Maintenance > SNMP (LX/MX)

The functions for configuring communities and traps are grouped together under **SNMP**. Communities are used to regulate SNMP data access authorizations. Traps are generated if system problems occur to inform administrators of errors and failures.

The following functions can be accessed by the service technician under **SNMP** in Expert mode:

- **Communities**
- **Traps**

Information on **SNMP** can be found under [SNMP \(Simple Network Management Protocol\) \(LX/MX\)](#).

#### 4.3.6 Expert Mode - Maintenance > Admin Log (LX/MX)

The administrator can use **Admin Log** to change the configuration (e.g., the language) of the administration log.

The following functions can be accessed by the service technician under **Admin Log** in Expert mode:

- **Configuration**
- **Admin Log Data**

Information on the administration log can be found under [Admin Log \(MX\)](#).

#### 4.3.7 Expert Mode - Maintenance > Actions (LX/MX)

The functions supported by the administrator for frequent administration tasks such as deleting log data are grouped together under **Actions**.



The following functions can be accessed by the service technician under **Actions** in Expert mode:

Menu tree	see
<b>Manual Actions</b>	• <a href="#">Manual Actions</a>
<b>Automatic Actions</b>	• <a href="#">Automatic Actions ( LX/MX)</a>

### 4.3.8 Expert Mode - Maintenance > Platform Diagnostics (LX/MX)

Platform Diagnostics Option (only for Development).

### 4.3.9 Expert Mode - Maintenance > Application Diagnostics (LX/MX)

Application Diagnostics Option (only for Development).

### 4.3.10 Experten-Modus – Telephony > Basic Settings (LX/MX)

Functions for configuring system flags, directory settings and speed dials, DynDNS, Quality of Service, date and time, and call charges are grouped together under **Basic Settings**.

The following functions can be accessed by the service technician under **Basic Settings** in Expert mode:

Menu tree	see
<b>System Flags</b> (System)	<ul style="list-style-type: none"> <li>• <a href="#">ISDN Stations (LX/MX)</a></li> <li>• <a href="#">Trunk Queuing</a></li> <li>• <a href="#">Calling Line Identification Presentation (CLIP)</a></li> <li>• <a href="#">Conference Management (LX/MX)</a></li> <li>• <a href="#">Trunks (MX)</a></li> <li>• <a href="#">Networking OpenScape Office</a></li> <li>• <a href="#">Account Codes (LX/MX)</a></li> </ul>
<b>Time Parameters</b> (System)	• <a href="#">Time Parameters (LX/MX)</a>
<b>Display</b> (System)	<ul style="list-style-type: none"> <li>• <a href="#">Journal</a></li> <li>• <a href="#">Voicemail Box</a></li> <li>• <a href="#">Date and Time (LX/MX)</a></li> <li>• <a href="#">Call Duration Display on Telephone (LX/MX)</a></li> </ul>
<b>DISA</b> (System)	• <a href="#">DISA (MX)</a>
<b>Intercept/Attendant/Hotline</b> (System)	<ul style="list-style-type: none"> <li>• <a href="#">Hotline after Timeout / Hotline (LX/MX)</a></li> <li>• <a href="#">Intercept</a></li> </ul>

Menu tree	see
LDAP (System)	• <a href="#">External Offline Directory (LDAP)</a>
Texts (System)	• <a href="#">Advisory Messages</a> • <a href="#">Message Texts</a>
Flexible Menu (System)	• <a href="#">Flexible Menus (LX/MX)</a>
Speed Dials (System)	• <a href="#">Individual Speed Dialing (ISD)</a>
Gateway	• <a href="#">Customized Display (LX/MX)</a>
DynDNS	• <a href="#">DynDNS (MX)</a>
AF/EF Code Points	• <a href="#">Quality of Service (LX/MX)</a>
Quality of Service	• <a href="#">Quality of Service (LX/MX)</a>
Date and Time	• <a href="#">Date and Time (LX/MX)</a>
Port Management	• <a href="#">Ports and Services (LX/MX)</a>
Call Charges	• <a href="#">Accounting (LX/MX)</a>
Voicemail	• <a href="#">Voicemail Box</a>

---

**Related Topics**

- [System Flags \(LX/MX\)](#)

### 4.3.11 Expert Mode – Telephony > Security (MX)

Security settings are grouped together under **Security**. These include settings for firewalls, filters, VPN, and SSL.

The following functions can be accessed by the service technician under **Security** in Expert mode:

Menu tree	see
MAC Address Filtering	• <a href="#">MAC and IP Address Filtering (MX)</a>
IP Address Filtering	• <a href="#">MAC and IP Address Filtering (MX)</a>
Deployment- und Licensing Client (DLSC)	•
Signaling and Payload Encryption (SPE)	• <a href="#">Signaling and Payload Encryption (SPE) (LX/MX)</a>
VPN	• <a href="#">VPN (Virtual Private Network) (MX)</a>
SSL	• <a href="#">SSL (Secure Socket Layer) (MX)</a>
Samba Share	• <a href="#">Samba Share (LX/MX)</a>

### 4.3.12 Expert Mode – Telephony > Network Interfaces (MX)

Functions such as LAN, WAN (DSL) and DMZ interface configuration are grouped together under **Network Interfaces**. The interfaces can be configured separately.

The following functions can be accessed by the service technician under **Network Interfaces** in Expert mode:

Menu tree	see
LAN	<ul style="list-style-type: none"> <li>• <a href="#">IP Addresses (LX/MX)</a></li> </ul>
WAN (DSL)	<ul style="list-style-type: none"> <li>• <a href="#">Internet Access (MX)</a></li> </ul>
DMZ	<ul style="list-style-type: none"> <li>• <a href="#">Security</a></li> </ul>
FTP Server	Preparatory effort for future versions.
DHCP	<ul style="list-style-type: none"> <li>• <a href="#">DHCP, Dynamic Host Configuration Protocol (LX/MX)</a></li> </ul>

### 4.3.13 Expert Mode – Telephony > Routing (MX)

Routing tables are managed under **Routing**. In small networks, a routing table can be set up manually on every router by the administrator. In larger networks, this task is automated with the help of a protocol that distributes routing information in the network.

The following functions can be accessed by the service technician under **Routing** in Expert mode:

Menu tree	see
IP Routing	<ul style="list-style-type: none"> <li>• <a href="#">DNS, Domain Name Service (MX)</a></li> <li>• <a href="#">IP Routing (MX)</a></li> </ul>
IP Mapping	<ul style="list-style-type: none"> <li>• <a href="#">IP Mapping (MX)</a></li> </ul>
NAT	<ul style="list-style-type: none"> <li>• <a href="#">NAT (MX)</a></li> </ul>
PSTN	<ul style="list-style-type: none"> <li>• <a href="#">Expert Mode – Telephony &gt; Routing (MX)</a></li> <li>• <a href="#">Remote Access (MX)</a></li> </ul>
LCR	<ul style="list-style-type: none"> <li>• <a href="#">End-of-Dialing Recognition</a></li> <li>• <a href="#">Call Routing &gt; Emergency Calls &gt; Trunk Release for Emergency Call</a></li> <li>• <a href="#">LCR (Least Cost Routing) (LX/MX)</a></li> <li>• <a href="#">Networking OpenScape Office</a></li> </ul>

### 4.3.14 Expert Mode – Telephony Voice > Voice Gateway (LX/MX)

The functions for IP telephony are grouped together under **Voice Gateway**.

The following functions can be accessed by the service technician under **Voice Gateway** in Expert mode:

Menu tree	see
<b>SIP Parameters</b>	• <a href="#">IP Protocols (LX/MX)</a>
<b>Codec Parameters</b>	• <a href="#">Audio Codecs (LX/MX)</a>
<b>Internet Telephony Service Provider</b>	• <a href="#">IP Telephony (Voice over IP, VoIP)</a>
<b>PBX</b>	• <a href="#">Networking OpenScape Office</a>

### 4.3.15 Experten-Modus – Telephony > Stations (LX/MX)

Functions for all stations are grouped together under **Subscriber**. These include the name and phone number of the subscriber, for instance, as well as key programming information.

The following functions can be accessed by the service technician under **Stations** in Expert mode:

Menu tree	see
<b>IP Clients</b> (Stations)	• <a href="#">IP Stations</a>
<b>Analog Stations</b> (Station)	• <a href="#">Analog Stations (LX/MX)</a>
<b>ISDN Stations</b> (Stations)	• <a href="#">ISDN Stations (LX/MX)</a>
<b>Virtual Stations</b> (Stations)	• <a href="#">Virtual Stations</a>
<b>Application Suite</b> (Station)	• <a href="#">Users of the UC Suite</a>
<b>DDI Extensions Overview</b> (Stations)	• <a href="#">Configuring Stations in Expert Mode (LX/MX)</a>
<b>Mobility Entry</b> (Stations)	• <a href="#">Virtual Stations for Mobility Entry</a>
<b>Key programming</b>	• <a href="#">Key Programming (LX/MX)</a>

### 4.3.16 Expert Mode – Telephony > Incoming Calls (LX/MX)

Call Management (CM) functions are grouped together under **Incoming calls**. These include settings for groups, for instance, and call forwarding—no answer.

The following functions can be accessed by the service technician under **Incoming Calls** in Expert mode:

Menu tree	see
Groups/Hunt groups	<ul style="list-style-type: none"> <li>• <a href="#">Group Call</a></li> <li>• <a href="#">Hunt Group</a></li> </ul>
Mobility Entry groups	<ul style="list-style-type: none"> <li>• <a href="#">myPortal for Mobile</a></li> </ul>
Team/Top	<ul style="list-style-type: none"> <li>• <a href="#">Team Configuration / Team Group</a></li> <li>• <a href="#">Executive/Secretary or Top Group</a></li> </ul>
Call pickup	<ul style="list-style-type: none"> <li>• <a href="#">Call pickup group</a></li> </ul>
UCD	<ul style="list-style-type: none"> <li>• <a href="#">UCD (Uniform Call Distribution) (LX/MX)</a></li> </ul>
Call Forwarding	<ul style="list-style-type: none"> <li>• <a href="#">Call Forwarding—No Answer (CFNA) With a Timeout (Fixed Call Forwarding)</a></li> </ul>

### 4.3.17 Expert Mode – Telephony > Trunks/Routing (LX/MX)

The functions for trunks and routes are grouped together under **Trunks/Routing**.

The following functions can be accessed by the service technician under **Trunks/Routing** in Expert mode:

Menu tree	see
Trunks	<ul style="list-style-type: none"> <li>• <a href="#">Trunks (MX)</a></li> <li>• <a href="#">Networking OpenScope Office</a></li> </ul>
Route	<ul style="list-style-type: none"> <li>• <a href="#">Call Signaling, Calling Line ID (LX/MX)</a></li> <li>• <a href="#">Routes (MX)</a></li> <li>• <a href="#">Networking OpenScope Office</a></li> </ul>
QSIG Feature	
assign MSN	<ul style="list-style-type: none"> <li>• <a href="#">Trunks (MX)</a></li> </ul>

### 4.3.18 Experten-Modus – Telephony > Classes of Service (LX/MX)

The trunk authorization functions (for instance, which calls can be set up by which subscribers) are grouped together under **Class of service**.

The following functions can be accessed by the service technician under **Classes of Service** in Expert mode:

Menu tree	see
Subscribers/Stations	<ul style="list-style-type: none"> <li>• <a href="#">Classes of Service, Toll Restriction (LX/MX)</a></li> </ul>
Class of Service Groups	<ul style="list-style-type: none"> <li>• <a href="#">Night Service (LX/MX)</a></li> </ul>
Allowed lists	<ul style="list-style-type: none"> <li>• <a href="#">Classes of Service, Toll Restriction (LX/MX)</a></li> </ul>
Denied lists	<ul style="list-style-type: none"> <li>• <a href="#">Classes of Service, Toll Restriction (LX/MX)</a></li> </ul>

Menu tree	see
Night service	• <a href="#">Night Service (LX/MX)</a>
CON Group Assignment	• <a href="#">CON Groups (LX/MX)</a>
CON Matrix	• <a href="#">CON Groups (LX/MX)</a>
Autom. night service	• <a href="#">Night Service (LX/MX)</a>
Special Days	• <a href="#">Night Service (LX/MX)</a>

### 4.3.19 Expert Mode – Telephony > Auxiliary Equipment (LX/MX)

The functions for auxiliary equipment such as Music on Hold (MoH) or for connecting an entrance telephone/door opener at the system ports (trunks) are grouped together under **Auxiliary Equipment**.

The following functions can be accessed by the service technician under **Auxiliary Equipment** in Expert mode:

Menu tree	see
Announcement	• <a href="#">Music on Hold (LX/MX)</a> • <a href="#">Announcements (LX/MX)</a>
Entrance telephone (MX)	• <a href="#">Entrance Telephone and Door Opener (MX)</a>

### 4.3.20 Experten-Modus – Telephony > Payload (LX/MX)

The functions for displaying and configuring port types and protocols are grouped together under **Payload**.

The Service technician can access the following functions under **Payload** in Expert mode:

- **Devices:** collective name for stations, features, and functions that require specific channels.
- **Protocols:** transmission-specific parameters. The protocols should not be changed!
- **Media Stream Control (MSC):** monitors and manages streams and provides for the transmission of media data between LAN and ISDN.
- **HW Modules:** DSP channels (digital signal processors) for voice, modem and fax.

### 4.3.21 Experten-Modus – Telephony > Statistics (LX/MX)

The functions for displaying statistics are grouped together under **Statistics**.

The service technician can access the following functions under **Statistics** in Expert mode:

- **Device Statistics:** Statistics on LAN Usage and SCN.
- **SNMP Statistics:** statistics of the SNMP protocol with data and error data from the network traffic.
- **Telephony Statistics:** Statistics on Telephony.

## 4.3.22 Expert Mode – Applications > UC Suite

Under **UC Suite** you will find a group of unified communications functions such as conferencing, departments and groups, configuring the external directory, holiday and other schedules, the Contact Center and the server settings for the UC Suite.

The following functions can be accessed by the service technician under **UC Suite** in Expert mode:

Menu tree	Description
<b>User Directory</b>	Configuring Users for the UC Suite. See also: <ul style="list-style-type: none"> <li>• <a href="#">Departments</a></li> <li>• <a href="#">Subscribers/Stations</a></li> </ul>
<b>Departments</b>	Configuring departments. See also: <ul style="list-style-type: none"> <li>• <a href="#">Departments</a></li> </ul>
<b>Groups</b>	Only existing groups for voice and fax messages can now be edited here. The addition of new groups occurs using Team functions. See also: <ul style="list-style-type: none"> <li>• <a href="#">Voicemail Group and Fax Box Group (LX/MX)</a></li> </ul>
<b>Templates</b>	Configuring the SMS template for SMS notification See also: <ul style="list-style-type: none"> <li>• <a href="#">Notification Service for Messages</a></li> </ul> Configuring the user template for the AutoAttendant See also: <ul style="list-style-type: none"> <li>• <a href="#">Central AutoAttendant</a></li> </ul>
<b>External directory</b>	Importing a CSV file for an external directory. See also: <ul style="list-style-type: none"> <li>• <a href="#">External directory</a></li> </ul>
<b>External Providers Config</b>	Integrating an LDAP server in the external directory. See also: <ul style="list-style-type: none"> <li>• <a href="#">External Offline Directory (LDAP)</a></li> </ul>

Menu tree	Description
<b>Contact Center</b>	Configuration of the Multimedia Contact Center See also: <ul style="list-style-type: none"> <li>• <a href="#">Multimedia Contact Center</a></li> </ul>
<b>Schedules</b>	Configuring schedules for the AutoAttendant. See also: <ul style="list-style-type: none"> <li>• <a href="#">Schedules</a></li> </ul>
<b>File Upload</b>	Loading of announcements for the AutoAttendant and voicemail box as well as centralized fax cover sheets. See also: <ul style="list-style-type: none"> <li>• <a href="#">AutoAttendant</a></li> <li>• <a href="#">Voice and Fax Messages</a></li> <li>• <a href="#">Sending Fax Messages with Fax Printer</a></li> </ul>
<b>Recorder</b>	Recording announcements for the AutoAttendant. See also: <ul style="list-style-type: none"> <li>• <a href="#">AutoAttendant</a></li> </ul>
<b>Conferencing</b>	Displaying the details of a scheduled phone conference (Meet-Me conference). See also: <ul style="list-style-type: none"> <li>• <a href="#">Conference Management (LX/MX)</a></li> </ul>
<b>Site List</b>	Configuring locations for networking.
<b>Servers</b>	Configuring business and office hours for AutoAttendant, the password length for applications and the call number of the intercept position. See also: <ul style="list-style-type: none"> <li>• <a href="#">Schedules</a></li> <li>• <a href="#">Configuring Users of the UC Suite</a></li> <li>• <a href="#">Intercept</a></li> </ul> Configuring the retention period for voicemails and call information in the call journal. See also: <ul style="list-style-type: none"> <li>• <a href="#">Voice and Fax Messages</a></li> <li>• <a href="#">Journal</a></li> </ul> Configuring the parameters for the voicemail box such as the language, playback order and message length See also: <ul style="list-style-type: none"> <li>• <a href="#">Voice and Fax Messages</a></li> </ul>



Menu tree	Description
<b>Profiles</b>	Central configuration of user settings for clients. See also: • <a href="#">Station and User Profiles</a>
<b>Fax Headlines</b>	Configuring fax headers. See also: • <a href="#">Sending Fax Messages with Fax Printer</a>
<b>Holiday Schedules</b>	Configuring holiday schedules for the AutoAttendant. See also: • <a href="#">Schedules</a>

### 4.3.23 Expert mode – Applications > Web Services (LX/MX)

Configuration options for web interfaces, e.g., for web collaboration, can be found under **Web Services**.

The following functions can be accessed by the service technician under **Web Services** in Expert mode:

Menu tree	Description
<b>XMPP</b>	Configuring XMPP. See also: • <a href="#">XMPP</a>
<b>Mobility/Web Clients</b>	Configuring the interface for Mobility Clients, Web Clients and the Application Launcher. See also: • <a href="#">Configuring myPortal for Mobile and Mobility Entry (LX/MX)</a>
<b>Web Collaboration</b>	Configuring the interface for Web Collaboration. See also: • <a href="#">Web Collaboration Integration</a>

## 4.4 Service Center

The **Service Center** of OpenScape Office Assistant provides administrators with software, documentation and other diagnostics functions.

---

#### Related Topics

- [Updates and Upgrades](#)

- [Remote Access \(MX\)](#)
- [Shutting Down the OpenScape Office MX Communication System](#)

### **4.4.1 Service Center - Download Center**

The **Download Center** provides documents, PC clients, tools and links to related information.

The following documents are available:

- Administrator Documentation
- User Guides for Clients
- Mobility Entry, Quick Reference Guide
- TUI Menu Structure (Phone Menu of the Voicemail Box)
- CSV Templates for Importing Station Data, Speed-Dial Numbers and Port Data

The following PC clients are available (sometimes combined in one package):

- myPortal for Desktop
- myAttendant
- myPortal for Outlook
- Fax Printer
- myAgent
- myReports

The following tools are available:

- Application Launcher
- Call Charge Manager (Accounting Manager)
- ISDN message decoder
- OSO Observer  
Displays the operating state of the UC Suite under Windows.
- Audio Wizard  
Enables the creation of audio files for the voicemail box and central AutoAttendant with the mixing of two sources, e.g., background music and announcements.
- SNMP MIB

### **4.4.2 Service Center – Inventory**

**Inventory** provides an overview of the basic configuration data of the system.

### 4.4.3 Service Center – Software Update

**Software Update** checks whether a software update is available on the web server and performs the update.

### 4.4.4 Service Center – E-mail Forwarding

**E-mail Forwarding** enables the sending of e-mails with system messages from the UC Suite to the administrator and e-mails with attached voicemail of fax messages to subscribers.

### 4.4.5 Service Center – Remote Access (LX/MX)

**Remote Access** is used to configure access for the site-independent administration of the system.

### 4.4.6 Service Center – Restart / Reload

**Restart / Reload** enables a restart of the system, optionally resetting it back to factory settings.

### 4.4.7 Service Center – Diagnostics > Status (LX/MX)

**Status** provides status information on the network, subscribers, call setup, ITSP and VPN.

See also

### 4.4.8 Service Center – Diagnostics > Event Viewer (LX/MX)

**Event Viewer** logs system events.

See also

## **4.4.9 Service Center – Diagnostics > Trace**

**Trace** provides options for fault logging.

See also

## 5 Connection to Service Provider (LX/MX)

The communication system supports different connections to service providers for Internet access and Internet telephony via an Internet Telephony Service Provider (ITSP, SIP Provider). OpenScape Office MX also provides access to outside lines via ISDN or analog connections through optional gateway modules.

Access to the Internet occurs via either an Internet modem or an Internet router. In order to connect OpenScape Office MX to the Internet, the communication system must be configured as described below. In the case of OpenScape Office LX, access to the Internet is configured in the Linux operating system and is therefore not a part of this documentation.

Access to an outside line occurs via additionally available gateway modules in OpenScape Office LX and is described in the following. For OpenScape Office LX, an external gateway is needed to access an outside line. The configuration of the outside line is described in the instructions for the gateway.

### 5.1 Internet Access (MX)

A broadband connection (DSL or connection) is required for access to the Internet. This provides for fast data transmissions over the Internet and enables Internet (or DSL) telephony.

#### Internet Access via a DSL Connection

Conventional telephone lines are used for broadband Internet access via DSL (digital subscriber line). The Internet access can be used at the same time as the normal phone. Fax, analog phone or ISDN are also available during the DSL connection. This makes it possible to implement Internet access that is permanently available as in the case of a dedicated line (flat rate).

For Internet access via DSL, you need a modular jack (analog or ISDN) and an Internet Service Provider (ISP). The ISP provides a splitter and an Internet modem (DSL modem) or an Internet router with a built-in Internet modem. The splitter divides the signal into DSL and telephony parts and forwards the DSL signals to the Internet modem.

The communication system can be connected directly to the Internet modem or to the Internet router with an integrated Internet modem. In the first case, the access data of the ISP must be entered in the communication system; in the second, the Internet router must be made known to the communication system. The access data of the ISP is saved in the Internet router.

To use Internet telephony, you will also need an Internet Telephony Service Provider (ITSP, SIP provider).

### **Internet Access via a Cable Connection**

The broadband connection to the Internet is implemented via the TV cable. In addition to transmitting TV signals, the TV cable connection can be used for accessing the Internet and making calls. This means you do not need a telephone line to surf and for telephony.

For Internet access via cable, you need a cable provider that offers this feature. The cable provider is also your Internet Service Provider (ISP). This cable provider supplies you with a cable port with a back channel and a cable modem that transmits the data over the TV cable network. The cable port and the communication system are connected to the cable modem over Ethernet. Internet data filtration takes place directly in the cable modem.

The communication system can be connected directly to the cable modem or to an Internet router that is connected to the cable modem. In both cases, the cable modem or the Internet router must be made known to the communication system.

To use Internet telephony, you will also need an Internet Telephony Service Provider (ITSP, SIP provider).

### **Configuring Internet Access**

Internet access is configured with OpenScape Office Assistant. You have the following options:

- Internet access via an external Internet router  
You want to operate the communication system at an external Internet router. The communication system and the Internet router are either in the same LAN segment or in different LAN segments. This variant also applies if you want to access the Internet with a cable modem.
- Internet access via an Internet modem  
You want to operate the communication system directly at an Internet modem. Use the WAN port for this.
- Deactivate Internet access (default setting)  
You do not want to use the Internet. Then leave the WAN port disabled.

## **5.1.1 Internet Access via an External Internet Router (MX)**

The **Network Configuration** wizard helps you configure your Internet access via an additional Internet router.

To set up Internet access, you have the following options:

- The communication system and the Internet router are in the same LAN segment. In this case, you must enter the IP address of the Internet router and that of the DNS server and connect the Internet router with the LAN port of the communication system.
- The communication system and the Internet router are to be located in different LAN segments. You will need to configure your WAN port as a LAN port for this. This scenario requires a network specialist and is not covered in this documentation.

## 5.1.2 Internet Access via an Internet Modem (MX)

The **Internet Configuration** wizard helps you configure your Internet access via an Internet modem. An Internet modem is directly connected for this to the WAN port on your communication system. You can use an ISP that was preconfigured in the communication system or a standard ISP type (consult ISP for type).

To set up Internet access, you have the following options:

- Setting up Internet Access via a Preconfigured ISP  
You are using an ISP preconfigured in the communication system. You can then select your preconfigured ISP from a list.
- Setting up Internet Access via the Standard ISP PPPoE  
You are using the standard ISP type **Provider PPPoE**. Obtain the required settings from your ISP.
- Setting up Internet Access via the Standard ISP PPTP  
You are using the standard ISP type **Provider PPTP**. Obtain the required settings from your ISP.

---

**INFO:** You can also use the WAN port to operate OpenScape Office MX as a router between two internal networks. OpenScape Office MX uses the integrated router function to enable communication between two different internal networks. More Information can be found in the Administrator documentation in the topic *Network* under *Configuring the WAN Connection as a LAN Connection*.

---

### Connection Clear-down Depending on the Tariff Model

Depending on the tariff model, you can define whether or not the connection to the ISP should be maintained in the event of inactivity.

- With the flat-rate tariff model, the Internet connection does not have to time out on inactivity. Many ISPs require forced timeout every 24 hours. You can enter the time when the connection should time out.
- With the time-based tariff model, the Internet connection should time out on inactivity. You can specify the inactivity timeout for connection clear-down (for instance, 60 seconds). The connection is automatically reestablished the next time an Internet request is made. If VPN is configured, the connection should not be cleared due to inactivity; the flat rate tariff model should hence be selected here.

---

**INFO:** Network-based programs or services can automatically set up an Internet connection and thereby incur additional connection charges for you if your tariff is time-based.

---

### Bandwidth

Different bandwidths for downloading and uploading are usually provided by the ISP. The bandwidth is specified in Kbps. If Internet telephony is also used, the bandwidth is shared by voice and data transmission. We therefore recommend reserving sufficient bandwidth to guarantee good voice quality during voice transmission. However, this can lead to data transfer bottlenecks (for example, slower downloads) during periods with a high volume of voice transmissions.

You can choose whether bandwidth control for voice connections should be enabled only for uploading for both uploading and downloading. If the download bandwidth is high and the upload bandwidth is low, bandwidth control should be enabled only for uploading to prevent an unnecessarily high amount of download bandwidth from being reserved for voice transmissions.

---

**INFO:** About 128 Kbps of bandwidth is reserved for an Internet call.

---

## 5.1.3 WAN Port (MX)

A wide area network (**Wide Area Network WAN**) is a computer network that, in contrast to a LAN (local area network), encompasses a very large geographical area.

The number of connected nodes is not limited to a specific number. WANs can cover countries or even continents. WANs are used to network different LANs as well as individual nodes. Some WANs belong to specific organizations and are used exclusively by them. Other WANs are set up or enhanced by Internet providers so that they can offer Internet access.

### System-Specific Information

OpenScape Office MX uses the WAN port for Internet access.

## 5.1.4 NAT (MX)

NAT (network address translation) is a procedure for replacing one IP address in a data packet with another. The clients in an internal network use private IP addresses. As private IP addresses are not forwarded in a public network, you can use NAT to map the private IP addresses to a public IP address. This gives internal clients access to the public network while masking the structure of the internal network with its private IP addresses and keeping it separate from the public network (for example, the Internet).

Address translation is performed at the gateway between an internal and a public network. NAT can run on an Internet router, a server or another specialized device. An Internet router can use NAT, for instance, to connect the internal network to the Internet.



The internal network appears on the Internet with only a single public IP address, which is assigned to the Internet router by the Internet Service Provider (ISP). All access attempts made from the internal network are routed via this official IP address with different port numbers. The Internet router replaces the private IP addresses with the official IP address assigned by the ISP. In the case of incoming data packets, the official IP address is replaced by the private IP addresses. The relevant port numbers are important for allocation. Only specially enabled private IP addresses can be reached directly from the Internet.

### **NAT rules**

You can use NAT rules to define if private (local) IP addresses should be reached directly from the Internet. Individual NAT rules can be defined for this or the default NAT rules already set can be used for the services FTP Server, HTTP Server, etc. A total of 20 NAT rules can be defined. In order to use the NAT rules, the local address data of the client PC that will provide these services for the Internet must be entered, and the NAT rule must be activated. Multiple NAT rules can be configured together with the help of a NAT table editor. You can delete NAT rules that are no longer needed.

## **5.1.5 DNS, Domain Name Service (MX)**

The main task of the Domain Name Service (DNS) is to translate "names" such as `www.wikipedia.com` to their associated IP addresses.

The DNS client requests the IP address of a DNS name from the DNS server. Example: for `www.wikipedia.com`, the DNS server returns the IP address `91.198.174.2`.

The DNS is a hierarchical database that manages the Internet name space and is distributed over a collection of servers worldwide. This name space is divided into so-called zones. Separate Internet-independent DNS servers are usually operated for local requirements – for example, within a corporate network.

### **System-Specific Information**

OpenScape Office MX can serve as a DNS client and send requests to an external DNS server, support gateway DNS functionality for other DNS clients and also be used as a DNS server for the administration of DNS zones.

## **5.1.6 Gateway DNS Functionality (MX)**

The communication system offers you the same functions as a DNS server (gateway DNS functionality). DNS servers include data about a particular section of the DNS domain tree structure and process name resolution requests received from DNS clients.

On receiving a request, DNS servers provide the required information, return a reference to some other server that can help resolve the request, or return an acknowledgment to indicate that the information is not available or does not exist.

### **Primary/Secondary DNS Servers**

A request is first forwarded to the primary DNS server. If this request can be satisfied, it returns a response. If not, the request is forwarded to a second DNS Server (if configured).

## **5.1.7 DNS Zones (MX)**

A DNS zone is a contiguous segment of a namespace for which there are one or more authorizing servers. The DNS objects of a domain (e.g., the computer names) are maintained as a set of resource records in a zone file that resides on one or more authorizing name servers.

### **Forward Master Zones**

In forward master zones, domain names of DNS servers are assigned to IP addresses (for example, "google.de" is resolved into its IP address).

If an IP address cannot be resolved in the DNS server of the OpenScape Office MX, this request is sent to a next, higher-level DNS server. This is determined via the Forward Master Zone. Two Forward DNS Servers must be defined in OpenScape Office MX.

### **Reverse Master Zones**

In reverse master zones, IP addresses are resolved into domain names (for example, the IP address here is translated into the name "google.de").

### **Slave Zones**

This zone type is a partial copy of another zone. A slave zone contains only the resource items that are needed to identify the authorizing DNS Server for the master zone.

## **5.1.8 DynDNS (MX)**

DynDNS (Dynamic Domain Name Service) is an Internet service that assigns a fixed DNS name to an IP address that changes dynamically.

### **DNS Name**

With DynDNS, a client who is connected to the Internet with a dynamic IP address can always be addressed with the same name, the DNS name. A DynDNS account with a DynDNS provider (such as [www.dyndns.org](http://www.dyndns.org)) is needed for this. If the communication system is assigned a new IP address (for example, by the Internet Service Provider), this IP address is automatically sent to the DynDNS provider and saved in the DynDNS account. The refresh interval is adjustable. If a DNS name is addressed, a request is sent to the DynDNS provider to translate the name into the IP address currently valid. The entire DNS name (also known as the domain name) is composed of a host name of your choice (myhost, for

instance) and the selected DynDNS provider (dyndns.org, for instance), producing, in this instance, myhost.dyndns.org. More information on this can, for example, be found at the Internet address:

<http://www.dyndns.org/services/dyndns>

DynDNS also lets you set up a virtual private network (VPN) over an Internet Service Provider that supplies dynamic IP addresses. This enables teleworkers, for example, to access the internal network via the Internet. More Information can be found under [VPN \(Virtual Private Network\) \(MX\)](#).

### **Mail Exchanger**

The Mail Exchange entry (MX record) in the Domain Name Service (DNS) specifies the IP address to which e-mails should be sent for the domain name configured (myhost.dyndns.org, for instance). The mail server (Mail Exchanger) must be located at the IP address specified. An e-mail address for this domain name could be as follows: mymail@myhost.dyndns.org.

The Backup MX function buffers e-mails that could not be delivered to the Mail Exchanger specified above (because of temporary unavailability, for instance) and delivers them as soon as Mail Exchanger availability is restored.

## **5.1.9 IP Routing (MX)**

In data technology, routing describes the definition of paths (routes) for data streams.

### **Default Router**

A network address is configured as a default router where clients send their data if the destination address is outside their own network and they are unfamiliar with the path to the destination client. The default router will then redirect the data to the parent network.

### **Static Routes**

Static routes are used to establish the path along which data will travel to a network that cannot be reached via the default router.

### **ARP (Address Resolution Protocol)**

The Address Resolution Protocol (ARP) is a network protocol that facilitates the assignment of network addresses to hardware addresses. Although it is not restricted to Ethernet and IP protocols, it is almost exclusively used in conjunction with IP addressing in Ethernet networks.

Node A wants to communicate with node B in a network. Node A needs the MAC address of node B for this. Node A queries the MAC address by sending an ARP request with the IP address of the node it wants to find (node B) to all nodes in the network. Node B sends the ARP reply and shares its MAC address with node A.

## **Connection to Service Provider (LX/MX)**

### **IP Telephony (Voice over IP, VoIP)**

The prerequisites for communication are therefore satisfied. Node A saves the association of the MAC address to the IP address of Node B in its ARP cache. This speeds up communication connections in the network in future.

## **5.1.10 IP Mapping (MX)**

IP mapping translates public IP addresses into internal IP addresses. The internal clients can therefore be reached at an external IP address.

## **5.2 IP Telephony (Voice over IP, VoIP)**

IP Telephony describes telephony within IP networks. The signals required for the call are transmitted using IP Protocols over IP networks that can be used for data transmission. This type of telephony is also called Voice over IP (VoIP). IP telephony is implemented on the one hand for calls within an internal network (LAN or WAN in coupled corporate networks) and, on the other hand, for calls over the Internet between two IP stations or for calls over the Internet to conventional telephone networks. If the IP telephony occurs over the Internet, this is also referred to as Internet telephony. Both PCs as well as IP telephones suitable for IP telephony may be used as IP stations. To guarantee loss-free transmission and good voice quality, voice signals are compressed using audio codecs and marked using special procedures (Quality of Service) so that voice transmission has priority over data.

### **IP Telephony in the Internal Network (LAN Telephony)**

IP stations can telephone each other over the internal network (LAN, local area network) using the Internet protocol. IP telephony is also possible if two internal networks, for example, two branches in different locations, are connected via a WAN (wide area network). The communication system must support VoIP for this. All of the communication system's telephony features can be used within the internal network with the corresponding protocol.

### **IP Telephony via the Internet (Internet Telephony)**

Internet telephony means that IP stations can communicate directly with other IP stations over the Internet or with stations from the conventional telephone network.

To use Internet telephony, you will need access to an Internet Telephony Service Provider (ITSP).

Calls are set up and cleared down via the Session Initiation Protocol (SIP). The voice data is combined in IP packets and transferred over the Realtime Transport Protocol (RTP). Call stations such as IP phones, PCs, and conventional phones connected via special adapters can set up the connection to the Internet.

### **Connecting to the Internet (to the ITSP)**

The communication system can be connected to the Internet either directly or via an additional Internet router.

- Communication system with direct Internet access
- Communication system with Internet access via existing Internet router:  
The internal network is connected to the Internet over an existing Internet router. NAT is typically used in this environment so that the IP addresses used in the internal network are not visible in the Internet. To be able to receive incoming calls over the Internet, the relevant IP station must be able to determine its IP address used in the Internet and forward this information to the communication partner. To do this, a STUN server operated by the ITSP is required..

### **Call Flow**

A connection between two IP station is set up via the SIP server. The SIP server is no longer needed for the actual telephone call because the call data is sent directly by the IP station. Connections are again set up via the SIP server.

## **5.2.1 ITSP Requirements (LX/MX)**

An Internet Telephony Service Provider (ITSP, SIP Provider) lets you conduct calls over the Internet. To do this, an Internet telephony connection must be applied for from the ITSP, and a user account must be set up for the IP station.

Internet Telephony Service Providers do not always offer the same range of SIP features. It is therefore important that the ITSP is certified for OpenScape Office. A list of certified ITSPs can be found at the following link:

[http://wiki.siemens-enterprise.com/wiki/Collaboration\\_with\\_VoIP\\_Providers](http://wiki.siemens-enterprise.com/wiki/Collaboration_with_VoIP_Providers)

### **Types of Internet Telephony Connections**

- The Internet telephony user connection is a connection with the registration of individual call numbers. With this connection type, a registration and authentication from the ITSP is required for every individual station connection call number.
- The Internet telephony point-to-point connection is a connection with the registration of a call number range. With this connection type, only a single registration and authentication from the ITSP is required for the entire call number range.

### **ITSP user account**

The ITSP user account (SIP User Account) must be applied for from the ITSP. The ITSP provides an SIP Registrar server at which the IP station must first log in (provider-specific) for this purpose.

---

**INFO:** Special numbers and emergency numbers that cannot be supported by the ITSP are routed over fixed network connections.

---

---

**INFO:** In the event of ITSP failure, the connection is guaranteed over fixed network connections via least cost routing (LCR).

---

## **5.2.2 Internet Telephony via a Station Connection (LX/MX)**

An Internet telephony station connection is a connection with the registration of individual call numbers. With this connection type, a registration and authentication from the ITSP is required for every individual station connection call number.

## **5.2.3 Internet Telephony via a Point-to-Point Connection (LX/MX)**

An Internet telephony point-to-point connection is a connection with the registration of a call number range. With this connection type, only a single registration and authentication from the ITSP is required for the entire call number range.

## **5.2.4 STUN (Simple Traversal of UDP through NAT (LX/MX))**

When operating the communication system behind a NAT router, STUN enables determination of the own IP address/port, which is required for Internet telephony via SIP. The functionality is made available on the Internet on STUN servers, whose addresses must be stored in the configuration of the communication system.

The following function can be implemented in the communication system with STUN:

- **Detecting the NAT type**

The communication system determines independently whether STUN must and can be used. No STUN requests occur if no NAT router exists or if a NAT type not supported by STUN is detected. For routers with symmetric NAT, for example, STUN cannot determine any valid public address, so VoIP is possible in this case.

---

**INFO:** Some ITSPs use session border controllers (SBC), which obtain knowledge of where they should send their own RTP data stream from the incoming RTP data stream instead of the SIP signaling. In this case, Internet telephony is also possible with symmetric NAT.

---

- **Monitoring the Public IP address**

The IP address under which the communication system is seen on the Internet is determined cyclically. This is done by sending a request to the STUN server, which indicates in its response with which public IP address it had seen the IP packet. If the IP address changes, STUN notifies the required components of the communication system.

- **Determining the RTP/RTCP Address per Call**

If STUN is active, the public RTP and RTCP ports are determined for each call. To do this, a request is sent to the STUN server via each of the respective ports that will also be later used for the voice packets. In its response the STUN server indicates with which public IP address / port the IP packet arrived. This information is used in the SIP signaling to transmit to the communication partner to which IP address and port it should send its voice packets.

- **Opening the NAT Bindings for Early Payload per Call**

STUN opens the NAT Binding in the NAT router for Early Payload by sending an empty UDP packet. This makes it possible to hear announcements before "Connect" in the case of outgoing calls, for example.

## 5.3 Outside Line (MX)

The outside line connects the communication system to the public network (PSTN) via ISDN or analog connections.

Wizards are available to facilitate the configuration of an ISDN outside line or analog outside line.

### 5.3.1 Trunks (MX)

Trunks connect the communication system with the public network (PSTN). Every trunk is assigned a route through which different properties can be assigned to the trunk.

By default, all trunks are assigned a seizure code and a route. These assignments can be changed by the administrator.

In the case of an ISDN trunk connection, the trunks are also referred to as B-channels.

**Trunk code**

Using the trunk code, the communication system seizes the specific trunk assigned to that trunk code. The trunk code is also used to program a trunk key or to test a trunk.

**MSN Allocation**

An MSN can be assigned directly to an ISDN trunk for external call forwarding in the case of multiple PMP trunks (PMP=point-to-multipoint), for example.

**ISDN Protocol**

The used ISDN protocol is determined by the country initialization. It should only be changed if the PSTN connection explicitly requires some other deviant protocol. Several protocol templates, which can be adapted to individual requirements, are available. The requisite information for this can be obtained from your Service Provider.

**B Channel Seizure Mode**

Individual B channels of an ISDN trunk can be blocked for outgoing and/or incoming traffic.

The following B channel seizure modes are possible:

- outgoing only
- incoming only
- outgoing and incoming (default)

The B channel seizure mode is only evaluated when the communication system must offer a B-channel. The applies in the following situations:

S <sub>2</sub> outgoing:	The communication system must offer a B-channel.
S <sub>2</sub> incoming:	The remote station must offer a B-channel. This B-channel is accepted by the communication system without checking the setting. It is thus of no direct significance.
S <sub>0</sub> outgoing:	Since the communication system does not pre-assign a B-channel (any channel), this setting is of no direct significance.
S <sub>0</sub> incoming:	When the remote station sets up a call without specifying a B-channel, the communication system offers a B-channel, while taking the set B channel seizure mode into account.

**Dialing Method for Analog CO Trunks (MSI)**

The dialing method is automatically detected by the communication system whenever the line is seized. For special cases, the dialing method can also be set directly to Dual Tone Multifrequency (DTMF) or Dial Pulsing (DP).



## 5.3.2 Routes (MX)

Routes enable trunks (B channels) to be grouped. Separate parameters can be configured for each trunk group.

Each trunk can be assigned to exactly one route. By default, all trunks are assigned to route 1.

For each route, a name and a seizure code can be assigned.

---

**INFO:** Seizure codes only work if LCR has not been activated.

---

### B Channel Allocation

The allocation of B channels to different trunk groups is also called the B-channel allocation. Typical use cases include ISDN trunk connections with multiple B-channels such as S<sub>2M</sub> trunk connections, for example.

For outgoing calls, only B-channels that are included in the trunk group can be selected (e.g., trunk group selected via the seizure code, overflow trunk group or trunk group selected using LCR)

Incoming calls are always accepted, regardless of the trunk group. As a rule, the B-channel offered by the peer is seized. If the peer system or the public network does not support B-channel allocation, the correct allocation of the call to the correct trunk group cannot be guaranteed.

### Trunk group key

A subscriber can assign a route to a trunk group key on the telephone. One trunk group key is reserved for outbound calls. Calls placed via trunk group keys are subject to COS toll restriction levels and rules.

When a subscriber presses a trunk group key (or dials a seizure code), the communication system seizes a free trunk that is assigned to the appropriate route. The telephone shows the trunk number in the display. If all trunks of the route are seized, the corresponding LED lights up, even in the case of a successful overflow.

### Overflow route

For each route, the administrator can also define an overflow route. If all the trunks of a route are busy during a seizure attempt, the search for trunks continues among all trunks in the overflow route. If all the trunks in the overflow route are busy as well, no further overflow occurs.

### Type of seizure

For an outgoing route seizure, the administrator can specify the criteria to be used by the communication system when searching for a free trunk in the required direction. This is done by defining the type of seizure as follows:

**Connection to Service Provider (LX/MX)**  
Outside Line (MX)

- cyclic:  
after the last outbound seized trunk - search begins at the next higher trunk number, as of the last outgoing trunk reserved for that direction.  
Consequently, all trunks are used with the same frequency.
- linear  
always the first free trunk - search begins at the lowest trunk number assigned to that direction.

**Entering a PABX Number, Incoming and Outgoing**

To implement the CLI no screening feature, the administrator can define the PABX number for incoming and outgoing calls separately. If no "PABX number outgoing" has been configured, the communication system will always use the data of the "PABX number incoming" setting. In the case of an incoming seizure on an ISDN line, the communication system truncates the PABX number (left-aligned) from the received phone number and interprets remaining portion as the Direct Inward Dialing number. For call number information to the PSTN, the communication system automatically inserts the PABX number as the leading portion of the call number. This does not apply to dialing information (destination address). In Germany, the PABX number must omit the area code and the attendant code.

**Station Number Transmission**

The station number that is sent to the PSTN and to the receiver can be composed as follows:

Type	Station number transmitted to the PSTN
Unknown	only DID number (default setting)
PABX number	PABX number + DID number
Local area code	+ Local area code + PABX number + DID number
Country code	Country code + Local area code + PABX number + DID number
Internal	Only for networked system: number prefixes may not be added for closed numbering plans. Call number prefixes are suppressed here.

In addition, you can specify which call number information is to be transmitted from the dialing station to the destination station.

Type	Station number transmitted to the PSTN
Internal	In this case, only the internal call number is transmitted. If the destination is an external station, either no number is transmitted or only that of the attendant. The internal call number can be displayed when the destination is an internal station.
Direct inward dialing	In this case, only the DID number is transmitted. The internal call number is not provided for display at internal destinations in other nodes. The call number information is sufficient for external destinations.
Internal / DID	This setting is useful for networking purposes. Both the internal call number and the DID call number are transmitted to the destination station. If an internal station is called within the network, the internal call number of the caller can be displayed for this station. If the internal destination station has activated call forwarding to an external destination, for example, a DID number can also be transmitted in this case.

In addition, the communication system can extend the call number for outgoing and incoming connections by adding the seizure code (direction prefix).

#### **Second CO Code**

A second trunk code is defined only if the communication system is a subsystem of another communication system or is networked with several other communication systems. In this case, the second trunk code is the seizure code for the main system. With this code, the subsystem can access the CO trunks of the main system.

### **5.3.3 Prioritization for Exchange Line Seizure (LX/MX)**

The prioritization for exchange line seizure defines in what order different network providers (ISDN/analog or ITSPs) are selected.

The exchange line seizure normally occurs by dialing the prefix "0". Within this code, different providers are prioritized (depending on what is preset). For example, an outbound call may be first routed via an ITSP and, if the exchange line seizure fails, be then sent via ISDN.

### **5.3.4 Dial Tone Monitoring**

When setting up a connection over an analog trunk line, the dialed digits can be sent to the Central Office only when a dial tone (audible signal) has been detected. Since the time until the arrival of the dial tone varies depending on the network provider and network state, the arrival of the dial tone can be monitored.

### **Delay Period for Dial Tone Monitoring**

The monitoring of the dial tone can be done immediately or only after a pause. In some cases, additional tones may need to be played back to the subscriber after the line is seized, for example, to inform him or her that call forwarding has been enabled at the Central office. For such cases, a delay period for the dial tone monitoring (Analog trunk seizure, 1-9 seconds) can be programmed. The dialed digits will then be sent to the CO only after this pause.

---

**INFO:** Notes for Brazil:

If the DTMF dialing method is used from analog phone devices in conjunction with analog trunks (TLAx and TML8W) and pulse dialing after the dial tone monitoring, problems may arise with toll restriction when the country code is set to Brazil. In this case, the DTMF signals from the analog devices go directly to the analog trunk lines. All DTMF signals that were dialed before receiving the dial tone are lost. Consequently, for such cases, least cost routing (LCR) must be enabled for the dialing method and toll restriction to operate properly at the device.

---

### **Analysis of the Second Dial Tone**

The communication system can recognize an additional dial tone (2nd dial tone). This is relevant for public network providers who transmit at a second dial tone for international calls, e.g., for Belgium after 00 and for France after 16 or 19. For Germany, this feature is not relevant.

## 6 Subscribers/Stations

A subscriber or station is a communication partner connected to the communication system. In general, every station (apart from virtual stations) is assigned a terminal. A terminal is, for example, a telephone, a PC or fax device. The subscribers can also be users of the OpenScape Office clients (e.g., users of myPortal for Outlook). A default dial plan facilitates the administration.

The following types of stations exist:

- IP stations (also known as IP clients)
- ISDN stations
- Analog stations
- Mobile stations (Mobility Clients)
- Virtual stations for call forwarding

The data of subscribers (name, station number, DID number, e-mail address, etc.) can be imported (see [Individual Dial Plan for OpenScape Office LX/MX](#)) and exported (see [Exporting Subscriber Data](#)) as a CSV file.

### 6.1 Dial Plan

A dial plan, which is also called a numbering plan, is a list of all phone numbers and codes available in the communication system. It includes, among other things, the internal call numbers, DID numbers and group call numbers. Most of the call numbers are preassigned default values, but these can be changed as required.

The dial plan with the currently configured phone numbers and codes can be displayed via the OpenScape Office Assistant Service Center. If names have been assigned to the call numbers, these are shown.

All types of call numbers and codes are summarized in the following table, using OpenScape Office MX as an example.

A sample dial plan of OpenScape Office LX can be found under *OpenScape Office V3, Administrator documentation , Installing OpenScape Office LX*.

**Subscribers/Stations**  
Dial Plan

Type of call numbers	Preset value	Action
Station numbers for IP stations (max. 297 + 3)	100 – 249 (+ 7070, 7080 and 7090)	deletable
Phone numbers for analog stations (25 preset / max. 96)	250 – 274	deletable
Phone Numbers for ISDN stations (25 preset / max. 48)	275 – 299	deletable
Station numbers for virtual stations (max. 70)	1025 – 1094	deletable
DID numbers of the stations	not preset	deletable
Internal group station numbers & direct inward dialing	not preset	deletable
Trunk numbers (max. 250)	not preset	deletable
Announcement call numbers (max. 16)	#801 - #816	only editable
Station numbers for online users	7070	only editable
Call number for remote access	7080	only editable
Call number for automatic licensing	7090	only editable
Call number for voicemail	71	only editable
Conference phone numbers (5 preset / max. 20)	7400 – 7404, 7430	only editable
Call number for parking	7405	only editable
AutoAttendant Phone Numbers (max. 20)	7410 – 7429	only editable
Seizure codes (6 preset / max. 64)		
Seizure code 1 (external code)	0 = World / 9 = USA	only editable
Seizure code 2-6	80 – 84	only editable
Access Code for Music on Hold	#817	only editable
Station number for Attendant Console	9 = World / 0 = USA	only editable
Substitution for "#" (for service codes)	72	deletable
Substitution for "#" (for service codes)	73	deletable
Service Codes	Service Codes Table (see <a href="#">Codes for Activating and Deactivating Features (LX/MX)</a> )	not editable

---

**INFO:** When setting up call numbers or codes, error messages may be produced if the desired number is already being used. The dial plan can be used to check which call numbers can still be assigned.

---



---

**INFO:** If an internetwork with multiple communication systems is involved, it must be noted that only a closed numbering system for the station numbers may be used (see [Dial Plan in the Network](#)).

---

## 6.1.1 Default Dial Plan for OpenScape Office LX/MX

Most of the call numbers in the default dial plan for OpenScape Office LX/MX are predefined with default values.

## 6.1.2 Individual Dial Plan for OpenScape Office LX/MX

OpenScape Office LX/MX allows you to set up an individual dial plan by editing the predefined call numbers.

The following actions are useful for this purpose:

- Delete defaults: apart from some exceptions (special default numbers), default call numbers can be deleted. These call numbers are identified as "deletable" in the "Action" column.
- Edit special defaults: these call numbers must not be deleted. However, their values may be edited. These call numbers are identified as "only editable" in the "Action" column.
- Import call numbers and station data: station data can be imported via a CSV file. The call numbers and DID numbers of the stations are imported as well.

### Importing Station Data via a CSV File

An individual dial plan can be imported into OpenScape Office. The data must be available as a CSV file.

A sample CSV file with the appropriate explanations can be found in the OpenScape Office Assistant Administration Program under **Service Center > Download Center > CSV Templates**. You can also use the CSV file stored there as a template for your data.

Structure of a CSV file:

- Column A contains the call number (possible values: 0-9, \*, #)
- Column B contains the DID number (possible values: 0-9, \*, #)
- Column C contains the name (in the format `First Name Last Name` or `Last Name, First Name`)  
The name of a subscriber can consist of up to 16 characters, but must not include any diacritical characters such as umlauts or special characters.
- Column D contains the subscriber type (e.g., 1=System Client, 2=SIP User, 3=SIP Fax, 4=RAS User, 5=Analog, 6=Analog Fax, ...)
- Column E contains the license type (<no entry> or 0=No Licence, 1=Comfort User, 2=Comfort Plus User)
- Column F contains the e-mail address  
Users of the UC Suite are automatically sent an e-mail with a link to the installation file(s) if their respective e-mail addresses were imported via the CSV file.
- Column G contains the mobile number (possible values: 0-9, \*, #)
- Column H contains the private number (possible values: 0-9, \*, #)

## Subscribers/Stations

### IP Stations and LAN Telephony (LX/MX)

- Column I contains the node ID (possible values: 0–999)  
This column must be assigned a value; otherwise, no import will occur. If the system is not networked, 0 must be entered here.
- Column J contains the IP address of the second gateway

---

**IMPORTANT:**

CSV files must be available in ANSI/ASCII format.

CSV files of older OpenScape Office versions are not supported.

---

## 6.2 IP Stations and LAN Telephony (LX/MX)

The term LAN telephony refers to making and receiving calls in the internal network (LAN). To enable this, the communication system and IP stations must be integrated in the LAN infrastructure during the initial startup.

The communication partners (IP stations) can be PCs as well as any phones suitable for LAN telephony (e.g., system telephones or even SIP phones).

In order to enable the system telephones to log into the communication system automatically during the initial startup and obtain the latest software updates, a DHCP server is required in the internal network.

To guarantee loss-free transmission and good voice quality, voice signals are compressed using audio codecs and marked using special procedures (Quality of Service) so that voice transmission has priority over data.

### 6.2.1 IP Stations

An IP station uses a LAN line to transmit digital signals. The communication system connects the IP station via the LAN ports. An IP station is generally a LAN or WLAN phone.

The following types of IP stations exist:

- **System Client:** A system client is an IP station that can use all the features of the communication system for communication in the internal network. This can be a system telephone such as an OpenStage 60 HFA, for instance, or a PC with CTI software such as OpenScape Personal Edition.
- **SIP client:** A SIP client is an IP station that uses the SIP protocol. It can access only limited functionality of the communication system via the SIP protocol. A SIP client is a SIP phone such as the OpenStage 15 S, for example.
- **RAS User:** A RAS user (Remote Access Service user) is granted Internet access to the IP network via the ISDN connection. This allows the communication system to be maintained remotely.



Three IP stations are reserved for the Online User (call number 7070), for remote access via ISDN (call number 7080) and licensing via ISDN (call number 7090). The remaining IP stations are assigned internal call numbers, e.g., 100 through 297, depending on the communication system. If the three reserved stations are not required, these stations can be converted to IP stations in Expert mode.

For each connected IP station, a license is required.

### **Configuring IP Stations**

The following configurations can be performed for an IP station:

- Configuration of standard parameters with the **IP Telephones** wizard (see *OpenScape Office V3, Administrator documentation , Subscribers/Stations*).
- Configuration of all parameters (standard and advanced parameters in Expert mode (see *Configuring Stations in Expert Mode (LX/MX)*).

## **6.2.2 LAN Telephony Requirements (LX/MX)**

To ensure the quality of the voice transmission in LAN telephony, the IP networks being used and the communication system must meet certain requirements. The voice quality and voice communication reliability always depend on the network technology in use.

### **Requirements**

- LAN with 100 Mbps or higher
- Every component in the IP network must be connected to a separate port on a switch or to a router; a hub should not be used.
- Not more than 50 msec delay in one direction (One Way Delay); not more than 150 msec total delay
- Max. 3% packet loss; if a fax/modem via G.711 is used, the packet loss must not exceed 0.05%.
- Not more than 20 msec jitter
- Support for Quality of Service (QoS): IEEE 802.p, DiffServ (RFC 2474) or ToS (RFC 791)
- Maximum 40% network load

## **6.2.3 IP Addresses (LX/MX)**

In order to integrate the communication system in the LAN infrastructure, the IP address and internal IP address range of the communication system must be adapted to the IP address scheme of the internal network.

The IP address and subnet mask of the communication system are defined during the initial startup. The IP address and subnet mask can also be changed later if required.

## Subscribers/Stations

### IP Stations and LAN Telephony (LX/MX)

By default, the communication system uses the IP address range 192.168.2.xxx for the internal communication of its modules. If this IP address range is already being used by other clients in the internal network, the communication system automatically switches to another predefined IP address range. Overall, the communication system can switch the IP address range automatically up to four times.

The internal IP address range can also be set to a desired IP address range. The internal subnet mask is 255.255.255.0 and cannot be changed.

To activate the changes, a restart of the communication system is required.

The changes to the IP address and internal IP address range remain in effect with a software update, but will be reset to the default values in the event of a reload. These changes cannot be stored in a backup set.

## 6.2.4 DHCP, Dynamic Host Configuration Protocol (LX/MX)

DHCP (Dynamic Host Configuration Protocol) automatically assigns IP configuration parameters (such as the IP address and default gateway, for example) to the IP stations of a network (e.g., LAN or Internet) with the help of a DHCP server.

DHCP must also be enabled at the IP stations themselves (e.g., system telephones, PCs, etc.) in order to receive the IP configuration parameters. This enables system telephones to be supplied with data for an automatic login and to be updated automatically with new software updates.

### DHCP Server

OpenScope Office MX is configured as a DHCP server by default. For OpenScope Office LX, the Linux server can be configured as a DHCP server. Alternatively, any existing DHCP server in the network could also be used (e.g., DHCP server of the Internet router). In this case, the DHCP server of the communication system must be disabled, and some IP configuration parameters (vendor-specific data) must be set in the external DHCP server so that system telephones can log in automatically and be supplied with new software updates. The decision as to whether the DHCP server of the communication system or an external DHCP server (e.g., the DHCP server of the Internet router) is to be used should be made during the initial startup. The DHCP server of the communication system can also be enabled or disabled later. In addition, the required IP configuration parameters can be configured.

### DHCP Address Pool (IP Address Ranges)

Whenever an IP station logs in at the DHCP server, it receives, among other things, a dynamically assigned IP address. The administrator can optionally define an IP address range from which the DHCP server can assign IP addresses to the IP stations. In this case, for example, not all IP addresses from the range 192.168.1.xx are to be assigned, but only those from 192.168.1.50 to 192.168.1.254, since the lower IP addresses up to 192.168.1.49 are to be reserved for IP stations with static IP addresses.

### **DHCP Relay Agent**

OpenScape Office MX can also be configured as a DHCP relay agent. The DHCP relay agent is used to forward DHCP requests in a remote network to the actual DHCP server.

## **6.2.5 IP Protocols (LX/MX)**

IP protocols permit telephony in IP networks by transferring the signals needed for the call.

Telephone calls consist of three stages: connection setup, voice transmission, and connection teardown. The voice signals are combined into individual IP packets and transmitted via a protocol separate from connection setup and teardown (call signaling).

### **IP protocols for Call Signaling in IP Telephony**

The IP protocols for call signaling are based on the following IP protocol:

- **TCP (Transmission Control Protocol)**  
TCP is a reliable, connection-oriented protocol for the transmission of IP packets. Before transfer starts, a virtual channel is set up between the two terminal points. Data can be transmitted in both directions on this channel. TCP is mainly used in the WorldWideWeb and in e-mail and peer-to-peer networks. It is also used for call signaling in IP telephony because it can detect and automatically rectify data losses during transmission.

The following IP protocols are used for call signaling:

- **SIP (Session Initiation Protocol)**  
SIP is usually used in Internet telephony but is not restricted to it. It can also be used for telephony in the internal network, for example. However, SIP does not support all telephony features associated with a communication system.
- **Vendor-specific communication system protocol**  
OpenScape Office MX uses CorNet-IP (CorNet Internet Protocol) for IP telephony within the internal network. CorNet-IP, which was developed on the basis of H.323, supports all telephone features in (HiPath ComScendo functional scope).

The protocol used depends on the IP station used. The communication system's own IP phones (system clients) support CorNet-IP and thus provide all the telephony features of OpenScape Office MX, whereas system phones can only offer a restricted functional scope.

The SIP protocol is more widely used than H.323 in Internet telephony. The most important Internet Telephony Service Providers (ITSP) use SIP exclusively.

### **IP Protocols for Voice Transmission in IP telephony**

The IP protocol for transmitting IP voice packets is based on the following IP protocol:

## Subscribers/Stations

### IP Stations and LAN Telephony (LX/MX)

- UDP (User Datagram Protocol)  
UDP is a reliable, connectionless protocol for the transmission of IP packets. In contrast to TCP/peer scenarios, a virtual channel is not set up before transfer starts so that the PCs can start transferring data without delay. In UDP, the port number of the service that should receive the data is included when addressing voice packets. It is mainly used in the DNS sector and for voice transmission in IP telephony. However, since a connectionless protocol does not check if the peer actually received the data, this option can result in voice transfer losses.

The following IP protocol is used for the transmission of IP voice packets:

- RTP (Realtime Transport Protocol)  
RTP is a packet-based protocol for the transmission of real-time sensitive data streams such as video and audio data. It is used, for example, for voice transmission in IP telephony.

#### Parameter Settings for H.323

The parameters for the H.323 Standard are appropriately predefined for the operation of OpenScope Office MX and should not be modified.

#### Parameter Settings for SIP

Most of the parameters for the SIP Protocol are appropriately predefined for the operation of OpenScope Office MX and should not be modified. However, the value that defines the maximum number of DSL calls that may be conducted concurrently, even if more bandwidth is available, can be set as required.

## 6.2.6 Audio Codecs (LX/MX)

An audio codec ("codec" is created by combining the terms coder and decoder) is a program that encodes and decodes voice in digital data packets (IP packets). The encoding operation compresses data; the extent to which this data is compressed depends heavily on the codec used. The bandwidth requirement for transferring an IP packet is lower if the packet is compressed. The decoding of data packets can, however, have a negative impact on voice quality and the playback continuity.

The recipient and sender must use the same codec to ensure that the data can be correctly decoded back into voice after transport.

#### Supported Audio Codecs

The following audio codecs are supported:

- G.729, G.729A, G.729B, G.729AB: voice encoding with 8 Kbps - good voice quality.
- G.711 (A-law and  $\mu$ -law): voice encoding with 56 or 64 Kbps - very high voice quality. G.711 is used in fixed networks (ISDN).

The audio codecs can be assigned priorities between 1 (high) and 7 (low). OpenScope Office MX automatically tries to use the audio codec with the highest priority available for every connection. Using an audio codec with low voice

compression (good voice quality) increases network load. In the case of intensive IP telephony, this can lead to diminished voice quality in a network already overloaded by data transfers.

OpenScape Office MX can enable voice activity detection (VAD) for certain codecs. This can reduce network load during long voice pauses.

You can specify a frame size (IP packet size) of 10 to 90 msec for every codec. This specifies the sampling rate at which the audio codec splits the voice signal into IP packets. While a higher value (90 msec, for instance) results in a better relationship between payload and the IP packet overhead, it also increases the transfer delay.

## 6.2.7 RTP Payload for Telephony Tones According to RFC2833 (LX/MX)

The RTP payload for telephony tones according to RFC2833 transmits tones for signaling in RTP packets.

As an administrator, you can enable or disable the function for the following types of tones:

- DTMF
- Fax

## 6.2.8 Quality of Service (LX/MX)

Quality of Service (QoS) encompasses various procedures for guaranteeing the highest possible quality and integrity during the transmission of data packets (IP packets). For good voice quality during voice transmission, QoS is used in the IP network to give IP voice packets priority over IP data packets from other applications.

The IP packets are assigned a special marker (code point) for prioritization. The marker is set in the IP-packet control information. Categorization in different classes is performed based on priority information. If the components available in the IP network (communication system, SIP stations, and Internet routers, for instance) support QoS, you can assign different bandwidth to these classes and thus transport the IP voice packets first.

### AF/EF Code Points

For DiffServ-based prioritization, two different code points are defined so that IP-packet transmission can be split into different classes.

- Expedited Forwarded (EF) Code point: guarantees constant bandwidth. The bandwidth is always the same for IP packets marked with this code point.

## Subscribers/Stations

### IP Stations and LAN Telephony (LX/MX)

- Assured Forwarding (AF) Code point: guarantees minimum bandwidth. IP packets that are marked with this code point have a lower priority than EF and must share the bandwidth not used by EF. Once the set value is reached, all IP packets that exceed this bandwidth are rejected.  
The four classes AF1x (highest priority) through AF4x (lowest priority) are reserved for AF; x stands for "dropping level". A "dropping Level" can be defined for every class and specifies how long IP packets can be buffered if the system is unable to forward them fast enough.
  - 1 (low): IP packets are buffered for a long time.
  - 2 (medium), IP packets are buffered for a medium length of time.
  - 3 (high): IP packets are only buffered for a short length of time and then discarded.

You can set the code point used for marking the IP packets to be transmitted for the following transmission types.

- Signaling Data: for the transmission of signaling data for connection startup and clear-down in IP telephony
- Voice Payload: for voice transmission in IP telephony. Code point EF is the recommended setting here.
- Fax-/Modem-Payload: for fax/modem data transmission in IP networking, for example
- Network Control: for transmitting SNMP traps, for example

The AF/EF code points can be displayed in the form of hexadecimal values.

#### Priority classes

The priority classes for transmission types can be set in both of the following forms:

- Layer 3 Prioritization - EF/AF code points:  
Application in the WAN, e.g., preferred transmission of IP packets via a router. The following values can be set in addition to the EF/AF code points:
  - Best Effort: Best Effort can be used to mark packets that do not require any prioritization, e.g., for the administration.
  - CS7: Class Selector 7 can be used to mark important network services such as SNMP packets, for instance.
- Layer 2 Prioritization - Layer 2 QoS values from 0 To 7:  
Application in the VLAN, e.g., preferred transmission of IP packets between switches.

## 6.2.9 CorNet-IP Security (LX/MX)

With CorNet-IP Security, sent messages are checked for integrity.

If CorNet-IP Security is to be activated in the IP network, the following settings must match for all the components involved. Otherwise, communication between the IP stations cannot occur.

- H.323/TS - Security  
Two security modes are available for CorNet-IP Security: Reduced Security and Full Security.
  - Reduced security: The IP stations send a realtime stamp (called a crypto token), and the gatekeeper checks this realtime stamp. However, the gatekeeper does not send any such token of its own.
  - Full Security: Both sides send and verify tokens (realtime stamps).
- Global Gatekeeper ID  
The global gatekeeper identity is specified here. If multiple gatekeepers are available in a network, all gatekeepers must use the same gatekeeper ID.
- Password for Trunking  
All systems that communicate with one another in the network must use the same password.
- Security time window  
This value defines the time for monitoring the lifetime of IP packets. This means that a check is performed in the gateway to ensure that the incoming IP packets are not older than the current time plus the specified time. The size of the Security time depends on the dynamic runtimes in the IP network. If the selected time is too small, and long runtimes occur, disruptions may be noted in the VoIP traffic. A value of 90 seconds should work without problems in most cases.

### **Gatekeeper**

OpenScape Office MX has the integrated functionality of a gatekeeper, i.e., OpenScape Office MX functions as a gatekeeper. Signals for setting up and controlling calls are transmitted via the gatekeeper. In addition, the gatekeeper also translates IP addresses into E.164 addresses (phone numbers).

The predefined ID **H323-ID** for the internal gatekeeper is significant for the operation of OpenScape Office MX and should not be changed.

## **6.2.10 Key Programming (LX/MX)**

Every system phone comes with a certain number of function keys. A number of these function keys are programmed by default with functions. You can modify this default setting and program the remaining function keys that were not preprogrammed.

System phones with display allow you to program certain function keys directly at the phone.

Users of the applications **myPortal**, **myPortal for Outlook** and **myAttendant** can also program the keys on their phone via these applications (see the respective User Guide of the application).

A system phone is always assigned to an IP station. The system phone's key layout can be preconfigured for an IP station, even if a system phone is not yet connected.

### **Programming Function Keys on Different Levels**

The function keys of the OpenStage phones can be programmed twice, that is, on the first and second levels. You can program all available functions on the first level. You can program external phone numbers on the second level. The Shift key must be programmed on the system phone before you can use the second level. The function key LEDs are always assigned to the first level.

## **6.3 ISDN Stations and Analog Stations**

ISDN stations and analog stations cannot be integrated in the internal network via the LAN ports. With hardware-based communication systems, they are connected directly to additionally required gateway modules or boards. With software-based communication systems, these stations are connected to additionally required gateways or adapters.

### **6.3.1 ISDN Stations (LX/MX)**

An ISDN station uses the  $S_0$  bus for transmitting digital signals and is therefore often referred to an  $S_0$  station. The ISDN station is connected to the communication system via the  $S_0$  interfaces.

The following ISDN stations can be connected:

- ISDN phone
- Fax Group 4
- ISDN modem
- PC with ISDN card

A maximum of 48 ISDN stations can be set up in OpenScape Office MX. By default, the first 25 ISDN stations are assigned the station numbers from 275 to 299.

The following types of ISDN stations can be defined:

- Default: for ISDN phone, Fax Group 4, ISDN modem or PC with ISDN card
- Fax: prerequisites for setting up the "Info from Fax/Answering Machine" key. If a PC with an ISDN card and Fax software is attached to the  $S_0$  bus and assigned the type "Fax", for example, then an "Info from Fax/Answering Machine" key could be set up on every device. When this key lights up, this indicates that a fax has been received.
- Answering machine: prerequisites for picking up a call when the answering machine has already accepted it. If a Gigaset ISDN phone with an answering machine is connected and assigned the type "Answering Machine", for example, a call that has already been accepted by the answering machine can be picked up at any terminal. To do this, the terminal must be programmed with the internal call number of the Gigaset.



### Connecting ISDN Stations to the S<sub>0</sub> Port

To be able to connect an ISDN station to the communication system, you must configure at least one of the S<sub>0</sub> ports that are used for the ISDN subscriber line or the ISDN point-to-point connection as an internal S<sub>0</sub> bus (S<sub>0</sub> EURO bus).

---

**INFO:** If there is more than one ISDN station connected to an S<sub>0</sub> port (up to 8 ISDN stations are possible) in an ISDN point-to-multipoint connection, each individual ISDN station must be assigned to a unique MSN. This assignment must be made in the configuration menu of the ISDN station.

---

### Configuring ISDN stations

The following configurations can be performed for an ISDN station:

- Configuration of standard parameters with the **ISDN Devices** wizard (see *OpenScape Office V3, Administrator documentation , Subscribers/Stations*).
- Configuration of all parameters (standard and advanced parameters via Expert mode (see *Configuring Stations in Expert Mode (LX/MX)*)).

### Allowing only Configured Numbers for MSNs

The administrator can specify that further MSNs at an S<sub>0</sub> bus may only be configured for call numbers that already exist there. This prevents subscribers from adding an MSN without authorization through an outgoing seizure of the S<sub>0</sub> bus with a further MSN. Without this restriction, the communication system would normally assign a free internal call number to the S<sub>0</sub> bus for that MSN.

### Terminal Portability

The communication system supports Terminal Portability (TP), that is, it lets you park a call on the S<sub>0</sub> bus, unplug the terminal, and plug it back in at a new location to resume the call. The parked station receives a message indicating that the user is porting. Three minutes are available for the entire operation.

The feature is not supported for services such as telefax, teletex or data transfer.

## 6.3.2 Analog Stations (LX/MX)

An analog station uses a two-core analog cable to transmit analog signals. The communication system connects the analog station via the analog ports.

Typical analog stations include the following:

- Standard (analog telephone)
- Fax (Group 3)
- Answering Machine
- Modem, 9600 bps or higher
- Loudspeaker

A maximum of 72 analog stations can be set up in OpenScape Office MX. By default, the first 25 analog stations are assigned the station numbers from 250 to 274. With OpenScape Office LX, analog stations can be added via adapters or gateways.

Analog modems with a fixed speed of 56 kbps or higher are not supported, since speeds of 56 kbps or higher cannot be processed.

For multibox systems, analog modems must be connected to the central box, where the external lines are also connected. In addition, the station type **Modem** must be assigned to the associated analog port (see *OpenScape Office V3, Administrator documentation , Subscribers/Stations*).

DTMF must be enabled for analog stations.

### **Configuring Analog Stations**

The following configurations can be performed for an analog station:

- Configuration of standard parameters with the **Analog Devices** wizard (see *OpenScape Office V3, Administrator documentation , Subscribers/Stations*).
- Configuration of all parameters (standard and advanced parameters via Expert mode (see *Configuring Stations in Expert Mode (LX/MX)*)).

## **6.4 Users of the UC Suite**

Users of the advanced unified communications solution UC Suite are subscribers that use the UC Suite communication clients, such as **myPortal for Desktop** or **myPortal for Outlook**, for example. The users of the UC Suite can be IP stations and analog stations, for example.

All users of the UC Suite are listed in the user directory. For proper operation, additional user data must be configured in the user directory (see *Configuring Users of the UC Suite*).

## **6.5 Virtual Stations**

Virtual stations behave like real stations, but have no physical telephones assigned to them.

Virtual stations are only set up for special functions:

- In the case of Mobility Entry, virtual stations are used for the integration of mobile phones.
- During call forwarding, virtual stations such as real stations are configured so that they can be used, for example, for signaling calls.

## 6.5.1 Virtual Stations for Mobility Entry

Virtual stations for Mobility Entry are mobile stations used for integrating mobile phones (GSM phones) in the communication system. Mobile stations are treated like internal stations, so the features of the communication system can be used from mobile phones.

For an overview of the possible system features and the configuration of mobile subscribers, see [Mobility](#).

## 6.5.2 Virtual stations for call forwarding

Virtual stations are needed for call forwarding. These stations must be configured like real stations so that they can be used for the signaling of calls, for example.

A maximum of 70 virtual stations can be set up.

### Configuring Virtual Stations for Call Forwarding

The parameters associated with a virtual station are configured in Expert mode (see [Configuring Stations in Expert Mode \(LX/MX\)](#)).

## 6.6 Station and User Profiles

The values and properties of subscribers are stored in profiles. One or more subscribers (members) can be assigned to a profile. The same values and properties then apply to all members of that profile.

A distinction is made between two profiles:

- **Station Profiles**  
Station profiles are assigned to the IP stations. Up to 10 station profiles can be created. The station profiles can be exported or imported individually or collectively. The files are of type `xml`.
- **User Profiles**  
User profiles are assigned to the users of OpenScape Office clients.

Every subscriber can be a member of exactly one profile. If the values and properties of a station that is a member of a profile are changed directly, i.e., not through the profile, the station is deleted from the profile.

## 6.7 Configuring Stations

You can define specific values (for example, phone number, name, and DID number) and properties (for example, type of call signaling) for the station.

Station configuration is split into standard configuration and advanced configuration. The default settings for IP stations, ISDN stations and analog stations are configured via wizards (possible with an administrator ID). The advanced settings are configured using Expert mode (only possible with a service technician ID). Virtual stations and mobile stations are configured entirely in Expert mode (both the standard and advanced settings). The default settings can be conveniently edited in a list for all stations of a station type (e.g., IP stations or analog stations).

The *Customer administrator* account cannot be used to configure stations, but can be used to define the names of stations.

A dial plan should be available for the stations connected to the communication system.

Station numbers, names and DID numbers of subscribers can be retrieved via the dial plan in the Service Center.

### **Classes of Service**

IP stations, ISDN stations and analog stations can be assigned classes of service. The following classes of service are possible:

- **Internal:** the subscriber may only make internal calls.
- **Incoming:** the subscriber can receive external calls but is not authorized to make external calls (= outward-restricted trunk access).
- **Blocked Phone Numbers:** the subscribers is not authorized to dial blocked phone numbers. Blocked phone numbers can be defined with the *Class of Service* wizard.
- **Allowed Numbers:** the subscriber is authorized to dial only Allowed numbers. Blocked phone numbers can be defined with the *Class of Service* wizard.
- **International:** the subscriber may make both internal and external calls (= unrestricted).
- **Emergency calls:** the subscriber may only dial emergency numbers. Emergency numbers can be defined with the *Class of Service* wizard.

Speed-dial destinations can always be used, regardless of the assigned class of service.

## **6.7.1 Configuring Stations Using Wizards (LX/MX)**

You can use wizards to configure the standard settings of IP stations, ISDN stations and analog stations.

### **Default Settings**

The default settings should be verified for every station and adapted if required.

- **Station Number, Name, DID Number**

Every station is assigned a station number by default (such as 101). The station can be reached internally under this call number. In system phones, this phone number appears both on the actual display and the communication partner's display. If a station number other than the actual station number is to be displayed at the external station called, this number can be defined here. You can also assign a DID number to each station. The station can be accessed directly from an external location with the DID number. The station can be reached internally via the call number 101, for example, and externally via the DID number 3654321 (MSN in a point-to-multipoint connection) or <PABX number>-101 (in a point-to-point connection). In the case of a point-to-point connection, you can configure whether the internal phone number should be automatically entered as a DID number during initial startup. The DID number may also differ from the phone number. If you are using Internet telephony, you can also define a DID number that can be used to reach the station via Internet telephony. This phone number is made available by the Internet Telephony Service Provider.

You can also assign a name to each station. This name appears on the communication partner's display (system phones only).

If a dial plan exists, the phone numbers, DID numbers, and names of the subscribers should be adjusted based on the dial plan.

- **Type**

The station type can be selected for every station. The station type of an IP client could be **system client** or **SIP client**, for example.

- **License type** (IP phones only)

A system phone can be assigned the functional scope of a Comfort User or Comfort Plus User. Appropriate licenses are needed for this.

---

**INFO:** For information on the functional scope of a Comfort User or Comfort Plus User, see [Licenses](#).

---

- **Classes of Service**

Different classes of service may be assigned to a station. The classes of service **Internal**, **Incoming** and **International** can be used to define whether the subscriber can accept and conduct external calls. Similarly, the classes of service **Blocked Phone Numbers**, **Allowed Numbers** and **Emergency Numbers** can be used to define Allowed and Denied lists to control which phone numbers may or may not be dialed by subscribers (see [Classes of Service, Toll Restriction \(LX/MX\)](#)).

- **Call pickup group**

Every station can be assigned to a call pickup group.

- **Language, call signaling**  
The language used for the menu controls of the attached system telephones can be set.  
The ring tone for an internal or external call can be selected.

## 6.7.2 Configuring Stations in Expert Mode (LX/MX)

You can configure all settings for all types of stations in Expert mode. The default settings should be verified for every station and adapted if required. The advanced settings can be left unaltered for default operation and only have to be changed if required.

### Configuring Parameters (Default Settings)

With three exceptions, the station parameters correspond to the default settings as they can be configured via the wizards. Explanations for the default settings can be found under the topic *Configuring Stations using Wizards*.

The following settings can still be configured:

- **LCR Class of Service**  
You can use the LCR class of service to permit or deny subscribers access to certain outdial rules/routes. Every subscriber is assigned a class of service (COS), 15 being the highest and 1 the lowest class of service.
- **Hotline**  
You can activate the Hotline function for every station. You can also define whether the connection to the hotline destination should be established as soon as you lift the handset (hotline) or after a short delay (off-hook alarm after timeout).
- **Signaling & Payload Encryption (SPE)**  
Phone calls are encrypted with SPE. This requires SPE to be enabled at the phones involved. SPE can be enabled or disabled per phone. optiPoint 410/420 phones do not support SPE.

### Activating or Deactivating Features (Advanced Settings)

Different features can be activated or deactivated for each station. These features are listed as station flags. The explanations of these features can be found in the Administrator documentation by searching for the name of the feature.

### Configuring IP Parameters (Advanced Settings)

Special IP parameters can only be configured for system clients and SIP clients.

The following IP parameters can be configured:

- **Status Display** (for system clients only)  
You can activate status transfer to system phones. If a system phone fails, for example, it is flagged as inactive after four minutes.

---

**INFO:** If a system phone is configured as a teleworker, status transmission should be inactive. This reduces the number of messages between the communication system and the system phone.

---

- **Authentication at the communication system**  
If you want the IP client to be able to identify himself/herself at the communication system with a password, authentication must be activated and a password set. This is an advantage especially for clients that are not connected to the internal LAN, but that dial in from outside. You can also set restrictions for SIP clients, specifying that login is only permitted by an SIP client with a specific IP address.
- **Mobile System Client** (for system clients only)  
Normally, the phone number is permanently assigned to the IP telephone of a system clients (type: "non mobile"). A system client may not be permanently assigned to an IP station ("mobile" type). A subscriber can log into any other IP phone using the login procedure (\*9419) and the phone number of the mobile system client. The type "non mobile and blocked" must not be set, however, at this IP telephone.

---

**INFO:** To guarantee correct initialization, the first time every system client logs on to the system they must log in as "non-mobile" system clients; only thereafter can they be configured as "mobile".

---

If "non mobile and blocked" is set as the type for a system client, a subscriber cannot log into this IP telephone with a mobile system client.

- **Defining a redundant gatekeeper** (secondary system)  
If the internal IP network contains a redundant gatekeeper, you can program the IP client to redirect to this redundant gatekeeper if the original gatekeeper fails.
- **Special SIP parameters** (for SIP clients only)  
SIP clients must log into an SIP registrar. This can be the internal SIP registrar of OpenScape Office or an external SIP registrar. Depending on what the SIP registrar demands for login, the user ID and the associated realm must also be specified.

### Setting Classes of Service (Advanced Settings)

Every subscriber can be assigned one class of service for day and another for night. There are 15 classes of service to choose from. You will find more information in the topic *Operation, Optimization and Monitoring - CO Call Privileges, Toll Restriction*.

### Defining the Call Pickup Groups (Advanced Settings)

Every station can be assigned to a call pickup group. There are 32 call pickup groups to choose from.

### Configuration before gateway modules are inserted

In Expert mode, the call numbers and names of stations can be configured even if the associated gateway modules have not yet been inserted. When inserting the gateway modules, care must be taken to ensure that they are inserted in the order in which the phone numbers and station names were configured (e.g., the gateway modules with the S<sub>0</sub> ports should be inserted first, and then the modules with the analog interfaces). A new gateway module may only be inserted after the previously inserted module has been recognized in the system.

## 6.7.3 Configuring Users of the UC Suite

The values and settings of users of the UC Suite can be configured via the User Directory.

The User Directory contains a list of all stations in the communication system. The symbol in the first column of the list shows you the presence status of the user. The administrator can change this presence status for every user. If names were defined when setting up the stations, the names are also transferred over to the user directory.

The following information is displayed in the user directory for every user:

- **Symbol for presence status**  
Shows the current presence status of the user
- **Extension**  
Shows the internal call number of the user. The internal call number cannot be edited in the user directory.
- **Username**  
Shows the user name, which can be freely defined for every user.
- **Name**  
Shows the first name and last name of the user.
- **Department**  
Shows the associated department (if a department was configured and assigned to the user)
- **E-mail**  
Shows the e-mail address of the user
- **Is Agent**  
Shows if the user was configured as an agent for the multimedia Contact Center.
- **Voicemails**  
Shows if the user can receive voicemails.
- **Call Forwarding**  
Shows whether call forwarding was configured for the user.



The following values and settings can be configured:

Values and settings	Keywords
<b>Personal details</b>	
My Personal Details	Own name, user name, password, e-mail address, department, additional phone number, XMPP ID
My Picture	My Picture
User Level	Receiving voicemails: see <i>OpenScape Office V3, Administrator documentation , Subscribers/Stations</i>  User as Attendant Console: see <i>OpenScape Office V3, Administrator documentation , Subscribers/Stations</i>  User as agent: see <i>OpenScape Office V3, Administrator documentation , Subscribers/Stations</i>
<b>My Preferences</b>	
Appearance	Skin colors, language of the user interface
Notifications	Screen pops
Outlook connectivity	Automatic creation of Outlook appointments when absent, automatic update of presence status via Outlook appointments
Hotkeys	Hotkey for functions
Miscellaneous	Automatic reset of the presence status, transfer method, retention period for Journal entries, server address, function keys of the telephone
<b>Call Rules</b>	
Forwarding destinations	Status-based call forwarding
Rules Engine	Rule-Based Call Forwarding
<b>Communications</b>	
Voicemail settings	Recording or announcement mode, language of the voicemail box
VM Notification	Notification Service for Messages
Fax Notification	Notification Service for Messages
<b>Profiles</b>	
Busy, No Answer, Meeting, Sick, Break, Away, Vacation, Lunch, Home Ph.	profile for personal AutoAttendant
<b>Sensitivity</b>	
Security and Access	Retrieval of your voice and fax messages by the Attendant; password check for the voicemail box
Presence Visibility	Visibility of your Presence Status for Others

Values and settings	Keywords
VoiceMail Presence	Announcement of your presence status for external callers; announcement of your presence status for specific callers
<b>myAttendant</b>	
LAN Messages	Text module for Instant Messaging
DIDs	MSN
Communications	Call forwardings

More detailed information on the values and settings of the users can be found in the User Guides of the communications clients **myPortal for Desktop**, **myPortal for Outlook** and **myAttendant** under the keywords listed in the table.

The length of the password for using the communications clients is 6 characters by default. The password length can, however, be adapted as required. (min. six digits; max. ten digits). An administrator with the **Advanced** profile can reset the password of a user (if the user has forgotten it, for example).

---

**INFO:** The First Name and Last Name of a user are overwritten in the User Directory when they are changed by using a wizard or in Expert mode. By contrast, if the First Name and Last Name of a user are changed in the User Directory, the user data displayed when using a wizard or in Expert mode are not overwritten. This results in the existence of two different user names for the same user.

---

Subscribers for whom an e-mail address has been configured and who use the communications clients **myPortal for Desktop** or **myPortal for Outlook** receive a welcome e-mail with Getting Started Instructions.

#### Resetting User Data

All entered data for users can be deleted, and the changed settings can be reset to their default values. Note that the voicemails, journal entries, scheduled conferences, e-mails, faxes and personal announcements for the voicemail box are also deleted for the selected user in the process.

### 6.7.4 Exporting Subscriber Data

Important data of subscribers can be exported to a CSV file.

In addition to the names and station numbers of subscribers, the CSV file may also include other subscriber data such as their license types and e-mail addresses, for example.

A sample CSV file with the appropriate explanations can be found in the OpenScape Office Assistant Administration Program under **Service Center > Download Center > CSV Templates**.

Structure of a CSV file:

- Column A contains the call number (possible values: 0-9, \*, #)
- Column B contains the DID number (possible values: 0-9, \*, #)
- Column C contains the name (in the format `First Name Last Name` or `Last Name, First Name`)  
The name of a subscriber can consist of up to 16 characters, but must not include any diacritical characters such as umlauts or special characters.
- Column D contains the subscriber type (e.g., 1=System Client, 2=SIP User, 3=SIP Fax, 4=RAS User, 5=Analog, 6=Analog Fax, ...)
- Column E contains the license type (<no entry> or 0=No Licence, 1=Comfort User, 2=Comfort Plus User)
- Column F contains the e-mail address  
Users of the UC Suite are automatically sent an e-mail with a link to the installation file(s) if their respective e-mail addresses were imported via the CSV file.
- Column G contains the mobile number (possible values: 0-9, \*, #)
- Column H contains the private number (possible values: 0-9, \*, #)
- Column I contains the node ID (possible values: 0-999)  
This column must be assigned a value; otherwise, no import will occur. If the system is not networked, 0 must be entered here.
- Column J contains the IP address of the second gateway

---

**IMPORTANT:**

CSV files must be available in ANSI/ASCII format.

CSV files of older OpenScape Office versions are not supported.

---

## 6.8 Configuring Station and User Profiles

The values and properties stored in profiles can be configured here. The profiles of the stations and users of the OpenScape Office clients can be configured.

### 6.8.1 Configuring Station Profiles (LX/MX)

The values and properties of IP stations are stored in station profiles.

Using the **Profiles** wizard, an administrator with the **Advanced** profile can perform the following configuration tasks:

- Create a new profile

## Subscribers/Stations

### Configuring Station and User Profiles

- Display profiles and their members
- Add members to a profile
- Delete members from a profile
- Export or import a single profile

In Expert mode, an administrator with the **Expert** profile can also perform the following configuration tasks:

- Change values and settings of a station profile
- Export or import all profiles

Station profiles that have already been created cannot be deleted, but can be overwritten.

## 6.8.2 Configuring the User Profiles of UC Clients

All relevant values and properties of the users of the UC clients are stored in the user profiles of the UC clients.

The following values and settings can be configured:

Menu items	Values and settings for
<b>Personal details</b>	
My Personal Details	Visibility of phone numbers
<b>My Preferences</b>	
Appearance	Skin colors, language of the user interface
Notifications	Screen pops
Outlook connectivity	Automatic creation of Outlook appointments when absent, automatic update of presence status via Outlook appointments
Miscellaneous	Automatic reset of the presence status, transfer method, retention period for Journal entries, server address
<b>Call Rules</b>	
Forwarding destinations	Status-based call forwarding
<b>Communications</b>	
Voicemail settings	Recording or announcement mode, language of the voicemail box
VM Notification	Notification Service for Messages
Fax Notification	Notification Service for Messages
<b>Profiles</b>	

Menu items	Values and settings for
Busy, No Answer, Meeting, Sick, Break, Away, Vacation, Lunch, Home Ph.	profile for personal AutoAttendant
<b>Sensitivity</b>	
Security and Access	Retrieval of your voice and fax messages by the Attendant; password check for the voicemail box
Presence Visibility	Visibility of your Presence Status for Others
VoiceMail Presence	Announcement of your presence status for external callers; announcement of your presence status for specific callers

More detailed information on the values and settings of the profiles can be found in the User Guides of the UC clients and under the keywords listed in the table.

## 7 Licensing

Licensing is mandatory for the operation of OpenScape Office. Following the initial startup, the licensing must be completed within 30 days (called the Grace Period); otherwise, when this period expires, the system will only operate in restricted emergency mode.

### 7.1 Licensing Procedure

Licensing is handled via a centralized License Management procedure for the administration and activation of licenses. The product/feature is supplied together with a License Authorization Code (LAC) with which a license file is obtained from the Central License Server (CLS). This license file is used for activating licenses. This procedure provides protection against any potential manipulation of the licenses.

The license activation for OpenScape Office LX/MX and OpenScape Office HX occurs with the administration program OpenScape Office Assistant and HiPath 3000 Manager E, respectively.

---

**INFO:** In order to successfully activate additional licenses, the license for the basic package must already have been activated in advance or be activated at the same time as the additional licenses.

---

#### 7.1.1 License Server (Central License Server, CLS)

The Central License Server (CLS) generates and manages the license files.

A license file is generated when the License Authorization Code is sent to the CLS by the communication system. The transmission of the license file to the communication system occurs automatically via the Internet or ISDN. If an automatic transmission is not possible, the license file can also be loaded manually into the communication system.

Every customer or sales partner has a separate license account on the CLS. The accounts can be maintained at the CLS via a separate web-based user interface. All available and already purchased licenses can be displayed.

To reach the CLS, enter the address <https://www.central-license-server.com> or the IP address <https://188.64.16.4> in a web browser.

---

**INFO:** The IP address of the CLS (Central License Server) can be checked via OpenScape Office Assistant under **License Management > Settings** and changed if required.

---

## 7.1.2 Grace Period

After installing the software or upgrading the software from V2 to V3, the license activation must be completed made within a period of 30 days (grace period). During the grace period, the product is fully functional; however, systems in the internetwork may be subject to restrictions.

---

**IMPORTANT:** If the licensing is not completed before the grace period expires, the system will only operate in Emergency mode thereafter. In Emergency mode, the external functionality is restricted to one IP client (with the default station number 100) with access to the communication system via Remote Access. All other IP clients can only make internal calls.

---

## 7.1.3 MAC Address

MAC addresses are unique worldwide, and every communication system may be associated with one or more MAC addresses. To ensure unique licensing, these MAC addresses are used in the licensing process.

For an OpenScape Office MX multi-box system, the licenses are always bound to the MAC address of the central box. If OpenScape Office MX is in the grace period, a wrong MAC address may possibly be shown under the license information. The correct MAC address can be checked via the **Service Center** under **Inventory**.

For OpenScape Office LX/HX, the licenses are bound to the MAC address of the network card in the Linux server. If the Linux server has multiple network cards, the network card that was used at the initial startup of the Linux server must be selected.

## 7.1.4 Advanced Locking ID (LX)

The Advanced Locking ID of OpenScape Office LX is required when OpenScape Office LX is operated in a virtualized environment. An Advanced Locking ID is generated a variety of system and network parameters and is used for licensing instead of the MAC address of the server PC.

The following system and network parameters must be configured, since they are used to generate the 24-digit Advanced Locking ID.

- IP address of the default gateway
- Hostname
- IP address of the host
- IP Address of DNS Server

- Time zone

If one or more of these system and network parameters are not set, then the Advanced Locking ID cannot be generated.

The Advanced Locking ID is displayed in the OpenScape Office Assistant. If any of the system and network parameters listed above changes, OpenScape Office LX reverts to the remaining term of the grace period, and a new locking Advanced ID is generated. To exit the remaining term of the grace period again, a rehost from the old to the new Advanced Locking ID must be conducted at the Central License Server (CLS).

### 7.1.5 Licensing Process using OpenScape Office MX as an Example

The licensing process is presented below with an example of OpenScape Office MX using OpenScape Office Assistant and the License Authorization Code (LAC).

1. On purchasing OpenScape Office MX, the customer receives a License Authorization Code (LAC). The information on the licenses purchased (basic licenses and extension licenses, if any) are stored in the database of the CLS.
2. The customer or service technician installs OpenScape Office MX. The grace period begins (period of 30 days in which the licensing must be completed).
3. The customer or service technician transfers the License Authorization Code to the CLS via the Internet or ISDN by using OpenScape Office Assistant. Some customer-specific hardware data (such as the MAC address of OpenScape Office MX) is sent to the CLS along with the LAC. The CLS uses the License Authorization Code and the customer-specific hardware data to generate a license file and then sends this back to OpenScape Office Assistant in an encrypted format. The license file contains the procured licenses.
4. OpenScape Office Assistant checks whether the MAC address saved in the license file matches the MAC address of OpenScape Office MX. If the check is successful, the license is activated, and OpenScape Office MX is ready for use. If the check fails, OpenScape Office MX continues to run in the grace period until it expires and then only in emergency mode.

## 7.2 Licenses

In order to use the communication system after the grace period, licenses are required. The licenses define the scope of features available at the communication system. As soon as the license is activated, the corresponding feature can be used.

For OpenScape Office V3, different basic license packages are available for basic operation. To expand OpenScape Office V3, additional licenses (e.g., 5 additional Comfort User licenses) can be purchased. If the OpenScape Office Contact Center is to be used, additional licenses are required for it. An upgrade license is needed to upgrade to the latest version.



Regardless of the selected basic license package, OpenScape Office MX can be expanded to a maximum of 150 IP stations, and OpenScape Office LX/HX to a maximum of 500 IP stations. For every IP station, a Comfort User or Comfort Plus User license is required. Analog stations are automatically recognized as Comfort User devices. No Comfort User or Comfort Plus User license is required for this.

The Comfort User and Comfort Plus User licenses are assigned permanently to individual IP stations with OpenScape Office Assistant. The number of IP stations licensed cannot exceed the number of available licenses. The assignment of other licenses occurs dynamically, i.e., depending on the requirements and availability, licenses are assigned for the components that require them.

## 7.2.1 Basic Licenses

A basic license consists of the system license and extension licenses. Every basic license includes different extension licenses.

The following basic licenses are available:

- **OpenScape Office V3 MX Base 10 Plus**
  - 1 x system license for the operation of OpenScape Office MX
  - 10x licenses for Comfort Plus User
  - 1x license for OpenScape Office Directory Service
- **OpenScape Office V3 MX Base 20 Plus**
  - 1 x system license for the operation of OpenScape Office MX
  - 20x licenses for Comfort Plus User
  - 1x license for OpenScape Office Directory Service
- **OpenScape Office V3 MX Base 5 Plus**
  - 1 x system license for the operation of OpenScape Office LX
  - 5x licenses for Comfort Plus User
  - 1x license for OpenScape Office Directory Service
- **OpenScape Office V3 LX Basic 20 Plus**
  - 1 x system license for the operation of OpenScape Office LX
  - 20x licenses for Comfort Plus User
  - 1x license for OpenScape Office Directory Service
- **OpenScape Office V3 HX Base 5**
  - 1 x system license for the operation of OpenScape Office HX
  - 5x Licenses for Standard User
  - 1x license for OpenScape Office Directory Service
- **OpenScape Office V3 HX Base 10**

- 1 x system license for the operation of OpenScape Office HX
- 10x Licenses for Standard User
- 1x license for OpenScape Office Directory Service

## 7.2.2 Extension Licenses

Extension licenses are needed to expand the communication system. Some extension licenses are also offered in packages of 100 units.

The following extension licenses are available:

- **OpenScape Office V3 LX/MX Comfort User**

- Usage of all communication functions of OpenScape Office
- Unified Communications functions via myPortal for Desktop.
- Voicemail box (Voicemail)

Comfort User licenses are permanently bound to the stations.

- **OpenScape Office V3 LX/MX Comfort Plus User**

- Usage of all communication functions of OpenScape Office
- Unified Communications functions via myPortal for Desktop
- Voicemail box (Voicemail)
- Fax box
- Conference management
- Mobility Entry, incl. myPortal for Mobile/Tablet PC web client

Comfort Plus User licenses are permanently bound to stations.

- **OpenScape Office V3 HX Standard User**

- Usage of all communication functions of OpenScape Office
- Unified Communications functions via myPortal for Desktop.
- Voicemail box (Voicemail)
- Fax box

Standard user licenses are permanently bound to the stations.

- **OpenScape Office V3 myPortal for Outlook (Outlook Integration)**

For the use of unified communications functions through the interface of Microsoft Outlook. The licenses for myPortal for Outlook are "floating" licenses, i.e., are not permanently bound to the subscribers; however, the maximum number of subscribers who can log in simultaneously is restricted to the number of available licenses. In order to use myPortal for Outlook, additional Comfort User or Comfort Plus User licenses are required. A

maximum of 150 myPortal for Outlook users can be licensed for OpenScape Office MX, and a maximum of 500 myPortal for Outlook users can be licensed for OpenScape Office LX/HX.

- **OpenScape Office V3 myPortal for Zimbra**  
For the use of unified communications functions through the interface of Zimbra. The licenses for myPortal for Zimbra are "floating" licenses, i.e., are not permanently bound to the subscribers; however, the maximum number of subscribers who can log in simultaneously is restricted to the number of available licenses. The myPortal for Zimbra license also includes the required Comfort Plus User license (LX/MX) or Comfort Standard User license (HX). A maximum of 100 web clients (myPortal for Mobile/Tablet PC and myPortal for Zimbra) can be operated at an OpenScape Office MX/HX, and a maximum of 200 web clients can be operated at an OpenScape Office LX.
- **OpenScape Office V3 myAttendant**  
For using a PC attendant (Attendant Console). The licenses for myAttendant "floating" licenses, i.e., are not permanently bound to the subscribers; however, the maximum number of subscribers who can log in simultaneously at the Attendant Console is restricted to the number of available licenses. The myAttendant license also includes the required Comfort User license. A maximum of 20 myAttendants can be licensed.
- **OpenScape Office V3 CSTA Application Interface (free of charge)**  
For a CSTA connection to enable the use of CSTA applications. A total of 7 CSTA connections may be licensed. For every CSTA connection, a separate CSTA license is required. Different priorities (levels) are assigned to the CSTA applications.
  - OpenScape Office: Level 1
  - TAPI 170 V2 R1: Level 2
  - Other CSTA applications: Level 3If all CSTA connections are in use and a further CSTA application is started, the CSTA application with the lowest priority is automatically terminated. If the new CSTA application has the lowest priority or an equivalent level to one of the other applications, the new application is not started. This automatic prioritization ensures that the OpenScape Office application can always be used even if all CSTA connections are already in use.
- **OpenScape Office V3 OpenDirectory Connector**  
For using the OpenScape Office Directory Service (ODS) so that the UC Suite can also be connected to an external database.
- **OpenScape Office V3 Application Launcher**  
For call-related control of applications on a client PC during incoming and outgoing calls, e.g., launching an application or displaying caller information. A maximum of 100 Application Launcher licenses per system are possible.

- **OpenScape Office V3 Gate View**  
For video surveillance, which provides real-time video images on your OpenStage phone, PC or iPhone. A maximum of 2 cameras can be connected to an OpenScape Office V3 MX, and a maximum of 8 cameras can be connected to an OpenScape Office V3 LX/HX.
- **OpenScape Office V3 HX VoiceMail**  
For using the voicemail box of OpenScape Office without having to purchase an OpenScape Office HX Standard User license. Only the functions operated via the telephone can be used.

### 7.2.3 Licenses for Multimedia Contact Center

In order to use the Multimedia Contact Center, additional licenses are required.

The following licenses are available for the Multimedia Contact Center:

- **OpenScape Office V3 Contact Center Basic License Package**
  - 1x license for usage of the contact center
  - 4x licenses for Contact Center agents (myAgent), incl. the 4 required Comfort User licenses
- **OpenScape Office V3 myAgent**  
For use of one myAgent user (Agent or Supervisor) in the Contact Center. The licenses for agents are "floating" licenses and not permanently bound to the agents. Any number of subscribers can be set up as agents, but the maximum number of agents who can log in simultaneously is restricted to the number of available licenses. The Contact Center basic license package is a prerequisite. The myAgent license also includes the required Comfort User license. A maximum of 64 agents can be licensed. For OpenScape Office MX one-box systems, a maximum of 10 agents can be licensed.
- **OpenScape Office V3 myReports**  
To use the extended reporting functionality (report analysis and creation) for the Contact Center. Standard reporting is already included in myAgent. myReports can only be started once per system, so only one license is required for it.
- **OpenScape Office V3 Contact Center Fax**  
For setting up one or more fax boxes to send and receive faxes for Contact Center agents. One license per system is required for this purpose. The Contact Center basic license package is a prerequisite.

- **OpenScape Office V3 Contact Center E-Mail**  
For setting up one or more e-mail boxes to send and receive e-mails for Contact Center agents. One license per system is required for this purpose. The Contact Center basic license package is a prerequisite.

## 7.2.4 Evaluation Licenses

An evaluation license can be used to test applications with full functionality over a fixed time period (called the evaluation period) free of charge. If regular licenses for the application are activated during the evaluation period, the evaluation license is disabled.

The evaluation period is 90 days. After 60 days, the remaining time in days is counted backwards on the display of system telephones. When the evaluation period expires, the application is automatically disabled.

The activation of the license occurs at the Customer License Server (CLS) and can only be performed once.

The following evaluation licenses are available:

- **OpenScape Office V3 Contact Center Evaluation License (free of charge)**
  - 1x license for usage of the contact center
  - 64x licenses for Contact Center agents (myAgent), incl. the 64 required Comfort User licenses
  - 1x license for Contact Center reporting (myReports)
  - 1x Contact Center Fax license
  - 1x Contact Center E-mail license

This evaluation license is intended for customers who are already using OpenScape Office and want to test the Multimedia Contact Center. All features of the Multimedia Contact Centers can be used with the evaluation license.

---

**INFO:** If the Multimedia Contact Center is not licensed within the evaluation period, the administrator must undo the Contact Center settings (e.g., delete schedules and queues, deactivate agents, etc.) before the evaluation license expires. Otherwise, errors may occur in OpenScape Office.

---

- **OpenScape Office V3 HX Evaluation License (free of charge)**  
This Evaluation License is intended for HiPath 3000 customers who have not used OpenScape Office HX in the past. All OpenScape Office HX features can be used with this evaluation license. The activation of the license occurs via the Customer License Agent (CLA). In order to enable all the features of OpenScape Office HX to be used, the number of HG 1500 B channels for an HG 1500 board is increased to 30 during the evaluation period.

## 7.2.5 Upgrade Licenses

Upgrade licenses are required to upgrade the product or feature to the latest version.

The following upgrade licenses are available:

- **OpenScape Office V3 MX Upgrade from OSO MX V2**

For the upgrade from HiPath OpenOffice ME V1 and OpenScape Office MX V2 to OpenScape Office V3 MX. HiPath OpenOffice ME V1 must be first upgraded to OpenScape Office MX V2 software. It is not possible to directly upgrade the software from HiPath OpenOffice ME V1 to OpenScape Office V3 MX.

With this license, all purchased licenses are converted to V3 licenses. HiPath OpenOffice ME V1 licenses can be upgraded to OpenScape Office V3 MX licenses directly at the CLS.

---

**INFO:** In V3, the licenses for the Contact Center Basic License Package, myAgent and myAttendant include the required Comfort User licenses, which had to be ordered separately for V2. When upgrading to V3, only the licenses for the Contact Center Basic License Package, myAgent and myAttendant need to be upgraded; the total number of Comfort User licenses available remains the same.

---

---

**INFO:** After an upgrade to OpenScape Office V3 MX, 15 Comfort User licenses from the OpenScape Office MX V2 basic package are converted to Comfort Plus User licenses.

---

- **OpenScape Office V3 LX/MX Upgrade from Comfort to Comfort Plus User**

For upgrading a Comfort User to a Comfort Plus User

An upgrade from OpenScape Office HX V2 to OpenScape Office HX V3 occurs automatically with the upgrade from HiPath 3000 to Version 9.

## 7.3 Activating and Updating Licenses

Products or features must be enabled via licenses. Following a hardware defect, these licenses must be updated.

The activation and updating of licenses for OpenScape Office HX are performed using HiPath 3000 Manager E and a license file. This type of licensing is described in the HiPath 3000 Manager E documentation. The following sections explain the licensing of OpenScape Office MX and OpenScape Office LX.

### 7.3.1 Activating Licenses (MX/LX)

After purchasing a product or feature, you must activate the licenses provided with the product or feature to enable it. The License Authorization Code (LAC) or the license file itself is required for this purpose.

Licenses can be activated by one of the following two methods:

- **Activating a License using the License Authorization Code**  
License activation via the LAC is the standard method. Using the LAC, a license file is generated at the Central License Server (CLS) and forwarded to OpenScape Office Assistant. The license file is used to activate the associated license and release the product. To access the CLS, you will need an Internet connection or an ISDN connection. The IP address of the CLS or the phone number for the ISDN connection is stored in OpenScape Office Assistant under **License Management > Settings** and can be changed by an administrator with the **Expert** profile if required.
- **Activating a License via a License File**  
License activation via a license file is needed if a license file is directly available instead of a LAC. The license file was generated at the Central License Server (CLS) earlier and downloaded. The license file is used to activate the associated license and release the product. The IP address of the CLS is saved in OpenScape Office Assistant under **License Management > Settings**.

If the communication system is to be expanded, further licenses (e.g., 5 additional Comfort User licenses) can be purchased. On purchasing more licenses, an additional License Authorization Code (LAC) with which the newly procured licenses can be activated is supplied. After activation, all features for which a license is required will be available.

---

**INFO:** In order to successfully activate additional licenses, the license for the basic package must already have been activated in advance or be activated at the same time as the additional licenses.

---

#### Assigning the Licenses

The Comfort User and Comfort Plus User licenses are assigned permanently to individual IP stations with OpenScape Office Assistant. The number of IP stations licensed cannot exceed the number of available licenses. The assignment of other licenses occurs dynamically, i.e., depending on the requirements and availability, licenses are assigned for the components that require them.

### Connecting to the License Server without Internet Access

As a rule, the connection to the Central License Server (CLS) is set up via the Internet. If no Internet access is available or configured, the connection to the CLS is automatically established via ISDN. The correct license station number must be configured and selected for this purpose. Logging on to the CLS then occurs automatically. The license station number for the CLS is saved in OpenScape Office Assistant under **License Management > Settings** and can be changed by an administrator with the **Expert** profile if required.

## 7.3.2 Updating a License (MX/LX)

Licenses must be updated whenever any hardware that has a MAC address (e.g., the motherboard of OpenScape Office MX, network card or the Linux server of OpenScape Office LX) is replaced at the communication system. To perform the update, the License Authorization Code (LAC) and the login details for the Central License Server (CLS) are required.

After replacing the hardware, the configuration data must be restored using the latest backup set (see [Restore](#)).

Since the licenses are bound to the MAC address of the hardware, the MAC address changes on replacing the hardware, and the licenses are thus no longer valid. After the hardware is replaced, the communication system reverts to the grace period. The LAC must therefore be transferred to the CLS again. The LAC of the basic license or the LAC of a further product/feature of OpenScape Office MX may be used for this purpose. The new license file, which is bound to the new MAC address, is transferred to the communication system, and all existing licenses are then automatically activated.

For OpenScape Office MX, the MAC address of the first system box is used (visible as a sticker on the front of the device). For OpenScape Office LX, the MAC address of the network card of the Linux server, which was selected on installing the Linux operating system (visible via YaST), is used. The MAC address can also be read by using OpenScape Office Assistant.

---

**INFO:** Before the licenses can be updated, a rehost must be performed at the CLS. Every rehost is logged. A license can be used for a rehost up to three times.

---

---

**INFO:** The IP address of the CLS (Central License Server) can be checked via OpenScape Office Assistant under **License Management > Settings** and changed if required.

---

---

### Related Topics

- [Immediate Backup](#)



## 7.4 Licensing in an Internetwork

If multiple OpenScape Office (nodes) systems are combined into an internetwork, licensing occurs centrally via the master node.

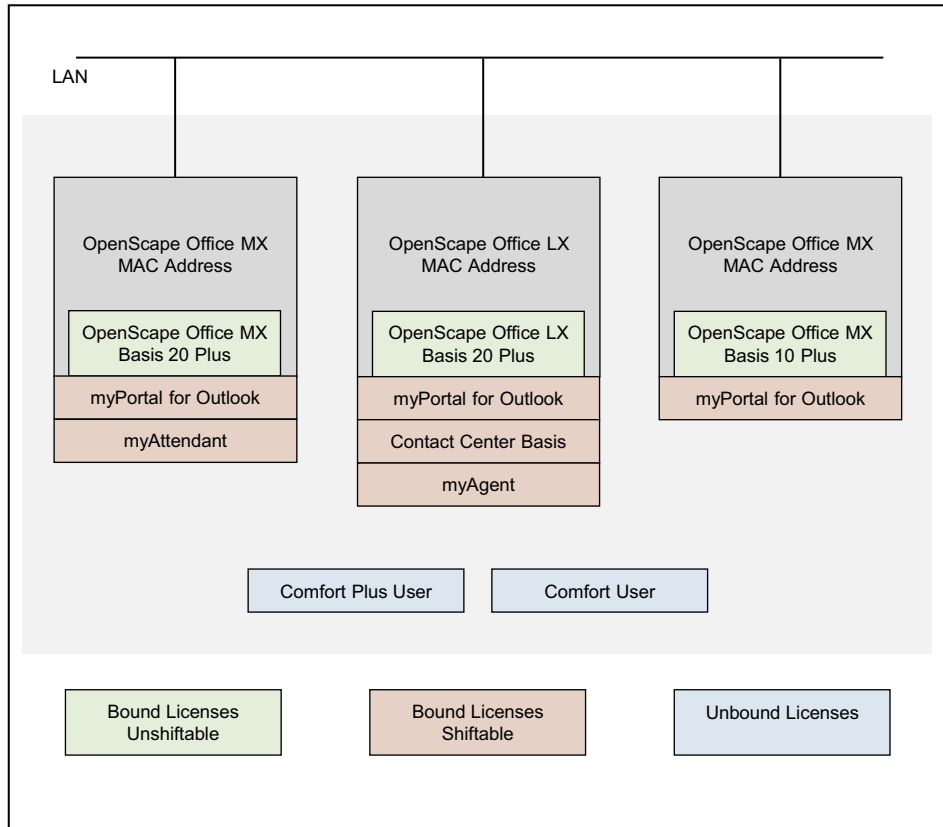
The master node contains the central license agent (central CLA; central Customer License Agent). All other nodes (slave nodes) in the internetwork use this CLA for the licensing. To enable this, the IP address of the master node must be made known to the slave nodes using OpenScape Office Assistant.

Only one network license file exists for the entire internetwork. This license is bound to the MAC address of the master node and stored in the central CLA. The network license file contains all the license information in the internetwork and can only be activated at the master node using OpenScape Office Assistant. Only the master node has access to the CLS; at all other nodes, the access is disabled.

The network license file includes two types of licenses:

- **Bound licenses**  
Bound licenses are bound to the MAC address of a node and can only be used from that node. All basic licenses and licenses for the UC clients such as **myPortal for Outlook** or **myAttendant** are bound licenses.. If bound licenses are to be used from another node, they must first be shifted with the aid of the CLS. The basic licenses for OpenScape Office cannot be shifted.
- **Unbound licenses**  
Unbound licenses can be used from all nodes in the internetwork. The Comfort User and Comfort Plus User licenses are unbound licenses (except for those included in the basic licenses). The Comfort User and Comfort Plus User licenses are assigned to IP stations. These licenses can be reassigned to other nodes without being shifted. This is achieved by unassigning the licenses from the IP stations at the old node and assigning them to the IP stations at the new node.

**Figure:** Overview of Bound and Unbound Licenses



**Shifting Licenses**

One or more licenses can be shifted from one node to another. The transfer of licenses is performed at the CLS. The CLS generates a new network license file, which must then be loaded into the central CLA.

**Combining Licenses**

If one or more nodes that have already been licensed are to be combined into an internetwork, the administrator must combine the individual license files via the CLS into a single license file and load it into the central CLA. The IP address of the master node with the central license agent must then be entered at all other nodes by using the Networking wizard of OpenScape Office Assistant.

**Behavior during Network Problems (Failover)**

If the connection to the master node and thus to the central CLA fails, the message "Failover Period" appears on the displays of the system telephones. During this failover period (max. 30 days), all nodes and their features continue to operate normally. Once the network problems have been resolved and the connection to the central CLA is restored, all nodes revert to the regular license status.

If the network problems cannot be resolved within the failover period, the nodes switch to operating in emergency mode. The entire internetwork will then need to be relicensed.

## 7.4.1 Licensing Process in the Internetwork

The licensing process for a sample internetwork consisting of one OpenScape Office LX and two OpenScape Office MX systems is illustrated below:

1. On purchasing the communication systems, the customer receives a License Authorization Code (LAC). The information on the licenses purchased (basic licenses and extension licenses, if any) are stored in the database of the CLS.
2. Using the network wizard of OpenScape Office Assistant, the customer or service technician first installs the OpenScape Office LX as a master node. The system runs in the Grace Period (period of 30 days during which the licensing has to be completed).  
For a description, see [Configuring Scenario 3](#)
3. Using the network wizard of OpenScape Office Assistant, the customer or service technician then installs the two OpenScape Office MX systems. The system runs in the Grace Period  
For a description, see [Configuring Scenario 3](#)
4. After the customer or service technician has installed all the systems in the internetwork, he or she generates a network license file at the CLS with the License Authorization Code and uploads this to the master node with the help of OpenScape Office Assistant. The network license file contains all the customer-specific hardware information (such as the MAC addresses or the Advanced Locking IDs of all systems in the internetwork) and all associated licenses.  
For a description, see *OpenScape Office V3, Administrator documentation , Licensing*
5. OpenScape Office Assistant checks whether the MAC addresses or Advanced Locking IDs stored in the license file match those of the systems. If the check is successful, the licenses are activated, and the systems switch to the regular license status. If the check is not successful, the systems continue to run in the Grace Period until it expires and then only in emergency mode.

## 7.5 License Information in OpenScapeOffice Assistant

Information on the available and assigned licenses, products and features is displayed with OpenScape Office Assistant. The license information on all licenses available in the internetwork can be retrieved.

The following information can be displayed:

## Licensing

License Information in OpenScapeOffice Assistant

- **MAC Address:** MAC address of OpenScape Office MX or the OpenScape Office Linux server to which the licenses are bound.

---

**INFO:** If OpenScape Office MX is in the grace period, a wrong MAC address may possibly be shown here. The correct MAC address can be checked via the **Service Center** under **Inventory** (*OpenScape Office V3, Administrator documentation , Licensing*).

---

- **Locking ID:** Advanced Locking ID of OpenScape Office LX in a virtualized environment, to which the licenses are bound.
- **Node:** Name of the communication system to which the license is bound.
- **Product Name:** Name of the product for which the license is assigned.
- **Feature:** Feature for which the license has been assigned.
- **Used licenses:** Shows the number of used and available licenses.
- **Available for distribution:** Shows the licenses still available in the internetwork.
- **Status:** Status of the license.

### 7.5.1 License Information without a Network (Standalone)

All licenses permanently assigned to the communication system can be displayed.

### 7.5.2 License Information in an Internetwork

All existing licenses in an internetwork and the relevant information on them can be displayed.

The display of the license information in the internetwork is grouped as follows:

- **Display of bound licenses**  
These are licenses that are permanently assigned to a single communication system (node).
- **Display of unbound licenses**  
These are licenses that are not permanently assigned to any communication system and can be freely distributed in the internetwork.
- **Display of local licenses**  
These are licenses that are permanently assigned to the local communication system, including the free unbound licenses.

## 8 Unified Communications

Unified Communications offers features such as the Presence status and CallMe, conferencing (not with OpenScape office HX), as well as voicemail and fax functionality in the myPortal for Desktop and myPortal for Outlook clients. myAttendant also provides Attendant Console functions.

---

**INFO:** For more information on with the clients myAgent and myReports, see [Multimedia Contact Center](#).

---

### 8.1 UC Clients

UC clients provide subscribers with convenient user interfaces for unified communications.

The system offers the following UC clients for the following devices:

Client type	Client	Device
Communications Client	myPortal for Desktop	PC
	myPortal for Outlook	
	Fax Printer (see <a href="#">Voice and Fax Messages</a> )	
	myAttendant	
	myPortal for OpenStage	OpenStage telephone
Mobile Client	myPortal for Mobile (see <a href="#">Multimedia Contact Center</a> )	Mobile Phone
Contact Center Client	myAgent (see <a href="#">Multimedia Contact Center</a> )	PC
	myReports (see <a href="#">Multimedia Contact Center</a> )	

Subscribers with a configured e-mail address receive a welcome e-mail with Getting Started Instructions.

#### Custom Settings

The custom (i.e., subscriber-specific) settings for myPortal for Desktop are stored in ini files on the PC. A separate ini file is created for every user. The custom settings for myPortal for Outlook, myAttendant and Fax Printer are stored in the registry of the PC. This enables different users to use the myPortal for Desktop, myPortal for Outlook, myAttendant and Fax Printer applications on a single PC

(Desk Sharing) and also the deployment in Windows Terminal Server and Citrix Server environments. This allows different users to access the applications from their PCs without a local installation.

---

**Related Topics**

- [Multimedia Contact Center](#)
- [Mobility](#)

## 8.1.1 myPortal for Desktop

myPortal for Desktop is a client for unified communications on your PC. Besides convenient dialing aids via phone directories and favorites and information on the presence status of other subscribers, users can, for example, also access their voicemails and fax messages.

myPortal for Desktop provides the following features:

- Directories
- Favorites List
- Journal
- Desktop Dialer
- Screen pops
- Presence status
- CallMe service with ONS (One Number Service)
- Status-based call forwarding
- Personal AutoAttendant
- Conference management (LX/MX)
- Record conferences (LX/MX)
- Record calls
- Instant Messaging
- Voice and Fax Messages

---

**Related Topics**

- [Prerequisites for UC PC Clients](#)

## 8.1.2 myPortal for Outlook

myPortal for Outlook is the client for unified communications in Microsoft Outlook (plug-in) and is analogous to myPortal for Desktop.

myPortal for Outlook provides the following features in addition to those of myPortal for Desktop:

- How to Call an Outlook Contact

- How to Create an Outlook Contact from the Sender of a Voice Message
- How to Send a Voice Message as an E-mail
- How to Send a Fax Message as an E-mail

---

**Related Topics**

- [Prerequisites for UC PC Clients](#)

### 8.1.3 myPortal for Zimbra

myPortal for Zimbra is a web-based client for unified communications in the Web Client of the Zimbra Collaboration Suite (plug-in). Besides convenient dialing aids via phone directories and favorites and information on the presence status of subscribers, you can, for example, also access your voicemails.

myPortal for Zimbra offers the following features in addition to telephony:

- Directories
- Favorites List
- Journal
- Presence status
- CallMe service with ONS (One Number Service)
- Status-based call forwarding
- Voicemails

Other features you can use with myPortal for Desktop.

### 8.1.4 myPortal for OpenStage

myPortal for OpenStage is the user portal for accessing the system's unified communications functions on your OpenStage telephone.

myPortal for OpenStage can be configured via the OpenStage telephone as well as OpenStage Manager web browsers.

myPortal for OpenStage provides the following features:

- Presence status
- Voicemails

---

**Related Topics**

- [Prerequisites for myPortal for OpenStage](#)

## 8.1.5 Fax Printer

Fax Printer is an application for sending fax messages with individually created cover sheets from Windows applications such as Microsoft Word, for example.

Fax Printer consists of the following components:

- Fax Printer Cover Editor
- Fax Printer Driver

---

### Related Topics

- [Prerequisites for UC PC Clients](#)

## 8.1.6 myAttendant

myAttendant is a unified communications solution for Attendant functions. Besides convenient Attendant functions, dialing aids via phone directories and information on the presence status of other subscribers, myAttendant can, for example, also be used to access voicemails and faxes. Instant Messaging supports the communication with internal subscribers.

myAttendant provides the following features:

- Attendant functions
- Directories
- Journal
- Pop-up windows
- Presence status
- Record calls
- Message Center
- User Buttons
- Voice and Fax Messages
- Instant Messaging
- Team functions

---

### Related Topics

- [Prerequisites for UC PC Clients](#)

## 8.1.7 Prerequisites for UC PC Clients

In order to use UC PC clients, the client PC must be equipped with the appropriate hardware and software configurations. Depending on the configuration, administration rights are required for the installation and automatic updates. The available functionality depends on the licenses being used.



---

**INFO:** Please make sure that you refer to the notes in the ReadMe first.rtf file.

---

## Telephones

myPortal for Desktop, myAttendant and myPortal for Outlook can be used in combination with the following telephones:

- OpenStage HFA
- OpenStage T (HX)
- optiPoint 410 HFA
- optiPoint 420 HFA
- optiPoint 500 (HX)
- optiPoint WL2 professional HFA
- SIP Phone
- Analog telephone
- HiPath Cordless IP
- HiPath Cordless Office (HX)
- optiClient 130 HFA
- OpenScape Personal Edition HFA
- OpenScape Personal Edition SIP

---

**INFO:** For analog and DECT telephones, the Message Waiting Indication (MWI) is not supported, and only limited support is available for displaying information on the phone.

---

## Operating System

myPortal for Desktop, myAttendant, myPortal for Outlook and Fax Printer can be used in combination with the following web browsers:

- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows XP

Local administration rights on a client PC are required for the installation, but not for automatic updates. The Russian user interface of myPortal for Outlook requires a Russian Windows installation.

myPortal for Desktop can also be used with the following operating systems:

- Apple Mac OS X v10.7 Lion

## Windows Update

The PCs always need the current status of all available updates, including Service Packs.

### Web Browsers

myPortal for Desktop, myPortal for Outlook and Fax Printer can be used in combination with the following web browsers:

- Microsoft Internet Explorer Version 7
- Microsoft Internet Explorer Version 8 in compatibility mode
- Microsoft Internet Explorer Version 9
- Mozilla Firefox Version 4 or later

### Additional Software

Additional Software	myPortal for Desktop	myAttendant	myPortal for Outlook
Sun Java >= 1.6.x (see <b>Service Center &gt; Download Center</b> )	X	X	
Microsoft Office 2010 or Microsoft Office 2007(32 bit) with installed .NET components for Outlook or Microsoft Office 2003 (32 bit) Microsoft Office 365			X
Access to Microsoft Exchange Server (for Outlook contacts and appointments), including Exchange Server from Office 365	X		X
Microsoft .NET Framework >= 3.5			X

### Minimum Hardware Requirements

- 2 GHz CPU
- RAM: 2 GB  
(Microsoft Windows XP: 1 GB)  
(Microsoft Windows 2003 Server: 1 GB)
- 100 Mbps LAN
- XGA (1024x768) screen resolution, myPortal for Outlook: SVGA (800x600) screen resolution

### Microsoft Terminal Server, Citrix Server

myAttendant, myPortal for Desktop, myPortal for Outlook and Fax Printer can be used in Microsoft Terminal Server and Citrix Server environments under the following preconditions:

---

**INFO:** Terminal Server and Citrix Server environments, including hosted services and virtual environments are the responsibility of the customer.

---

Operating system:

- Microsoft Windows 2008 R2 Server (64 bit) with Citrix XenApp 6.0 Server (Desktop Mode)
- Microsoft Windows 2008 R2 Server (64 bit) with Citrix XenApp 5.0 Server (Desktop Mode)
- Microsoft Windows 2008 R2 Server (64 bit) as Microsoft Terminal Server
- Microsoft Windows 2008 Server as Microsoft Terminal Server
- Microsoft Windows 2003 Server as Microsoft Terminal Server

Office applications:

- Microsoft Office 2010
- Microsoft Office 2007 (32 bit)
- Microsoft Office 2003 (32 bit)

Hardware Prerequisites: The number of installable clients depends on the server performance and on the amount of available memory. If the server is also being used for other applications, their memory requirements must also be taken into account. More information on the configuration of Citrix XenApp Server can be found under:

[http://wiki.siemens-enterprise.com/wiki/OpenScape\\_Office](http://wiki.siemens-enterprise.com/wiki/OpenScape_Office)

### Installation Files

The following options are available for providing installation files to users:

- The administrator downloads the installation files from the **Download Center** and provides them to users via a network drive, for example.
- They can access the installation files directly via a network drive connected with \\<IP address of communication system>\applications (User: hooome, Password: hoomesw). The installation files are located in the install-common folder.

---

### Related Topics

- [myPortal for Desktop](#)
- [myPortal for Outlook](#)
- [Fax Printer](#)
- [myAttendant](#)
- [Silent installation/Uninstallation for UC PC Clients](#)
- [Automatic Updates](#)

## 8.1.8 Prerequisites for myPortal for Zimbra

In order to use myPortal for Zimbra, the client PC must be equipped with the appropriate hardware and software.

### Web Browsers

myPortal for Desktop, myPortal for Outlook and Fax Printer can be used in combination with the following web browsers:

- Microsoft Internet Explorer Version 8 in compatibility mode
- Microsoft Internet Explorer Version 9
- Mozilla Firefox Version 3 or later
- Safari 4 or later
- Chrome

### Zimbra

Access to the Zimbra Collaboration Suite is available via the Web Client.

### Web Services for Mobile Phones

Web services for mobile phones must be enabled in the system. The ports configured in the system must be open in the firewalls on the LAN and the client PCs.

## 8.1.9 Prerequisites for myPortal for OpenStage

In order to use myPortal for OpenStage, the phone must be equipped with the appropriate hardware and software.

### Telephones

myPortal for OpenStage can be used with the following telephones:

- OpenStage 60 V2 and later
- OpenStage 80 V2 and later

### Web Browsers

myPortal for OpenStage can be used in combination with the following web browsers (for configuration and administration):

- Microsoft Internet Explorer Version 7
- Microsoft Internet Explorer Version 8 in compatibility mode
- Mozilla Firefox Version 4 or later

---

### Related Topics

- [myPortal for OpenStage](#)

## 8.1.10 Silent installation/Uninstallation for UC PC Clients

Silent installation/uninstallation is a command-line based method to automatically install, uninstall or modify UC PC clients on a PC without requiring any further user inputs.

---

**INFO:** Please make sure that you refer to the notes in the ReadMe `first.rtf` file.

---

The silent installation/uninstallation option is available as of V3 and requires local administration rights on the relevant PC. The silent installation/uninstallation process can also be logged in a file.

The following parameters are available for silent installations / uninstallations:

Parameters	Components
ALL	<ul style="list-style-type: none"> <li>• myPortal for Desktop / myAttendant</li> <li>• myPortal for Outlook</li> <li>• Fax Printer</li> <li>• myAgent</li> <li>• Automatic Updates</li> </ul>
myPortal	myPortal for Desktop / myAttendant
OutlookIntegration	myPortal for Outlook
FaxPrinter	Fax Printer
myAgent	myAgent

---

### Related Topics

- [Prerequisites for UC PC Clients](#)

## 8.1.11 Automatic Updates

Automatic updates keep Windows applications (e.g., UC clients, Application Launcher) up to date.

If an application determines that there is a newer version than the one currently running, it is automatically updated. If required, a message that the application must be exited in order to to perform the automatic update appears.

---

### Related Topics

- [Prerequisites for UC PC Clients](#)

## 8.2 Presence Status and CallMe Service

The Presence status and CallMe service display and optimize the availability of subscribers. The Presence status enables simple status-based call forwarding as well as rule-based call forwarding, which can be flexibly configured with myPortal for Desktop or myPortal for Outlook.

### 8.2.1 Presence Status

The Presence status indicates the availability of internal subscribers (including Mobility Entry subscribers) in the Favorites list, the internal directory, the virtual conference room (not for OpenScape Office HX) and via voicemail announcements. In addition, the Presence status controls the availability of internal subscribers with status-based call forwarding, rule-based call forwarding and the personal AutoAttendant.

As a subscriber, you can change your Presence status in myPortal for Desktop and myPortal for Outlook or via the phone menu of the voicemail box. Deactivating call forwarding at the telephone returns you to the **Office** presence status. For every change in the Presence status (except for **Office** and **CallMe**), you also define the scheduled time of your return to the **Office** or **CallMe** status.

As a subscriber, you can select the following statuses:

- **Office**
- **Meeting**
- **Sick**
- **Break**
- **Out of the Office**
- **Vacation**
- **Lunch**
- **Gone Home**
- **Do Not Disturb**  
(not available for Mobility Entry or MULAP)

#### Mapping of the External XMPP Status Internally

Subscribers can see the presence status of external XMPP communication partners in the Favorites list or in the external directory, for example, provided XMPP has been configured. The following mappings apply (from left to right):

XMPP status	Represented as presence status
Online	Office
DND	Meeting
Away	Out of the Office
Extended Away	Vacation

---

**INFO:** Outlook contacts must include the XMPP ID in the IM address in accordance with the following pattern:  
xmpp:john.public@oso.example-for-a-domain.

---

### Mapping of the Internal Presence Status Externally

External XMPP communication partners can see the XMPP status of internal subscribers, provided XMPP has been configured. The following mappings apply (from left to right):

Presence status	Represented as XMPP status
Office	Online
Meeting	DND
Sick	Away
Break	Away
Out of the Office	Away
Lunch	Away
Gone Home	Away
Vacation	Extended Away

### Call Forwarding to the Voicemail Box

If Presence status of a subscriber is not **Office** or **CallMe**, the communication system redirects calls for him or her to the voicemail box by default and notifies the callers via status-based announcements about the nature of absence and the scheduled time for return.

### Info Text

You can enter any info text for your current presence status, e.g., "I am in Room No. ..." when attending a meeting. The info text is displayed in the Favorites list, in the internal directory and in the virtual conference room (not with OpenScape Office HX). The info text is deleted when you change your presence status.

### Automatic Reset of the Presence Status

As a subscriber, you can have your Presence status automatically reset to **Office** at the end of your scheduled absence. Otherwise, the system extends the current Presence status in increments of 15 minutes until you change it yourself.

### Visibility of your Presence Status

As a subscriber, you can specify for each subscriber in the internal directory whether or not that subscriber can see your Presence status other than **Office** and **CallMe** as well as the scheduled time of your return and any info text you may have entered.

### Automatic Update of Presence Status via Outlook Appointments (Windows)

As a subscriber, you can automatically control your Presence status via Outlook appointments by using the specific keywords in the Subject line: You can choose between the following calendars:

- Exchange calendar (on the Exchange Server)  
The automatic update of the presence status via Outlook appointments occurs independently, regardless of whether or not your PC is running. The administrator must configure the Exchange Calendar Integration for this function.

---

**INFO:** Appointments from a Microsoft Exchange Server 2003 that were created with Outlook Web Access are not visible for the system.

---

- Outlook calendar  
The automatic update of the presence status via Outlook appointments requires myPortal for Desktop or myPortal for Outlook to have been started on your PC.

You can use the following keywords:

- **Meeting**
- **Sick**
- **Break**
- **Out of the Office**
- **Vacation**
- **Lunch**
- **Gone Home**

The keywords depend on the language set for the user interface. The keywords may be located anywhere in the Subject line. If the Subject line contains more than one such keyword, only the first takes effect. When this function is enabled, your Presence status changes automatically at the start and end time of the relevant appointment.

---

**NOTICE:** When enabling this function, please bear in mind that any Outlook appointments with these keywords in the Subject line could lead to undesirable changes in your Presence status. Consequently, you may need to change the Subject line if needed.

---



### Automatic Creation of Outlook Appointments when Absent)

As a subscriber, you can have appropriate Outlook appointments created automatically when you are absent by a change in your Presence status. The Subject line of the corresponding Outlook appointment consists of your Presence status and the text "(Auto)", for example: "Meeting (Auto)". The start and end times for the appointment involved correspond to your entries in myPortal for Desktop or myPortal for Outlook. The end time of the Outlook appointment remains unchanged in the event of a possibly delayed return. You can define whether the Outlook appointments should be stored in the local PST file or on the Exchange server. If you are using a local PST file, your Outlook must be open when creating the Outlook appointments. If you are using a PST file on the Exchange server, the Outlook appointments are created, regardless of whether or not your Outlook is open. The administrator must configure the Exchange Calendar Integration for this function.

### Screen Pops on Changing the Presence Status

As a subscriber, you can have changes to your Presence status indicated by a screen pop.

---

#### Related Topics

- [CallMe Service](#)
- [Status-based call forwarding](#)
- [Rule-Based Call Forwarding](#)

## 8.2.2 CallMe Service

The CallMe service enables subscribers to define any phone at an alternative workplace as the CallMe destination at which they can be reached through their own internal phone numbers. The subscriber can use myPortal for Desktop or myPortal for Outlook at his or her alternative workplace exactly as in the office and thus also make outgoing calls from the CallMe destination.

### Inbound Calls

Inbound calls to the internal phone number are forwarded to the CallMe destination. The internal phone number of the called subscriber is displayed to the caller. Unanswered calls are forwarded to the voicemail box after 30 seconds.

### Outbound Calls

For outbound calls with myPortal for Desktop or myPortal for Outlook, the communication system sets up two connections. It first calls the subscriber at the CallMe destination. If the call is answered, the communication system then calls the desired destination and connects the subscriber with it. The internal phone number of the caller is displayed at the destination (One Number Service).

### Presence Status

When the CallMe service is enabled, the message "CallMe active" appears in the display of the relevant phone (not for analog and DECT phones). Other subscribers see the presence status **Office**.

### Activation

As a subscriber, you can activate the CallMe service manually. In addition, the Call-Me service is also reActivated by an automatic reset of the Presence status following an absence, provided it was active earlier. Then following types of CallMe destinations are not supported:

- Group
- Redirected telephone

### Displaying the CallMe Destination in the Favorites List

As a subscriber, you can have the number of your CallMe destination displayed in the Favorites list of other subscribers instead of your own phone number.

### Deactivation

The CallMe service remains active until your Presence status changes.

---

#### Related Topics

- [Presence Status](#)
- [Status-based call forwarding](#)
- [Rule-Based Call Forwarding](#)

## 8.2.3 Status-based call forwarding

Status-based call forwarding enables subscribers to forward calls based on their Presence status to one of their additional phone numbers or their voicemail box.

As a subscriber, you can configure status-based call forwarding for every presence status except **Office**, **CallMe** and **Do Not Disturb**. When you change your Presence status, the communication system activates call forwarding to the destination defined by you for this purpose. For example, if you are away from the office, to your mobile phone or if you are on vacation, to your representative.

---

#### Related Topics

- [Presence Status](#)
- [CallMe Service](#)
- [Rule-Based Call Forwarding](#)

## 8.2.4 Rule-Based Call Forwarding

Rules-based call forwarding enables subscribers to forward calls based on numerous conditions and exceptions even more flexibly than with status-based call forwarding.

In addition, rule-based call forwarding also supports:

- Any destinations
- Presence status **Office**, **CallMe** and **Do Not Disturb**

As a subscriber, you can define rules and activate or deactivate them at any time by using the Rules wizard. A rule can only be active if your phone has not been forwarded. Status-based call forwarding (except to the voicemail box) overrides rule-based call forwarding.

When a call forwarding rule is active, its name appears on the display of your telephone.

When an inbound call is received, the communication system checks the applicability of the active rule in accordance with its sequential order in the Rules wizard. Only the first applicable rule is executed. In this case, your phone will ring once, and the communication system will then forward your call to the defined destination.

You can define several types of conditions and exceptions (except when ...) in one rule. However, you cannot define a condition with an exception of the same type. For example, it is not possible to define a condition of the type "On certain weekdays" together with an exception of the type "Except on certain weekdays".

### Types of Conditions and Exceptions

- (except) for certain Presence status
- (except) from certain people (in the internal directory, external directory, personal directory or from any station number)
- (except) when transferred to you from certain people (in the internal directory, external directory, personal directory or from any station number)
- (except) from a certain type, i.e., **internal**, **external** or **Unknown Contact**
- (except) on a certain date (also on multiple dates)
- (except) on certain weekdays
- (except) between a certain Start and End date
- (except) between a certain Start and End time

---

### Related Topics

- [Presence Status](#)
- [CallMe Service](#)
- [Status-based call forwarding](#)

## **8.3 Directories and Journal**

Directories, the Favorites List and the Journal organize contacts and calls.

### **8.3.1 Directories**

Directories are used to organize the contacts of subscribers. Subscribers can access these contacts with myPortal for Desktop or myPortal for Outlook and via system phones with displays.

The system provides the following directories, which support the following functions:

Directory	myPortal for Desktop, my Attendant, Fax Printer	myPortal for Outlook	System telephone with a display
Outlook contacts	If required, the subscriber can import Outlook contacts on starting myPortal for Desktop when using Microsoft Windows.	Contains the personal contacts of a subscriber. Only the subscriber involved had write access to this data.	-
Personal directory	The subscriber can either import Outlook contacts on starting myPortal for Desktop or maintain personal contacts manually. Imported Outlook contacts cannot be edited.	-	-
Internal Directory	Contains all internal subscribers, possibly with additional phone numbers, provided the subscriber has made this information visible to other internal subscribers. Internal subscribers (with system telephones) are displayed with their Presence status and can be contacted through Instant Messaging. The Presence status of a subscriber can only be shown if allowed by that subscriber. If relevant, the scheduled time of return and any info text that may have been entered by the subscriber are also displayed. A subscriber is only provided read-access to this directory.		Contains all internal subscribers. The administrator can enable and disable the display of the internal directory for system telephones.
External directory	Contains contacts from a corporate directory and must be configured by the administrator. A subscriber is only provided read-access to this directory.		-
Public Exchange folder (not available with Exchange Server of Office 365)	Contains contacts of the public Exchange folder if configured by the administrator. These are shown in the external directory.		-
External Offline Directory (LDAP)	Contains contacts from the LDAP corporate directory and must be configured by the administrator. The external offline directory can only used for searches. The administrator can enable and disable the display of the external offline directory for system telephones.		
System Directory	-		Includes all internal stations and all central speed-dial numbers. The administrator can enable and disable the display of a subscriber in the system directory.

---

**INFO:** Phone numbers in directories should always be entered in canonical format.

---

### Simple Search

As a subscriber, you can search the directories by **First Name**, **Last Name** or a call number. The directories are searched in the order shown in the table above. The search can be conducted using whole words and also with partial search terms such as a part of a station number, for example. The set search options remain in effect for subsequent searches. All search terms used are saved. You can optionally delete the list of search terms used.

### Advanced Search

You can selectively search in the **Title, First Name, Last Name, Company, Extension, Company Ph., Business Ph. 1, Business Ph. 2, Home Ph. 1, Home Ph. 2, Mobile Number** and **E-mail** fields and limit the maximum number of hits. The modern interface of myPortal for Desktop does not support the advanced search.

### Sorting

The contacts of a myPortal for Desktop and myPortal for Outlook directory can be sorted by any column in ascending or descending alphanumeric order. The modern interface of myPortal for Desktop does not support sorting.

---

### Related Topics

- [System Directory](#)
- [Internal Directory](#)
- [External directory](#)
- [External Offline Directory \(LDAP\)](#)
- [OpenScape Office Directory Service](#)

## 8.3.2 Internal Directory

The internal directory contains the contact details of the internal subscribers of the communication system.

As a subscriber, you have read access to the contact details of other subscribers and write access to your own contact details with myPortal for Desktop, myPortal for Outlook and myAttendant. For your additional station numbers, you can define whether or not these numbers should be made visible in the internal directory. As an administrator, you have unrestricted access to all data in the internal directory. As a subscriber, you can dial from the internal directory.

The administrator can disable the display for all analog stations or for analog stations without an associated name. Subscribers whose names begin with - are not displayed in the latter case.

---

### Related Topics

- [Directories](#)
- [System Directory](#)
- [External directory](#)
- [External Offline Directory \(LDAP\)](#)
- [OpenScape Office Directory Service](#)

### 8.3.3 External directory

The external directory includes contacts from outside the communication system.

The data of the external directory is available to all subscribers in myPortal for Desktop, myPortal for Outlook, myPortal for Mobile, Fax Printer, myAttendant, myAgent and on phones equipped with a display. Subscribers can dial from the external directory. Users with myAttendant and myAgent can also edit data in the external directory.

#### Importing Data from a CSV File

As an administrator, you can import contacts from a CSV file in ANSI or ASCII format into the external directory.

A header in the CSV file allows the mapping of field names in the CSV file to fields in the system. A typical CSV file may be structured as follows:

- Header line:  
"Customer ID","Last Name","First Name","Company Phone Number","Company Name":
- Data line:  
"987654","Dubios","Natalie","+4989700798765","SEN"

You can map the data being imported from the CSV file to the following fields in the system:

- Customer ID
- Title
- First Name
- Last Name
- Company
- Business Ph.
- Business Ph2
- Mobile Ph.
- Home
- XMPP ID
- Fax Ph.
- E-mail
- City

If you want the import to overwrite data, the corresponding **Customer IDs** should be identical.

---

#### Related Topics

- [Directories](#)
- [System Directory](#)
- [Internal Directory](#)
- [External Offline Directory \(LDAP\)](#)

- [OpenScape Office Directory Service](#)

### 8.3.4 External Offline Directory (LDAP)

The external offline directory (LDAP) contains contacts from an LDAP server for myPortal for Desktop, myAgent, Fax Printer, myPortal for Outlook and for system telephones with displays.

The system supports LDAP Version 2 with authentication.

LDAP (Lightweight Directory Access Protocol) is a TCP/IP-based directory access protocol for accessing network directory services. LDAP has a unique format world-wide in which all names can be represented. It provides for different layouts and enables unique associations between names and their internal representation. This data is defined by the administrator together with the IT administrator of the customer when planning and setting up a project. LDAP can be used under the MS Windows and Linux operating systems.

In a Microsoft environment, the Active Directory Server (ADS) or the Exchange Server also serves as the LDAP server. Under Microsoft Windows, user data can be administered with the Active Directory (AD) application or ESTOS Metadir, for example. The administration of this data is generally performed by the IT administrator of the customer.

Under Linux, the user data can be administered with OpenLDAP, for example.

Setting up an LDAP directory service can be simplified with an LDAP browser (e.g., the freeware from Softerra).

Phone numbers on the LDAP server may only include "-" and blanks as delimiters. Other delimiters cannot be filtered out by the system.

As an administrator, you can adapt the mapping of fields to the names of the used LDAP server during the configuration of an external offline directory. Deleted fields are ignored when searching for names via phone numbers. The search always occurs with the last 4 positions of the phone number preceded by a wildcard. You can deactivate the search for names via phone numbers for incoming calls.

If the default port 389 is already being used, some other port must be configured

---

**INFO:** More detailed information can be found on the Internet under: [http://wiki.siemens-enterprise.com/wiki/OpenScape\\_Office\\_Interaction\\_with\\_3rd\\_Party\\_Applications](http://wiki.siemens-enterprise.com/wiki/OpenScape_Office_Interaction_with_3rd_Party_Applications).

---

The data of the external directory is available to subscribers in myPortal for Desktop, myAttendant, Fax Printer and myPortal for Outlook during the search.



### System Telephones with Displays

As a subscriber, you can select between the internal directory and the LDAP directory via the menu., provided these have been configured for system telephones. The LDAP directory supports searches in the appropriate contacts and the subsequent calling of a contact.

The name information provided by the LDAP server is not displayed in ringing or call status. The call numbers for incoming calls are also not replaced by the name information provided by the LDAP server (as when call numbers are replaced by SSD names).

A system subscriber can only be reached from the LDAP directory if a DID number was configured for him or her and if this entry corresponds to the entry in the LDAP database. Call numbers provided by the LDAP server can only be routed within the network if the internal call number and the DID number are identical.

---

#### Related Topics

- [Directories](#)
- [System Directory](#)
- [Internal Directory](#)
- [External directory](#)
- [OpenScape Office Directory Service](#)

## 8.3.5 System Directory

The system directory contains all internal stations and every central speed-dial number for which a name was assigned. System telephones with a display can access the system directory.

The administrator individually disable the display for every subscriber and every speed-dial number with a name.

---

#### Related Topics

- [Directories](#)
- [Internal Directory](#)
- [External directory](#)
- [External Offline Directory \(LDAP\)](#)
- [OpenScape Office Directory Service](#)

## 8.3.6 Departments

Departments classify subscribers in the internal directory into groups based on their organizational affiliation. The internal directory allows you to search and sort by department.

## 8.3.7 OpenScape Office Directory Service

OpenScape Office Directory Service is an open, integrated metadirectory service that can be accessed by several different types of clients, applications and communication devices in a company. The OpenScape Office Directory Service performs two functions: it enables additional contact data from external databases to be integrated in the directories of the system, while also making the directories available to clients, communication devices and applications.

OpenScape Office Directory Service runs as a separate service based on OpenLDAP. Firewalls must be open for port 389. OpenScape Office Directory Service is disabled by default.

### Internal Data Sources

The following data sources are available by default in the OpenScape Office Directory Service:

- OpenScape Office: This includes
  - internal directory
  - external directory
- central speed-dial numbers

For these data sources, the field names are permanently mapped to the data schema of the OpenScape Office Directory Service.

These data sources cannot be deleted or modified.

### External Data Sources

As an administrator, you can integrate contact information from the following types of databases as data sources for read-only access via ODBC.

- Microsoft SQL Server
- mySQL
- PostgreSQL
- Sybase SQL Server

Maximum number of different types of databases: 4

Maximum number of external data sources: 10

Make sure that the OpenScape Office Directory Service is authorized to access the external database. Contact the responsible database administrator in advance to ensure that this is the case. A separate user may need to be added in the external database for access by the system.

External data sources can be used in the context of both directory searches and the resolution of call numbers into names.

You can configure direct access to a database table from an external data source or a custom SQL query for the data source.

### Custom SQL Queries for External Data Sources

Custom SQL queries also support related tables, e.g.:

```
SELECT * FROM users LEFT OUTER JOIN phonenumbers ON users.id  
= phonenumbers.uid;
```

The data structure must be of the type 1:1 or n:1, i.e., each record can have only a single row.

Access via custom SQL queries can sometimes run much slower than direct access to a database table.

Custom SQL queries with potential security risks are not executed, for example:

- Modifying data
- Stopping the SQL server
- Running programs via the SQL server
- Changing user rights

Custom SQL queries with the following SQL commands are therefore not executed:

- CHECKPOINT
- CLOSE
- CLUSTER
- COMMIT
- COPY
- CREATE
- DEALLOCTAE
- DECLARE
- DELETE
- DISCARD
- DO
- DROP
- END
- EXECUTE
- EXPLAIN
- FETCH
- GRANT
- INSERT
- LOAD
- LOCK
- MOVE
- PREPARE
- REASSIGN OWNED
- REINDEX
- RELEASE SAVEPOINT
- RESET

- REVOKE
- SAVEPOINT
- SECURITY LABEL
- SELECT INTO
- SET
- SHOW
- START TRANSACTION
- TRUNCATE
- UNLISTEN
- UPDATE
- VACUUM
- VALUES

### Field Mapping for Data Sources

For these data sources, you can customize the mapping of field names to the data schema of the OpenScape Office Directory Service. You can assign each field in the data schema of the OpenScape Office Directory Service to no more than one field of the external data source. However, you can assign a field of the external data source to multiple fields in the data schema of the OpenScape Office Directory Service.

### LDAP Data Output Mappings

An LDAP data output mapping determines which of the fields in the data schema of the OpenScape Office Directory Service are to be output via LDAP, e.g., for specific LDAP clients or for different groups of subscribers who do not want to see all the details, but only a defined subset.

The LDAP data output mapping **web** is available by default and cannot be deleted or changed. All fields of the data schema in the OpenScape Office Directory Service are permanently assigned to the LDAP output in it. You can also configure other LDAP data output mappings.

LDAP clients can access a specific LDAP data output mapping via the `dc` parameter in the LDAP login, for example: `dc=web`.

### Normalization of Phone Numbers in the Canonical Format

For each data source, you can configure the normalization of phone numbers in the canonical format. During this process, blanks, parentheses, hyphens and commas are removed. This is required to correctly identify the caller's name and for desktop dialing. You should not skip the normalization, unless the phone numbers used in the data source are already present in canonical format. You can have the normalization-related values `s` such as the area code, etc., entered automatically from the system. If the external database is located at a different site than the system, you may need to adjust these values.

### Status of Data Sources

The status display under **OpenDirectory > Data Sources** has the following significance:

Color	Status
green	active
red	ODBC and LDAP is not OK, wrong configuration or data source unavailable
yellow	LDAP not ok: restart the OpenScape Office Directory Service
gray	Configuration incomplete

### Provision of directories

The following types of clients, communication devices and applications can use the directories provided by the OpenScape Office Directory Service: UC

- Clients
- System Directory
- OpenStage with local LDAP support
- DECT IP phones (via LDAP)
- SIP phones (via LDAP)
- Applications, e.g., CRM Suites such as Microsoft Dynamics CRM (via LDAP, ODBC or OpenLDAP CSV export)

OpenScape Office Directory Service can identify in the search results from which data source a hit is obtained.

---

### Related Topics

- [Directories](#)
- [System Directory](#)
- [Internal Directory](#)
- [External directory](#)
- [External Offline Directory \(LDAP\)](#)

## 8.3.8 Favorites List

The Favorites list provides you (as a subscriber) with a constant view of selected contacts. These contacts can also be called very easily directly from the Favorites list. All internal subscribers with system telephones and external XMPP communication partners are shown together with their Presence status and can be contacted via instant messaging.

As a subscriber, you can add contacts from all directories to the Favorites list. For favorites that do not come from the internal directory, instead of the symbol for the Presence status, the symbol for the source of the contact is displayed.

The Favorites list manages contacts in groups. The contacts in all groups can be sorted by First Name, Last Name or their original sorting order.

When an internal subscriber is absent, you can determine the scheduled time of his or her return by positioning the mouse pointer over the entry for that subscriber, provided the subscriber has allowed his or her Presence status to be visible to you.

For favorites with multiple phone numbers, you can specify a default number with which the contact is to be called. The default phone number of a favorite can be determined in the context menu from the symbol with the activated check box.

## 8.3.9 Journal

The journal is the list of all incoming and outgoing calls of a subscriber. It enables subscribers to quickly and easily respond to missed calls and call back their contacts or call them again directly from within the journal.

### Folder for Call Types

The calls are arranged in the following groups:

- **Open**

Contains the unanswered missed calls for which a call number was transmitted. As soon as one of these calls is answered, all associated entries with that call number are dropped from the list.

- **All calls**

- **Missed**

- **Answered**

- **Internal**

- **External**

- **Inbound**

- **Outbound**

- **Scheduled**

Contains all the calls that you (as a subscriber) have scheduled for specific dates/times. The Scheduled Calls feature is not available to Contact Center agents. In order for the communication system to execute a scheduled call, myPortal for Desktop or myPortal for Outlook must be open at the scheduled time; your presence status must be **Office** or **CallMe**, and you must confirm the execution of the call in a dialog. If you are busy at the time the scheduled call is to be made, the system defers the scheduled call until you are free again. myPortal for Desktop or myPortal for Outlook informs you of any pending scheduled calls on exiting the program. On starting the application, myPortal for Desktop or myPortal for Outlook notifies you about any scheduled calls for which the scheduled time has elapsed. You can then either delete such calls or save them with a new scheduled time.

Not all folders for call types are available in the modern user interface myPortal for Desktop.

### Retention Period

The system saves a record of the calls in the Journal for a maximum period of time, which can be configured by the administrator. As a subscriber, you can reduce this time. After the retention period expires, the system automatically deletes all associated entries.

---

**INFO:** The retention period also determines the maximum time period for evaluations with myReports.

---

### Grouped by time period

The calls in each group are arranged by time, e.g.: Today, Yesterday, etc., Last Week, Last Month and Older. Your administrator can set the duration for which calls should be saved in the Journal. After this set time period expires, the entries are automatically deleted. The grouping by time period is not available in the modern user interface of myPortal for Desktop.

### Call Details

Every call is shown with the Date and Time and, if available, with the call number. If a directory contains further details on the call number such as the **Last Name**, **First Name** and **Company**, then this information is also shown. In addition, the **Direction**, **Duration** and **Call Complete** columns are also displayed in most folders. Not all call details are available in the modern user interface of myPortal for desktop.

### Sorting

You can sort the calls in the Journal by any column in ascending or descending alphanumeric order.

You can jump within the Journal to the first call whose entry begins with a specific character in the sorted column, e.g., to the first Last Name beginning with "P". By entering subsequent characters, you can then narrow the search. Sorting is not available in the modern user interface of myPortal for Desktop.

### Export

As a subscriber, you can export the journal as a CSV file using myPortal for Desktop or myPortal for Outlook:

## 8.4 Calls

For calls, convenient features such as a desktop dialer, screen pops and the option to record calls and conferences (LX/MX) are available to subscribers.

## 8.4.1 Call Number Formats

Call numbers can be specified in different formats.

Format	Description	Example
Canonical	Begins with + and always includes the country code, area code and the full remaining station number. Blanks and the special characters + ( ) / - : ; are allowed.	+49 (89) 7007-98765
Dialable	Exactly as you would dial the call number on the phone, always with the trunk access code.	<ul style="list-style-type: none"><li>• 321 (internal)</li><li>• 0700798765 (own local network)</li><li>• 0089700798765 (external local network)</li><li>• 0004989700798765 (international)</li></ul>

---

**INFO:** If possible, you should always use the canonical call number format. This ensures that a phone number is always complete, unique and consistent in any situation, even in a network.

---

When dialing an external station (dialable format) manually, the CO access code must always be dialed as well. The CO access code must likewise also be specified when manually entering the destination number for the CallMe service.

When dialing an external phone number in dialable format from a directory and when using the Desktop Dialer, the communication system automatically adds the CO access code (route 1). The automatic addition of the CO access code also occurs when you select a phone number of your own personal data (**Mobile number, Private Number, External Number 1, External Number 2**, etc.) as a destination number for the CallMe service.

---

**INFO:** For calls within the USA via CSTA to a number in canonical format, phone numbers are converted to the dialable format.

---

## 8.4.2 Desktop Dialer

Desktop Dialer enables users with myPortal for Desktop (Windows) or myPortal for Outlook to call a marked destination via a key combination from many Windows applications, e.g., from an Outlook e-mail.

Depending on the type of string used, the Desktop Dialer works as follows:

- A phone number in dialable or canonical format is dialed directly.
- A string containing letters is searched in the directories as a first name or company.



Windows applications that were implemented with standard Windows-compliant components usually support the Desktop Dialer, but 16-bit applications do not.

### 8.4.3 Screen pops

Screen pops in myPortal for Desktop and myPortal for Outlook offer you convenient ways to respond to incoming calls or new voicemails with a single mouse click, for example.

Some buttons in the screen pops change, depending on the situation.

Screen pops for calls show the caller's phone number and name (if the name details are available in a directory). The directories are searched in a specific order: The first hit, if found, appears in the screen pop.

As a subscriber, you can activate or deactivate the following screen pops (also called pop-up windows or tray pops):

Screen pops	myPortal for Desktop	myPortal for Outlook
Inbound call	x	x
Outbound call	x	-
New voicemail	x	x
New fax message	x	x
Change of own Presence status	x	-
Open personal contact on incoming call	x	
Opening Outlook Contacts for Incoming Calls		x

### 8.4.4 Record calls

A subscriber can record calls. Recorded calls appear in the voicemail box.

---

**INFO:** Note that in most countries you are legally required to notify the other party that you are recording the call. In some countries (such as France, for example), the other party is automatically notified by the system.

---

As an administrator, you can allow or prevent the recording of calls and conferences (LX/MX) on a system-wide basis. In addition, you can optionally configure the playback of an announcement or warning tone at the start of the recording.

As a subscriber, you can control the recording of calls via myPortal for Desktop or myPortal for Outlook. Recorded calls are identified in the voicemail box with a red dot and show the call number of the other party if available.

Ongoing recordings are automatically stopped by a consultation hold, placing a call on hold, transfers and the initiation of a conference.

## 8.5 Conferences

In a conference, multiple participants (including external parties) can communicate with one another at the same time.

### 8.5.1 Conference Management (LX/MX)

Conference management enables subscribers to use different types of conferences.

#### Types of Conferences

The different types of conferences offer the following features:

	Ad-hoc	Scheduled	Permanent	Open
Usage	<ul style="list-style-type: none"> <li>Phone-controlled</li> <li>Application-controlled</li> </ul>	<ul style="list-style-type: none"> <li>Application-controlled</li> </ul>	<ul style="list-style-type: none"> <li>Application-controlled</li> </ul>	<ul style="list-style-type: none"> <li>Application-controlled</li> </ul>
Start	<ul style="list-style-type: none"> <li>Manually</li> </ul>	<ul style="list-style-type: none"> <li>Scheduled</li> </ul>	<ul style="list-style-type: none"> <li>Manually</li> </ul>	<ul style="list-style-type: none"> <li>Manually</li> </ul>
End	<ul style="list-style-type: none"> <li>Manually</li> </ul>	<ul style="list-style-type: none"> <li>Scheduled</li> <li>Manually</li> </ul>	<ul style="list-style-type: none"> <li>Manually</li> </ul>	<ul style="list-style-type: none"> <li>Manually</li> </ul>
Duration of the reservation of conference channels	<ul style="list-style-type: none"> <li>1 hour by default</li> </ul>	<ul style="list-style-type: none"> <li>Scheduled</li> </ul>	<ul style="list-style-type: none"> <li>Until the deactivation or deletion of the conference</li> </ul>	<ul style="list-style-type: none"> <li>Until the deactivation or deletion of the conference</li> </ul>
Extension	x	x	-	-
Recurrence	<ul style="list-style-type: none"> <li>Manually</li> </ul>	<ul style="list-style-type: none"> <li>Scheduled</li> </ul>	-	-
Direction of connection setup from the viewpoint of OpenScape Office	<ul style="list-style-type: none"> <li>Outbound</li> </ul>	<ul style="list-style-type: none"> <li>Outbound</li> <li>Inbound</li> </ul>	<ul style="list-style-type: none"> <li>Inbound</li> </ul>	<ul style="list-style-type: none"> <li>Inbound</li> </ul>
Set of participants	<ul style="list-style-type: none"> <li>Fixed</li> </ul>	<ul style="list-style-type: none"> <li>Fixed</li> </ul>	<ul style="list-style-type: none"> <li>Fixed</li> </ul>	<ul style="list-style-type: none"> <li>Open</li> </ul>
Authentication of conference participants	-	<ul style="list-style-type: none"> <li>Individual conference ID (optional)</li> <li>Password (optional)</li> </ul>	<ul style="list-style-type: none"> <li>Individual conference ID (optional)</li> <li>Password (optional)</li> </ul>	<ul style="list-style-type: none"> <li>Shared conference ID (optional)</li> </ul>

	Ad-hoc	Scheduled	Permanent	Open
Recording, if enabled in OpenScape Office	<ul style="list-style-type: none"> <li>Manually (On Demand Conference Recording)</li> </ul>	<ul style="list-style-type: none"> <li>Automatically (Auto Conference Recording)</li> <li>Manually (On Demand Conference Recording)</li> </ul>	<ul style="list-style-type: none"> <li>Automatically (Auto Conference Recording)</li> <li>Manually (On Demand Conference Recording)</li> </ul>	<ul style="list-style-type: none"> <li>Automatically (Auto Conference Recording)</li> <li>Manually (On Demand Conference Recording)</li> </ul>
Invitation by E-mail with:	<ul style="list-style-type: none"> <li>Conference Name</li> <li>Link for Web Collaboration session</li> </ul>	<ul style="list-style-type: none"> <li>Conference Name</li> <li>Dial-in number</li> <li>Conference ID</li> <li>Password</li> <li>Date and time of the start and end of the conference</li> <li>Link for Web Collaboration session</li> </ul>	<ul style="list-style-type: none"> <li>Conference Name</li> <li>Dial-in number</li> <li>Conference ID</li> <li>Password</li> <li>Link for Web Collaboration session</li> </ul>	<ul style="list-style-type: none"> <li>Conference Name</li> <li>Dial-in number</li> <li>Conference ID</li> <li>Password</li> </ul>
Outlook appointment as an e-mail attachment (.ics)	-	x	-	-

### Application-controlled conference

As a subscriber, you can initiate, control and manage a conference with the Conference Management feature of myPortal for Desktop or myPortal for Outlook.

### Phone-controlled Conference

As a subscriber, you can initiate a phone-controlled conference and then control it via the phone by the following methods:

- Call the desired conference participant and connect him or her to the conference
- Extend a consultation call into a conference
- Extend a second call into a conference

### Virtual conference room

The virtual conference room enables you to follow a conference and its participants in a graphical environment (for application-controlled conferences) and to also manage the conference if you are the conference controller. The virtual conference room shows the phone number, name and presence status to the conference participants, where available.

### Dial-in number

As an administrator, you can change the conference dial-in numbers that were set up during basic installation. As a subscriber, you can display the dial-in number for a conference.

### **Conference Controller**

The initiator of the conference is automatically the conference controller until this is explicitly changed. Depending on the type of conference, the controller can:

- Add or remove conference participants (for application-controlled conferences):  
Removed participants do not remain in the conference.
- Disconnect or reconnect conference participants:  
Disconnected participants remain in the conference. When the conference controller is connecting a conference participant, all other conference participants remain connected to one another. If there is only one participant connected, that participant will hear music on hold.
- Record a conference  
Recorded conferences are identified in the voicemail box with a red dot and show the call number of the first conference participant, if available. Conferences in which a participant is on hold cannot be recorded.
- Set another internal participant on the same node as the conference controller
- Extend the conference
- Leave the conference without ending it:  
The longest attending internal participant of the conference automatically becomes the conference controller.
- End the conference

### **Conference Participants**

Conference participants can leave the conference and optionally dial-into it again (scheduled and permanent conferences). As long as a conference has only one participant, the participant hears music on hold. As an administrator, you can specify whether multiple external conference participants are allowed. The maximum number of external conference participants is determined, among other things, by the number of available trunks.

### **Conference Tone**

When connecting or disconnecting a conference participant, the other participants hear the conference tone. As an administrator, you can activate or deactivate the conference tone.

### **Automatic Termination without a Conference Controller**

If there are only external subscribers left in a conference, the participants will hear an alert tone after a specified time period. Following a further timeout, the conference is automatically terminated by OpenScape Office. As an administrator, you can edit these time values.

### **Notification by E-mail and Outlook Appointment**

OpenScape Office can automatically notify conference participants by e-mail and, for scheduled conferences, additionally through an Outlook appointment as an attachment (.ics).

Event	Notified conference participants	Outlook appointment
New conference	All	Automatic creation
Delete the conference		Automatic deletion
Reschedule the conference		Automatic update
Adding conference participants	Those affected	Automatic creation (those affected)
Remove conference participants		Automatic deletion (those affected)

This requires the administrator to have configured the sending of e-mails. In addition, an internal conference participant must have specified his or her e-mail address. For external conference participants, the initiator of the conference must enter their individual e-mail addresses.

---

**INFO:** For e-mail notifications, no return acknowledgments are obtained for failed deliveries or absence messages, since the e-mails are sent directly from OpenScape Office due to the integration of Web Collaboration.

When using Microsoft Office 365, e-mails can only be sent to Microsoft Office 365 accounts.

---

### Further Calls

While participating in a conference, making a call or accepting another call disconnects the participant from the conference.

### Park, Toggle/Connect

The Park and Toggle/Connect features are not available in a conference.

### Call Charges

Toll charges are assigned to the party who set up the toll call. When a conference is transferred to another conference controller, all further charges are assigned to that controller.

### System Load

As an administrator, you can display both active and saved conferences.

---

**INFO:** Permanent conferences occupy system resources permanently. Since every subscriber can configure permanent conferences with myPortal for Desktop or myPortal for Outlook, you should, as the administrator, review the saved conferences regularly to avoid resource bottlenecks.

---

### Video Monitoring

Any ongoing video transmission, e.g., with OpenScape Personal Edition, must be terminated before participating in a conference.

---

#### Related Topics

- [Ad-hoc Conference \(LX/MX\)](#)
- [Scheduled Conference \(LX/MX\)](#)
- [Permanent Conference \(LX/MX\)](#)
- [Open Conference \(LX/MX\)](#)
- [Web Collaboration Integration](#)
- [Configuration Limits and Capacities](#)

## 8.5.2 Ad-hoc Conference (LX/MX)

An ad-hoc conference occurs spontaneously and is started manually by the conference controller. The conference controller can save ad-hoc conferences in order to set them up again at some later point in time.

### Starting the Conference

The system opens the window with the virtual conference room automatically for all internal conference participants, provided they have started myPortal for Desktop with the classic user interface or myPortal for Outlook. The system calls all conference participants simultaneously. On joining the conference, each conference participant hears a greeting announcement with the name of the conference controller.

### Recording the Conference

Conference controllers can record a conference manually for themselves or for all connected internal conference participants, provided the live recording of calls has been activated in the system. Participants located in the own node receive the recording of the voicemail box; participants in other nodes, via e-mail. The duration of the recording is only limited by the available storage capacity of the system.

### Ending the Conference

The conference controller can end the conference in the client or simply hang up. Alternatively, the conference ends when all conference participants have left the conference.

---

#### Related Topics

- [Conference Management \(LX/MX\)](#)
- [Scheduled Conference \(LX/MX\)](#)
- [Permanent Conference \(LX/MX\)](#)

- [Open Conference \(LX/MX\)](#)
- [Web Collaboration Integration](#)

### 8.5.3 Scheduled Conference (LX/MX)

A scheduled conference (Meet-Me conference) occurs at a pre-defined point in the future with a defined duration and may be set up to recur repeatedly at the same time.

A scheduled conference will run for the entire scheduled duration even if there are no connected participants. The conference controller saves a scheduled conference under a specified name.

#### Options for Configuring a Scheduled Conference

The initiator of the conference can define the following properties:

- Start time and End time
- Recurring conference
- Presence of conference controller required
- Authentication of conference participants on joining the conference required (by entering a conference ID and password via the phone keypad).

---

**INFO:** Mobility Entry users must enter the code for DTMF suffix dialing before their authentication.

---

The default password for conferences is 123456. The conference controller can change this for the conference participants individually.

- Language of announcements before the conference begins
- Direction for the connection setup for each conference participant (default: **outbound**).

#### Starting the Conference

The system opens the window with the virtual conference room at the scheduled time automatically for all internal conference participants, provided they have started myPortal for Desktop with the classic user interface or myPortal for Outlook. If the presence of the conference controller is required, the system first calls the controller. After the successful authentication of the controller, all the other conference participants are called simultaneously. Conference participants who have forwarded their calls to their voicemail boxes or who are determined to be absent by their presence status are not called. Depending on how the connection setup has been configured, the system calls the conference participants or the participants can dial in themselves. The system

announces every participant who joins the conference by name, as in: ". . . has joined the conference", provided the initiator has recorded his or her name announcement.

---

**INFO:** Conference participants of a scheduled conference without authentication can only hear the announcement with the name of the conference controller at the start of the conference, provided they have already initiated a conference with authentication earlier on one occasion.

---

### Dialing In

Every conference participant can use the dial-in number to dial into the conference within the scheduled time period, regardless of which direction for the conference setup was set for that participant. Attempts to dial into the conference outside the scheduled time period result in a corresponding announcement. To dial in via an ITSP, the ITSP must support RFC 2833 (DTMF characters).

### Forcing Authentication with the Star (\*) Key

The conference controller can set the conference so that each conference participant is forced to provide authentication by at least by pressing the \* key. This ensures that only the participants who are actually present are connected to the conference, as opposed to a voicemail box, for example.

### Extending the Conference

Ten minutes before the scheduled end of the conference, the participants hear an announcement indicating that the conference is about to end and are offered the option of extending the conference by dialing a specific digit. Any conference participant can extend the conference by dialing that specific digit. The conference controller can extend the conference in myPortal for Outlook at any time.

### Recording the Conference

Conference controllers can record a conference automatically or manually for themselves or for all connected internal conference participants, provided the live recording of calls has been activated in the system. Participants located in the own node receive the recording of the voicemail box; participants in other nodes, via e-mail. The duration of the recording is only limited by the available storage capacity of the system.

### Ending the Conference

The conference ends at the time scheduled for the end of the conference or if the conference controller terminates the conference.

---

### Related Topics

- [Conference Management \(LX/MX\)](#)
- [Ad-hoc Conference \(LX/MX\)](#)



- [Permanent Conference \(LX/MX\)](#)
- [Open Conference \(LX/MX\)](#)
- [Web Collaboration Integration](#)

## 8.5.4 Permanent Conference (LX/MX)

A permanent conference is not subject to time restrictions. The conference participants can dial in at any time.

The conference controller saves a permanent conference under a specified name. The conference is retained until it is explicitly deleted.

### Options for Configuring a Scheduled Conference

The initiator of the conference can specify:

- whether the conference participants need to authenticate themselves by entering a conference ID and password via the phone keypad when joining the conference.

---

**INFO:** Mobility Entry users must enter the code for DTMF suffix dialing before their authentication.

---

The default password for conferences is 123456. The conference controller can change this for the conference participants individually.

- in which language the announcements before the start of then conference are to be made.

### Starting the Conference

As soon as the first conference participant dials in, the system opens the window with the virtual conference room automatically for all internal conference participants, provided they have started myPortal for Desktop or myPortal for Outlook. All conference participants dial in themselves. The system announces every participant who joins the conference, as in: "... has joined the conference."

### Dialing In

Every conference participant can use the dial-in number to dial into the conference at any time. To dial in via an ITSP, the ITSP must support RFC 2833 (DTMF characters).

### Recording the Conference

Conference controllers can record a conference automatically or manually for themselves or for all connected internal conference participants, provided the live recording of calls has been activated in OpenScape Office. Participants located in the own node receive the recording of the voicemail box; participants in other nodes, via e-mail. The duration of the recording is only limited by the available storage capacity of OpenScape Office.

---

### Related Topics

- [Conference Management \(LX/MX\)](#)
- [Ad-hoc Conference \(LX/MX\)](#)
- [Scheduled Conference \(LX/MX\)](#)
- [Open Conference \(LX/MX\)](#)
- [Web Collaboration Integration](#)

## 8.5.5 Open Conference (LX/MX)

Open conferences are intended for a fixed number of arbitrary participants. Any participant who has the requisite access data can dial into them.

The conference controller saves an open conference under a specified name. The conference is retained until it is explicitly deleted.

### Options for Configuring an Open Conference

The initiator of the conference can specify:

- The number of conference participants (max. 16).
- whether the conference participants need to authenticate themselves by entering a conference ID and password via the phone keypad when joining the conference.

---

**INFO:** Mobility Entry users must enter the code for DTMF suffix dialing before their authentication.

---

The default password for conferences is 123456. The conference controller can change this for the conference participants individually.

- what common conference ID is valid for all conference participants.
- in which language the announcements before the start of then conference are to be made.

### Starting the Conference

All conference participants dial in themselves. The system announces every internal participant who joins the conference, as in: "... has joined the conference."

### Dialing In

Every conference participant can use the dial-in number to dial into the conference at any time. To dial in via an ITSP, the ITSP must support RFC 2833 (DTMF characters).

### Recording the Conference

Conference controllers can record a conference automatically or manually for themselves or for all connected internal conference participants, provided the live recording of calls has been activated in the system. Participants located in the own node receive the recording of the voicemail box; participants in other nodes, via e-mail. The duration of the recording is only limited by the available storage capacity of the system.

---

#### Related Topics

- [Conference Management \(LX/MX\)](#)
- [Ad-hoc Conference \(LX/MX\)](#)
- [Scheduled Conference \(LX/MX\)](#)
- [Permanent Conference \(LX/MX\)](#)

## 8.5.6 Web Collaboration Integration

Together with myPortal for Desktop (Windows) and myPortal for Outlook, the system also supports the convenient integration of the separate product OpenScape Web Collaboration for simultaneous multi-media collaboration during phone calls as well as phone-controlled and application-controlled (LX/MX) teleconferences. This gives you quick access to functions such as desktop and application sharing, file sharing, co-browsing, whiteboarding, URL Push, IM chat and video chat with multiple participants.

#### Supported Types of Connections

The Web Collaboration integration supports phone calls as well as the following types of application-controlled phone conferences of the system:

- Ad-hoc conference (LX/MX)
- Scheduled conference (LX/MX)
- Permanent conference (LX/MX)

On initiating or configuring a telephone conference, the conference controller can start one Web Collaboration session for simultaneous use with the same participants. On rescheduling, deleting or ending a conference call, the related Web Collaboration session is also rescheduled or deleted automatically.

#### FastViewer

Web Collaboration includes FastViewer as a client. No local installation of FastViewer is required. More information can be found in the Web Collaboration product documentation.

#### Connecting to the Web Collaboration Session (LX / MX)

Internal conference participants with UC PC clients are automatically connected to the appropriate Web Collaboration session on starting the conference. To do this, FastViewer is automatically downloaded and opened in the background,

which may take several seconds. External conference participants with known e-mail addresses receive an e-mail with an appropriate link to the Web Collaboration session.

---

**INFO:** Users of a Mac OS must copy the link for the Web Collaboration session into the web browser.

---

For a scheduled conference, it is possible to connect to the Web Collaboration session as early as 5 minutes before the start of the scheduled conference.

### **Conference ID and Password (LX/MX)**

The conference ID and password for a Web Collaboration session are identical to the conference ID and password of the associated phone conference.

### **Instant Messaging and Web Collaboration**

Note that Instant Messaging of the system and Instant Messaging of a Web Collaboration session are mutually independent, i.e.: the instant messages from a UC client do not appear in a Web Collaboration session of the same participant, and vice versa.

---

### **Related Topics**

- [Conference Management \(LX/MX\)](#)
- [Ad-hoc Conference \(LX/MX\)](#)
- [Scheduled Conference \(LX/MX\)](#)
- [Permanent Conference \(LX/MX\)](#)

## **8.6 Voice and Fax Messages**

The Voicemail and Fax services integrated in the system (not for OpenScape Office HX) enable subscribers to receive and manage voicemails and fax messages via myPortal for Desktop and myPortal for Outlook. Fax messages can be sent by subscribers using Fax Printer.

### **8.6.1 Voicemail Box**

The voicemail box records central voicemail and recorded calls. Subscribers can access it via myPortal for Desktop and myPortal for Outlook.

Only voice messages longer than two seconds are recorded.

## Managing Voicemail Messages

As a subscriber, you can listen to your voicemails:

- via a PC with myPortal for Desktop or myPortal for Outlook
- via your phone if your Presence status is **Office** or **CallMe**
- via any external telephone

Using myAttendant, the Attendant can also listen to voicemails of other subscribers who have explicitly allowed this.

The subscriber uses folders such as Inbox, Played, Saved or Deleted to manage incoming voicemail messages.

Voice messages can also be played back, paused and forwarded to another subscriber. The subscriber can also save voicemail messages in .wav format and redirect them to any selected e-mail account. When listening to a voicemail, the subscriber can directly call back the person who left a message.

The voicemail box can also be used by subscribers to manage recorded calls. Recorded calls are identified in the voicemail box by an appropriate symbol.

## Retention Period

As an administrator, you can configure the retention period for voice messages.

## Prioritizing voicemail messages

Callers can flag their voicemail messages as normal, urgent or private.

In myPortal for Desktop and myPortal for Outlook, the prioritization of existing voicemail messages is represented by different colors.

Subscribers who listen to their voicemail messages through the phone are first notified how many messages are urgent, private and normal. Urgent messages are played back first.

If the voicemail messages are forwarded as e-mails, the voicemails identified as urgent are flagged as e-mails with high priority.

## Functionality of the Voicemail Box

The administrator can define the scope of the voicemail box. He or she can choose between:

- **Full**  
Full functionality of the voicemail box (default value)
- **Short Menu**  
After the status-based or personal announcement is made, a connection to the operator is offered.
- **No Menu**  
After the greeting announcement is played, the caller is directly taken to record a message.

## Displaying New Messages at the Telephone

Voicemail messages are signaled at the telephone. As soon as the voicemail has been played, the indicators are deleted.

The type of signaling used for new voicemail messages depends on the phone

- For all telephones, acoustic signaling occurs using a special dial tone.
- For system telephones without a display, the Mailbox key also lights up (if configured).
- For system telephones with a display, the Mailbox key lights up (if configured), and a message appears on the display.

### Notification Service

Subscribers who are using myPortal for Desktop or myPortal for Outlook can define whether the notification about the arrival of new voicemails should be forwarded and, if so, to what destination.

Subscribers can also define whether the message should be forwarded as an e-mail. In addition, they can choose to be notified about the arrival of new voicemails by a phone call or an SMS.

### Language of the Voicemail Box

As an administrator, you can select the default language of the voicemail box for the menu prompts and the the internal system announcements on a system-wide basis.

### Dependencies

Topic	Dependency
Playing a message over the phone	Subscribers can play back voicemails through the phone only in the <b>Office</b> or <b>CallMe</b> presence status. For all other settings, the message can only be played back via the PC.

---

### Related Topics

- [AutoAttendant](#)

## 8.6.2 Voicemail Announcements

Voicemail announcements notify callers about the Presence status of a subscriber, for example.

Standard announcements are available in all languages. As a subscriber, you can also record or import personal announcements for your voicemail box. The corresponding standard announcement is overwritten by the personal announcement in the process. As an administrator, you can change the standard announcements by importing different announcements. The personal announcements of subscribers are overwritten in the process. OpenScape Office performs the automatic level control and normalization needed to meet the "USA / TIA 968 Signal Power Limitations" requirements.

### Status-based Voicemail Announcements

Depending on the Presence status, the announcements for the voicemail box change automatically; for example, if the Presence status is **Meeting**, then the announcement may be something like: The subscriber is in a meeting until 3 p.m. If the entered end of a meeting is reached, but the subscriber has not yet changed his or her status back to "In Office", then the voicemail announcement is adapted automatically or the voicemail announcement reverts automatically to "In Office" (this is configurable by the subscriber).

### System Language for Voicemail Announcements

The system language for the voicemail box is set at the country initialization. In addition, the subscriber can set the language of his or her own voicemail box. A caller will then hear the station-specific announcements in the language set by the subscriber and the system-specific announcements in the system language.

### Announcements Depending on Presence Status and Profile

The following table describes which greeting is heard by the caller, depending on the set Presence status and profile. The caller menu refers to the central AutoAttendant. The profile refers to the personal AutoAttendant of the subscriber here. The default greeting, name and custom greeting for profiles must be recorded by the subscriber. Depending on the configuration, the caller menu may vary in length or may not be available at all.

	<b>Busy No answer Do Not Disturb</b>	<b>Meeting Sick Break Out of the Office ...</b>
Voicemail with Presence status	Default greeting + Caller menu	Name + Presence status + Caller menu
Voicemail box with blocked Presence status	Default greeting + Caller menu (if enabled)	
Profile with dynamic greeting	Custom Profile Greeting	Name + Presence status + Custom Profile Greeting
Profiles if dynamic greeting is to be skipped	Custom Profile Greeting	

---

### Related Topics

- [Central AutoAttendant](#)
- [Personal AutoAttendant](#)

### 8.6.3 Phone Menu of the Voicemail Box

You can access your voicemail box, change your Presence status and also use other functions from a phone.

The password for accessing your voicemail box is the same as for myPortal for Desktop or myPortal for Outlook. Selections are made in the phone menu by entering digits at the phone. You can also enter a digit during an announcement to speed up operations.

#### Main Menu

The main menu is the first menu you hear on reaching the voicemail box. Depending on your choices, you are then taken to further menus or functions.

Digit	Function
1	<b>Mailbox</b>
1	<b>New</b>
1	<b>Replay</b>
2	<b>Call back</b>
3	<b>Next message</b>
4	<b>Save</b>
5	<b>Save as new</b>
6	<b>Delete</b>
7	<b>Copy to other voicemail box</b>
0	<b>Date and Time</b>
2	<b>Played</b>
	(same functions as those under <b>New</b> )
3	<b>Saved</b>
	(same functions as those under <b>New</b> )
4	<b>Deleted</b>
	(same functions as those under <b>New</b> )
2	<b>Change Status</b>
1	<b>Office</b>
2	<b>Meeting</b>
3	<b>Sick</b>
4	<b>Break</b>
5	<b>Out of the Office</b>
6	<b>Vacation</b>
7	<b>Lunch</b>
8	<b>Gone Home</b>



Digit	Function
3	<b>Record announcements</b>
1	<b>Name</b>
2	<b>Default Greeting</b>
3	<b>Presence-based greetings</b>
0	<b>Busy</b>
1	<b>No Answer</b>
2	<b>Meeting</b>
3	<b>Sick</b>
4	<b>Break</b>
5	<b>Out of the Office</b>
6	<b>Vacation</b>
7	<b>Lunch</b>
8	<b>Gone Home</b>
4	<b>CLI Recognition</b>
4	<b>Change Password</b>
5	<b>Leave message for extension</b>
6	<b>Connect to extension</b>
9 / 0	<b>Connect to Attendant Console</b>

#### General functions

The following functions are available under different menu items:

Digit	Function
1	<b>Confirm</b>
2	<b>Edit</b>
*	<b>Enter the station number</b>
#	<b>Up one level</b>

## 8.6.4 Fax box

The fax box enables subscribers to receive and send fax messages via myPortal for Desktop or myPortal for Outlook without a fax machine.

As an administrator, you can configure a fax box for licensed Comfort Plus subscribers. In addition, you can connect fax devices or fax servers via the a/b or ISDN interface.

As a subscriber, you can access your fax messages via myPortal for Desktop or myPortal for Outlook. myAttendant can access the fax messages of subscribers who have explicitly allowed this.

### Managing Fax Messages

The subscriber can manage received fax messages by moving them to different folders (Saved or Deleted, for instance). The fax messages can also be forwarded to another subscriber. The subscriber can also save fax messages as TIFF files and redirect them to any selected e-mail account.

### Retention Period for Fax Messages

OpenScope Office automatically deletes fax messages for which the following retention periods are exceeded:

Fax message	Retention period (days)
New	120
Read	365
Sent	365
Deleted	60

## 8.6.5 Sending Fax Messages with Fax Printer

Fax Printer is an application for sending fax messages with centrally provided or individually created cover sheets from Windows applications such as Microsoft Word, for example.

Fax Printer consists of the following components:

- Fax Printer Cover Editor
- Fax-Drucker-Treiber

Fax Printer can be used from all the usual Windows programs. Fax groups make distribution easier. Fax messages are sent as an e-mail or directly to the Desktop. A screen pop notifies the subscriber when the fax is sent successfully.

### Header Rows

As an administrator, you can configure different header lines for Fax Printer users. You can also define a header line as the default. Header lines may include the following elements:

Details	Placeholder
Date / Time	{{date_time}}
Company Name	{{company_name}}
User name	{{user_name}}

Details	Placeholder
Company Ph.	{{company_number}}
Page number	{{page_number}}
Number der pages	{{page_count}}

The header lines of fax messages sent with Fax Printer may only include characters from the ANSI character set. In other words, no special or diacritical characters such as umlauts are allowed. Since the header line may basically include the sender's name, no special or diacritical characters should appear in the names of the subscribers as well.

## 8.6.6 Notification Service for Messages

The system can optionally notify you (as a subscriber) about a new message by e-mail, by phone or with an SMS.

The Notification Service works as follows:

Notification	for voicemail	for fax message	Prerequisites
E-mail	You receive an e-mail with the message as a WAV file, the date and time it was received, the duration of the message and, if available, the phone number and name of the sender. If the size of the WAV file exceeds a defined value, it is not attached to the e-mail. This value can be changed by the administrator of the communication system; the default is 10 MB. Voicemails with "urgent" priority are flagged as e-mails with "High" importance. E-mails with a voicemail have a separate symbol in Outlook. If you are using an IMAP mailbox that shows only the e-mail headers, the usual e-mail icon will appear instead.	You receive an e-mail with the message as a TIFF file, the date and time it was received, the number of pages and, if available, the phone number and name of the sender. If the size of the TIFF file exceeds a defined value, it is not attached to the e-mail. This value can be changed by the administrator of the communication system; the default is 10 MB. E-mails with a fax message have a separate symbol in Outlook. If you are using an IMAP mailbox that shows only the e-mail headers, the usual e-mail icon will appear instead.	The sending of e-mails has been configured
by phone	Your voicemail box calls you at the number you have specified and plays back the message to you.	-	
SMS	You receive an SMS about the received message at the phone number defined by you.		The SMS template has been configured.

As a subscriber, you can enable or disable every type of notification for each Presence status individually. The notification by phone can be restricted to the business hours configured by the administrator. You can define the number and intervals for the repeated attempts for the notification by phone.

---

**INFO:** When using Microsoft Office 365, e-mails can only be sent to Microsoft Office 365 accounts.

---

### 8.6.7 Sending E-mails

The feature for sending e-mails enables e-mail notifications about new voice and fax messages to be sent to subscribers and system messages to be sent to administrators by e-mail.

## 8.6.8 SMS Template

An SMS template enables subscribers to be notified about new voicemails with an SMS.

In order to receive SMS messages, a personal mobile e-mail address of the respective provider must be first activated. To do this, the subscriber sends an activation SMS to a speed-dial number. The subscriber then receives an SMS with his or her personal e-mail address, which is usually composed of the call number and the gateway name. For example, the mobile e-mail address for a T-Mobile customer with the phone number 0171/1234 567 would be: 01711234567@t-mobile-sms.de. This applies analogously to other networks as well.

An SMS template consists of the Template Details and SMS Details areas. The administrator must enter the name of the template in the Template Details area. This is usually the name of the E-mail-to-SMS Provider.

The specifications in the SMS Details area depend on the Provider. Under Recipient, the administrator must enter the e-mail address to which the SMS is to be sent. The entry for the Subject line may be freely selectable or require the customer number to be entered by the administrator.

---

**INFO:** Every Provider requires a specific template. The required data can be obtained from the respective mobile service provider.

---

### Placeholder

SMS templates may include the following placeholders in the **Recipient**, **Subject** or **Text** field:

Details	Placeholder
Mobile number to which the message is to be sent	{{MobileNumber}}
Name or call no. of the sender	{{Sender}}
Date and time of receiving a message	{{DateTime}}
Caller number	{{CallingNumber}}
Priority of message	{{Priority}}

### System-Specific Information

The length of the message is reduced to the first 160 characters.

## 8.6.9 Fax over IP (T.38 Fax) (LX/MX)

Fax over IP enables the transmission of fax messages over the Internet in accordance with the G2 and G3 standards by using the network protocol IFP (Internet Facsimile Protocol).

The system supports the following scenarios for T.38:

- A subscriber receives fax messages via an ITSP (Internet Telephony Service Provider) at his or her fax box and sends faxes to external locations with Fax Printer via the ITSP.
- A subscriber receives fax messages via an AP 1120 (SIP) at his or her fax box and sends faxes with Fax Printer via an AP 1120 (SIP).
- A subscriber receives fax messages via a Mediatix 4102S (SIP) at his or her fax box and sends faxes with Fax Printer via a Mediatix 4102S (SIP).
- Stations can receive fax messages via an ITSP (Internet Telephony Service Provider) on a fax device that is directly connected to a GMSA, GMAA, GMAL or GMS module and send faxes from this fax device via the ITSP to external destinations.
- Stations can receive fax messages via an ITSP on a fax device that is connected to an AP 1120 and send faxes from this fax device via the AP 1120 and ITSP to external destinations.
- Stations can receive fax messages via an ITSP on a fax device that is connected to a Mediatix 4102S and send faxes from this fax device via the Mediatix 4102S and ITSP to external destinations.
- Stations can receive fax messages via ISDN (GMSA module) on a fax device that is connected to an AP 1120 and send faxes from this fax device via the AP 1120 and ISDN to external destinations.
- Stations can receive fax messages via ISDN (GMSA module) on a fax device that is connected to a Mediatix 4102S and send faxes from this fax device via the Mediatix 4102S and ISDN to external destinations.
- A station can send fax messages from a fax device that is connected to an AP 1120 to another fax device that is also connected to an AP 1120.
- A station can send fax messages from a fax device that is connected to a Mediatix 4102S to another fax device that is also connected to a Mediatix 4102S.
- Internal fax message from a fax device at a GMSA module to a fax device at an AP 1120 and vice versa.
- Internal fax message from a fax device at a GMSA module to a fax device at a Mediatix 4102S and vice versa.
- Internal fax message from a fax device at a GMSA module to a fax box and vice versa.

---

**INFO:** T.38 and G.711 must be activated in the system and in the AP 1120. SIP must be activated in the AP 1120.

T.38 must be activated in the system for the fax box. In order to send faxes from OpenScape Office via an ITSP, the ITSP must support T.38.

---

## 8.7 Instant Messaging

Instant Messaging refers to communicating with instant messages (usually called a chat).

### 8.7.1 Instant Messaging

Instant Messaging enables you to chat with other peers. The system also supports instant messaging with an external communication partner via XMPP and multi-user chats, as well as both in combination.

Instant Messaging is possible with the following clients:

- myPortal for Desktop
- myPortal for Outlook
- myAgent
- myAttendant

As an administrator, you can enable or disable instant messaging on a system-wide basis. The sent and received instant messages are presented to the communication partners as an interactive dialog. On selecting a recipient, the client shows whether the communication partner is currently online. If one of the communication partners is offline, the following occurs with the instant message, depending on the type of the selected recipient:

Recipients	Behavior
Individual subscribers	The instant message is displayed at the next login.
Group in Favorites	The instant message is never displayed for the subscribers who are offline.

#### External Instant Messaging

As a subscriber, you can also chat with *one* external XPP communication partner (e.g., a Google Talk user).

#### Multi-user chat

A multi-user chat is the exchange of instant messages with multiple communication partners. Here too, the system supports a maximum of one external XMPP communication partner.

#### Instant Messaging and Web Collaboration

Note that Instant Messaging of the system and Instant Messaging of a Web Collaboration session are mutually independent, i.e.: the instant messages from a UC client do not appear in a Web Collaboration session of the same participant, and vice versa.

## 8.8 AutoAttendant

Depending on the presence status of the called party, the AutoAttendant offers callers options to route voice calls to fixed numbers or their voicemail box. Callers signal their choice by entering digits at the phone.

---

### Related Topics

- [Voicemail Box](#)

### 8.8.1 Central AutoAttendant

The central AutoAttendant is the system AutoAttendant, which can be configured by the administrator.

As an administrator, you can do the following for any station numbers:

- Record or import announcements for the central AutoAttendant. On importing announcements, the system performs the automatic level control and normalization needed to meet the "USA / TIA 968 Signal Power Limitations" requirements.

By default, announcements for the central AutoAttendant are available in all languages. Consequently, if you change these announcements, please take all languages into account.

- Configure profiles for the central AutoAttendant
- Configure the central AutoAttendant for specific times and on the basis of rules by using schedules Schedules also make it possible to offer advanced selection options such as dialing by name, for example.

---

### Related Topics

- [Voicemail Announcements](#)

### 8.8.2 Personal AutoAttendant

The personal AutoAttendant is the customized AutoAttendant, which can be configured by subscribers.

#### Personal AutoAttendant

As a subscriber, you can do the following for your station number with myPortal for Desktop or with myPortal for Outlook:

- Record or import announcements for the personal AutoAttendant.
- Configure profiles for the personal AutoAttendant



The relevant calls are first handled by the central AutoAttendant.

---

**Related Topics**

- [Voicemail Announcements](#)

### 8.8.3 Announcements for the AutoAttendant

The AutoAttendant uses the following voicemail announcements: name announcements, automatic situation-specific (dynamic) announcements and personal announcements.

When this profile is activated, the voicemail box plays back the following announcements:

- **Name announcement:**  
If dynamic announcements have been activated, the name announcement recorded by the subscriber is used as a greeting, except in cases where the presence status of that subscriber is **Office**, **CallMe** or **Do Not Disturb**.
- **Dynamic announcements:**  
If dynamic announcements have been activated, the voicemail box generates situation-based announcements for the presence status (except for **Office**, **CallMe** and **Do Not Disturb**) with an indication of the scheduled time of return for that subscriber, e.g., "... is in a meeting until two thirty p.m. today". The playback of dynamic announcements can be activated separately for each profile. If the dynamic announcements for a profile have been activated, subscribers can activate or deactivate the announcements for their presence status for certain callers and for all external callers separately.
- **Personal announcement for the profile:**  
In order activate a profile, an announcement for that profile must be first recorded to indicate the appropriate digits and associated choices to callers, e.g.: "To leave a message, press 1. To speak with an operator, press 2". If the subscriber has disabled dynamic announcements for the profile, he or she may find it useful to start the personal announcement by indicating his or her presence status.

The voicemail box plays back announcements for a profile in the following order (from left to right):

Profile	Name announcement	Dynamic greetings	Personal announcement for profile
<b>Busy</b>	-	-	x
<b>No answer</b>	-	-	x

Profile	Name announcement	Dynamic greetings	Personal announcement for profile
Meeting	x (if dynamic announcements have been enabled)	x (if dynamic greetings have been enabled)	x
Sick			
Break			
Out of the Office			
Vacation			
Lunch			
Gone Home			
Do Not Disturb	-	-	x

**Example: dynamic announcements enabled**

Profile	Name announcement	Dynamic greetings	Personal announcement for profile
Meeting	"Natalie Dubois"	"is in a meeting until two thirty p.m. today".	"To leave a message, press 1. To speak with my representative, press 2."

**Example: dynamic announcements disabled**

Profile	Name announcement	Dynamic greetings	Personal announcement for profile
Out of the Office	-	-	"I am currently out of the office. To leave a message, press 1. To speak with my representative, press 2. To forward this call to my mobile phone, press 3."

---

**INFO:** Continuous announcements may only be in the first position of the call list.

After an SST or CT from the AutoAttendant, the call list of the subscriber is followed, but no announcements are played back.

The accompanying announcement feature for calls is only implemented with continuous announcements in the first position of the call list.

---

## 8.8.4 Profiles for the AutoAttendant

Profiles for the AutoAttendant define the choices for callers, depending on the presence status.

Each profile can be activated separately. By default, no profile is active. If a profile has been deactivated, the default behavior of the voicemail box applies to the presence status involved.

---

**INFO:** In order to enable callers to reach the voicemail box on **Busy** and **No Answer**, the administrator must set up call forwarding to the voicemail box. Alternatively, you can also do this as a subscriber, by setting up a "call diversion after time" on your phone.

---

## 8.9 Attendant Console Functions

A wide range of Attendant Console functions are available to you via the myAttendant application. Subscribers can be easily managed here via user buttons. In addition, messaging functions (voicemail, faxes, instant messages, SMS, and e-mails) are available via the Message Center.

### 8.9.1 Subscriber Management

Subscriber management is performed in myAttendant via user buttons, the internal directory, and the external directory. Internal subscribers are referred to as users in the user interface; external subscribers are referred to as contacts.

#### User Buttons

The user buttons are located on the **Default** tab and are a part of the main window of myAttendant.

The user buttons are sorted in alphabetical order by default.

There are 90 user buttons available on a user buttons tab.

You can configure multiple tabs for user buttons and select the names for these user buttons freely.

Internal subscribers (users) can be assigned to user buttons.

### 8.9.2 Message Center

All voicemails, faxes, instant messages as well as SMS messages and e-mails are recorded and managed via the **Message Center** of myAttendant.

Messages can also be managed for other subscribers, provided these subscribers have granted the appropriate permission for this.

The Subscriber List window, contains a list of all communication system subscribers with their presence/absence status. Your own status is displayed first in a drop-down message overview. The other subscribers follow in alphabetical order.

Depending on what is selected in the message overview, message details are displayed, including a table of message-specific information that can be selected for further processing.

The various message types can be processed as follows:

- **Voice Messages (i.e., voicemails)** can be played back, deleted and forwarded,
- **Instant messages** (Instant Messaging) can be read, written and sent to internal subscribers.

- **SMS** messages can be read, written and sent to internal subscribers.
- **E-mails** can be read, written and sent to internal subscribers.
- **Fax messages** can be forwarded.

---

**INFO:** Instant messages are frequently referred to as LAN messages or LAN notes in the user interface.

---

### **Text Modules for Instant Messaging**

You can use instant messages saved as text modules to communicate with subscribers.

## 9 Functions at the Telephone (LX/MX)

The communication system offers a comprehensive set of telephony features extending from the usual features such as hold, toggle/connect and consultation hold, etc., through various call signaling mechanisms, down to call transfers, call deflections and call forwarding.

### 9.1 Making Calls (LX/MX)

The communication system offers many ways to make calls, including, among other things, direct station selection and speed dialing.

#### 9.1.1 Digit Dialing

In the case of digit dialing, every digit is transmitted as soon as it is dialed.

The call setup begins immediately after the input of the first digit. Consequently, the subscriber has no way to edit the dialed number.

---

##### Related Topics

- [En-Bloc Dialing](#)

#### 9.1.2 En-Bloc Dialing

In en-bloc dialing, connections are only established after the complete phone number has been entered. The call number is transferred as a single block.

The transmission of the dialed number can be initiated by entering the end-of-dialing code (#).

En-bloc dialing is mandatory for:

- ITSP trunk connection
- ISDN Primary Rate Interface in the U.S.

After 5 seconds without the input of a digit, the last entered digit is interpreted as the final digit of the number block.

---

##### Related Topics

- [Digit Dialing](#)

### 9.1.3 End-of-Dialing Recognition

End-of-dialing is either recognized automatically after five seconds or indicated manually by the user with the end-of-dialing code "#".

### 9.1.4 Editing the Telephone Number

This option lets subscribers modify the digits entered for the station number. This function is common in mobile phones. A call number can only be corrected as it is being entered.

After entering a sequence of digits, the user can edit it from right to left by pressing a key; each time the key is pressed, one digit is deleted. Once the correct digit sequence is entered in full, the user can press the confirm key or lift the handset to start digit transmission.

It is not possible to edit a saved call number, for example, for number redial.

---

**INFO:** This feature can be individually activated for every station.

---

#### Dependencies

Topic	Dependency
Call waiting	Call waiting is possible during editing because the telephone is in digit input state and is busy for incoming traffic.
Consultation	The telephone is in digit input state after a consultation. This makes it possible to edit station number digits.

### 9.1.5 Redialing

The phone number dialed is saved after an external call is set up. If the destination was busy or not reachable, a user can press the Redial key to redial the same number.

Internal calls are ignored by the redial memory.

Post-dialed digits (also called DTMF characters), if any, are **not** seen as part of the dialing information and are therefore not saved (e.g., digits sent to a connected voicemail box).

The Redial function can only be activated via a key, not via an access code.

To retrieve a specific number and use it to set up another call, press the Redial key. Press the key once to dial the last number dialed. Press the key twice to dial the next-to-the-last number dialed. Press the key three times to dial the number that was stored the longest.

The station number saved is automatically dialed after 2 seconds when you press the Redial key. If you need more time to read the displayed station number, select "scroll" with the Confirm Key. Click "Next" to display the next phone number saved. This phone number is dialed only on selecting the "Make Call" command. This gives you much more time to check if the correct phone number was selected.

**Dependencies**

Topic	Dependency
System/station speed dialing	The used speed-dial number is stored in the redial memory.
Lock code	You cannot use redial if the telephone lock is active.

**Background Information**

If a call is routed via LCR (least cost routing), only the number dialed by the station is stored.

Account codes (ACCT) entered are also stored in the redial memory. This is true only if the appropriate system-wide flags are set.

### 9.1.6 System Speed Dialing

You can save frequently needed external phone numbers in the communication system. Every number is then represented by a speed-dial number which is used instead of the full phone number.

Speed-dial numbers consist of 3-digit numbers.

All subscribers are members by default of a group that is assigned all SSD numbers. This means that every subscriber can use all SSD numbers.

The numbers for system speed dialing are configured by the administrator in groups. The subscribers can each be assigned to one of these groups. A subscriber can only use the speed-dial numbers of his or her allocated group. A group can only be assigned a single SSD range.

To program a "dial pause" and DTMF changeover for suffix dialing of DTMF characters (e.g., for controlling voicemail boxes), you can use the Redial "P-key" or "#" (pound) key.

- A name can be associated with each destination.
- Suffix-dialing is also possible:



- Manual suffix-dialing  
The user can select additional numbers by selecting the access code and entering the index number (speed-dial number). These are added to the station number saved in this index and dialed.
- Automatic suffix-dialing  
When configuring an SSD, the number entered can be split into two parts. A dash "-" is used as the separator. The first part is always sent. A timer then starts. If the user does not dial any more digits before the timer expires, the second part of the number entered is automatically suffix-dialed, otherwise the manually dialed digits are transmitted.

For example: SSD = 7007-0

If the station does dial a DID (manual suffix-dialing) after selecting the SSD and before the specified time has expired, 0 is automatically dialed (automatic suffix-dialing).

You can import speed-dial lists from a CSV file in ANSI or ASCII format. File structure: 3-digit speed dial;CO access code (0) with long number;last name, first name (separated by semicolons). Example:

- 000;089700798765;SEN\_000

---

**INFO:** A CSV template for importing speed-dial numbers can be found under **Service Center > Download Center > CSV Templates**.

---

## Dependencies

Topic	Dependency
Translation of station numbers to names	You can assign a name to each speed-dialing destination. As soon as a call is received from a saved phone number, the system automatically enters the name and displays it instead of the phone number if CLIP is set.
Tenant system	System speed dialing can only be configured once per communication system. CON groups must be configured to restrict access to speed-dial number ranges to prevent system-based subscribers in a tenant systems from using the SSDs of the other system. If not, the dialing attempt is rejected with the message "not authorized". The speed-dial number ranges can overlap in the CON group.
Entrance Telephone (Door Opener)	The entrance telephone cannot access speed-dialing numbers.
Lock code	System speed dialing is possible when the lock code is active.
Toll restriction	SSD overrides the toll restriction rules.
Redialing	The used speed-dial number is stored in the redial memory.

### Background Information

The subscriber must enter the external call number with the external code (e.g., 0).

---

### Related Topics

- [Individual Speed Dialing \(ISD\)](#)

## 9.1.7 Individual Speed Dialing (ISD)

Individual Speed Dialing (ISD) enables every subscriber to save 10 external numbers as individual speed-dial numbers in addition to the system speed-dial numbers.

All authorized phones and PC clients can access this feature.

You cannot store internal station numbers and features as station speed-dial numbers.

### Dependencies

Topic	Dependency
Non-display telephones	Following station number entry, telephones without a display must wait for the confirmation tone.
Lock code	You cannot use station speed dialing if the telephone lock is active.

### Background Information

External numbers can be programmed in the ISD pool. Access depends on the station's dial-up access rights. Before entering the station number, the subscriber must enter the external code (e.g., 0).

The Redial key or the pound (#) key is used to program a dial pause or DTMF changeover.

Names cannot be assigned to station speed dial numbers.

---

### Related Topics

- [System Speed Dialing](#)

## 9.1.8 Direct station select

The function keys on a telephone or add-on device can be programmed as DSS keys. These are programmed with the phone number of an internal subscriber or a group for this. Press a key of this kind to initiate an immediate call to the programmed destination (DSS). The current status of the subscriber or of the group is indicated by the LED associated with the DSS key.

A DSS (direct station selection) key can also be used to transfer a call quickly to the programmed subscriber or group. Pressing a DSS key during a call with an external party places the ongoing call on consultation hold. The transferring subscriber can transfer the call to the transfer destination by replacing the handset (unscreened transfer). He or she can also wait until the transfer destination responds before transferring the call (screened transfer). If the transfer destination does not answer, an automatic recall is enabled.

### Statuses of a DSS Key LED

The DSS key LED shows the current status of the programmed station:

- Off: the associated subscriber is not conducting a call.
- Lit: the associated subscriber is conducting a call or has activated Do Not Disturb.
- Flashing fast: the associated subscriber is conducting a call. The call can be accepted by pressing the Direct Station Select (DSS) key.
- Flashing slowly: the associated subscriber is being called and has not yet answered. The call can be accepted by pressing the Direct Station Select (DSS) key.

### Dependencies

Topic	Dependency
ISDN phones, SIP phones	Direct Station Select (DSS) keys cannot be programmed for ISDN or SIP telephones.

## 9.1.9 Speaker Calls / Direct Answering

The Speaker call function lets you set up an internal connection without the called subscriber lifting the handset. The loudspeaker on the called station is automatically activated.

On phones equipped with a speakerphone (microphone), direct answering of the called station is possible by switching on the microphone. On lifting the handset, the call becomes a normal two-party call.

Speaker calls can be used via a function key programmed for this purpose, the associated menu item or by entering the code and then dialing the station number of the destination station or group. A function key can also be programmed with a station number. A connection to the programmed destination is immediately set up when you press a function key of this kind.

The Speaker Call feature can also be used to make announcements to groups of up to eight internal subscribers.

Direct answering can be activated via the menu item provided for this in the display or via a function key programmed for this purpose.

Speaker calls can be prevented for a subscriber by enabling an option to prevent voice calling. In this case, speaker calls are signaled like a normal call.

**Dependencies**

Topic	Dependency
Do Not Disturb, Override Do Not Disturb	Speaker calls are not possible at stations where Do Not Disturb is active. If the subscriber who wants to use the "Speaker calls" feature is authorized to override Do Not Disturb, he or she hears the busy tone for five seconds. The destination station is then called, but not directly addressed.
Toggle, consultation hold, transfer	The specified features cannot be used in a speaker calls/ direct answering connection.
ISDN phones, SIP phones	The "Speaker call" and "Direct answering" features cannot be used with ISDN or SIP telephones.

**9.1.10 Associated Dialing**

Associated dialing enables an authorized subscriber to dial a phone number on behalf of any other subscriber. The effect is the same as when the other subscriber dials the phone number.

The user accesses the function by dialing a code and specifying the station for which a number should be dialed. The system then interprets this information as though the station specified earlier were dialing.

**9.1.11 Trunk Queuing**

A subscriber can reserve a trunk in advance if there are no free trunks available (busy signal). As soon as a trunk becomes free, it is offered to the subscriber through an automatic recall.

If the user is busy at the time of the recall, the trunk will camp on to the busy station. If the camp-on tone is not answered, the reservation is canceled, and the trunk is offered to the next station in the queue. If the user activated DND prior to receiving the recall from the queued trunk, the trunk reservation is canceled and the trunk is offered to the next station in the queue.

If a number of stations queue a trunk, the trunk is assigned in the order that the requests were received.

Only one queue/reservation request is accepted per telephone. If a second reservation is attempted, it overwrites the first.

### Dependencies

Topic	Dependency
S <sub>0</sub> telephones	S <sub>0</sub> phones do not support this feature (not for U.S.).
Speakerphone mode	Users can also use trunk queuing in speakerphone mode

### Background Information

It is not possible to invoke the Trunk Queuing feature if the attempted call was placed through LCR (least cost routing).

The Trunk Queuing feature ignores an existing call forwarding—no answer instruction. Trunk reservation is canceled if not answered within 20 seconds.

A recalling trunk cannot be picked up by either Call Pick up - group or Call pick up - Directed.

Trunks can be reserved in one of the following ways:

- Manual reservations only work in telephones with a display
- Automatic reservation (for all other telephones)  
When this flag is activated and if a station is not assigned a free trunk after the usual simplified dialing procedures, the busy tone is signaled at the station. After five seconds, a positive acknowledgment tone is applied and the trunk is reserved, provided that the station has the appropriate CO call privilege.

## 9.1.12 Private Trunk

A private trunk is a CO trunk that is available exclusively to a specific subscriber.

## 9.2 Call Signaling, Calling Line ID (LX/MX)

The communication system offers various options for call signaling and call number display such as CLIP, CLIR, COLP and COLR, for example.

## 9.2.1 Different Call Signaling

Different call signaling enables a distinction to be made between internal and external incoming calls.

Incoming calls are signaled visually and acoustically on the phone. The following displays appear on the screen:

- Caller number
- For call forwarding, the dialed call number

The incoming call can also be signaled via an LED. Different acoustic signals are used for internal and external calls.

### **Call signaling internal**

Each subscriber can be assigned one of a total of eight possible acoustic call signals for internal calls. The station then uses the modified ringing tone to distinguish its calls at other internal stations. For example, a special internal ringing tone can be set for the manager so that every staff member knows when the manager is calling simply from the ringing tone.

### **Call signaling external**

There are three different call types, each with different acoustics, that can be set for an external call. Different acoustic signals can be applied, for instance, to distinguish between calls from two different groups such as Sales and Warehouse.

- In Germany, the administrator can configure three different ring types for analog, ISDN and system phones.
- In other countries, the ring types for analog phones are the same.

## 9.2.2 Calling Line Identification Presentation (CLIP)

Calling Line Identification Presentation (CLIP) shows the caller's number at the called station.

The CLIP (Calling Line Identification Presentation) refers to incoming calls and must be supported by the network provider.

If the caller's name and phone number are programmed as a system speed dialing (SSD) number in the communication system, you will see the name on your display.

The Calling Line Identification Presentation (CLIP) and Calling Line Identification Restriction (CLIR) features are mutually exclusive, that is, as soon as CLIP is activated, CLIR is deactivated, and vice versa.

### Configurable CLIP

Configurable CLIP transmits a set call number (e.g., the call number of a hunt group) externally instead of the caller's number (e.g., the number of the hunt group member).

### System-Specific Information

Country	Enabled by default
USA	LIN (Location Identification Number). If CLIP is enabled for the USA, LIN is automatically disabled.
Remaining countries	CLIP

---

### Related Topics

- [Calling Line Identification Restriction \(CLIR\)](#)
- [Connected Line Identification Presentation \(COLP\)](#)
- [Connected Line Identification Restriction \(COLR\)](#)

## 9.2.3 Calling Line Identification Restriction (CLIR)

Calling Line Identification Restriction (CLIR) suppresses the station number of the caller at the station of the called subscriber.

CLIR (Calling Line Identification Restriction) applies to outbound calls. The PSTN must support the feature. The Calling Line Identification Restriction (CLIR) has precedence over the Calling Line Identification Presentation (CLIP).

The Calling Line Identification Presentation (CLIP) and Calling Line Identification Restriction (CLIR) features are mutually exclusive, that is, as soon as CLIP is activated, CLIR is deactivated, and vice versa.

CLIR and COLR can only be enabled or disabled together.

Calling Line Identification Restriction (CLIR) has no effect for certain call destinations (e.g., emergency numbers of the police and fire departments).

### System-wide Station Number Suppression (CLIR)

As an administrator you can enable or disable the CLIR station number suppression on a system-wide basis.

---

**INFO:** The flag "System-wide station number display suppression" does not apply to the U.S.

---

### **Temporary Station Number Suppression**

As a subscriber, you can activate or deactivate the temporary station number suppression (CLIR). A temporary station number suppression is only possible if the system-wide station number suppression has been deactivated.

### **Station Number Suppression (CLIR)**

As an administrator, you can configure the CLIR for each route so that only the PABX number is transmitted instead of the subscriber's station number.

---

#### **Related Topics**

- [Calling Line Identification Presentation \(CLIP\)](#)
- [Connected Line Identification Presentation \(COLP\)](#)
- [Connected Line Identification Restriction \(COLR\)](#)

## **9.2.4 Connected Line Identification Presentation (COLP)**

Connected Line Identification Presentation (COLP) transmits the call number of the called subscriber to the caller as soon as the two are connected.

Connected Line Identification Presentation (COLP) is an ISDN feature.

COLP makes sense with call forwarding, for example, so the caller can see the phone number of the actual communication partner instead of the originally dialed phone number.

The Connected Line Identification Presentation (COLP) and Connected Line Identification Restriction (COLR) features are mutually exclusive, that is, as soon as COLP is activated, COLR is deactivated, and vice versa.

---

#### **Related Topics**

- [Calling Line Identification Presentation \(CLIP\)](#)
- [Calling Line Identification Restriction \(CLIR\)](#)
- [Connected Line Identification Restriction \(COLR\)](#)

## **9.2.5 Connected Line Identification Restriction (COLR)**

Connected Line Identification Restriction (COLR) suppresses the display of the called station at the station of the caller.

The Connected Line Identification Restriction (COLR) applies to incoming calls.

The Connected Line Identification Restriction (COLR) has precedence over the Connected Line Identification Presentation (COLP).



The Connected Line Identification Presentation (COLP) and Connected Line Identification Restriction (COLR) features are mutually exclusive, that is, as soon as COLP is activated, COLR is deactivated, and vice versa.

CLIR and COLR can only be enabled or disabled together.

---

#### Related Topics

- [Calling Line Identification Presentation \(CLIP\)](#)
- [Calling Line Identification Restriction \(CLIR\)](#)
- [Connected Line Identification Presentation \(COLP\)](#)

## 9.2.6 CLIP No Screening (Transmission of Customer-Specific Phone Number Information)

CLIP No Screening transmits a call number specified by the caller instead of the caller's own number.

The outgoing system number does not have to be identical to the incoming system number.

The "Suppress station number" flag can be activated for special customer applications. This prevents the system from sending out the DID number of the station along with the outgoing system number.

**Example:** You want to prevent direct customer access to a service staff member who is reached centrally with a general service number. To conceal the staff member's own DID number, enter the general service number as the outgoing PABX number and activate the "CLIP no screening" flag. Then called subscribers see only the general service number on their display as the CLIP.

Incoming and outgoing calls usually use the same system number. In this case, the entry under "System number - outgoing" is either empty or the same as the one under "System number- incoming". If this is not the case, you can

- enter a different number under "System number - outgoing".
- use the routing parameter "No. and type, outgoing" to define whether the "System number - outgoing" entered contains the station number without area code, with area code (national), or also with the international country code (international).

---

**INFO:** CLIP no screening must be supported by the Network Provider and be activated.

---

## 9.2.7 CLIP for Analog Telephones

CLIP for analog telephones transmits the call number of an analog device of the caller to the called party and displays the CLIP (Calling Line Identification Presentation) on suitable devices of the called party analogously.

The additional transmission of CNIP name information (Calling Name Identification Presentation) can be configured.

---

**INFO:** CNIP is device-independent. Please also refer to the vendor specifications.

---

## 9.2.8 Ringer Cutoff

The Ringer Cutoff feature signals incoming calls acoustically with only a brief alert tone (beep) and on the display.

Ringer Cutoff is only available on phones with displays and has no effect on the signaling of appointments.

## 9.2.9 Translating Station Numbers to Names for System Speed Dialing

For calls made using system speed-dials (SSD) and for incoming calls from system speed-dial numbers, the name associated with the speed-dial destination is displayed after dialing instead of the speed-dial number.

## 9.3 Functions During a Call (LX/MX)

The communication system offers several functions during calls, e.g., holding, redirecting and transferring calls.

### 9.3.1 Placing a call on hold

Placing a call on hold causes the call to be held in a waiting state. During this period, the caller usually hears an announcement or music on hold.

The hold ends when the held call is retrieved (i.e., resumed).

The following types of holds are possible:

- **Common hold:**  
Any station with the appropriately configured trunk or call key can retrieve the call.
- **Exclusive hold: (only for Team or Top function and at the Attendant Console)**  
Only the initiating party can retrieve the call.

### **Placing a Call on Hold and Automatic Recall**

A parked call results in an automatic recall when the "Time for parking + change to hold" timer expires.

### **System-Specific Information**

"Time for parking + change to hold" timer: 180 seconds by default

## **9.3.2 Parking**

Parking a call causes that call to be placed in a waiting state. During this period, the caller usually hears an announcement or music on hold. A parked call can be retrieved from any telephone.

As a subscriber, you assign a park slot (0-9) for a call to be parked. If the park slot you select is already occupied, a negative confirmation tone sounds and the number does not appear on the screen. You can then select another park slot. To retrieve a parked call, you must specify its park slot.

A parked call can be retrieved (unparked) via a code or a correspondingly programmed key and can also be retrieved if another call is waiting at the same time.

### **Parking and Automatic Recall**

A parked call results in an automatic recall when the "Time for parking + change to hold" timer expires.

### **Parking and Call Forwarding**

In the case of a recall, a parked call does not follow call forwarding.

### **Parking and DISA**

Parking cannot be enabled via DISA.

### **Parking and Conference Calls**

You cannot park a conference call.

### **Parking and Networking**

A parked call can only be retrieved in the same node. An incoming call over a network can only be parked at the destination node.

### **Parking and Do Not Disturb**

A station with DND enabled can place a call in a park slot; however, if a recall occurs from the parked call, and no other destination was defined in the call management, the call will be automatically disconnected after the recall timer expires.

### **System-Specific Information**

"Time for parking + change to hold" timer: 160 seconds by default

## **9.3.3 Consultation**

In the case of a consultation hold, a subscriber initiates a second call from the same phone or accepts a waiting call. In the meantime, the first call is placed on hold.

A consultation hold is terminated on:

- retrieving the held call or
- Disconnect  
This results in either:
  - a transfer of the held call or
  - an immediate automatic recall from the party on hold to the party that has just hung up

### **Consultation Call using the Direct Station Select (DSS) Key**

Pressing a Direct Station Select (DSS) key during a call initiates a consultation call to the corresponding destination.

### **Connecting two External Parties**

During an external call, a consultation call to another external destination followed by a transfer connects the two external parties.

## **9.3.4 Alternate (Toggle/Connect)**

The Toggle/Connect feature enables a subscriber to switch between two calls. When the subscriber is talking to one party, the other party is placed on hold.

The subscriber can toggle between the two calls by pressing the appropriate trunk key.

### **Toggle/Connect and Placing a Call on Hold**

The Toggle function is not available to an on-hold subscriber.

## **9.3.5 Transfer**

A transfer enables a subscriber to transfer his or her call to another destination. As soon as a subscriber initiates a transfer, the waiting party is placed on hold for the time being.

The following types of transfers are possible:

- **Blind transfer (also called an unscreened transfer):**  
You can transfer the call without an answer from the subscriber at the destination of the transfer. If the station at the transfer destination is busy, the call is camped on (i.e., call waiting is signaled). If a third party now tries to transfer a call to this busy station or if call waiting rejection has been turned on at the transfer destination, an immediate recall occurs. If the subscriber at the transfer destination does not accept the transferred call within a specified time period ("Dial time during transfer before answer" timer), an automatic recall occurs.
- **Consultation transfer:**  
You can transfer the call only if the subscriber at the destination of the transfer answers. The transfer is completed by hanging up the handset.

### **Transfer with Call Forwarding**

Any call forwarding set at the transfer destination will be followed, i.e., the call will be forwarded accordingly. The display shows the final destination of the transfer.

### **Transfer with Do Not Disturb**

Transferring a call to a station at which Do Not Disturb is enabled results in an immediate recall to the transferring station even if the transferring station itself also has Do Not Disturb enabled.

### **System-Specific Information**

"Dial time during transfer before answer" timer: 45 seconds by default

Up to 5 calls can be transferred simultaneously to a busy station.

## **9.3.6 Automatic Recall**

An automatic recall is received by the originator of a call if his or her call was placed on hold or parked for too long or if an attempt to transfer that call was unsuccessful.

An automatic recall occurs in the following cases:

- A held or parked call is not picked up again within a specific time period ("Time for parking + change to hold" timer).
- In the case of unscreened transfers, under the following circumstances:
  - The call is not answered before a certain time period expires ("Dial time during transfer before answer" timer)
  - The destination does not exist
  - The destination is busy with a second call
  - The digital phone at the destination is defective
  - The transfer type is not allowed

If the originator (i.e., initiating party) is busy during the recall, the automatic recall will camp on the line. As soon as the originator is free again, the automatic recall is signaled. Either the caller's phone number or that of the destination can be shown on the display or the originator. If the recalled party does not answer the

call before the "Intercept time for automatic recall" timer expires, an intercept to the intercept position occurs (if the "On unanswered recall" flag is set). If the intercept position does not answer the recall before the "Time for activation of automatic recall at attendant console" timer expires, the recall is automatically disconnected.

**Automatic Recall and Call Pickup**

Every station in a call pickup group with the initiating party (originator) can pick up an automatic recall if the system-wide flag "Call Pickup after Automatic Recall" is set.

**Automatic Recall and Do Not Disturb**

An automatic recall ignores the Do Not Disturb setting.

**System-Specific Information**

"Intercept time for automatic recall" timer: 30 seconds by default

"Time for activation of automatic recall at attendant console" timer: 60 seconds by default

**9.3.7 Call Monitoring (Selected Countries Only)**

Call monitoring allows authorized subscribers to listen in on a call conducted by any internal subscriber. The microphone of the party listening in is automatically muted. The participants in the monitored call are not advised of the monitoring operation by any signal such as a tone or display.

This feature can only be activated in the following countries: Argentina, Australia, Belgium, Brazil, France, United Kingdom, Hong Kong, India, Ireland, Malaysia, Netherlands, Portugal, Singapore, Spain, South Africa, Thailand, United States.

Authorized subscribers need a system phone and the Override class of service.

The subscriber you want to monitor must be actively conducting a call. When you start and end call monitoring, you may encounter a lapse of up to two seconds of the conversation. The monitored connection is released as soon as one of the stations in the connection is put on hold, transferred or the call is ended. The monitored connection can only be resumed when the station to be monitored is again engaged in a call.

**Dependencies**

Topic	Dependency
Cordless phones	You cannot use call monitoring at cordless telephones because they do not support automatic microphone muting.
Conferencing	Call monitoring restricts the number of possible conferences. Maximum number of conferences possible in the system = maximum number of simultaneous call monitoring stations.

## 9.4 Controlling Availability (LX/MX)

To control accessibility, the system offers features such as call forwarding, do not disturb and call rejection.

### 9.4.1 Call Forwarding on Busy

Call forwarding on busy forwards an incoming call for a busy extension to a station number defined by the administrator.

If the call forwarding destination is also busy, the caller hears a busy signal. For an internal call, the call remains at the forwarding destination, which is cyclically checked until the destination is free. The administrator defines the cycle.

If the call forwarding destination is not available and if no further call forwarding has been configured for it, then no call forwarding is performed.

#### Dependencies

Topic	Dependency
Ext. call forwarding	The Call Forwarding wizard can be used by the administrator to configure whether external call forwarding is to be followed.
External Call Forwarding - No Answer	If external call forwarding - no answer is active, this has precedence over other call forwarding instructions.
Call waiting	If a subscriber enabled call waiting, an incoming call is camped on if call forwarding—busy is configured for him or her.
Group Call	A group is always busy if all members of the group are busy.
Hunt Group	A hunt group is busy if all members are busy or have left the hunt group.
Night service	If the option "by day / by night" is enabled for a subscriber as the Call Forwarding - No Answer (CFNA) setting, external calls are forwarded in accordance with the settings for the night service. Internal calls continue are still handled as in the "by day" settings.

### 9.4.2 Call Forwarding—No Answer (CFNA) With a Timeout (Fixed Call Forwarding)

Call Forwarding—No Answer (CFNA) With a Timeout forwards calls that are not answered within a certain period of time.

**Functions at the Telephone (LX/MX)**  
Controlling Availability (LX/MX)

This type of forwarding is also referred to as fixed call forwarding, since it is only configurable by the administrator.

As an administrator, you can configure call forwarding separately for the following types of calls:

- External calls during the day (when the night service is inactive )
- External calls at night (during active night service)
- internal calls

**Station Number and Name of the Caller**

Under normal circumstances, the station number or name of the originally called subscriber and the station number or name of the caller are displayed at the call forwarding destination. As an administrator, you can disable the additional display of the station number or name of the caller.

Call Forwarding - No Answer after Timeout can only be changed via the Call Forwarding wizard. Up to 3 call forwarding destinations can be set up with this wizard.

**Dependencies**

Topic	Dependency
Call forwarding	Call Forwarding - No Answer (CFNA) after timeout is only executed when the call forwarding destination has not responded after a timeout period defined by the administrator.
DND	A secondary destination which has activated DND, will be skipped.
Analog telephones	There is no indication at these telephones that this call has been forwarded.
Hunt Group	If you enter a group or hunt group as the destination of a call forwarding—no answer instruction, every subscriber in the entire group is called before the next call forwarding destination is evaluated. Group calls and hunt groups can be seen as a call forwarding configuration within a call forwarding configuration.
Night service	If the option "by day / by night" is enabled for a subscriber as the Call Forwarding - No Answer (CFNA) setting, external calls are forwarded in accordance with the settings for the night service. Internal calls are still handled as in the "by day" settings.

**9.4.3 Call Forwarding (CF)**

Subscribers can use Call Forwarding (CF) to redirect incoming calls to a destination of their choice.



If trunk keys (incl. MULAP trunk keys) have been configured, users can also activate call forwarding individually for a specific trunk (or MULAP trunk).

The following calls can be diverted:

- All calls
- External calls only
- Internal calls only

The following destinations are possible for call forwarding:

- Other phone (internal or external)
- Attendant Console
- Voicemail Box
- Hunt Group
- UCD group (UCD Universal Call Distribution)

Outgoing calls can still be made when call forwarding is activated.

### **External destination**

If the call forwarding destination is external, you must enter the trunk access code followed by the external phone number of the forwarding destination.

### **Call Forwarding to External Destinations**

If a subscriber has entered an external call forwarding destination in his or her call destination list, forwarding ends at this destination, and any further call forwarding destinations that may have been entered in call destinations list are ignored.

If call forwarding to additional destinations is to occur, the system flag **Hunting to external call forwarding destination** must be activated by the service technician.

If call forwarding to an external destination is to be followed even for a call over an analog trunk, the system flag **Call forwarding to main station interface permitted** must be activated by the service technician.

**Dependencies**

Topic	Dependency
Do Not Disturb	You cannot program call forwarding to a telephone where DND is active.
Appointment, automatic wake-up system	If an appointment comes due, it is signaled at the forwarded telephone, irrespective of any active call forwarding settings.
UCD group as call forwarding destination	<p>A call is not forwarded to a UCD group in the following cases:</p> <ul style="list-style-type: none"> <li>• If a hunt group is called and a subscriber with call forwarding to a UCD group is next, this call is not forwarded. In this case, the next station in the hunt group is immediately called.</li> <li>• A subscriber is a member of a group call with the property "Group" and has activated call forwarding to a UCD group.</li> <li>• A station is a member of a group call no answer. If the group is called, the call is not forwarded to the UCD group. Exception: The first subscriber entered has activated call forwarding to a UCD group. In this case, the call is forwarded.</li> </ul>

**9.4.4 Call Forwarding After Timeout**

Call Forwarding after Timeout forwards unanswered calls after a specific period of time. Call Forwarding after Timeout is analogous to Call Forwarding No Answer, the only difference being that subscribers can set the call forwarding themselves.

The subscriber can set call forwarding after timeout for his or her own phone and can also enter external destinations and groups.

The call deflection destination is not permanently saved, but deleted after you deactivate the feature.

If a subscriber is busy, the rules of call forwarding - no answer apply, that is, the system proceeds to the next destination.

**System-Specific Information**

You can set three destinations for each station. In addition, there is also a special ID "User-defined", via which the administrator can release or lock the Call Forwarding after Timeout feature for a station. The feature is released by default.

If a call is not answered after the preset timeout, the system searches for and calls the call deflection destination saved. If the subscriber has not entered an individual call deflection destination, the system proceeds with the next destination in the call destination list.

The administrator must release the call forwarding after a timeout for the individual subscribers via the call destination lists.

## 9.4.5 External Call Forwarding - No Answer (Not for U.S.)

Every station assigned an MSN (multiple subscriber number at the ISDN point-to-multipoint connection) as a DID number can activate or deactivate call forwarding—no answer for this MSN, provided that the user is authorized to use external call forwarding—no answer.

If you have assigned an MSN to a subscriber group, any member of the group can activate and deactivate external call forwarding-no answer for this MSN.

Users can enter only one forwarding destination per MSN. A total of 10 multiple subscriber numbers can be forwarded.

There are three different versions of the feature:

- Call Forwarding Unconditional (CFU): The network provider forwards all calls to this MSN directly, regardless of the MSN status.
- Call Forwarding Busy (CFB): Calls are forwarded only if the MSN dialed is busy.
- Call Forwarding No Reply (CFNR): Calls are forwarded only if the destination does not answer the incoming call within a preset period of time.

### Dependencies

Topic	Dependency
Night service	External call forwarding—no answer has a higher priority than night service.

## 9.4.6 Ringing Assignment / Call Allocation

The ringing assignment enables incoming calls of an analog or  $S_0$  trunk to be forwarded to a station or group, depending on the dialed number and the activation state of the night service.

Different destinations are possible for the day and night service. An incoming call is not signaled at the called station, but according to the call destination lists for that station.

## 9.4.7 Rejecting Calls

The subscriber can reject internal and external incoming initial calls. These calls can be rejected by pressing the Disconnect key.

The rejected call is then forwarded in accordance with the CFNA instruction. If there is no other call forwarding destination, an external call is intercepted by the attendant console, provided the relevant intercept criteria were configured. If no destination can be called, the caller continues to receive a busy signal.

Transferred recalls, queued callbacks, held or parked calls cannot be rejected. An intercepted call sent to the Intercept position cannot be rejected.

**Dependencies**

Topic	Dependency
Group call, hunt group call, MULAP	In these cases, the entire group call is terminated and the call follows the call forwarding instruction configured. The call is terminated if there is no other call destination.

**9.4.8 Deferring a Call**

Subscribers are provided the option of deferring an incoming call. The subscriber called can set up a connection without picking up the incoming call.

The waiting call is then signaled as a camped-on call.

If an incoming call is signaled, the subscriber can press a call or trunk key to conduct the external call. Two call keys and one trunk key must be programmed for this. One of the relevant keys must be free to execute the feature.

The calling party does not notice a change in signaling if call waiting is set for ringing on call waiting.

**9.4.9 Do Not Disturb**

Do Not Disturb prevents incoming calls from being put through.

A subscriber who has activated DND hears a special dial tone when he or she lifts the handset. When active, the Do Not Disturb feature is also indicated on display phones. In all other phones, the LED on the DSS key flashes with a brief interruption on stations where Do Not Disturb is active.

The Do Not Disturb feature, if set, can be overridden by the Attendant or an authorized subscriber. The call can also be immediately put through for a subscriber with an active Do Not Disturb feature.

A caller who dials a telephone with DND activated receives a busy signal and is not allowed to camp on.

## Dependencies

Topic	Dependency
Attendant/night destination	The attendant and the current intercept position cannot activate the Do Not Disturb feature.
Call forwarding	You cannot specify DND if call forwarding is active on the same telephone. You cannot activate call forwarding to a telephone with DND.
Callback	If a callback is initiated to a station with DND activated, the callback is not executed until DND is deactivated. If the subscriber with DND activated initiates a callback, this will override the DND function.
Appointment, automatic wake-up system	If a station has set an appointment and activated DND, an audible signal is sent to the telephone when the appointment comes due.
DISA	DISA can be activated by the subscriber for his or her own phone or by a user for another phone (associated services).

## 9.5 Optimizing Communication (LX/MX)

The communication system offers various options to conveniently and effectively handle calls, e.g., through callbacks or call waiting.

### 9.5.1 Callback

A callback can then be activated if the subscriber called does not answer or is busy. An active callback triggers a call as soon as the called subscriber is available.

#### Automatic Callback When Free or Busy

If a call cannot be set up because the subscriber called is busy or does not accept the call, the calling subscriber can activate a callback to set up the call at a later time. If the subscriber called was busy, the Callback function monitors the call to see when it ends. The calling subscriber receives a signal in the form of a call from the communication system when the other subscriber's line is free. If he or she accepts this call, the subscriber who was previously busy is redialed. If a call set up via the Callback function is not successful, this function remains active. The callback attempt is repeated once the required subscriber has conducted another call.

A telephone can initiate up to two Callback requests and be the destination for up to two requests. Any further outgoing requests are rejected.

Callback requests are deleted when

- the call is completed; if not, the callback remains in effect (for an internal callback),
- the callback was established without a call being completed (for an external callback),
- the initiator cancels the request,
- the system deletes all callbacks daily at 23:57.

Callback requests can be made for internal subscribers and groups. Callback requests for a group call are stored at the first subscriber. When a callback is made to a group, the ring is heard at all phones that are free.

#### **Automatic Call Completion on No Reply (CCNR) on the Trunk Interface**

An internal subscriber who cannot reach an available external subscriber can activate a callback request at the central office. The system then monitors the connection of the called subscriber. As soon as the called subscriber initiates a connection setup and then ends this connection, the central office attempts to establish a connection between the two subscribers. This feature must be supported by the central office.

#### **Callback on busy**

This feature sets enables a manual callback to be set on an external station that is busy. When the station becomes free, the trunk attempts to set up a connection between the two stations. The feature must be supported and enabled by the central office and peer.

## **9.5.2 Call waiting**

Call waiting signals the arrival of a further incoming call to a subscriber who is on the phone.

The incoming call is visually signaled by a message on the display. It can also be signaled acoustically by a short call waiting tone. The call waiting tone can be heard every 5 seconds.

The subscriber called can accept this second call or ignore it. To answer the second caller, the subscriber can optionally end the first call and answer the second or select the **Call waiting** function offered in the display. In the latter case, the first call is placed on hold.

You cannot camp on to a subscriber if someone is already camped on (a maximum of 4 subscribers can camp on) or if the subscriber has activated call waiting rejection. The caller receives a busy signal if call forwarding—busy is not configured.

#### **Enabling Call Waiting**

If the **Call waiting rejection** flag is set, the subscriber can use a menu or code to either enable or suppress call waiting. If a subscriber has enabled call waiting, an incoming call is camped on if call forwarding—busy is configured.

### Call Waiting (Camp On) by Attendant Console

The default setting is always "call waiting after timeout". However, the Attendant Console can also camp on immediately.

#### Dependencies

Topic	Dependency
Call waiting tone	The subscriber can activate/deactivate the call waiting tone with a code. Call waiting is still visually signaled on the phone's display. The call waiting tone is active by default.
Override	If call waiting rejection is active, an ongoing call by this subscriber cannot be overridden.
Group Call	If one or more stations in a group call are free, the call will be offered to them. If all stations are busy, all of them receive a call waiting signal, apart from any stations where call waiting rejection is active.
Speaker call	Speaker calls to busy stations are not possible.

### 9.5.3 Override

The Override feature enables an authorized subscriber to override (i.e., intrude into) a call of another internal subscriber.

The override (intrusion) occurs by means of a code or key, and the subscriber involved is notified by a warning tone (beep) and a visual signal on the display.

The feature can be invoked during the busy signal or during the camp on state.

During an override condition, the following applies:

- If the called party hangs up, he or she receives a call from the switching party.
- If the overriding party (who wants to switch the call and overrides) hangs up, the call is switched through to the destination station.
- If the party which was connected to the called party hangs up, the overridden and called parties remain connected.

You can configure every telephone connected to the system for this feature.

It is not possible to prevent an override to a particular telephone.

**Dependencies**

Topic	Dependency
Voice Channel Signaling Security	You cannot override a call if the called station or the internal party it is connected to is entered as a data station (voice channel signaling security), or if the called party is dialing a number.
Do Not Disturb	If the called station has activated Do Not Disturb, only one call can be overridden when the subscriber is conducting a call.
Hunt group	Busy override is not possible if all stations are busy when a group or hunt group is called.
S <sub>0</sub> station	It is not possible to override an S <sub>0</sub> station.

**9.5.4 Advisory Messages**

The advisory message of a subscriber appears in the caller's display.

Variable parameters can also be assigned in advisory messages (also referred to as absence texts). These parameters (for example, time) are entered in the course of activation. Users can use the numeric keypad on the telephone to enter additional characters. The advisory message can be activated/deactivated at a phone via a code or a preconfigured function key.

**Dependencies**

Topic	Dependency
Call Forwarding (CF)	The called subscriber's advisory message is displayed and the call is forwarded.

**Background Information**

This feature can be activated/deactivated via a DISA connection, by its own station user or for another user with the aid of the feature Associated Services.

**9.5.5 Message Texts**

Message texts are internal system texts that can be selected by a subscriber and sent to internal subscribers.

A message text (also called an Info text) can be sent to one or more recipients.

If you want to send the text to all members of an internal group or an internal hunt group, you must specify the phone number of the group or the hunt group - not an individual subscriber - as the recipient.



The message is sent by pressing the relevant button or via the Send Message menu.

The message can be sent in idle, ringing, talk or busy state. In ringing state it is not necessary to specify the recipient's station number.

## **9.5.6 Associated Services**

An authorized station can control certain features on behalf of any other station, e.g., call forwarding, turning the lock code or hunt group on/off, etc. The effect is the same as if the feature involved were activated or deactivated by the other station itself.

The following features can be controlled on behalf of other stations:

- Call forwarding on / off
- COS changeover on / off
- Ringing group on / off
- Advisory message on / off
- Hunt Group and Group Call on / off
- Night service on / off
- Timed reminder on / off
- Send message / Delete sent message
- Edit lock code password
- UCD agent log in / log out
- UCD agent Available/Not available
- UCD agent Wrapup on / off
- UCD agent Night service on / off
- Forward Line Key (MULAP) on / off
- Resetting Activated Features

This is operated via a procedure. The station must specify the following:

- the code for Associated Services
- the station number of the subscriber for whom the action is to be performed.
- the code of the feature to be controlled

Before any subscriber can use the Associated Services, he or she must first disable the lock code of the other subscriber (if enabled).

## **9.5.7 Reset activated features**

You can reset specific features at your terminal using a code.

This is possible for the following functions:

- Call forwarding
- Delete received infos

**Functions at the Telephone (LX/MX)**  
 Optimizing Communication (LX/MX)

- Advisory message on / off
- Ringing group on / off
- Hunt group on / off
- Station number suppression on / off
- Silent camp-on on / off
- Do not disturb on / off
- Ringer cutoff on / off
- Appointment
- Cancel all callbacks

**9.5.8 Procedures**

The communication system lets the subscriber program a key with codes, phone numbers, and other dialing information. If a subscriber presses the Procedure key as a suffix or during a call, the communication system transmits the corresponding DTMF character (DTMF = dual tone multifrequency).

Sample applications:

- Code for callback
- Code for call waiting
- Code for override
- Digit string for voicemail or answering machine
- Trunk flash code + destination station number
- Code for controlling a service + destination phone number, for example, code for send/retrieve message (message waiting) + phone number + text number
- ACCT (account code) + trunk code + destination station number

Procedures that require PIN input cannot be saved.

Only the first key level supports Procedure keys.

Depending on the situation, a subscriber can use the following features in procedures:

Feature	Ready to dial	Busy	On the phone	Outgoing call	Incoming call
Directed call pickup	x	–	x	–	–
Call Forward on, (not for tenant systems; not for individual MSNs in an S <sub>0</sub> trunk connection)	x	–	x	x	–
External call forwarding on / off; toggle function; (not for tenant services);	x	–	x	x	–
Call forwarding, login/UCD (uniform call distribution), logout; toggle function	x	–	x	x	–
Call forwarding, night destination on / off; toggle function	x	–	x	x	–
Call forwarding per team configuration	x	x	x	x	x

<b>Feature</b>	<b>Ready to dial</b>	<b>Busy</b>	<b>On the phone</b>	<b>Outgoing call</b>	<b>Incoming call</b>
Advisory message on / off; toggle function	X	–	X	X	–
Associated Dialing	X	X	X	X	X
Associated Services	X	–	X	X	–
Speaker call	X	–	X	–	–
Release trunk (emergency trunk access)	X	–	X	X	–
Send message (message waiting)	X	–	X	X	–
Dial station speed dialing	X	–	X	X	–
Dial system speed dialing	X	–	X	X	–
DTMF transmission	–	–	X	–	–
DTMF transmission in the talk state using procedure key	X	X	X	X	X
Night service on / off; toggle function	X	–	X	X	–
Retrieve call; toggle function	–	X	X	X	–
Account code ACCT	X	–	X	–	–
Account code ACCT in prefix	X	–	X	–	–
Callback requests - display or delete; toggle function	X	–	–	–	–
Ringing group on / off; toggle function	X	–	X	X	–
Language selection	X	X	X	X	X
Telephone Data Service TDS	X	–	X	X	–
Door opener via adapter cabinet	X	X	X	X	X
Timed reminder; toggle function	X	X	X	X	X
Retrieval of an external call from common hold	X	X	X	X	X
System Telephone Lock	X	–	X	–	–

**System-Specific Information**

A procedure key can store up to 32 characters.

## 10 Working in a Team (Groups) (LX/MX)

Several features are provided by the communication system to enable and facilitate working in a team. Besides call pickup groups, group calls and hunt groups, this also includes groups with team and executive/secretary functions as well as voicemail box and fax box groups. The "UCD (Uniform Call Distribution)" feature enables incoming calls to be uniformly distributed to a group of users (UCD group).

### 10.1 Call Pickup Group, Group Call and Hunt Group (LX/MX)

The communication system offers several methods of combining stations into groups so that multiple subscribers and phones can be reached under one call number, for example, or a call to one station can also be signaled at other stations.

In the case of a call pickup group, a call for one member of the group is also signaled at all other group members.

With a group call, by contrast, all members can be reached via a single phone number (group phone number). The first station to answer the call is connected to the calling party.

For a hunt group, the incoming calls are distributed to the members. All members of the hunt group can be reached at the same phone number.

#### 10.1.1 Call pickup group

A call for a member of a call pickup group is also signaled at all other group members. The call can be accepted by all group members via a function key programmed for this purpose, the associated menu item or the code.

The call is signaled acoustically and visually (on the display) for the subscriber originally called. If configured, the call is also signaled via an LED.

The other group members are only notified of the call by a visual signal. The phone number or name of the subscriber originally called and the phone number or name of the caller are shown on the phone's display. The display of the station number or name of the caller can be disabled by an administrator with the **Expert** profile in **Expert mode**. If configured, the call is also signaled via an LED.

If the call is not accepted within four ring cycles (4 x 5 seconds), the other group members receive a warning tone (acoustic signaling). The time from the start of call signaling till the warning tone is not variable. The warning tone can be disabled for all group members by an administrator with the **Expert** profile in **Expert mode**.

If more than one call is received for a call pickup group, signaling occurs in the sequence in which the calls are received.

If recalls for members of a call pickup group are also to be picked up by other members in the group, this must be enabled by an administrator with **Expert** profile in **Expert mode**.

A station can belong to only one call pickup group.

Any call charges incurred for a picked-up call are accrued to the subscriber who picked up the call.

### SIP Phones

SIP telephones can be integrated in a call pickup group.

---

**INFO:** No programming of function keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of a call pickup group are not supported.

---

### Call Pickup Outside a Call Pickup Group

Another version of the feature is the "call pickup outside a call pickup group". This permits the pickup of calls for internal subscribers that do not belong to the same call pickup group. The call can be picked up via a function key programmed for this purpose, the associated menu item or by entering the specific call pickup code followed by the station number of the called station.

### Dependencies

Topic	Dependency
Callback	Recalls and callbacks are signaled at the other group members only if the station flag <b>Call Pickup after automatic recall</b> has been activated.
Do Not Disturb	Stations that have activated DND do not receive call pickup signaling.
ISDN Phones	It is not possible to include ISDN telephones in call pickup groups.
MULAP	It is not possible to include MULAP phone numbers in call pickup groups.

## 10.1.2 Group Call

A group call can be defined in cases where multiple subscribers need to be reached via a single phone number (group phone number). Incoming external and internal calls are signaled at the same time at all group member phones. The first station to answer the call is connected to the calling party.

Every member of a group call can also be reached at his or her own station number.

## Working in a Team (Groups) (LX/MX)

Call Pickup Group, Group Call and Hunt Group (LX/MX)

The group call must be assigned one of the following properties:

- **Group**  
Incoming calls are simultaneously signaled at all available group members. Available group members are subscribers who are not busy. If all group members are busy, a call is signaled by a camp-on tone. Call signaling continues at all group members (camp-on tone at busy group members) even if the subscriber hangs up.  
A caller hears the busy tone if all group members are busy and all have activated the DND feature. If a call forwarding destination has been defined for this group, the caller does not hear a busy tone, but is forwarded directly to the next call forwarding destination.
- **RNA**  
Incoming calls are simultaneously signaled at all group members. If a group member is busy, the entire group call is marked as busy. Other callers receive the busy tone.
- **Call waiting**  
Incoming calls are simultaneously signaled at all available group members. Available group members are subscribers who are not busy. A call is signaled by a camp-on tone for busy group members.  
This requires that all group members have the Do Not Disturb feature disabled.

Group calls are treated like stations by the Call forwarding—no answer function. In other words, if a call cannot be accepted by any of the members in a group call, it is redirected to a call forwarding destination in accordance with the call destination list. You can specify whether call forwarding should be performed on RNA (ring no answer) or busy.

When a call is not answered by any member of a group call, it appears as a missed call in the journal of the OpenScape Office clients of all members. An accepted call appears only in the journal of the member who answered the call.

An individual subscriber can belong to multiple group calls and hunt groups.

The group name assigned is shown on the internal caller's display. After a call is accepted, the name of the subscriber who accepted the call is displayed.

If a member has defined rules using the AutoAttendant, e.g., to forward calls, these rules will apply only to calls to his or her own station number. The rules are ignored for group calls.

An administrator with the **Advanced** profile can configure up to 8 stations per group call by using the **Group Call / Hunt Group** wizard. An administrator with the **Expert** profile can configure up to 20 stations per group call in **Expert mode**.

Every group call can be assigned a name containing up to 16 characters.

### **Voicemail Box for Group Call**

When setting up a group call, a voicemail box is created automatically. The call number of this voicemail box for the group call always matches that of the group call. If a group call is not accepted by any member, the call is forwarded to the

voicemail box for the group call. This requires the group call voicemail box to have been defined as the CFNA (call forwarding on no answer) destination of this group call.

If a member does not accept an incoming call to his or her own station number, this call is redirected to a call forwarding destination in accordance with the call destination list.

Example of a group call of type RNA (ring no answer) with the group call number 404 and the members A (call number 200), B (201) and C (202). Call Forwarding-No Answer after Timeout to the voicemail box of the group call was set up for the group call. Every member has defined Call Forwarding-No Answer (CFNA) after Timeout to his or her own voicemail box.		
Inbound call for Member A (200)	All members are free.	Member A does not accept the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of member A.
	Member A has defined Call Forwarding Unconditional (CFU) to his or her own voicemail box. Members B and C are free.	The call is forwarded immediately (CFU) to the voicemail box of member A.
Inbound call for the group call (404)	All members are free.	The call is signaled at all other members. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the group call.
	Member A has defined Call Forwarding Unconditional (CFU) to his or her own voicemail box. Members B and C are free.	The call is signaled at members B and C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the group call.
	Member A has defined Call Forwarding Unconditional (CFU) to an external destination. Members B and C are free.	The call is signaled at members B and C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the group call.
	Member A has defined CFNA rules using the AutoAttendant. Members B and C are free.	The call is signaled at all other members. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the group call.

### Activating/Deactivating a Group Call

If a subscriber is a member of a group call, he or she can use codes to leave and rejoin the group call.

## Working in a Team (Groups) (LX/MX)

Call Pickup Group, Group Call and Hunt Group (LX/MX)

If a subscriber is a member of both multiple group calls and multiple hunt groups, he or she can use codes to leave and rejoin all group calls and hunt groups. Subscribers are added to or removed from a specific group call or hunt group by entering codes and then making a selection from the group calls and hunt groups displayed.

You can also program function keys with a shift function for joining and leaving. You can program a function key here that applies for a specific group call and hunt group or all group calls and hunt groups. Variable programming is also possible. After you press a function key of this kind, you must select one of the group calls and hunt groups displayed to define the group call or hunt group you want to leave/join.

### Ring type

For every group call, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

### SIP Phones

SIP telephones can be integrated in a group call.

---

**INFO:** No programming of function keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of a group call are not supported.

---

### Dependencies

Topic	Dependency
Call forwarding	If a group member activates call forwarding for all calls, all calls are signaled at the destination telephone.
Do Not Disturb	If a group member activates the Do Not Disturb feature, incoming calls for his or her phone are not put through. This applies to calls via the group phone number and the member's own station number.
Override	Override is not possible if all members of a group call are busy.
ISDN Phones	It is not possible to include ISDN telephones in a group call.



### 10.1.3 Hunt Group

Hunt groups permit the distribution of incoming calls to associated subscribers (members). If a subscriber is busy or does not accept an incoming call, the call is automatically forwarded to the next free member of the hunt group. All members of the hunt group can be reached at the same phone number.

Every member of a hunt group can also be reached at his or her own station number.

The hunt group must be assigned one of the following properties.

- **Linear**  
An inbound call is always signaled first at the first member of a hunt group. Further signaling is performed on the basis of the sequence in which the members are entered in the group table.
- **Cyclic**  
An inbound call is always signaled first at the member that follows the subscriber who answered the last call. Further signaling is performed on the basis of the sequence in which the members are entered in the group table.

The call is automatically forwarded to the next free hunt group member when the forwarding time expires, provided the call is not answered or a member is busy or DND is activated.

You can program a call forwarding destination (call destination list) if a call cannot be answered by any of the members of the hunt group.

An individual subscriber can belong to multiple hunt groups and group calls.

The name assigned to the hunt group is shown on the internal caller's display. After a call is accepted, the name of the subscriber who accepted the call is displayed.

If a member has defined rules using the AutoAttendant, e.g., to forward calls, these rules will apply only to calls to his or her own station number. The rules are ignored for hunt group calls.

An administrator with the **Advanced** profile can configure up to 8 stations per hunt group by using the **Group Call / Hunt Group** wizard. An administrator with the **Expert** profile can configure up to 20 stations per hunt group in **Expert mode**.

Every hunt group can be assigned a name containing up to 16 characters.

#### **Voicemail Box for Hunt Group**

When setting up a hunt group, a voicemail box is automatically created for it. The call number of this voicemail box for the hunt group always matches that of the hunt group. If a call for a hunt group is not accepted by any member, the call is forwarded to the voicemail box for the hunt group. This requires the hunt group voicemail box to have been defined as the CFNA (call forwarding on no answer) destination of this hunt group.

If a member does not accept an incoming call to his or her own station number, this call is redirected to a call forwarding destination in accordance with the call destination list.

**Working in a Team (Groups) (LX/MX)**

Call Pickup Group, Group Call and Hunt Group (LX/MX)

<p>Example of a linear hunt group with the call number 404 and the members A (call number 200), B (201) and C (202). Call Forwarding-No Answer after Timeout to the voicemail box of the hunt group was set up for the hunt group. Every member has defined Call Forwarding-No Answer (CFNA) after Timeout to his or her own voicemail box.</p>		
<p>Inbound call for Member A (200)</p>	<p>All members are free.</p>	<p>Member A does not accept the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of member A.</p>
	<p>Member A has defined Call Forwarding Unconditional (CFU) to his or her own voicemail box. Members B and C are free.</p>	<p>The call is forwarded immediately (CFU) to the voicemail box of member A.</p>
<p>Inbound call for the hunt group (404)</p>	<p>All members are free.</p>	<p>The call is signaled first at member A, then at member B and then at member C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the hunt group.</p>
	<p>Member A has defined Call Forwarding Unconditional (CFU) to his or her own voicemail box. Members B and C are free.</p>	<p>The call is signaled first at member B and then at member C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the hunt group.</p>
	<p>Member A has defined Call Forwarding Unconditional (CFU) to an external destination. Members B and C are free.</p>	<p>The call is signaled first at member B and then at member C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the hunt group.</p>
	<p>Member A has defined CFNA rules using the AutoAttendant. Members B and C are free.</p>	<p>The call is signaled first at member A, then at member B and then at member C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the hunt group.</p>

**Activating/Deactivating the Hunt Group**

If a subscriber is a member of a hunt group, he or she can use codes to leave and rejoin the hunt group.

If a subscriber is a member of both multiple hunt groups and multiple group calls, he or she can use codes to leave and rejoin all hunt groups and group calls. Subscribers are added to or removed from a specific hunt group or group call by entering codes and then making a selection from the hunt groups and group calls displayed.

You can also program function keys with a shift function for joining and leaving. You can program a function key here that applies for a specific or all hunt groups and group calls. Variable programming is also possible. After you press a function key of this kind, you must select one of the hunt groups and group calls displayed to define the hunt group or group call you want to leave/join.

### Ring type

For every hunt group, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

### SIP Phones

SIP telephones can be integrated in a hunt group.

---

**INFO:** No programming of function keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of a hunt group are not supported.

---

### Dependencies

Topic	Dependency
Call forwarding	If a hunt group member activates call forwarding for all calls, all calls are signaled at the destination telephone.
Do Not Disturb	If a hunt group member activates the Do Not Disturb feature, incoming calls for his or her phone are not put through. This applies to calls for the hunt group and the member's own station number.
Queue	For cyclical and linear hunt groups, it is not possible to set up a call queue.
ISDN Phones	It is not possible to include ISDN telephones in hunt groups.

## 10.1.4 Configuring Call Pickup Groups, Group Calls and Hunt Groups using Wizards

Several different wizards are available to conveniently configure call pickup groups, group calls and hunt groups.

## Working in a Team (Groups) (LX/MX)

Team Configuration / Team Group and Executive/Secretary or Top Group (LX/MX)

The **Call Pickup** wizard can be used to combine subscribers into a group to enable mutual call pickups. The following application cases, which can be configured using the wizard, are described here:

- *How to Configure a Call Pickup Group*
- *Add or delete a member to or from a call pickup group*

The **Group Call / Hunt Group** wizard can be used to configure group calls of the type Group. The following application cases, which can be configured using the wizard, are described here:

- *How to Add a Group Call (Group)*
- *How to Edit a Group Call (Group)*
- *Deleting a Group Call (Group)*
- *How to Add or Delete a Member to or from a Group Call (Group)*
- *How to Add a Hunt Group*
- *How to Change a Hunt Group*
- *How to Delete a Hunt Group*
- *How to Add or Delete a Member to or from a Hunt Group*

### 10.1.5 Configuring Call Pickup Groups, Group Calls and Hunt Groups using Expert Mode

Besides the configuration options available through wizards, administrators with the **Expert** profile are also offered additional options to configure call pickup groups, group calls and hunt groups via the **Expert mode**.

The procedure for the following application cases, which can be configured using the **Expert mode** wizard, is described here:

- *How to Enable or Disable the Display of a Caller's Station Number and Name*
- *How to Activate or Deactivate the Warning Tone*
- *How to Enable or Disable Call Pickup for Recalls*
- *How to Add a Group Call (RNA or Call Waiting)*
- *How to Display or Edit a Group Call (RNA or Call Waiting)*
- *How to Delete a Group Call (RNA or Call Waiting)*
- *How to Add or Delete a Member to or from a Group Call (RNA or Call Waiting)*
- *How to Enable or Disable Do Not Disturb for a Group Member*

### 10.2 Team Configuration / Team Group and Executive/Secretary or Top Group (LX/MX)

A Team Configuration / Team Group offers several convenient team functions. The station numbers of all team members are programmed on MULAP keys (trunk keys). Every team member can thus access all trunks (for instance, for call

pickup) and can also conduct calls simultaneously via multiple trunks. An Executive/Secretary or Top Group offers convenient Executive and Secretary functions (Top function) for up to three executives and up to three secretaries.

## 10.2.1 Team Configuration / Team Group

MULAP (Multiple Line Appearance) keys (trunk keys) are programmed on a telephone with team function with the individual telephone's number and the phone numbers of all other team members. Every team member can access all trunks (for instance, for call pickup) and can also conduct calls simultaneously via multiple trunks. In addition, DSS keys with which the team members can directly call one another are programmed automatically.

The MULAP keys give team members access to the phone numbers of all members. An incoming call for a team member can thus also be accepted by all other members by pressing the flashing MULAP key. Team members can also toggle between multiple trunks. By pressing a MULAP key, a team member can make an outbound call via the associated line. The station number of this line will then appear on the display of the called party.

Incoming calls are visually signaled at the same time on all team member phones via the MULAP key LED. You can also specify for each team member if incoming calls should also be signaled acoustically.

Every team member can use a group call key to activate or deactivate incoming call signaling for each individual trunk.

An administrator with the **Advanced** profile can configure up to 3 stations per Team configuration/Team group by using the **Team Configuration** wizard. An administrator with the **Expert** profile can configure up to ten stations per Team configuration or Team group in **Expert mode**.

Every team configuration / team group can be assigned a name containing up to 16 characters.

When setting up a Team configuration or Team group, the following properties are assigned to its members (these settings can be changed by an administrator with the **Expert** profile in **Expert mode**):

- **Master**  
This parameter changes a member into a master of the Team configuration / Team group. If a master activates call forwarding, this applies to all members (phones) in the Team configuration / Team group.  
Default setting: master is the first member of the Team configuration / Team group.
- **Acoustic ring**  
If this parameter is activated, incoming calls are signaled acoustically.  
Default setting: the parameter is activated.

## Working in a Team (Groups) (LX/MX)

Team Configuration / Team Group and Executive/Secretary or Top Group (LX/MX)

- **Automatic seizure outgoing**  
If this parameter is active, a call is automatically made via the MULAP trunk of this member on lifting the handset. If the parameter is not active, the subscriber must press the MULAP key before dialing is possible.  
Default setting: the parameter is activated.
- **No automatic incoming call acceptance**  
If this parameter is activated, you cannot answer an incoming call by lifting the handset. An incoming call must be accepted by pressing the MULAP key.  
Default setting: the parameter is not activated.
- **Automatic conference release**  
If the parameter is active, you can release the seized MULAP line for a conference by pressing the MULAP key. The release of this line is signaled to all other members by the flashing MULAP key. They can join the conference by pressing the MULAP key.  
Default setting: the parameter is not activated.
- **MULAP key set up**  
If the parameter is active, a MULAP key is programmed on the associated phone. Pressing the key sets up an outgoing call via the MULAP trunk of the master. The MULAP station number of the master appears on the called party's display.  
Default setting: the parameter is not activated.

### Using MULAP Keys

Every team member is assigned a separate trunk (MULAP trunk). The member's own trunk and the trunks of all other members are programmed as MULAP keys (trunk keys) for every team member. This means that every team can use all available MULAP trunks.

The LED on a MULAP key (trunk key) can have different statuses with the following meaning:

- Off: the relevant trunk is free and can be used.
- Lit: the relevant trunk is busy.
- Flashing fast: call on the relevant trunk.
- Flashing slow: an on-hold call is waiting on the relevant trunk.

### Using DSS Keys

Every team member has a DSS key for every other team member. This means that team members can reach each other directly at the push of a button.

A Direct Station Select (DSS) key can also be used to quickly transfer an existing call to the team member programmed on it.

The LED on a DSS key can have different statuses with the following meanings:

- Off: the associated Team member is not conducting a call.
- Lit: the associated Team member is conducting a call or has activated Do Not Disturb.
- Flashing fast: the associated Team member is conducting a call. The call can be accepted by pressing the Direct Station Select (DSS) key.

- Flashing slowly: the associated Team member is being called and has not yet answered. The call can be accepted by pressing the Direct Station Select (DSS) key.

**Ring type**

For every Team configuration / Team group, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

**Fax Box for Team Configuration / Team Group**

For each Team configuration or Team group, a fax box can be set up via which the members can receive Fax messages directly through myPortal for Desktop or myPortal for Outlook. As a prerequisite, at least one member must be licensed as a Comfort Plus User.

If a fax box was already configured for the master (the first member) of the Team configuration/Team group, this fax box is taken over when setting up the Team configuration/Team group. Previously configured fax boxes of other members are deleted.

After a Team configuration or Team group is dissolved, only the prior master (i.e., the first member) can use his or her fax box.

**SIP Phones**

SIP telephones can be integrated in a Team configuration / Team group. As a prerequisite, a system telephone (IP phone, HFA) must have been defined as the first member of the Team configuration / Team group.

Dual-mode mobile phones that are configured as Mobility Entry stations, for example, can be integrated. Dual-mode mobile phones support both GSM/UMTS networks and WLAN networks. A dual-mode mobile phone can be registered as an IP station (SIP client) at the communication system over a WLAN.

---

**INFO:** No programming of MULAP keys and DSS keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of the Team configuration / Team group are not supported.

---

## Working in a Team (Groups) (LX/MX)

Team Configuration / Team Group and Executive/Secretary or Top Group (LX/MX)

### Dependencies

Topic	Dependency
Call forwarding	One team member has activated call forwarding for all calls. In this case, all calls for his or her own station number will be forwarded.
Do Not Disturb	If a Team member activates the Do Not Disturb feature, incoming calls are not put through.
ISDN Phones	It is not possible to include ISDN telephones in Team configurations / Team groups.

---

### Related Topics

- [Direct station select](#)

## 10.2.2 Executive/Secretary or Top Group

Top groups can be configured if you need user-friendly executive and secretary functions (Top function).

Executive/secretary functions can be configured for groups with up to three executives and up to three secretaries.

---

**INFO:** The terms "executive" and "secretary" also apply to groups with more than one executive and more than one secretary. The terms "executive" and "secretary" used in this document are gender-neutral.

---

Every Top member (every executive and every secretary) is assigned a separate trunk, known as a MULAP (Multiple Line Appearance) trunk. The member's own MULAP trunk and the MULAP trunks of all other members are programmed as MULAP keys (trunk keys) for every Top member. The MULAP phone number is shown on the called party's display for outgoing calls via the MULAP trunk. The Secretary station can make calls via its own trunk or the MULAP trunk of all executives and other secretary stations. For example, if a connection is to be set up for an executive, the MULAP trunk of that executive can be used.

DSS keys are also programmed to allow the executive to call the secretary directly, and vice versa.

Incoming calls are visually signaled at the same time on all Top member phones via the LED on the trunk key. You can also specify for each Top member if incoming calls should also be signaled acoustically. Acoustic signaling depends here on the ring transfer key.



You can use a ring transfer key to change the signaling for incoming calls. Incoming calls are signaled either at the executive or secretary phone. If the executive presses the ring transfer key, incoming calls will still be displayed to the executive via a tray pop. Accepting a call can, however, only be done via an appropriate key on the phone and not via the tray pop.

You can use a group call key on Secretary phones to add or remove the station to or from the Executive/Secretary configuration or Top group. In this case, ring transfer has priority.

---

**INFO:** If the secretary uses the group call key to leave the Executive/Secretary configuration or Top group without activating ring transfer for the executive, incoming calls are not signaled at either the executive or the secretary.

---

An administrator with the **Advanced** profile can define up to two executives and two secretaries per Executive/Secretary configuration or Top group using the **Executive/Secretary** wizard. An administrator with the **Expert** profile can define up to three executives and three secretaries per Executive/Secretary configuration or Top group in **Expert mode**.

For every executive, a maximum of three phones can be set up; for every secretary, a maximum of two phones.

Every Executive/Secretary configuration or Top group can be assigned a name containing up to 16 characters.

When setting up an Executive/Secretary configuration or Top group, the following properties are assigned to its members (these settings can be changed by an administrator with the **Expert** profile in **Expert mode**):

- **Master**  
This parameter assigns executive functions to a member. The Executive MULAP trunk is automatically selected for a call on lifting the handset. Incoming calls via the associated Executive MULAP phone number are only signaled visually by default.  
Default setting: All executives of the Executive/Secretary configuration or Top group receive Executive functions.
- **Acoustic ring**  
If this parameter is activated, incoming calls are signaled acoustically.  
Default setting: the parameter is active for all members with the secretary function.
- **Automatic seizure outgoing**  
If this parameter is active, a call is automatically made via the MULAP trunk of this member on lifting the handset. If the parameter is not active, the subscriber must press the MULAP key before dialing is possible.  
Default setting: the parameter is activated for all members.
- **No automatic incoming call acceptance**  
If this parameter is activated, you cannot answer an incoming call by lifting the handset. An incoming call must be accepted by pressing the MULAP key.  
Default setting: the parameter is not activated.

## Working in a Team (Groups) (LX/MX)

Team Configuration / Team Group and Executive/Secretary or Top Group (LX/MX)

- **Automatic conference release**

If the parameter is active, you can release the seized MULAP line for a conference by pressing the MULAP key. The release of this line is signaled to all other members by the flashing MULAP key. They can join the conference by pressing the MULAP key.

Default setting: the parameter is not activated.

- **MULAP key set up**

If the parameter is active, a MULAP key is programmed on the associated phone. You can press the key to set up an outgoing call via the Executive MULAP trunk. The Executive MULAP phone number appears on the called party's display.

Default setting: the parameter is activated.

### Using MULAP Keys

Every Top member is assigned a separate trunk (MULAP trunk). The member's own trunk and the trunks of all other members are programmed as MULAP keys (trunk keys) for every Top member. This means that every Top member can use all available MULAP lines.

The LED on a MULAP key (trunk key) can have different statuses with the following meaning:

- Off: the relevant trunk is free and can be used.
- Lit: the relevant trunk is busy.
- Flashing fast: call on the relevant trunk.
- Flashing slowly: an on-hold call is waiting on the relevant trunk or the relevant trunk was released for a conference.

### Using DSS Keys

Every Top member has a DSS key for every other Top member. This means that Top members can reach each other directly at the push of a button.

A Direct Station Select (DSS) key can also be used to quickly transfer an existing call to the Top member programmed on it.

The LED on a DSS key can have different statuses with the following meanings:

- Off: The associated Top member is not conducting a call.
- Lit: the associated Top member is conducting a call or has activated Do Not Disturb.
- Flashing fast: the associated Top member is conducting a call. The call can be accepted by pressing the Direct Station Select (DSS) key.
- Flashing slowly: the associated Top member is being called and has not yet answered. The call can be accepted by pressing the Direct Station Select (DSS) key.

### Ring type

For every Executive/Secretary configuration or Top group, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)

- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

**Fax Boxes for Executive/Secretary Configuration or Top Group**

For each member of an Executive/Secretary configuration or Top group, a fax box can be set up via which the members can receive Fax messages directly through myPortal for Desktop or myPortal for Outlook. As a prerequisite, at least one member must be licensed as a Comfort Plus User.

If a fax box was already configured for the first executive of the Executive/Secretary configuration or Top group, this fax box is taken over when setting up the Executive/Secretary configuration or Top group. Previously configured fax boxes of other members are deleted.

After an Executive/Secretary configuration or Top group is dissolved, only the prior first executive can use his or her fax box.

**SIP Phones**

SIP telephones can be integrated in an Executive/Secretary configuration or Top group. As a prerequisite, a system telephone (IP phone, HFA) must have been defined as the first member of the Executive/Secretary configuration or Top group (Exec. 1).

Dual-mode mobile phones that are configured as Mobility Entry stations, for example, can be integrated. Dual-mode mobile phones support both GSM/UMTS networks and WLAN networks. A dual-mode mobile phone can be registered as an IP station (SIP client) at the communication system over a WLAN.

---

**INFO:** No programming of MULAP keys and DSS keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of the Executive/Secretary configuration / Top group are not supported.

---

**Dependencies**

Topic	Dependency
Call forwarding	A Top member has activated call forwarding for all calls. In this case, all calls for his or her own station number will be forwarded.
Do Not Disturb	If a Top member activates the Do Not Disturb feature, incoming calls are not put through.
ISDN Phones	It is not possible to include ISDN or SIP phones in Executive/Secretary configurations or Top groups.

---

**Related Topics**

- [Direct station select](#)

### **10.2.3 Configuring Team Configurations / Team Groups and Executive/Secretary Functions / Top Groups using Wizards**

Several different wizards are available to conveniently configure team configurations (team groups) and executive/secretary functions (top groups).

The **Team Configuration** wizard can be used to set up Team configurations (Team groups). The following application cases, which can be configured using the wizard, are described here:

- *Adding a Team Configuration / Team Group*
- *Editing a Team Configuration / Team Group*
- *Deleting a Team Configuration / Team Group*

The **Executive / Secretary** wizard can be used to configure convenient Executive and Secretary functions (Top function). The following application cases, which can be configured using the wizard, are described here:

- *How to Add an Executive/Secretary or Top Group*
- *How to Edit an Executive/Secretary or Top Group*
- *How to Delete an Executive / Secretary or Top Group*

### **10.2.4 Configuring Team configurations / Team groups and Executive/Secretary functions / Top groups using Expert mode**

Besides the configuration options available through wizards, administrators with the **Expert** profile are also offered additional options to configure Team configurations / Team groups and Executive/Secretary functions / Top groups via the **Expert mode**.

The procedure for the following application cases, which can be configured using the **Expert mode** wizard, is described here:

- *How to Add or Delete a Member to or from a Team Configuration or Team Group*
- *How to Edit a Member of a Team Configuration / Team Group*
- *How to Edit the Properties of Members in a Team Group*
- *How to Change the Programmed Feature Keys for a Team Configuration / Team Group*
- *How to Add a Fax Box to a Team Configuration / Team Group*
- *How to Add or Delete a Member to or from an Executive/Secretary or Top Group*
- *How to Edit a Member of an Executive/Secretary or Top Group*

- *How to Edit the Properties of an Executive/Secretary or Top Group*
- *How to Add a Fax Box to an Executive/Secretary or Top Group*

## 10.3 Basic MULAP and Executive MULAP (LX/MX)

A Basic MULAP enables a subscriber who uses multiple telephones (e.g., a fixed-network telephone and a mobile phone) to be reached under a single phone number. You can configure Executive MULAPs if you want to use restricted executive and secretary functions.

### 10.3.1 Basic MULAP

Basic MULAPs can be configured if a subscriber is using a number of different phones (for example, a fixed-network phone and mobile phone) but would like to be reached at a single phone number (Basic MULAP phone number).

If a caller rings the Basic MULAP phone number, the call is visually signaled at all phones belonging to the Basic MULAP. The subscriber can also set whether or not incoming calls should also be acoustically signaled for each individual member. The status of the Basic MULAP changes to busy and other callers hear the busy signal when a call is answered.

The Basic MULAP phone number is shown on the called party's display for outgoing calls via the Basic MULAP trunk.

Up to 20 members can be configured per Basic MULAP.

Every Basic MULAP can be assigned a name containing up to 16 characters.

Each of the subscriber's phones is a member of the Basic MULAP and each member can be assigned the following properties:

- **Master**  
This parameter changes a member into a master of the Basic MULAP. If a master activates call forwarding, this feature applies to all members (phones) in the Basic MULAP. If the master activates an automatic callback on a Basic MULAP, the callback is initiated as soon as all masters are free.  
Default setting: master is the first member of the Basic MULAP.
- **Acoustic ring**  
If this parameter is activated, incoming calls are signaled acoustically.  
Default setting: the parameter is active for all masters.
- **Automatic seizure outgoing**  
If this parameter is active, the Basic MULAP trunk is automatically called when the subscriber lifts the handset. If the parameter is not active, the subscriber must press the MULAP key before dialing is possible.  
Default setting: automatic outgoing seizure is assigned to all masters.

- **No automatic incoming call acceptance**  
If this parameter is activated, you cannot answer an incoming call by lifting the handset. An incoming call must be accepted by pressing the MULAP key.  
Default setting: the parameter is not activated.
- **Automatic conference release**  
If the parameter is active, you can release the seized MULAP line for a conference by pressing the MULAP key. The release of this line is signaled to all other members by the flashing MULAP key. They can join the conference by pressing the MULAP key.  
Default setting: the parameter is not activated.
- **MULAP key set up**  
If the parameter is active, a MULAP key is programmed on the associated phone. You can press the key to set up an outgoing call via the Basic MULAP trunk. The Basic MULAP number appears on the called party's display.  
Default setting: the parameter is activated.

### **Using MULAP Keys**

The LED on a MULAP key can have different statuses with the following meaning:

- Off: the relevant trunk is free and can be used.
- Lit: the relevant trunk is busy.
- Flashing fast: call on the relevant trunk.
- Flashing slowly: an on-hold call is waiting on the relevant trunk or the relevant trunk was released for a conference.

### **Ring type**

For every Basic MULAP, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

### **SIP Phones**

SIP telephones can be integrated in a Basic MULAP. As a prerequisite, a system telephone (IP phone, HFA) must have been defined as the first member of the Basic MULAP.

Dual-mode mobile phones that are configured as Mobility Entry stations, for example, can be integrated. Dual-mode mobile phones support both GSM/UMTS networks and WLAN networks. A dual-mode mobile phone can be registered as an IP station (SIP client) at the communication system over a WLAN.

---

**INFO:** No programming of MULAP keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of the Basic MULAP are not supported.

---

### Dependencies

Topic	Dependency
Do Not Disturb	When Do Not Disturb is activated, incoming calls are no longer put through.
ISDN Phones	It is not possible to include ISDN telephones in Basic MULAPs.

## 10.3.2 Executive MULAP

You can configure Executive MULAPs if you want to use restricted executive and secretary functions.

All members of an Executive MULAP can be reached at the Executive MULAP phone number as well as at their personal station numbers.

---

**INFO:** The terms "executive" and "secretary" used in this document are gender-neutral.

---

Up to 20 members can be configured per Executive MULAP.

Every Executive MULAP can be assigned a name containing up to 16 characters.

The parameters described below define which members of an Executive MULAP can use executive functions (Executive) and which can use secretary functions (Secretary).

If a caller rings the Executive MULAP phone number, the call is visually signaled at all phones belonging to the Executive MULAP. Incoming calls are also signaled acoustically for members with secretary functions.

The Executive MULAP phone number is shown on the called party's display for outgoing calls via the Executive MULAP trunk.

The members of an Executive MULAP can be assigned the following properties:

- **Master**  
This parameter is used to assign executive functions to a member. The Executive MULAP trunk is automatically selected for a call when you lift the handset. Incoming calls via the Executive MULAP phone number are only signaled visually.  
Default setting: the first member of the Executive MULAP is assigned executive functions.
- **Acoustic ring**  
If this parameter is activated, incoming calls are signaled acoustically.  
Default setting: the parameter is active for all members with the secretary function.
- **Automatic seizure outgoing**  
If this parameter is active, the Executive MULAP trunk is automatically called when you lift the handset. If the parameter is not active, the subscriber must press the MULAP key before dialing is possible.  
This parameter cannot be used by members with the secretary function.  
Default setting: the parameter is active for all members with the executive function.
- **No automatic incoming call acceptance**  
If this parameter is activated, you cannot answer an incoming call by lifting the handset. An incoming call must be accepted by pressing the MULAP key.  
Default setting: the parameter is not activated.
- **Automatic conference release**  
If the parameter is active, you can release the seized MULAP line for a conference by pressing the MULAP key. The release of this line is signaled to all other members by the flashing MULAP key. They can join the conference by pressing the MULAP key.  
Default setting: the parameter is not activated.
- **MULAP key set up**  
If the parameter is active, a MULAP key is programmed on the associated phone. You can press the key to set up an outgoing call via the Executive MULAP trunk. The Executive MULAP phone number appears on the called party's display.  
Default setting: the parameter is activated.

### **Using MULAP Keys**

The LED on a MULAP key can have different statuses with the following meaning:

- Off: the relevant trunk is free and can be used.
- Lit: the relevant trunk is busy.
- Flashing fast: call on the relevant trunk.
- Flashing slowly: an on-hold call is waiting on the relevant trunk or the relevant trunk was released for a conference.

### **Ring type**

For every Executive MULAP, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:



- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

### SIP Phones

SIP telephones can be integrated in an Executive MULAP. As a prerequisite, a system telephone (IP phone, HFA) must have been defined as the first member of the Executive MULAP (Exec. 1).

Dual-mode mobile phones that are configured as Mobility Entry stations, for example, can be integrated. Dual-mode mobile phones support both GSM/UMTS networks and WLAN networks. A dual-mode mobile phone can be registered as an IP station (SIP client) at the communication system over a WLAN.

---

**INFO:** No programming of MULAP keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of the Executive MULAP are not supported.

---

### Dependencies

Topic	Dependency
Do Not Disturb	When Do Not Disturb is activated, incoming calls are no longer put through.
ISDN Phones	It is not possible to include ISDN telephones in Executive MULAPs.

## 10.3.3 Configuring Basic MULAPs and Executive MULAPs

The configuration of Basic and Executive MULAPs can only be performed by an administrator with the **Expert** profile and in **Expert mode**.

The procedure for the following application cases, which can be configured using the **Expert mode** wizard, is described here:

- *How to Add a Basic MULAP*
- *Display or Edit a Basic MULAP*
- *How to Delete a Basic MULAP*
- *How to Add or Delete a Member to or from a Basic MULAP*
- *How to Edit a Member of a Basic MULAP*
- *How to Add an Executive MULAP*
- *How to Display or Edit an Executive MULAP*
- *How to Delete an Executive MULAP*
- *How to Add or Delete a Member to or from an Executive MULAP*

- *How to Edit a Member of an Executive MULAP*

## 10.4 Voicemail Group and Fax Box Group (LX/MX)

A voicemail group enables a subscriber group to access voicemails. When a call is placed to the call number of a voicemail group, the call is sent directly to the voicemail box (i.e., the voicemail) of the group and not to the group members. A fax box group (fax group) enables a subscriber group to access fax messages. The fax box of the group is reached directly via the station number of the fax box group.

### 10.4.1 Voicemail Group

A voicemail group enables a specific group of subscribers to access voicemails. When a call is placed to the call number of a voicemail group, the call is sent directly to the voicemail box (i.e., the voicemail) of the group and not to the group members. After a voicemail is left in the voicemail box of the group, it is forwarded to the voicemail boxes of all members.

All members receive the voicemail simultaneously. Whenever a member deletes a voicemail, this voicemail is also deleted from the voicemail boxes of all members and the voicemail box of the group. The personal voicemails of all members are not affected by this.

Every member of a voicemail group can be reached under his or her own station number.

Up to 20 members can be configured per voicemail group.

Every voicemail group can be assigned a name containing up to 16 characters.

#### Dependencies

Topic	Dependency
Ringling group on	The <i>Ringling group</i> feature cannot be used.

### 10.4.2 Fax Box Group

A fax box group (fax group) enables a specific group of subscribers to access fax messages. The fax box of the group is reached directly via the station number of the fax box group. After a fax message is left in the fax box of the group, it is forwarded to the fax boxes of all members.

All members receive the fax message simultaneously. Whenever a member deletes a fax message, this voicemail is also deleted from the fax boxes of all members and the fax box of the group.

Every member of a fax box group can be reached under his or her own station number.

Up to 20 fax box groups can be configured.

Every fax box group can be assigned a name containing up to 16 characters.

### 10.4.3 Configuring Voicemail Box Groups and Fax Box Groups

The configuration of voicemail box groups and fax box groups can only be performed by an administrator with the **Expert** profile and in **Expert mode**.

The procedure for the following application cases, which can be configured using the **Expert mode** wizard, is described here:

- *Add a voicemail group*
- *Display or edit a voicemail group*
- *Delete a voicemail group*
- *Add or delete a member to or from a voicemail group*
- *Edit a member of a voicemail group*
- *Configure a fax box group*
- *Display or edit a fax box group*
- *Add or delete a member to or from a fax box group*

## 10.5 Speaker Call for Groups (LX/MX)

Speaker call for groups enable the broadcasting of announcements to all internal members of a group.

### 10.5.1 Internal Paging

Internal paging enables up to eight internal members of a group to be addressed directly. This feature is also known as a group broadcast. Internal paging is not performed for group members who are busy or have activated the Do Not Disturb feature. Group members have no direct answering option. Answering is only possible by lifting the handset, which results in a transition to a normal two-way conversation.

Internal paging can be used via a function key programmed for this purpose, the menu item **Speaker call** or by entering the appropriate code and then dialing the station number of the target group. A function key can also be programmed with a group phone number. A connection to the programmed group is immediately set up when you press a function key of this kind.

### Dependencies

Topic	Dependency
Do Not Disturb	Group members who have activated DND do not receive any announcements.
ISDN phones, SIP phones	The "Internal Paging" feature cannot be used with ISDN or SIP phones.

## 10.5.2 Transfer to Group from Announcement

A call on consultation hold can be transferred to a group via Transfer from Announcement. An announcement to the group is initiated for this (internal paging). The system sets up a two-party call when another party in the group lifts the handset or turns on the loudspeaker and the party who transferred the call hangs up. The connection is cleared down for the other group members.

Internal paging can be used via a function key programmed for this purpose, the menu item **Speaker call** or by entering the appropriate code and then dialing the station number of the target group. A function key can also be programmed with a group phone number. A connection to the programmed group is immediately set up when you press a function key of this kind.

### Dependencies

Topic	Dependency
Do Not Disturb	Group members who have activated DND do not receive any announcements.
ISDN phones, SIP phones	The "Transfer to Group from Announcement" feature cannot be used with ISDN and SIP phones.

## 10.6 UCD (Uniform Call Distribution) (LX/MX)

The Uniform Call Distribution (UCD) feature of the communication system enables incoming calls to be uniformly distributed to a group of stations (UCD-group).

UCD groups are primarily used in technical hotline environments (e.g., customer service hotlines), for managing complaints, in market research, order processing and acceptance (e.g., by mail-order companies and ticketing services) and even for emergency services.

As a rule, call distribution occurs by sending an incoming call to a UCD group to the station (agent) in the UCD group whose last call lies furthest in the past. It is also possible to define other distribution rules.

If there is no agent free to accept an incoming call, the call is automatically forwarded to a queue. Waiting calls are distributed to free agents on the basis of priority and wait time.

Announcements or music on hold can be played for waiting callers.

### **Configuration**

The **UCD** wizard can be used to configure groups and stations for intelligent call distribution (UCD). The following application cases, which can be configured using the wizard, are described here:

- *Configuring Call Distribution / UCD Groups*
- *Adding/Deleting UCD Agents*
- *Changing Announcements / Music on Hold for UCD*

Besides the configuration options available through wizards, administrators with the **Expert** profile are also offered additional configuration options in **Expert mode**.

## **10.6.1 Call Distribution / UCD Group**

A UCD group contains agents (subscribers) that belong to a work group and can be reached at a single phone number. An incoming internal or external call is automatically delivered to the agent who is idle longest.

Every UCD group can be configured using OpenScape Office Assistant (in **Expert** mode) so that incoming calls to an agent are automatically accepted by the communication system (Unattended Incoming Call Connection AICC).

If all agents of a UCD group are busy, incoming calls can be placed in a queue. The maximum number of calls in the queue can be individually set for every UCD group. When the maximum number of queued calls is reached, further calls can be forwarded to an overflow destination (which may be an external destination, another UCD group, an internal station or a group).

If the overflow destination is another UCD group and if all other agents in this UCD group are busy, the call remains in the queue associated with the original group and is also entered in the queue of the other UCD group (overflow destination).

Announcements or music can be played for on-hold callers.

Every UCD group can be assigned a name containing up to 16 characters.

### Dependencies

Topic	Dependency
Call forwarding	A call is not forwarded to a UCD group in the following cases: <ul style="list-style-type: none"><li>• If a hunt group is called and a subscriber with call forwarding to a UCD group is next, this call is not forwarded. In this case, the next station in the hunt group is immediately called.</li><li>• A subscriber is a member of a group call with the property "Group" and has activated call forwarding to a UCD group.</li><li>• A station is a member of a group call no answer. If the group is called, the call is not forwarded to the UCD group. Exception: The first subscriber entered has activated call forwarding to a UCD group. In this case, the call is forwarded.</li></ul>

## 10.6.2 UCD Agents

The stations of a UCD group (agents) comprise a workgroup and are typically deployed for technical hotlines, for example, or in order processing, order acceptance, CRM, etc. All incoming calls are distributed to the available stations in a UCD group.

The assignment of agents to the UCD groups occurs via identification codes (IDS). An ID can be assigned to no more than one UCD group. An agent can be assigned multiple IDs. This lets an agent work in more than once UCD group. An agent, however, can only be logged on and therefore active in one UCD group at a time.

In order to use the UCD functions effectively, agents should have phones equipped with a display, function keys and a headset.

### Logging on/off

Agents can log into any phone of the communication system (except ISDN and SIP phones) by using their respective IDs (Identification Code). The agent is available following successful login and permanently assigned to the relevant phone until he or she logs off. The agent cannot log into another phone. Agents who have logged off are no longer considered for the call distribution.

The UCD functions for logging in, logging out and for changing the station status can be accessed by agents from the telephone via programmed function keys or via the associated menu items or via codes.

### Subscriber states

An agent's state is **available** following successful login. If required, a agent can set his or her own station status, or the status may be changed automatically, depending on the agent's current activity. The current subscriber state is shown on the phone's display.

The following displays are possible:

Display	Meaning
available	The agent is available and can accept UCD calls.
not available	The agent temporarily logged off his or her workstation (for example, for a break).
wrap up	The agent is in wrap-up mode. He or she does not receive any UCD calls during the wrap-up time. Depending on the configuration, this can be an individual wrap-up time (the agent independently defines the length of the wrap-up time by changing his or her subscriber status) or an automatic wrap-up time (a wrap-up time is automatically available to all agents after a UCD call).
for <UCD group name>	The agent receives a UCD call.

An agent logs off after his or her shift and is therefore no longer available for UCD calls. The agent can still be reached at his or her personal station number.

If all agents of a UCD group are in the state **not available**, incoming calls are forwarded to an overflow destination (an external destination, another UCD group, an internal station or a group).

If an agent does not accept a call although he or she is logged on and available, the communication system automatically sets the status of that station to **not available**.

### Dependencies

Topic	Dependency
Call forwarding	If an agent activates the Call Forwarding feature, he or she is automatically logged off and is no longer available for UCD calls.
ISDN phones, SIP phones	It is not possible to use ISDN and SIP phones here.

## 10.6.3 Wrap up

This feature temporarily removes an agent from the call distribution in order to allow the agent some time to wrap up the call just completed. The agent does not receive any UCD calls during the wrap-up time.

A distinction is made between:

- the individual wrap-up time.  
The agent sets the wrap-up time length by changing his or her subscriber state.
- the automatic wrap-up time.  
The Uniform Call Distribution (UCD) feature is configured for this in such a way that a wrap-up time is automatically made available to all agents in all UCD groups after a UCD call. The automatic wrap-up time is defined in ring cycles, that is, in increments of five seconds.  
An agent can manually extend the automatic wrap-up time by changing his or her subscriber state.

An agent can be reached throughout the wrap-up time via his or her personal station number.

## 10.6.4 Call Prioritization

You can set a priority for incoming internal and external calls for a UCD group. The queued calls are distributed to the agents in a UCD group on the basis of priority and the wait time.

A queued call with a high priority is answered before a call that has been waiting longer but has a lower priority. A queued call with low priority will be forwarded to an overflow destination before a queued call with high priority.

Priorities are assigned on the basis of trunks for external calls (per B channel), regardless of whether IP or TDM lines are involved.

Examples:

- Communication system with ISDN Primary Rate Interface ( $S_{2M}$  interface) and ISDN Point-to-Multipoint connection ( $S_0$  interface)  
Incoming calls via the ISDN Primary Rate Interface are normal customer calls. All B channels of the  $_{2M}$  interface are thus assigned a medium priority. Calls received via the ISDN point-to-multipoint connection are urgent calls, e.g., high-priority orders for spare parts. All B channels of the  $S_0$  interface are thus assigned a high priority.
- Communication system with a point-to-point connection to an Internet Telephony Service Provider ITSP and an ISDN point-to-multipoint connection ( $S_0$  interface)  
Incoming calls via the PABX number for IP telephony are normal customer calls. All B channels of the LAN interface are thus assigned a medium priority. Calls received via the ISDN point-to-multipoint connection are urgent calls, e.g., high-priority orders for spare parts. All B channels of the  $S_0$  interface are thus assigned a high priority.

The priority is set system-wide for internal calls and therefore applies equally to all internal calls.

Ten priority levels (1 = high, 10 = low) are available.

By default, priority = 10 is set for internal calls, and priority = 1 for external calls.



## 10.6.5 Accepting UCD Calls Automatically

This feature lets agents accept incoming calls without any additional operations (Automatic Incoming Call Connection AICC).

This feature can only be used if the agent's phone has a headset and Disconnect key. An audible tone notifies the agent via the headset about an incoming call that is then automatically put through.

An agent can clear down an ongoing call by pressing the Disconnect key.

The "AICC" feature is not activated by default. Activation is performed on a group-specific basis and applies to all agents in a UCD group, irrespective of whether or not the agent's phone features a headset.

## 10.6.6 UCD queue

If all agents of a UCD group are busy, incoming calls can be placed in a queue. Announcements or music can be played for on-hold callers.

If a call that is waiting in the queue for a specific period (first call cycle) is not accepted by the agent longest in **available** state, this agent's state is changed to **not available** and the call is transferred to the next available agent. If this agent does not answer the call either within a set period (second call cycle), the status of this agent is changed to **not available**. The call is routed to the overflow destination if the status of all agents is **not available**.

For every UCD group, the maximum number of calls in the queue can be set individually. If the maximum number of waiting calls is exceeded, further calls can be routed to an overflow destination.

You can select an external destination, another UCD group, an internal station or a group as the overflow destination. If the overflow destination is another UCD group and if all other agents in this UCD group are busy, the call remains in the queue associated with the original group and is also entered in the queue of the other UCD group (overflow destination).

An agent can query the number of calls in the queue for his or her UCD group with a specially programmed function key or via the assigned menu item or code.

### **Calls in a Queue**

The maximum number of calls in the queue is 30 for UCD groups 1 through 59 and 72 for UCD group 60.

The minimum number of calls in the queue is zero. There is no queue if the minimum number is set to zero. Calls are redirected or rejected directly at an overflow destination if there is no agent available.

## 10.6.7 UCD Overflow

UCD calls can be forwarded to an overflow destination if they are not accepted by the agents of a UCD group and if no queue was set up or if the maximum number of calls in the queue was reached.

The maximum number of calls in the queue can be individually set for every UCD group. If this number is exceeded, further calls can be routed to an overflow destination.

If you do not want a queue to be created, you can enter zero as the maximum number of calls in the queue. Unanswered calls are then immediately routed to an overflow destination.

### Dependencies

Topic	Dependency
AutoAttendant	It is not possible to use an AutoAttendant as an overflow destination.

## 10.6.8 UCD Night Service

An individual night service can be configured for every UCD group. Night service can also be activated and deactivated by every agent in a UCD group. Following activation, all calls for this UCD group are forwarded to the night destination.

The night service destination can be defined as an internal station, another group, an announcement/MoH, the voicemail box of the communication system or an external destination.

### Activating / Deactivating

Activation or deactivation of the UCD night service can be achieved via a programmed function key or via the associated menu items or via codes. The call number of the desired night service destination must be entered at activation.

For more information on the communication system's night service, see [Night Service \(LX/MX\)](#).

## Dependencies

Topic	Dependency
Subscriber state	If you activate the UCD night answer feature, your current subscriber status does not change. A forced logout of the agents who are still logged in does not occur.
Communication system's night service	The communication system's UCD night answer and night service can be activated and deactivated independently of one another. Example: A UCD group was entered as the night service destination for the communication system. Calls that reach this UCD group via the communication system's night service remain in this UCD group, irrespective of a UCD night answer.
Existing calls	Existing calls are not affected by the activation of UCD night answer.

## 10.6.9 Announcements / Music on Hold for UCD

Music On Hold (MoH) or announcements can be played to callers who cannot be switched through directly to the agents of a UCD group. Music on hold and announcements can be assigned to each UCD group individually.

You have the following options:

- Music On Hold (MOH)  
Queued callers can be played music from the integrated source of the communication system. Further Music on Hold file(s) can be loaded from a PC into the communication system.  
For more information, see [Music on Hold \(LX/MX\)](#)
- Announcements  
Queued callers can be played integrated announcements. Further announcements can be loaded from a PC into the communication system.  
For more information, see [Announcements \(LX/MX\)](#)

The time up to the start of the announcement can be set (**Ann. delay time**). You can suppress the announcement by setting the maximum value (600 seconds). It is assumed here that the call will be accepted within this time.

## 10.6.10 Transfer to UCD Groups

Internal and external calls can be transferred to UCD groups. If a call is not answered within a certain period, a recall is carried out.

The recall time is defined via the time parameter **Monitoring transfer to a UCD group prior to answer**. The default setting is 300 seconds. This setting (from 0 to 255 minutes) can be changed by an administrator with the **Expert** profile in **Expert mode**.

### Dependencies

Topic	Dependency
Announcements	Announcements can be played for the external transferred calls. This is not possible for internal calls.
Recall time	The recall time for a transfer to UCD groups differs from the recall time for transfers to other subscribers.

## 10.6.11 Releasing UCD from Analog Lines

When UCD calls over analog lines are not answered within a specific time, these calls are released. This prevents analog lines from freezing up.

The release time is defined via the time parameter **Monitoring a UCD call on an analog line**. The default setting is 300 seconds. This setting (from 0 to 255 minutes) can be changed by an administrator with the **Expert** profile in **Expert mode**.

# 11 Call Routing

The communication system offers Toll and Call Restrictions, a Night Service, powerful LCR (Least Cost Routing) capabilities and different options for making emergency calls.

## 11.1 Toll and Call Restrictions (LX/MX)

Toll and call restrictions collectively describe all the restrictive measures to control phone traffic such as the prioritization for exchange line seizures, the selective seizure of exchange lines, toll restrictions and CON groups.

### 11.1.1 Selective Seizure of Exchange Lines (LX/MX)

Exchange lines (aka "outside lines" or "CO trunks") can also be seized selectively by subscribers.

The prioritization for the seizure of exchange lines is handled via Least Cost Routing by default. In most cases, the least-cost provider is selected first, followed by the second-lowest cost provider, and so on.

If a subscriber wants to conduct a call over a provider that is not first in the LCR (because this provider is cheaper for long-distance calls, for example), he or she can select this provider via a seizure code.

Subscribers can likewise also use selective dialing via seizure codes to reach a number that can only be dialed using ISDN (in cases where Vodafone is otherwise preset as the provider, for example).

By default, the seizure code 88 is configured for the seizure of an outside line via ISDN. All codes can be configured later by the administrator or edited as required.

### 11.1.2 Classes of Service, Toll Restriction (LX/MX)

The classes of service control subscriber access to external toll calls. Individual subscribers are allocated to standardized classes of service to facilitate toll restriction.

#### **Toll restriction**

The following CO call privileges can be configured:

- No toll restriction/internal  
The subscriber may only make internal calls.

## Call Routing

### Toll and Call Restrictions (LX/MX)

- Outward-restricted trunk access (incoming authorized)  
The subscriber may only answer (not make) external calls.
- Allowed lists (1-6)  
The allowed external phone numbers are defined here. Outward-restricted trunk access applies if no number is entered.
- Denied lists (1-6)  
The disallowed external phone numbers are defined here. Unrestricted trunk access applies if no number is entered.
- Unrestricted trunk access  
Subscribers can answer and set up incoming and outgoing external calls without restriction.

The COS group assigned to a subscriber specifies the toll restriction type per direction for this subscriber.

System speed dialing destinations can always be used irrespective of the COS group assigned.

#### Allowed and Denied Lists

Allowed lists contain the digit strings permitted at the start of a phone number, while denied lists contain the disallowed digit strings. The Administrator can use exception filters for any Denied list to define which digits should not be compared with the corresponding Denied list. The communication system excludes the set range of digits before the digit analysis. The character(s) to be excluded and the digit range to which the filter is to be applied are configurable.

#### Day and Night Classes of Service

Different COS groups can be assigned for day and night. The system-wide changeover between Day and Night COS groups can occur at set times to prevent toll fraud. Authorized subscribers can also make this switch manually. The Class of Service to make this switch is assigned via the wizard.

#### Quantity structure

Feature	Number
Classes of Service	15
Allowed lists, long (100 entries)	1
Allowed lists, short (10 entries)	5
Denied lists, long (50 entries)	1
Denied lists, short (10 entries)	5
Number of characters in list entries	25

## Dependencies

Topic	Dependency
Speed Dials	Speed dialing destinations can always be dialed irrespective of any toll restriction.
LCR	COS groups and the LCR class of service are different; if both are configured, both apply.. If however, an overflow route was configured in the LCR route table and an extension receives a call with external FWD, the authorization is not analyzed if the call goes in the overflow route.

### 11.1.3 CON Groups (LX/MX)

The CON Groups feature is used to define which subscribers of OpenScape Office can establish connections to which other subscribers of the communication system.

CON groups can also be used to configure which lines individual subscribers can access for incoming and outgoing calls..

The CON functionality does not access the applications; it is only significant for telephony. The presentation of the presence status, for example, is not prevented by an access restriction through CON.

The CON Group feature (also referred to as a tenant system) is implemented in two steps:

- Create CON groups
- Configure CON matrix

#### 11.1.3.1 CON Groups (Traffic Restriction Groups) (LX/MX)

CON groups (also referred to as traffic restriction groups) control allowed and denied connections between subscribers and lines of the communication system.

Using CON groups, specific stations and lines can be combined into groups. These groups then operate as a kind of subsystem in OpenScape Office with different classes of service among them and externally.

You can assign a CON group to individual stations and lines in OpenScape Office via the CON Group Assignment. When coding the connection matrix, you can then access these groups and define which subscribers can reach which other subscribers and which lines can be accessed by them.

All stations and CO trunks are assigned to CON group 1 by default. This provides all subscribers with unrestricted access to other subscribers as well as trunks, both incoming and outgoing. The CON matrix specifies which of the six CON groups can set up connections to which other CON groups.

A maximum of 16 CON groups can be configured.

## Call Routing

### Night Service and Intercept (LX/MX)

#### 11.1.3.2 Assigning Speed-Dialing Numbers to CON Groups (LX/MX)

Every CON group is assigned a range of System Speed Dialing (SSD) destinations. When a subscriber dials an SSD, the associated CON group is checked to verify if the subscriber is authorized to do so. Dialing is performed if this speed-dialing number lies within the correct range for the relevant CON group, otherwise an error message is output.

The speed-dial number ranges can overlap in the CON group. The following are permitted, for example:

CON group	SSD range
1	0-999
2	50-150
3	200-500

Please note, however, that you cannot enter individual system speed-dial (SSD) numbers or multiple SSD ranges in a CON group instead of a range. The following are not permitted, for example:

CON group	SSD range
1	0, 5, 10
2	50-100, 300-500

## 11.2 Night Service and Intercept (LX/MX)

Calls that cannot be answered are redirected to another telephone (e.g., the Attendant Console) via the Night Service or Intercept functions.

### 11.2.1 Night Service (LX/MX)

The communication system lets you forward calls from the attendant to a preconfigured destination during periods when the attendant console is left unattended. The call forwarding destination can be a subscriber, a group or the voicemail box of a group. These calls can also be signaled by a central alarm clock.

Call destination lists dictate how incoming calls are forwarded.

The following night service variants exist:

- **Fixed Night Service**  
OpenScape Office activates and deactivates the night service in accordance with a schedule defined by the administrator.



- **Variable Night Service**

The variable night service is activated and deactivated manually by an authorized subscriber. The calls are handled as configured by the administrator in the call destination lists

You can also define an intercept position for the Night service. This intercept position can be an individual station or a group. Different intercept positions are possible for day and night calls.

Any phone can serve as a night service destination, provided the associated class of service group allows incoming calls. A telephone with internal authorization only cannot be entered as a night service destination.

If the night service destination has activated call forwarding, this is followed.

To prevent unauthorized deactivation of night mode, the individual lock code can be activated by subscribers at every authorized telephone.

### **UCD Night Service**

An individual night service can be configured for every UCD group. It can be activated and deactivated independently of the system-wide night service. It can also be activated and deactivated by every agent in a UCD group. The current status of the individual agents and existing calls are not affected. Following activation, all calls for this UCD group are forwarded to the night service destination.

Another UCD group, an internal station or an external destination can all be set as a night service destination.

### **System-Specific Information**

The Class of Service Groups 1-4 and 7-8 cannot be modified.

By default, the first subscriber in the communication system can activate and deactivate the night service. The administrator can authorize up to five subscribers to activate and deactivate the night service.

## **11.2.2 Intercept**

The communication system diverts incoming calls that cannot be assigned to a station or answered to a set intercept position to ensure that no calls are lost. As an administrator, you can configure the intercept criteria.

Possible intercepts are:

- Intercept position (Attendant Console)
- Subscribers/Stations
- Hunt Group
- Group Call
- External announcement equipment

## Call Routing

### Night Service and Intercept (LX/MX)

If an intercept position is configured in the system, intercepted calls are routed to this intercept position. If no intercept position is configured, intercepted calls are signaled at the first IP station.

You can also configure an intercept position for the Night service.

Intercepts cannot extend beyond a hunt group; the call is forwarded to the first hunt group station and remains in the hunt group.

Data calls are disconnected, not intercepted.

As an administrator, you can assign one attendant code each to the intercept position for internal and external, under which the intercept position can be directly reached.

The intercept applies system-wide, i.e., identically for all subscribers in tenant systems.

As an administrator, you can specify in which situations the Intercept feature is used via intercept criteria. The following intercept criteria are possible:

- On RNA (ring no answer) (LX/MX)  
The call follows the entries in Call Management (CM). If the end of the CM elements is reached, the system determines whether or not an intercept after timeout should occur. Calls are intercepted if they cannot be switched because there are no available stations.
- On busy, if no additional forwarding is possible (LX/MX)  
The system first checks if call waiting is possible. If call waiting is not possible, the call follows the entries in Call Management. If the call cannot be signaled at any station, the system determines whether the call should be intercepted or released. Intercept on busy is only performed for first calls, not for forwarded or outgoing connections. A recall of an external station is not immediately intercepted when the destination station is busy; instead, call waiting is activated.
- On Invalid (misdialing) (LX/MX)  
If the dialed station number is not configured or is inactive.
- On Incomplete (LX/MX)  
If the Dialed station number is too short, for example. Incomplete dialing is not evaluated if a central intercept position is used.
- On unanswered recall (LX/MX)  
If an external call is not answered following an unscreened transfer (transfer before answer) and if the automatic recall to the original destination is also not answered, then an intercept is initiated after a preset time.
- On missing phone number (LX/MX)  
As for On Invalid.
- On chained call forwarding (LX/MX)  
If a forwarded call encounters another forwarding instruction at the call forwarding destination, and the number of chained forwarding instructions allowed is exceeded, an intercept occurs. The number of chained forwarding instructions depends on the entries in the call forwarding. A maximum of 3 are allowed.

- On lock code (LX/MX)  
If a subscriber at a telephone with an activated lock code dials a seizure code, an intercept occurs. A separate intercept is defined by the administrator for this purpose.
- On announcement  
If a subscriber dials the attendant code while listening to a voicemail announcement or the AutoAttendant, an intercept occurs. A separate intercept is defined by the administrator for this purpose.

See also "Central Intercept Position in the Internetwork" In the section on Networking.

## 11.3 LCR (Least Cost Routing) (LX/MX)

The Least Cost Routing (LCR) function automatically controls the paths used for routing an outgoing connection. This path can be routed via the public network, various network providers (ITSPs) or a private network. The most suitable connection path is selected for a call on the basis of the dial plan, route tables, and outdial rules.

Connections can be voice calls, analog data connections via fax and modem and ISDN data connections.

### 11.3.1 LCR Functionality (LX/MX)

You can use the LCR function to specify the provider you want to use, for example, for trunk calls, mobile phone calls or international calls. You use OpenScape Office to define the least-cost provider and conduct all calls via this specific path.

If a pattern that matches the dialed phone number is found in the dial plan, the route tables are searched for a suitable route (each trunk is assigned to a route, see also Trunks/Routes). At the same time, the system checks if the class of service matches for this route.

The check determines if the caller has the required class of service to seize a route. This provides control over which stations of the communication system may use which routes or trunks (to ensure that faxes are routed exclusively via TDM trunks and not via ITSPs, for instance).

The dialed digits are buffered until the routing tables with the LCR classes of service have been evaluated. It is only on completing this step that the connection is set up, in accordance with the outdial rules. A dial tone can be issued to signal the ready-to-dial condition to the subscriber.

When configuring outdial rules, you can enter information for the subscriber, e.g., by specifying that this connection is routed via a specific provider (name of the provider) or that a connection is using a more expensive route. This information can either be displayed on the screen, output as a tone or output both on the display and as a tone.

## Call Routing

### LCR (Least Cost Routing) (LX/MX)

In general:

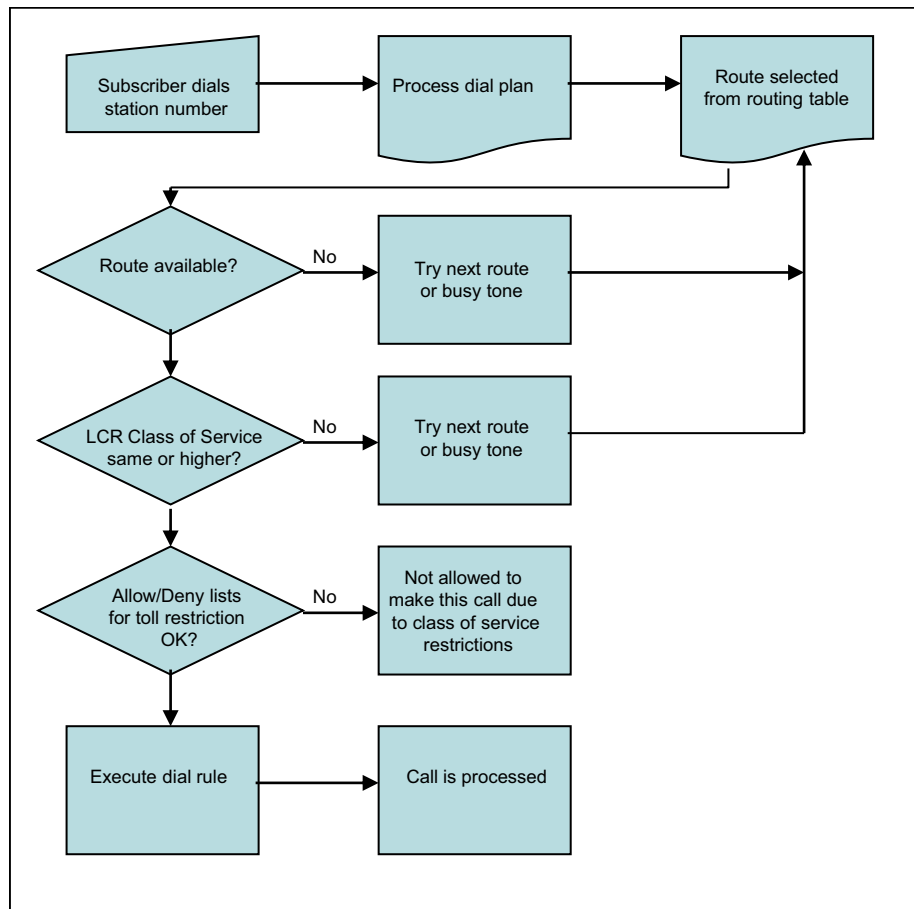
- When LCR is activated, the check is performed for every external dialing operation. Exception: when dialing a specific trunk code.
- If LCR determines that the preferred route cannot be used, the communication system will look for a (possibly more expensive) alternative from the routing table.
- Digits can be transmitted either individually or en-bloc, depending on the access method and the dial plan.

### System-Specific Information

The communication system evaluates up to 24 characters (comprising the digit string plus no more than 9 field separators). The digit string dialed can contain up to 32 digits, that is, LCR checks a total of 22 digits when 32 digits are dialed; the remaining 10 digits are not checked.

The communication system can manage up to 1000 dial plans and 254 route tables.

### LCR flow chart



### Dependencies

Topic	Dependency
System Speed Dialing	To ensure that system speed dial destinations work properly, the LCR access code, followed by the destination number, must be entered in the speed-dial destination.
Redialing	Station redial will insert the access code used for the original call.
Name keys	Repertory dial keys to external destinations must have the LCR access code for proper operation.
Toll restriction	The toll restriction classes of service are also applied in LCR.

### Digit transmission

There are two types of digit transmission: digit-by-digit and en-bloc sending. With digit-by-digit, each digit is transmitted and processed directly after it is dialed. With block dialing, by contrast, digits blocks are formed and transmitted.

The digit transmission for ITSP routes always occurs en-bloc, regardless of the setting of the LCR flag. For all other settings, the digit transmission occurs based on the setting of the LCR flag.

### Carrier Select Override

As a subscriber, you can deactivate the automatic Least Cost Routing by directly dialing a specific network carrier. For CSO (carrier select override) to work, the requested carrier must be included in the dial plan (also called a numbering plan) and in the routing table assigned by the dial plan, and you must have the required direct trunk access.

LCR is preconfigured in the system so as to allow a targeted seizure of the CO trunk even after the ITSP wizard has completed. Instead of "0", "88" must be dialed for this.

80	The first configured ITSP, then the overflow trunk
81	The second configured ITSP, then the overflow trunk
83	The third configured ITSP, then the overflow trunk
84	The fourth configured ITSP, then the overflow trunk
88	The CO trunk for ISDN or analog

## 11.3.2 LCR Dial Plan (LX/MX)

The dial plan is searched for patterns that match the dialed digits (dialing sequence). The result is used as a criterion for selecting the route table. At the same time, the system checks if the subscriber's class of service matches for this route.

The pattern of a digit string is assigned to a route in the dial plan so that this path is assigned to the subscriber for connection setup.

The dial plan is split into individual fields for identification and configuration purposes. The table shows the numbers 4922000 and 1603656260 entered in the dial-plan table.

Field 1	Field 2	Field 3	Field 4	Field 5
0	C 492	– 2000		
0	C 160	– 365	– 62	– 60

**The following entries apply for the phone numbers:**

- 0 . . . 9      Allowed digits
- Field separator
- C              Simulated dial tone (can be entered up to three times). This entry is also interpreted as a field separator

**Global character**

- X              Any digit from 0 to . . 9
- N              Any digit from 2 to . . 9
- Z              One or more digits to follow up to the end of dialing

A digit sequence can be divided into a maximum of 10 fields.

OpenScape Office inserts the field separators in the digit string in accordance with a preset schema. They are used to split the digit string into individual fields that can be evaluated separately. Example: After the first dialed digit, a separator is inserted so that a dialed “0” is detected as a separate field and thus simulates toll restriction.

Due to this field separation, these fields can be repeated or rearranged in the dial plan.

A “#” or “\*” character in the digit string dialed by the subscriber is the end-of-dial code or indicates dialing method changeover. This is why these characters are not valid entries in the dial plan.

Entries should be placed in ascending numeric order from 0 to 9. Specific dialed numbers must precede wildcard entries to prevent conflicts in matches with wildcard entries.

The fields formed by the field separators “–” and “C” in the dial plan can be addressed selectively to repeat, suppress, exchange, or insert digits.

Every station number dialed is checked for external traffic in the dial plan. If the number dialed matches an entry in the dial plan, the call is handled in accordance with the route table entered in the dial plan.

The account code entry can be enforced per dial plan. The Account Code Checking Procedure applies.

OpenScape Office can evaluate a dialing sequence of up to 22 characters (comprising the digit string plus no more than 9 field separators).

### 11.3.3 LCR Routing Tables (LX/MX)

Least Cost Routing (LCR) is achieved by searching for a suitable route in the LCR routing tables (every trunk is assigned a route). At the same time, the system checks if the class of service matches for this route. The outdial rule is also dependent on the assigned path.

The routing table describes:

- the route assigned to the relevant path.
- the outdial rule,
- the LCR Class of Service (COS) required for seizure,
- the warning method for a more expensive route (warning tone).

The table is searched from top to bottom in hierarchical order. The system checks to determine whether the route is free and the station has the requisite LCR class of service. If this is the case, dialing occurs in accordance the outdial rule and schedule entered in the route table.

If the first route selection in the route table is busy, the LCR function can advance to the next (possibly more expensive) route configured in the route group table. The system can notify the user of this with an audible signal, an optical signal, or both.

Up to 254 route tables with 16 routes each can be created.

#### **Dedicated Gateway**

A dedicated gateway is a permanently fixed set route in an internetwork. If a dedicated gateway is entered for a route, then routing via this gateway is enforced. All contradictory rules are then invalid for the routing.

### 11.3.4 LCR Class of Service (COS) (LX/MX)

Every subscriber is assigned a separate LCR class of service (COS). A subscriber can only seize a route if his or her COS is greater than or equal to the LCR COS in the route table, i.e., a subscriber with a COS 7 cannot seize a route with COS 8.

The authorization check only occurs only if the subscriber has set up the connection from his or her phone. The authorization check does NOT take place for ad-hoc and Meet-Me conferences or if the Call Me feature is used.

**Dependencies**

Topic	Dependency
Toll restriction	The LCR classes of service are subordinate to the toll restriction classes of service which assign various CO call privileges to the subscribers in OpenScope Office. Fifteen different classes of service exist.

**11.3.5 LCR Outdial Rules (LX/MX)**

LCR outdial rules can be used to convert the phone numbers entered into random new digit strings for additional processing. Access to different carriers is enabled via digit translation. The dial rule used is defined by the path or the route in the route table.

**System-Specific Information**

OpenScope Office can administer up to 254 outdial rules in the LCR dialing rules table. The name of a dial rule can contain up to 16 characters.

The dialing rules address the dial plan fields selectively for the following operations:

- Repeating digits
- Suppressing digits
- Exchanging digits
- Inserting digits
- Switching the signaling method
- Detecting a dial tone
- Inserting pauses

If the first route selection in the route table is busy, the LCR function can advance to the next (possibly more expensive) route configured in the route group table. The system can notify the user of this with an audible signal, an optical signal, or both.

**Dialing Rules Table**

You can define up to 254 outdial rules here with a maximum length of 40 characters each.

The LCR dialing rules table is also referred to as the routing table.

**Definition of Outdial Rules**

- A:  
Repeat remaining fields (transmit). This letter causes all subsequent digit fields to be transmitted. The point of reference is the last field pointer before "A". A field pointer is the number of the field as of which dialing is possible.



- **B:**  
It is used for the multi-gateway network when a station number of type TON (Type Of Number) that was called from outside is "unknown" and must be routed to the multi-gateway node. To ensure that this station number is unique, it is extended to national or international in accordance with the TON in the LCR. This is required when the DID numbers are not unique and need to be configured in the national or international format.
- **D (n):**  
Dial digit sequence (1 to 25 digits). This letter can be inserted multiple times and at any position in the string.
- **E (n):**  
Repeat field from dial plan (from 1 to 10 times). This letter can be inserted multiple times and at any position in the string. "E" can also appear in any order with relation to (n). A specific field can be addressed multiple times, including in sequence. With the exception of "E1", this letter can be surrounded by any parameters.  
With digit-by-digit dialing (opposite of en-bloc dialing), the last element in the outdial rule cannot be E(n); it may be E(n)A.
- **M (n):**  
Authorization code (1 to 16). This letter must not be in the final position.
- **P (n):**  
The letter "P" (Pause) can be inserted multiple times and at any position in the string.
- **S:**  
Switch, changes signaling methods from DP to DTMF (with CONNECT, PROGRESS or CALL PROC with PI). This letter can be inserted in the string only once and may not be in the final position. The "C" parameter cannot be used after "S".
- **C:**  
Access code. This letter can be inserted in the string only once. The subsequent characters are transmitted without a dial pause and are used for single stage, two-stage, DICS (not for U.S.), BRI, and PRI carrier access.
- **U:**  
Use subaddress signaling method. This letter can be inserted in the string only once and may not be in the final position. The "S", "P", "M", and "C" parameters cannot be used after "U".
- **N (n) (only for the U.S.):**  
Network SFG (1 to 5) or Band Number (1).

**Example:**

The system should automatically add a provider suffix.

Dial rule D010xxA means: the system first dials the Provider prefix (010XX), and then all the digits dialed by the subscriber (A).

## 11.3.6 Network Carriers (LX/MX)

You can assign network carriers to each route. The selection of the network carrier is defined by the LCR outdial rules.

### **Unknown**

No explicit specification about a network carrier.

### **Main network supplier**

When seizing a trunk using the main network supplier, simplified dialing into the public network is performed by en-bloc dialing or by dialing individual digits.

### **MCL Single Stage**

With MCL Single Stage, a prefix is used to dial the desired network carrier, and the station number is then dialed. Dialing occurs in the D channel for ISDN or as normal dialing for MSI.

### **MCL Two-Stage**

With MCL Two Stage, a prefix is used to dial the desired network carrier. After a synchronization phase, a configurable authorization code is initially sent followed by the destination call number as DTMF digits.

With synchronization during timeout, you must program a pause of 2 to 12 seconds.

### **Corporate Network**

For a corporate network, the alternative network is directly connected to OpenScape Office. The LCR function determines the appropriate trunk group based on the station number dialed and then routes the call either via the trunk group in the public exchange or via the trunk group in the corporate network.

### **Dial-In Control Server**

With this type of LCR, the desired network carrier is dialed with a prefix via a dial-in control server, and the call number and configurable authorization code are transmitted in the subaddress. Dialing occurs in the D channel.

### **Primary Rate Interface**

In the case of the Primary Rate Interface, the selection of the network carrier or of a calling service is encoded in SETUP message using following information elements: Network Specific Facility, Operator System Access and Transit Network Selection.

## Dependencies

Topic	Dependency
Receiving/forwarding call information	Temporary or permanent station number suppression cannot be activated.
ISDN/SUB addressing	The ISDN feature SUB must be applied for or released in the public network.

## 11.4 Emergency Calls (LX/MX)

The communication system and the phones connected offer different options for making emergency calls. The administrator can configure a hotline or hotline after timeout or an emergency service.

### Prerequisites

The emergency call center is reached by dialing the CO access code (e.g., 0) and the emergency number (e.g., 112). The destination number for emergency calls must therefore be dialed from applications together with the leading CO access code.

### Basic Sequence

Emergency calls are initiated by a subscriber of the communication system by dialing the CO access code and the emergency number. The emergency number is passed by the communication system on to the respective provider (PSTN or ITSP).

#### Case 1: Dialing the emergency call over the PSTN line

The emergency call is issued in the local network to which the communication system connection is assigned. The following must be observed here: All subscribers who are not in the same location as the communication system (e.g., Mobility users, CallMe users (teleworkers) or users with remote WAN-linked phones) should dial the emergency call via a cell phone or another land-line phone to issue the emergency call in the local area network of their site.

#### Case 2: Dialing the emergency call via an ITSP

Not all ITSPs support emergency calls. In this case, the LCR configuration should be used to ensure that emergency calls are routed via the PSTN.

#### Case 3: Special agreement with ITSP or PSTN providers

In cases where all subscribers of the communication system are not located at one site, but are nonetheless permanently assigned to a single site without a PSTN of its own, a customized procedure for emergency signaling can be agreed upon in cooperation with the Provider. For example, depending on the caller ID of

the caller, the emergency call could be routed by the Provider to the appropriate local area network as agreed. These agreements are made on an individual basis and not subject to any policy.

#### **Case 4: Emergency calls with Mobile Logon (IP Mobility)**

Mobile Logon (IP Mobility) means that subscribers can change their phones and take their phone numbers with them.

Emergency calls work in this case, so long as the phones are logged in at the locations of the gateways. All subscribers who are not at the site of the gateway (e.g., Mobility users, CallMe users, home workers and users with remote WAN-linked phones) should dial the emergency call via a cell phone or another land-line phone to issue the emergency call in the local area network of their site.

---

**NOTICE:** For multi-gateway scenarios in which the Mobile Logon feature is used, special requirements apply. The appropriate configuration is described in the section "Emergency Calls in combination with Mobile Logon".

---

### **11.4.1 Hotline after Timeout / Hotline (LX/MX)**

You can activate the Hotline function for every station. You can thus define whether the connection to the hotline destination should be established as soon as you lift the handset (hotline) or after a short delay (off-hook alarm after timeout).

#### **Hotline after timeout**

If the subscriber selects any digit during the predefined time (hotline timeout), **no** connection to the hotline destination is established.

The hotline timeout is configured centrally by the administrator and can be activated and deactivated individually for each station.

#### **Hotline**

When the hotline is activated, the subscriber has **no** way to enter a call number. On picking up the receiver, the subscriber always reaches the predefined internal or external hotline destination automatically.

If hotline destination is set for call forwarding or call forwarding-no answer (CFNA), the calling station will always be forwarded.

#### **System-Specific Information**

The administrator can configure six hotline destinations and the length of the hotline timeout (0-99 seconds). If the administrator specifies the value 0 for the hotline timeout, the hotline destination is called immediately.

### Dependencies

Topic	Dependency
Do Not Disturb	A caller hears the busy tone if Do Not Disturb (DND) is active at the destination called.

## 11.4.2 Trunk Release for Emergency Call (LX/MX)

If an emergency call is made, and no CO trunk is free, a forced disconnect occurs. The emergency caller is automatically assigned the free trunk.

Trunk release only works for ISDN trunks.

If all trunks are busy, subscribers can execute an automatic or manual trunk release.

- Automatic: The Least Cost Routing (LCR) feature is active.
- Manually: the feature is always active for the Attendant Console and is executed via keys or codes.

### System-Specific Information

The administrator can configure as many emergency numbers as required.

To ensure that trunk release occurs when all lines are busy, the emergency number must be saved in the LCR dial plan and the *Expert Mode* emergency flag must be set for it.

## 11.4.3 For U.S. and Canada only: E911 Emergency Call Service (LX/MX)

The enhanced E911 emergency service transmits geographical information on the caller (stored address) in addition to the phone number when an emergency call is dispatched.

The receiving station for the emergency call does not require human intervention to determine the site of the caller.

In the USA, this feature is only activated when the emergency number 911 is dialed.

Every station number must be assigned a valid DID number with LIN (location identification number) by the administrator for the E911 emergency service. Subscriber lines that are physically close to one another are given the same LIN. The emergency call center has a database that contains all LINs and uses the transmitted LIN to identify the name and address of the party placing the emergency call.

**Dependencies**

Topic	Dependency
CLIP	LIN is activated by default for the U.S. However, if CLIP (Calling Line Identification Presentation) is activated for the USA, LIN is automatically disabled.

### 11.4.4 Emergency Calls in Combination with Mobile Logon

If you use the Mobile Logon feature in a multi-gateway internetwork, switching to another phone may also change the physical location. Consequently, special measures are required for the routing of emergency calls.

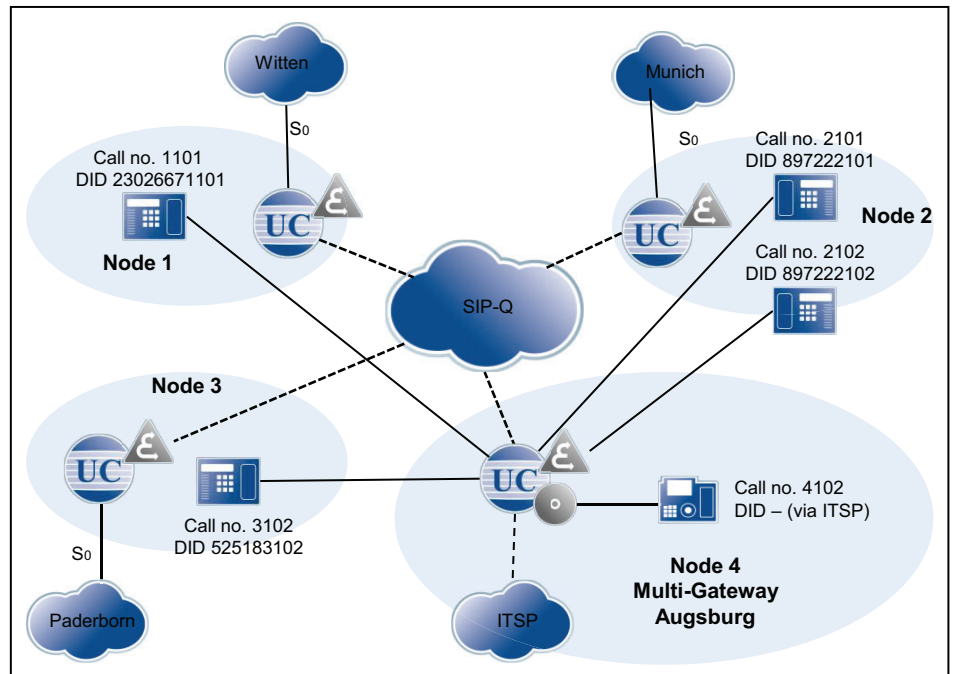
#### Description of the Algorithm for Dialing an Emergency Number

When a subscriber dials an emergency number (ID in the LCR), an algorithm checks whether or not an emergency number has been configured for the telephone. This is then used to produce a derived call number, which is used to route the call via the correct gateway in the internetwork.

Every number marked as an emergency number in the dial plan also features a reference to an entry in the route table. Every entry in the route table that is associated with an emergency number must be assigned a "low" class of service (COS). A low class of service means that every subscriber is authorized to call an emergency number.

#### 11.4.4.1 Configuring the Emergency Scenario

The configuration of the emergency scenario shows which steps must be performed to set up emergency calling for a multi-gateway internetwork.



Mobile Logon is supported only within a node, i.e., location changes - and thus the special requirements for emergency calls - are only relevant for phones operated on the multi-gateway node (4). In general, all affected phones are logged in at node 4, but are physically located at different sites.

- In all affected phones, one entry is required for emergency calling (connection portion of the canonical phone number of the location node + seizure code for emergency route)
- The LCR entry (node\_4local) in the following table is only required if phones are physically present at node 4 (multi-gateway). It is also preceded by the location number which, however, is incomplete here (only country code). The prerequisite for this is an ITSP access to node 4, which supports emergency calls into the local network.

### Handling of Emergency Numbers

- On dialing at the telephone, an LCR rule marked with an emergency flag (e.g., 0C11x) is taken.
- The emergency number that is stored in the phone (and transmitted to the system at logon) is compared with the location data of the system (country code, area code, PABX number).  
If identical (not the case in the example), the rule is used.  
If different, a "long" emergency number is formed:
  - Removal of the access code: 0112 -> 112
  - Insertion of <LDAP seizure code><international prefix><programmed emergency number>: e.g., 112 -> 0 00 49897220 112

- The "long" emergency number is routed through the LCR, either directly to the local CO (central office) using specific LCR rules or via tie lines to the respective partner node and from there into the CO.

---

**NOTICE:** Since the complete location number of the local node is not entered precisely in the telephone, a suitable LCR rule must also be entered for the local emergency call at the multi-gateway location.

---

#### Setting up the Location Data for Node 4

Node 4	Gateway Node
G.-Location Country	49
G.-Location Local Network	
G.-Location System	
International Prefix	00
National Prefix	0
LDAP seizure code	0

#### Routing parameters

Route	No. and type, outgoing	RNR type
Networking	National	Int/DID

Networking Route	
CO code (2nd. trunk code)	0

#### Node 4, telephones

Location Witten	
Call Number	1101
Emergency Number	4923026670

Location Munich	
Call Number	2101
Emergency Number	49897220

Location Paderborn	
Call Number	3102
Emergency Number	49525180



Location Augsburg	
Call Number	4102
Emergency Number	490

**Overview of Entries Relevant for Emergency Calls in the LCR for Node 4**

Dial Plan			Route table			Dial Rule		
Name	Dialed digits	Emergency operation	Route	Dedicated Gateway	Gateway ID	Dial Rule	Procedure	Type
Emergency calls <sup>1)</sup>	0C112	X	Networking	Multi-Gateway	1	E1A	Corp. Network	Unknown
Emergency calls <sup>1)</sup>	0C0110	X						
CO	0CZ							
Emergency_calls_to1	0C00492302667-0-11X	X	Networking	Mandatory	1	E3A	Corp. Network	Unknown
Emergency_calls_to2	0C004989722-0-11X	X			2			
Emergency_calls_to3	0C004952518-0-11X	X			3			
Emergency_calls_4local <sup>2)</sup>	0C0049-0-11X	X	ITSP	No		E4A	Main network supplier	Unknown

<sup>1)</sup> With the above rules in this example, only the emergency situation will be detected, but no routing will occur. The derived "long" emergency number is used to route the emergency call.

<sup>2)</sup> Since stations are physically connected at the multi-gateway location, a separate LCR rule must be entered for the local emergency call access (via the ITSP route).

## 12 Multimedia Contact Center

The OpenScape Office Contact Center is a powerful solution for the optimum distribution and handling of incoming calls, faxes and e-mails. Intelligent skills-based distribution ensures that callers are always connected to the best qualified agents, regardless of which contact medium is used. A number of convenient functions for handling and wrapping up calls, faxes and e-mails are offered to the Contact Center agents via the myAgent application. myReports provides a number of report templates for analyzing the Contact Center operations.

The OpenScape Office Contact Center is fully integrated in the OpenScape Office V3 software. All the required software components are included in the system software. The Contact Center functions themselves are released through licenses.

The Contact Center uses the resources of the communication system such as queues for incoming calls and unified communications functions to record and play back announcements.

The central software component of the Contact Center controls all routing functions for incoming calls, faxes, and e-mails and also controls the LAN-connected PC workplaces of agents and wallboard displays.

On the PC workplaces of agents, the myAgent application is installed. The myReports application can be optionally installed to generate and send reports. The required software can be downloaded directly from the download area of the communication system and installed on the client PC.

OpenScape Office Assistant is used to set up the Contact Center basic functions, schedules, distribution rules as well as the agents. The settings for the daily operation of the Contact Center such as the assignment of agents to queues, for example, can also be made directly via myAgent.

If the Contact Center is unavailable due to problems (such as a system crash, dropped connection, etc.), a fallback solution can be implemented via the UCD feature of the communication system. Distribution rules for emergencies must be taken into account when setting up UCD groups within the framework of the initial setup of the Contact Center.

---

**INFO:** For details on OpenScape Office and the unified communications functions, see [Unified Communications](#).

---

### 12.1 Contact Center Clients

A number of convenient functions for handling and wrapping up calls, faxes and e-mails are offered to the Contact Center agents via the myAgent application. The myReports application can be used to generate reports on the calls, queues, agents, performance, GOS (Grade of Service) and wrapup codes of the Contact Center. More than 100 predefined report templates are available. In addition, it is also possible to define and create custom report templates.

## 12.1.1 myAgent

Convenient functions for handling and wrapping up calls, faxes and e-mails are available to all agents via myAgent.

myAgent provides the following features:

- Processing of
  - Make Call
  - Faxes
  - E-mails
- Callback function for agents
- Displaying and changing the agent status
- Displaying and changing the presence status of internal subscribers of the communication system
- Real-time presentation of queues
- Recording of calls, if activated in the communication system
- Request for assistance through
  - Silent monitoring of calls (depending on country)
  - Overriding calls
  - Instant Messaging
- Integration of the internal directory, external directory and the external offline directory (LDAP) for searches by name
- Creation of reports based on predefined report templates

Depending on the authorization level assigned to an agent, either a set of standard functions (agent) or advanced functions (Supervisor or Administrator) are available to the agents in myAgent (see [Agent Functions Independent of the Authorization Level](#)).

The assignment of agents to queues occurs using the myAgent application. Only an agent with the authorization level of a Supervisor or an Administrator can make this assignment. The following properties, which affect the distribution of calls, faxes and e-mails in a queue, can be assigned here to the agents (agent assignment (binding)):

- **Primary Agent or Overflow Agent**  
Calls are distributed uniformly to primary agents. An overflow agent receives a call only when the number of calls exceeds a defined number or when a call has exceeded a specified waiting period.
- **Overflow after seconds in queue**  
Calls that exceed this waiting period and received by an overflow agent.
- **Overflow after calls in queue**  
Calls that exceed the maximum number are received by an overflow agent.

- **Skill Level**  
Skill levels control the distribution of calls to agents in call queues. Agents with higher skill levels are given precedence when calls are distributed. In cases where all agents have the same skill level the longest idle agent receives the call.
- **Enable agent callback**  
Agent callback enables a caller in the queue to leave a voicemail for agents. As soon as an appropriate agent becomes free, that agent receives a call, hears the voicemail left by the caller, and can then call back that caller.
- **Wrapup time**  
The wrapup time enables agents to finish any tasks, e.g., administrative tasks, that may be required after completing a call and before receiving the next call.

The **agent binding list** shows agents with the authorization level of a Supervisor or Administrator which agents are assigned to which queues. Agents with the agent authorization level can only see the queues to which they are assigned.

## 12.1.2 Prerequisites for myAgent

In order to use myAgent, the client PC of the subscriber must be equipped with the appropriate hardware and software configurations.

---

**NOTICE:** Please make sure that you refer to the notes in the `ReadMe first` file, which is located in the storage directory of the install files.

---

myAgent can be used in combination with the following telephones:

- OpenStage HFA
- OpenStage T (only HX via HiPath 3000)
- optiPoint 410 HFA
- optiPoint 420 HFA
- optiPoint 500 (only HX via HiPath 3000)
- DECT phones (HiPath Cordless Office)
- optiClient 130
- OpenScape Personal Edition

### Minimum Requirements for myAgent

- Operating system:
  - Microsoft Windows 7
  - Microsoft Windows Vista

- Microsoft Windows XP

---

**NOTICE:** The used operating system always requires the latest version of all available updates (Service Packs and patches).

---

- Web browser:
  - Microsoft Internet Explorer Version 7
  - Microsoft Internet Explorer Version 8 in compatibility mode
  - Microsoft Internet Explorer Version 9 in compatibility mode
  - Mozilla Firefox Version 4 or later
- Additional software for reports:
  - Adobe Reader 9
- Hardware:
  - 2 GHz CPU
  - 1 GB RAM for Microsoft Windows XP  
2 GB RAM for Microsoft Windows 7 and Microsoft Windows Vista
  - 100 Mbps LAN (1 Gbps LAN recommended)
  - XGA (1024x768) screen resolution

#### **Microsoft Terminal Server, Citrix XenApp Server**

myAgent can be used in terminal server environments under the following conditions: A project-specific release is required for this.

---

**INFO:** Terminal Server environments, including hosted services and virtual environments, are the responsibility of the customer.

---

- Software:
  - Microsoft Windows 2008 R2 Server with Citrix XenApp 6.0 Server (Desktop Mode)
  - Microsoft Windows 2008 R2 Server with Citrix XenApp 5.0 Server (Desktop Mode)
  - Microsoft Windows 2008 R2 Server as Microsoft Terminal Server
  - Microsoft Windows 2008 R2 Server as Microsoft Terminal Server
  - Microsoft Windows 2003 Server as Microsoft Terminal Server

---

**NOTICE:** The used software always requires the latest version of all available updates (Service Packs and patches).

---

- Hardware:
  - 2 GHz CPU
  - 100 Mbps LAN (1 Gbps LAN recommended)
  - XGA (1024x768) screen resolution

- 1 GB RAM for Microsoft Windows 2003 Server  
2 GB RAM for Microsoft Windows 2008 R2 Server and Microsoft Windows 2008 Server

Hardware Prerequisites: The number of installable clients depends on the server performance and on the amount of available memory. If the server is also being used for other applications, their memory requirements must also be taken into account. More information on the configuration of Citrix XenApp Server can be found under:

[http://wiki.siemens-enterprise.com/wiki/OpenScape\\_Office](http://wiki.siemens-enterprise.com/wiki/OpenScape_Office).

### Installation Files

The following options are available for providing installation files to users:

- The administrator downloads the installation files from the **Download Center** and provides them to users via a network drive, for example.
- You can directly access the installation files by connecting to the network drive with:

```
\\<IP address of the communication system>\applications
```

```
User: hoome, Password: hoomesw
```

The installation files are located in the `install-common` folder.

Please refer to the notes in the `ReadMe first` file, which is located in the storage directory of the install files.

---

**NOTICE:** The automatic distribution of the MSI file via a deployment service with Microsoft Windows Server is not supported.

---

## 12.1.3 myReports

Agents with the Supervisor or Administrator authorization level can use myReports to generate reports about agents and their activities, calls, queues, performance, GOS (Grade of Service) and wrap-up codes.

myReports offers the following features:

- More than 100 predefined report templates sorted by subject area (report groups) for the creation of reports
- Schedules for the scheduled generation of reports
- Immediate or scheduled sending of reports by e-mail
- Scheduled export of reports
- Output formats for report previews, sent e-mails and exported reports: Excel, PDF, and Word
- Report preview to check a report to be created in the desired output format.
- Integrated Report Designer for defining customized report templates (by the myReports administrator)

## User Roles

myReports has its own user management, which controls access to the functions of myReports through user roles. A distinction is made here between the myReports users (standard user) and the myReports administrator.

The current user role is set when you log into myReports.

The differences between the roles are summarized in the following table.

myReports: Activity	User Role	
	myReports User	myReports Administrator
<b>Reports</b>		
Preview report	X	X
Send report immediately by e-mail	X	X
Add report template	X	X
Delete added report template	X	X
Start Report Designer		X
Define new report template		X
Update predefined report templates		X
<b>Schedules</b>		
Add a schedule	X	X
Display details of a schedule	X	X
Edit schedule	X	X
Delete schedule	X	X
<b>Configuration</b>		
Change language of user interface	X	X
Change color of user interface	X	X
Configure e-mail template	X <sup>1</sup>	X
Change server address	X	X
Change administrator password		X
Configure e-mail account to send reports by e-mail		X
Configure phone number prefixes		X
language, selecting		X <sup>2</sup>
Set up default language		X <sup>2</sup>

1 The administrator password must be entered to configure the e-mail template

2 In order to configure languages and set the default language, you will need to log in as a myReports administrator with a special password.

## 12.1.4 Prerequisites for myReports

In order to use myReports, the client PC of the subscriber must be equipped with the appropriate hardware and software configurations.

---

**NOTICE:** Please make sure that you refer to the notes in the `ReadMe first` file, which is located in the storage directory of the install files.

---

### Minimum Requirements for myReports

- Operating system:
  - Microsoft Windows 7
  - Microsoft Windows Vista
  - Microsoft Windows XP

---

**NOTICE:** The used operating system always requires the latest version of all available updates (Service Packs and patches).

---

- Web browser:
  - Microsoft Internet Explorer Version 7
  - Microsoft Internet Explorer Version 8 in compatibility mode
  - Microsoft Internet Explorer Version 9 in compatibility mode
  - Mozilla Firefox Version 4 or later
- Additional Software:
  - Java 1.6.x
  - Adobe Reader 9 (for reports in PDF format)
  - Microsoft Excel (for reports in Excel format)
  - Microsoft Word (for reports in Word format)
- Hardware:
  - 2 GHz CPU
  - 1 GB RAM for Microsoft Windows XP
  - 2 GB RAM for Microsoft Windows 7 and Microsoft Windows Vista
  - 100 Mbps LAN (1 Gbps LAN recommended)
  - XGA (1024x768) screen resolution

### Multi-user PCs

Under Microsoft Windows 7, Microsoft Windows Vista and Microsoft Windows XP with multi-user PCs, every local user can use myReports with his or her own custom settings, provided the first local user has installed the client with local administration rights. Only the first local user with local administration rights can perform updates via the AutoUpdate.



## Microsoft Terminal Server, Citrix XenApp Server

myReports can be used in terminal server environments under the following conditions: A project-specific release is required for this.

---

**INFO:** Terminal Server environments, including hosted services and virtual environments, are the responsibility of the customer.

---

- Software:
  - Microsoft Windows 2008 R2 Server with Citrix XenApp 6.0 Server (Desktop Mode)
  - Microsoft Windows 2008 R2 Server with Citrix XenApp 5.0 Server (Desktop Mode)
  - Microsoft Windows 2008 R2 Server as Microsoft Terminal Server
  - Microsoft Windows 2008 R2 Server as Microsoft Terminal Server
  - Microsoft Windows 2003 Server as Microsoft Terminal Server

---

**NOTICE:** The used software always requires the latest version of all available updates (Service Packs and patches).

---

- Hardware:
  - 2 GHz CPU
  - 100 Mbps LAN (1 Gbps LAN recommended)
  - XGA (1024x768) screen resolution
  - 1 GB RAM for Microsoft Windows 2003 Server  
2 GB RAM for Microsoft Windows 2008 R2 Server and Microsoft Windows 2008 Server

Hardware Prerequisites: The number of installable clients depends on the server performance and on the amount of available memory. If the server is also being used for other applications, their memory requirements must also be taken into account. More information on the configuration of Citrix XenApp Server can be found under:

[http://wiki.siemens-enterprise.com/wiki/OpenScape\\_Office](http://wiki.siemens-enterprise.com/wiki/OpenScape_Office).

## Installation Files

The following options are available for providing installation files to users:

- The administrator downloads the installation files from the **Download Center** and provides them to users via a network drive, for example.
- You can directly access the installation files by connecting to the network drive with:

```
\\<IP address of the communication system>\applications
```

```
User: hoome, Password: hoomesw
```

The installation files are located in the `install-myReports` folder.

Please refer to the notes in the `ReadMe first` file, which is located in the storage directory of the install files.

---

**NOTICE:** The automatic distribution of the MSI file via a deployment service with Microsoft Windows Server is not supported.

---

## 12.1.5 Notes on Using myAgent and UC Clients Simultaneously

When myAgent and other UC clients are used simultaneously via one OpenScape Office user account, the possibility of mutual interactions cannot be excluded.

The term myPortal is used generically in this section to represent myPortal for Desktop, myPortal for Outlook, myPortal for Mobile and myPortal for OpenStage.

Examples of mutual interactions:

- Changing the presence status via myPortal
  - The examples apply to the default **Voicemail** setting for all call forwarding destinations.
    - myAgent: Agent is logged on.  
myPortal: The automatic reset of the presence status to Office is disabled. Changing the presence status via myPortal causes the agent to be immediately logged out of the queue(s). After the agent logs off via myAgent, the presence status in myPortal is reset to **Office**.  
A change in the agent status via myAgent (e.g., to **Break**) is registered by myPortal, but this does not apply to **Log in**, **Log out** and **Wrap up**.
    - myAgent: Agent is logged on.  
myPortal: The automatic reset of the presence status to Office is enabled. If the agent changes his or her status via myAgent to **Break**, he or she will be automatically available again after the break time has expired.  
A change of the presence status via myPortal to **Break** causes the agent to be immediately logged out of the queue(s).
    - myAgent: Agent is logged on.  
A change of the presence status via myPortal to **Do Not Disturb** causes the agent to be immediately logged out of the queue(s).
- Outbound Calls via myPortal
  - The presence status of the subscriber is visible via myAgent.
  - The calls appear only in the journal of myPortal. No transfer to the statistics of the Contact Center occurs, since these are not Contact Center calls.
- Incoming calls to the station number of the agent
  - The presence status of the subscriber is visible via myAgent.
  - The calls appear only in the journal of myPortal. No transfer to the statistics of the Contact Center occurs, since these are not Contact Center calls.

- Recording a call  
The recording of calls via myPortal is not registered by myAgent. myAgent offers this function even if the recording of a call is already occurring via myPortal.

## 12.2 Agents

The agents (stations) of a queue comprise a workgroup and are typically deployed for technical hotlines, for example, or in order processing, order acceptance, CRM, etc. The incoming calls, faxes and e-mails are distributed uniformly to the available agents for a queue.

In order to use a station of the communication system as an agent, this station must first be configured accordingly. The rights of the individual agents are defined by selecting their respective authorization levels (Agent, Supervisor or Administrator). An agent with the authorization level of a Supervisor or Administrator has elevated privileges (see [Agent Functions Independent of the Authorization Level](#)).

An agent can be defined as a permanently available agent. Such agents remain available for calls, faxes and e-mails even when they do not accept a call, fax or e-mail.

### System-Specific Information

Up to 64 agents can be licensed. The licenses for agents are "floating" licenses and not permanently bound to the agents. This means that any number of subscribers can be set up as agents. However, the number of agents that can log in at any given time is determined by the number of licenses available.

The following maximum capacity limits must be observed:

- OpenScape Office LX, via the gateway: up to 64 active agents (myAgent users) and up to 500 calls to the Contact Center per hour
- OpenScape Office MX One-box system: up to 10 active agents (myAgent users) and up to 200 calls to the Contact Center per hour
- OpenScape Office MX Multibox system: Up to 64 active agents (myAgent users) and up to 500 calls to the Contact Center per hour
- OpenScape Office HX, via HiPath 3000: up to 64 active agents (myAgent users) and up to 500 calls to the Contact Center per hour

### 12.2.1 Agent Functions Independent of the Authorization Level

When a user is configured as an agent, the rights of the agent are defined by selecting the appropriate class of service for that agent (i.e., the authorization level as an Agent, Supervisor or Administrator). An agent with the authorization level of a Supervisor or Administrator has elevated privileges.

The differences between the authorization levels are summarized in the following table.

**Multimedia Contact Center  
Agents**

myAgent: Activity	Authorization level (class of service)		
	Agent	Supervisor	Administrator
Assign an agent to a queue	–	X	X
Move an agent to another queue	–	X	X
Remove an agent from the queue	–	X	X
Change the status of an agent	–	X	X
Display / hide the agent binding list	Assigned queues	All queues	All queues
Edit an agent assignment	–	X	X
Display list of Contact Center calls	Assigned queues	All queues	All queues
Activate myAgent screen pop automatically for alarms	–	X	X
Activate alarm tone	–	X	X
Display wallboard	Assigned queues	All queues	All queues
Display the Grade of Service graph	Assigned queues	All queues	All queues
Display the Average Times graph	Assigned queues	All queues	All queues
Move call to first position in a queue	–	X	X
Record a call	Current call	All calls	All calls
Save recording of call as WAV file or send as WAV file by e-mail	–	X	X
Save fax as TIFF file or send as TIFF file by e-mail.	–	X	X
Save e-mail as EML file or send as EML file by e-mail.	–	X	X
Call monitoring (country dependent)	–	X	X
How to Override a Call	–	X	X
Accept a request for assistance	–	X	X
Create reports	–	X	X
Open the OpenScope Office Assistant	–	X	X

## **12.2.2 Preferred Agents**

Every caller (e.g., every calling customer) can be assigned one or more preferred agents of a queue. In such cases, the communication system first tries to switch the caller and his callback requests through to a preferred agent. If multiple preferred agents have been specified, a priority (sequence) can be defined to determine the order in which these agents are connected.

If no preferred agent is available, the call is forwarded to any available agent.

## **12.2.3 Agents in multiple queues**

An agent can be assigned to multiple queues with different skill levels. In such cases, the function of the agent as a primary agent or an overflow agent must be defined.

## **12.2.4 Contact Center Breaks**

In order to allow every agent the chance to take a defined break, Contact Center breaks of different lengths can be defined (e.g., for lunch or a cigarette break). Contact Center breaks are available system-wide and can be selected by an agent via myAgent as required.

## **12.3 Queues and Schedules**

Queues are the basis of the Contact Center. Calls, faxes and e-mails for a queue can be handled, depending on the skill levels of agents, the priorities and waiting periods. Announcements can be played for waiting callers. A schedule is used to define how incoming calls are to be handled on certain days and at specific times.

### **12.3.1 Queues**

As a rule, call distribution occurs by sending any incoming call, fax or e-mail for a queue to the specific station in the group (i.e., the agent) whose last call lies furthest in the past. It is also possible to define other distribution rules (based on the different skill levels of agents, for example). If all agents are busy, any additional calls, faxes and e-mails are placed in the queue and then distributed to the next free agent based on their priority and the waiting time.

Schedules and the rules contained in them (i.e., the CCVs or call control vectors) can be used to define how a call to a queue at a specific time and on a specific date is to be handled. The rules define which announcement is to be played back to callers, for example, or where a call is to be forwarded.

Faxes, e-mails and agent callbacks are assigned to queues directly, independently of schedules.

When assigning agents to queues, different properties, which affect the distribution of calls in a queue, can be assigned to agents (e.g., Primary Agent or Overflow Agent and Skill Level). Agents can be assigned to queues

- via OpenScape Office Assistant by an administrator with the **Advanced** profile.
- via the application myAgent by an agent with the Supervisor or Administrator authorization level.

If an agent is assigned to multiple queues, the queue priority can be used to define whether calls for a queue with higher priority should be forwarded to this agent with precedence over calls for other queues.

The following main settings can be made for queues via the OpenScape Office Assistant:

- Activating, deactivating and deleting queues  
Note: After the deletion of a queue, no reports for past time periods can be generated. Queues that are no longer required should be deactivated.
- Configuring queue alarms  
You have the following options:
  - Queue Alarm Count (alarm threshold value): If the number of calls waiting in the queue exceeds the number specified here, the queue symbol for the agent changes from green to orange. Agents with the Supervisor or Administrator authorization level can set whether they should be warned with an alarm tone and whether myAgent should be automatically brought to the foreground with a screen pop.
  - Queue Alarm Time (alarm threshold value): If the waiting time for a queued call exceeds the time specified here, the corresponding item in the list of Contact Center calls for the agents changes to red. Agents with the Supervisor or Administrator authorization level can set whether they should be warned with an alarm tone and whether myAgent should be automatically brought to the foreground with a screen pop.
- Defining timeouts for missed calls, faxes and e-mails  
If a phone call, fax or e-mail is not accepted by the agent at the end of the time specified here, the call, fax or e-mail will be forwarded to the next available agent.
- Defining an abandoned call threshold  
The time specified here determines whether or not an abandoned call is included in the statistics (i.e., in a report). Calls abandoned after the specified time has elapsed are included in the statistics.
- Setting up inbound fax pilots  
If configured, station numbers can be selected for incoming Fax messages. Faxes to these phone numbers will then be added to the queue and treated as incoming calls.

- Setting up an inbound e-mail service  
Multiple e-mail addresses can be set up for a queue. E-mails sent to these addresses are placed in the queue and treated like incoming calls.
- Setting up a return e-mail address  
E-mail address of the queue, which is displayed to the recipient when an e-mail is sent by an agent.
- Activating intelligent call routing  
An incoming call is forwarded to the agent with whom the caller was last connected, provided no preferred agent was defined for that caller.

## 12.3.2 Schedules

For each queue, a schedule can be defined with rules (Call Control Vectors or CCVs) to determine how incoming calls are to be handled on specific dates and at specific times.

For example, on work days, separate rules may be defined for the morning shift (from 6:00 to 14:00 hours), the afternoon shift (14:00 to 22:00 hours) and the night shift (from 22:00 to 06:00 hours). Similarly, a weekend rule can be defined for the weekends. For each of these rules, you can define whether an announcement is to be played, for example, and/or the destination to which the calls are to be forwarded.

Schedules are the core of the Contact Center configuration. Without the definition of at least one schedule, the configuration of a Contact Center cannot be completed successfully. Every queue must be assigned at least one schedule. This may also be the same schedule in every case.

A schedule, in turn, must have at least one rule (called a Call Control Vector or CCV) assigned to it. The rules determine how incoming calls for a queue are to be handled during the time period to which the schedule applies. Rules apply only to calls and not to faxes and e-mails.

Rules are created with the graphical rule editor (CCV Editor) by combining predefined CCV objects and can be saved under a user-defined name upon completion.

Saved rules can be assigned to one or more schedules as a default rule (default CCV) or an exception rule (exception CCV). They can be opened, edited and saved again at any time by using the rule editor.

After a schedule has been assigned a default rule (default CCV), this schedule can be saved under a user-defined name. A schedule with an assigned default rule applies to a queue 24 hours a day, 365 days a year. If different rules are to be applied at certain times (breaks, weekends, holidays, vacations, etc.), these can be assigned to the schedule as exception rules (Exception CCV). This means that you can define how incoming calls are to be handled during the holiday schedule, for example. Holiday schedules have precedence over the other schedules and rules of a queue.

### Rule Editor (CCV Editor)

The Rule Editor is used to create rules from predefined CCV objects. The arrangement of the CCV objects and their properties determine how incoming calls are to be handled.

The following predefined CCV objects are available:

---

**INFO:** For all of the named CCV objects, the two general properties listed below also apply:

**Description:** Optional entry to describe the CCV object, e.g., Greeting.

**Process digit:** specification of the digit(s) required without blanks, commas or other characters. The specification refers to the preceding CCV object. If 9 was specified there under Accepted Digits, then 9 must also be entered here.

---

- **Play Message**

Initiates the playback of a previously recorded and/or imported announcement

The playback of the announcement seizes one respective Media Stream channel.

Properties:

- **File Name:** Selection of an announcement (audio file in WAV format)
- **Interrupt Digits:** specification of a key or key combination on the dial pad with which callers can stop the playback of an announcement.
- **Record:** Record an announcement via a telephone
- **Upload:** Load (import) an audio file in wav format

- **Music on Hold**

Causes Music on Hold (MOH of the communication system) to be played for external calls for an adjustable period of time

Property:

- **Time Value:** Time, in seconds, for which the Music on Hold is to be played.

- **Disconnect Caller**

Causes the call to be disconnected.

After this CCV object, no further CCV object may be inserted.

- **Play Queue Position**

Causes information on the current queue position of the caller to be played.

- **Go to CCV**

Causes a loop to another CCV object

Property:

- **Target CCV:** Selection of the CCV object



- **Record Callback**

Enables a caller in a queue to enable an agent callback (record a voicemail). Instead of the actual caller, the agent callback remains in the queue. For agents with the **Enable agent callback** feature, the agent callback appears in the list of Contact Center calls.

After this CCV object, no further CCV object may be inserted.

Properties:

- **Type:** Selection of **Simple Callback** or **Extensive Callback**.

In contrast to simple callbacks, extensive callbacks offer callers additional options and information (e.g., the option to confirm or change the phone number that is to be called back and the option to confirm the voicemail).

- **Maximum message length:** Time, in seconds, that is available to a caller when recording a voicemail.

- **Process digit**

Causes the next CCV object(s) to be executed, depending on the digits specified there (process digit).

Properties:

- **File Name:** Selection of one or more announcements (audio file in WAV format)

- **Playlist:** List of selected announcements (audio file in WAV format) in the order in which they are played

- **Digits Timeout:** Time, in seconds, for which the communication system waits for the input of digits.

If the required digits are not entered fully within the specified time, the message (announcement) is played again.

The contents of the Playlist are presented in the Rule Editor by a tool tip on hovering with the mouse pointer over the CCV object.

- **Single Step Transfer**

This function depends on the **Normal Attendant Console SST** setting (OpenScape Office Assistant, **Expert mode: Applications > OpenScape Office > General Settings**):

- **Normal Attendant Console SST** enabled (default setting; not for U.S.): Causes the call to be transferred, regardless of whether the destination is free, busy or unavailable.

---

**INFO:** For stations with call waiting rejection enabled, the call is switched through only if the destination station is free. No call waiting on busy occurs.

---

- **Normal Attendant Console SST** disabled (default setting, only for U.S.):  
Causes the call to be transferred if the destination is free.  
If the destination is busy and call waiting rejection is disabled, or if the destination is unavailable, an announcement is played back to the caller. The caller can then optionally choose to leave a message in the voicemail box of the called subscriber or select the call number of another destination.  
If the destination is busy and call waiting rejection is enabled, the call is not switched through.

After this CCV object, no further CCV object may be inserted.

Property:

- **Target Extension:** specification of the internal call number (only IP phones (system clients) are supported) or external DID extension without the number of the CO trunk. Blanks, commas and other characters are not allowed.

The call number of the target extension is displayed in the CCV object.

- **Transfer To Queue**

Causes the call to be transferred to a queue.

After this CCV object, no further CCV object may be inserted.

Property:

- **Queue:** Selection of the queue

- **Record In Mailbox**

Causes the call to be sent to the desired voicemail box of a subscriber or a voicemail group

After this CCV object, no further CCV object may be inserted.

Property:

- **User Mailbox:** specifies the station number of the voicemail box of a subscriber or voicemail group

The station number and the name of the voicemail box or voicemail group are shown in the Rule Editor by a tool tip on hovering with the mouse pointer over the CCV object.

- **Supervised Transfer** (also called screened transfer)

Causes the call to be transferred to an internal destination.

In contrast to the single-step transfer CCV object, two further CCV objects must be inserted here. This is because we now need to define how the communication system should behave if the call destination is busy or does not answer the call. Usually, an announcement is played to the caller in such cases.

Properties:

- **Target Extension:** specification of the internal call number (only IP phones (system clients) are supported).

- **Ring Timeout:** Time, in seconds, within which the call must be accepted. If the call is not answered within the specified time, it is returned to the communication system, and the next CCV object is used.

---

**INFO:** The time specified here must be shorter than the time configured for call forwarding (the default setting for call forwarding = 15 seconds). See *OpenScape Office V3, Administrator documentation, Functions at the Telephone*.

---

- **Pull back call if destination device is forwarded / deflected:** Option (only applicable for internal call number.)  
If this option is enabled, the call destination is first checked, and if a forwarding destination or deflection has been set for it, the call is returned to communication system, and the next CCV object is used.
- **Check Presence status when transferring call:** Option  
If this option is enabled, the presence status of the call destination is checked, and if this status is any presence status other than Office, the call is forwarded to the voicemail box of the call destination.

- **Dial By Name**

Causes the caller to be prompted to enter the first three letters of the desired subscriber's last name via the dial pad.

If a unique subscriber name with the entered initial letters is found, a connection is established.

If there are several subscriber names with the entered initial letters, these subscriber names are announced to the caller (max. 10 subscribers). If a subscriber has no recorded name announcement, the call number is announced instead. After selecting the desired subscriber, a connection is made.

If none of the subscribers match the entered initial letters, the caller receives a corresponding message.

---

**INFO:** The keys on the dialpad respond to the first press of a key. With each key pressed, the system tries to determine whether there are subscriber last names with the letter assigned to that key.

Example: Let us assume the internal phone book has five last names with the initial letters t, u and v: Taylor, Taler, Ullrich, Vasquez and Volterra. To establish a connection with the subscriber Taylor, following keys must be pressed: 8 2 9

---

After this CCV object, no further CCV object may be inserted.

Properties:

- **Method:** Selection of **Transfer To Extension** or **Record In Mailbox**.  
Depending on the method selected, a connection to the desired extension or its voicemail box is established. Note that only internal extensions for which the first and last names of the subscriber are entered in the internal directory are supported here.

- **Dial By Extension**

Causes the caller to be prompted to enter the station number (extension) of the desired subscriber via the dial pad.

If the caller dials the station number of a virtual station, the caller is prompted to enter another station number. A connection is then established. If the desired subscriber does not respond, the call is accepted by his or her voicemail box.

After this CCV object, no further CCV object may be inserted.

Properties:

- **Method:** Selection of **Transfer To Extension** or **Record In Mailbox**.

Depending on the method selected, a connection to the desired extension or its voicemail box is established. Note that only internal extensions for which the phone number is entered in the internal directory are supported here.

- **Set language**

Selects the language for each standard announcement based on the phone number of the caller. It should be noted that only standard announcements (i.e., system announcements) and no personal greetings are taken into account here.

For example, it is possible to have German announcements played back to callers with the country code 0049 and French announcements for callers with the country code 0033.

Properties:

- **Default language:** Drop-down list to select a language.

The language selected here is used for all phone numbers for which no specific language was defined.

- **Pattern:** Specifies the phone numbers to which a particular language is to be assigned.

The following placeholders can be used \* = any digit, ? = any digit.

- **Language:** Drop-down list to select the language to be assigned to the relevant phone numbers (matching **Pattern**).

A language can be assigned to any number of different phone numbers (matching **Pattern**).

- **CLI Routing**

Causes the forwarding of a call to one or more sequential CCV objects based on the caller's number.

For example, it is possible to first have a German announcement played back to callers with the country code 0049 (CCV object **Play Message**) and then have the call forwarded to an internal phone (CCV object **Single Step Transfer**).

Properties:

- **Standard:** Drop-down list to select the CCV object.

The CCV object selected here is used for all phone numbers for which no specific destination was defined.

- **Pattern:** Specifies the phone numbers to which a specific CCV object is to be assigned as the destination.

The following placeholders can be used \* = any digit, ? = any digit.

- **Description:**  
Provides an explanation.  
For the **Pattern** 0049 (= country code for Germany), for example, Germany can be entered.  
The text entered here will appear in the Rule Editor.
- **Target:** Drop-down list to select the CCV object that is to be assigned as a destination to the related phone numbers (matching **Pattern**).  
A CCV object can be assigned as a destination to any number of different phone numbers (matching **Pattern**).
- **Branch on variable**  
Causes the forwarding of a call to one or more sequential CCV objects based on a given condition.  
You can thus define, for example, that an announcement (such as "Please call again later ...") should be played back to callers as soon as there are more than 20 calls in a queue.  
Properties:
  - **Variable:** Selection of **Calls** or **Available agents**.  
Depending on the selected variable, the number of calls waiting in a queue or the number of available agents (including agents in wrap up time) is used as the defined condition. In the associated drop-down list, the condition (**less than, greater than, less than or equal to, equal to or greater than, equal to**) must be selected, and the comparison value must then be entered in the corresponding input field.
  - **True branch:** Drop-down list to select the CCV object that is to be used as a destination when the condition is satisfied.
  - **False branch:** Drop-down list to select the CCV object that is to be used as a destination when the condition is not satisfied.

### 12.3.3 Wrap up

Wrapup reasons can be used to assign incoming calls to specific categories (orders, complaints, service, etc.). The assignment is made by an agent after completing the call (during the wrap-up time) by entering the appropriate wrapup reason using myAgent.

Wrapup reasons can be defined individually for each queue.

A distinction is made here between:

- **Simple Wrapup**  
One or more wrapup reasons can be defined for queues with the wrapup mode "Simple Wrapup".  
Example: The two wrapup reasons "hardware problem" and "software problem" were defined for a queue. Every call is assigned one of these wrapup reasons by an agent during the wrapup time. This makes it possible to subsequently create a report with an overview of all calls related to the subject of hardware problems, for example.

- **Multiple Wrapup**  
For queues with the wrapup mode "Multiple Wrapup", one or more wrapup reasons can be defined and then classified into groups and subgroups.  
Example: A Hardware group with the wrapup reasons Motherboard and Power Supply and a Software group with the wrapup reasons Operating System and Drivers were defined for a queue. Every call is assigned one of these wrapup reasons by an agent during the wrapup time. This makes it possible to subsequently create a report with an overview of all calls related to hardware problems or also all calls related specifically to motherboard hardware problems.

### 12.3.4 Grade of Service

The Grade of Service can be used to assess the response rate of the queue. This is achieved by comparing the waiting time for callers in the queue with target values, which can be specified individually for each queue.

The target values for the Grade Of Service (GoS) can be defined freely, depending on the acceptable waiting time for callers in a queue. For each call to an appropriate queue, the service level is determined after the call and committed to the database. The Grade of Service can be evaluated by agents with the authorization level of a Supervisor or Administrator by using the myAgent application.

### 12.3.5 Wallboard

Queue details can be retrieved and displayed using myAgent. The display contains a table with statistical information on queues in real time for the current 24-hour period. The display can then be presented on a large LCD monitor, for example, or via a beamer (wallboard).

Agents with the agent authorization level receive information on the queues to which they are assigned. Agents with the Supervisor or Administrator authorization level receive information on all queues.

A separate station should be set up for a wallboard display. A Comfort User license and a myAgent license are required for this.

### 12.3.6 Agent Callback

If the waiting time in the queue is too long for a caller, and the associated schedule includes the CCV object **Record Callback**, the caller can leave a callback request. This callback request retains the original position of the caller in the queue and is delivered to the agent in the form of a voicemail. After listening to the voice message, the agent can call back the caller via a screen pop.

If a preferred agent has been set for a caller, an attempt is first made to route the callback requests of that caller to the preferred agent. If the preferred agent is not available, the callback request is forwarded to any available agent.

## 12.4 VIP service

For each queue, you can individually define whether certain callers (with a VIP status) or callers which match configurable call number patterns should be given preferential treatment and thus allowed to reach a free agent faster.

If all agents of a queue are busy, VIP callers are preferentially connected to the next available agent.

### 12.4.1 VIP Caller Priority

The VIP Caller Priority can be defined individually for each queue in order to specify whether callers (customers, for example) included in the VIP Call List should be given preferential treatment.

The values for the VIP Caller Priority can be defined freely, depending on the waiting time for callers in a queue. This determines the level of preference for VIP callers as opposed to normal callers.

When a VIP caller activates an agent callback (by recording a voicemail with a callback request), the agent callback is retained in the queue instead of the VIP caller. but without the VIP Caller Priority.

VIP callers must be registered in the VIP call list directory (see [VIP Call List](#)).

### 12.4.2 VIP Call List

Callers who have already been registered in the communication system (external directory) can be added to the VIP call list. In addition, call number patterns can be entered. A call number pattern consists of a specific sequence of digits and a wildcard (placeholder). It can thus be used to transfer all employees of a company to the VIP call list, for example.

For each queue, the VIP caller priority can be used to define whether

- the callers included in the VIP call list and
- the callers who match the call number pattern contained in the VIP call list should be given preferential treatment.

It is not possible to enter call number patterns in the canonical call number format. The use of shortcut characters for country codes (for example +49 instead 0049) is likewise not possible. Call number patterns must always be specified without the CO access code.

Examples of call number patterns:

- 089 7577\* (089 = area code for Munich, 7577 = PABX number of a company, \* = wildcard for any number). By entering this call number pattern in the VIP call list, all callers from Munich, whose telephone number begins with 7577, are given priority.
- 0039\* (0039 = country code for Italy, \* = wildcard for any number). By entering this call number pattern in the VIP call list, all callers from Italy are given priority.

The following characters can be used as wildcards (placeholders) in a call number pattern:

- \* = wildcard for any number
- ? = wildcard for any digit

## 12.5 Fallback solution

If the Contact Center is unavailable due to problems (crash, connection down, etc.) the "Uniform Call Distribution (UCD)" feature of the communication system is automatically used. This feature thus serves as the fallback solution for the Contact Center.

In the event of a failure in the Contact Center, incoming calls are distributed according to the fallback solution. The distribution of faxes and e-mails is not possible.

Depending on requirements, one of the fallback solutions described below can be configured.

### **Default Fallback Solution**

In this case, the fallback solution is based on the UCD IDs of the agents:

- Agents are assigned to the UCD groups of the communication system based on UCD IDs.
- A UCD ID is assigned to an agent when configuring a subscriber as a Contact Center agent. The UCD ID determines to which UCD group this agent is assigned in the event of a failure at the Contact Center.

To ensure that the default fallback solution works properly, every queue must be assigned the Contact Center agents with the UCD IDs that were assigned to the appropriate UCD groups.

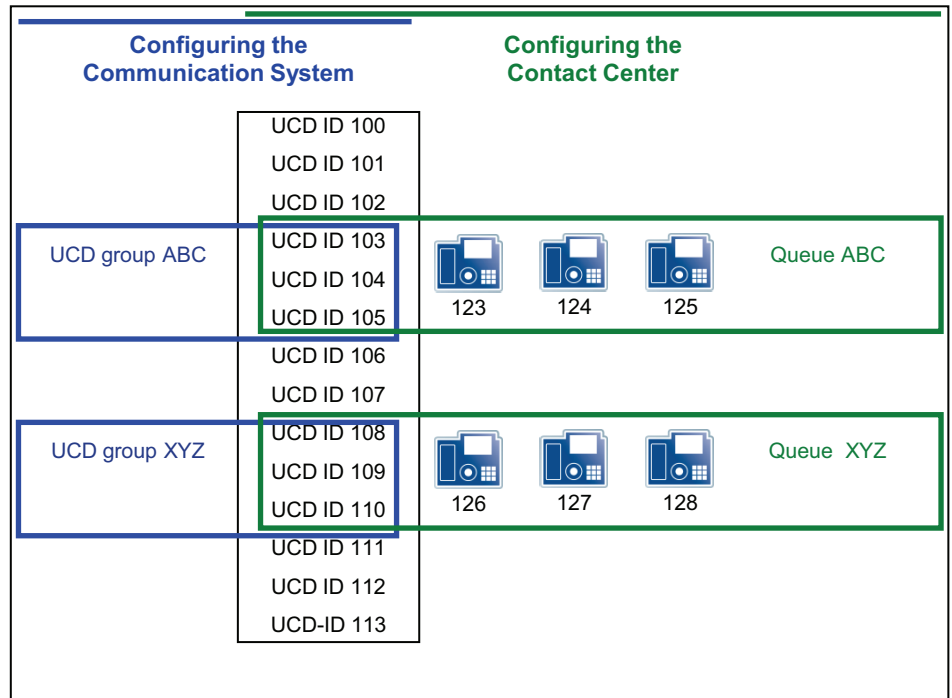
In the event of a failure in the Contact Center, incoming calls are distributed to the logged in agents via the different UCD groups.

Example:

- UCD IDs 103, 104 and 105 are assigned to UCD group ABC. UCD IDs 108, 109 and 110 are assigned to UCD group XYZ.
- The stations 123, 124 and 125 are configured as agents with the UCD IDs 103, 104 and 105. The stations 126, 127 and 128 are configured as agents with the UCD IDs 108, 109 and 110.



- When assigning agents to queues, the stations 123, 124 and 125 must be assigned to the queue ABC, and the stations 126, 127 and 128 to the queue XYZ.



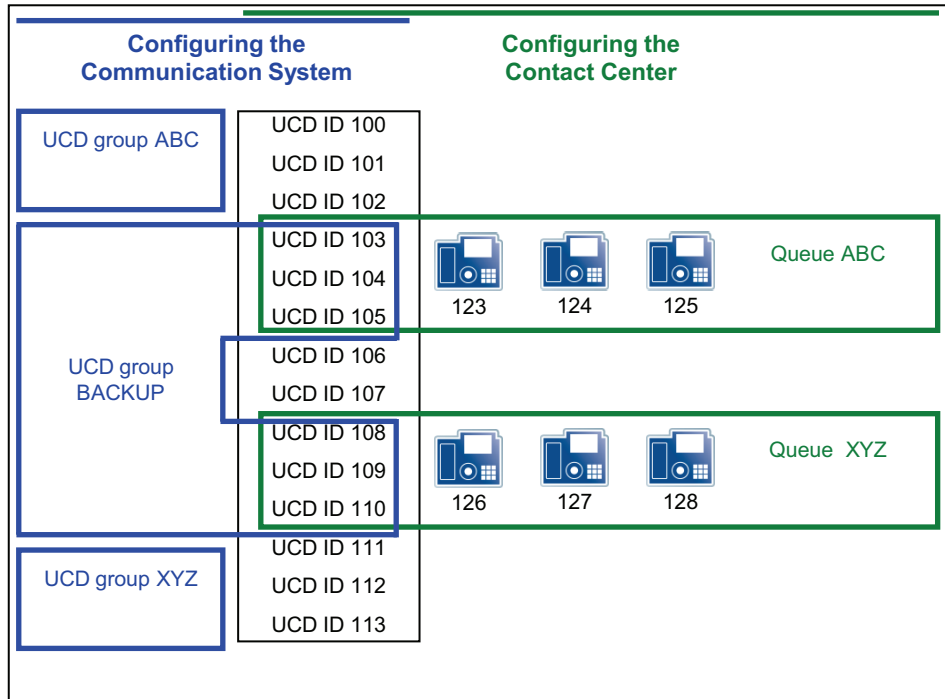
### Basic fallback solution

In this case, all agents of the Contact Center are assigned using their UCD IDs to only the Backup UCD group. By assigning the appropriate agents, these UCD IDs are then also used in the queues of the Contact Center. This ensures that in the event of a failure in the Contact Center, the agents do not have to manually log in at their phones with a different ID. This Backup UCD group is defined as a second call forwarding destination for all UCD groups of the communication system.

If the Contact Center fails, the incoming calls are then distributed to all agents of the backup UCD group.

Example:

- No UCD IDs were assigned to the UCD groups ABC and XYZ. UCD IDs 103 to 105 and 108 to 110 were assigned to the UCD group BACKUP.
- The stations 123, 124 and 125 are configured as agents with the UCD IDs 103, 104 and 105. The stations 126, 127 and 128 are configured as agents with the UCD IDs 108, 109 and 110.
- When assigning agents to queues, the stations 123, 124 and 125 are assigned to the queue ABC, and the stations 126, 127 and 128 to the queue XYZ.



**Custom fallback solution**

In this case, the customized configuration of the Contact Center is mapped via multiple UCD groups.

If the Contact Center fails, similar behavior is thus achieved by the fallback solution.

For details on configuring call distribution via the "Uniform Call Distribution (UCD)" feature of the communication system, see [UCD \(Uniform Call Distribution\) \(LX/MX\)](#).

The main advantage of the of the custom fallback solution, by contrast, lies in its accurate mapping of the Contact Center operations.

The disadvantage of the custom fallback solution is the high configuration effort involved. Furthermore, to achieve similar call distribution behavior, all changes made to the Contact Center configuration also need to be mapped to the fallback solution.

The main advantage of the default and basic fallback solution is the easy configuration.

**12.6 Configuring the Contact Center**

When configuring the Contact Center, the UCD groups must be defined first. The queues of the Contact Center are essentially workgroups that are based on the UCD groups of the communication system. The actual configuration of the Contact Center (schedules, queues, etc.) can then be performed.

For a Contact Center with OpenScape Office MX, the entire configuration occurs using the OpenScape Office Assistant.

For a Contact Center with OpenScape Office HX, the UCD groups and any possible fallback solution are configured using HiPath 3000 Manager E. The rest of the configuration is performed using OpenScape Office Assistant.

Before configuring the Contact Center, the standard processes for call distribution in normal and emergency modes must be coordinated with the customer.

---

**INFO:** The configuration of the Contact Center should only occur after the setup of the communication system and the UC suite have been fully completed.

---

The following licenses are a prerequisite for the operation of a Contact Center:

- Contact Center Basic License
- An appropriate number of licenses for agents (myAgent)
- Contact Center Fax License (for receiving and sending faxes), if necessary
- Contact Center E-mail License (for receiving and sending e-mails), if necessary

## 12.6.1 Example of an OpenScape Office MX Contact Center Configuration

The operating principle of the Contact Center with HiPath OpenScape Office MX and HiPath 3000 is presented here with the aid of an example. The structure and configuration of the example are based on a fictional customer scenario with standard Contact Center functions.

### Sample Scenario for an OpenScape Office MX Contact Center

Company XYZ operates a Contact Center with the following station numbers (queues):

- Station number 440 for the Service Department
- Station number 444 for the Sales department
- Station number 456 for free calls (Hotline). Callers receive an announcement and can then reach the Service or Sales Department by selecting the appropriate digit.

The Contact Center consists of six employees (agents), of which three work for the Service Department and three for Sales.

The queues for the Service and Sales Departments should be directly reachable during normal business hours from 09:00 to 17:00 hours. Both queues have a fax box and an e-mail address.

If all agents are busy or not available, callers are to be notified accordingly and have music played back to them. If no agent becomes free after a certain period of time, a caller can leave a callback request or reach the Attendant by dialing a specific number. If no digit is dialed, the caller should be automatically placed back in the queue.

During closed hours, callers are to hear an announcement enabling them to record a voicemail with a callback request (agent callback).

During the lunch break from 12:00 to 13:00 hours, an announcement is to be activated for the Service and Sales Departments to offer callers the option of recording a message with a callback request.

Fallback solution via Backup UCD group: If the Contact Center is unavailable due to problems (such as a system crash, dropped connection, etc.), the system should automatically switch to the "Uniform Call Distribution UCD" feature of the communication system as a fallback solution. This requires all of the Contact Center agents to be assigned to a single backup UCD group. For all UCD groups of the communication system, this Backup UCD group should be defined as a call forwarding destination. If the Contact Center fails, the incoming calls will then be distributed to the agents of the Backup UCD group.

### **Configuring the Sample Scenario**

The following actions must be performed for this sample scenario:

- **Configure UCD groups**  
The queues of the Contact Center are essentially workgroups that are based on the UCD groups of the communication system. The UCD groups must be defined before the actual configuration of the Contact Center.  
For this example of the Contact Center of company XYZ, three UCD groups (Service, Sales and Hotline) are to be configured.
- **Configure the fallback solution**  
For this example, a Backup UCD group is to be configured and defined as a call forwarding destination for all UCD groups of the communication system.
- **Configure subscribers as agents**  
For this example, six subscribers must be configured as agents.
- **Record individual announcements**  
For this example, various announcements are to be recorded. This includes an announcement for situations when no agent is available, for example, or an announcement to inform callers about possible options (using **Process after digits**).
- **Load individual announcements**  
For this example, the recorded announcements are to be loaded into the communication system.
- **Define schedules**  
For each time interval within a schedule, rules (Call Control Vectors or CCVs) can be defined to determine how incoming calls are to be handled on specific days and at specific times.  
In the example, a standard schedule XYZ is to be defined with a rule for the times outside business hours and with exceptions for business hours and the lunch break. In addition, a second schedule (Standard Schedule Hotline) is to be defined with a rule for free calls (Hotline).

Schedule	Rule (CCV)	
Standard Schedule XYZ	Out of the Office	Times outside business hours
	Open	Business hours 08:00 to 11:59 hours = Open1
		Business hours 13:00 to 17:00 hours = Open2
	Lunch Break	Lunch 12:00 to 12:59 hours
Standard Schedule Hotline	Hotline	24 Hours

- Adding three queues  
In this example, one queue is to be configured for the Service Department and one for Sales. A further queue (hotline) is to be configured for free calls.
- Assign agents to queues  
For this example, three agents are to be assigned to the Service queue and three to the Sales queue.

More details on the configuration of all Contact Center functions can be found under the [Configuration Procedure](#).

## 12.6.2 Example of an OpenScape Office HX Contact Center Configuration

The operating principle of the Contact Center with HiPath OpenScape Office HX and HiPath 3000 is presented here with the aid of an example. The structure and configuration of the example are based on a fictional customer scenario with standard Contact Center functions.

### Sample Scenario for an OpenScape Office HX Contact Center

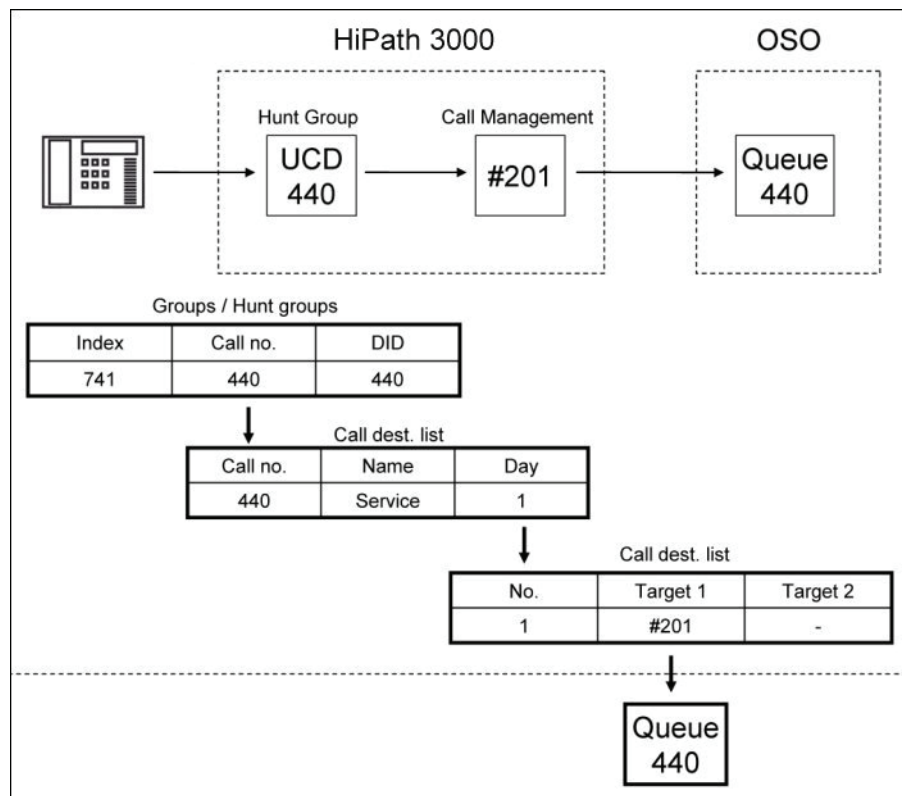
- Company ABC intends to operate a Contact Center with two dial-in numbers, of which one is to be used for "Service" and the other for "Sales". These two dial-in numbers are each to be processed via a separate queue. Both queues are to have group fax, group voicemail box and group e-mail.
- In addition to the two direct dial-in numbers, callers are also to be provided with a central toll-free dial-in option (Free Call). Using digit dialing, every caller is to be allowed to connect directly with Service, Sales or the respective group voicemail box.
- The Contact Center will consist of 6 staff members (agents) who accept calls from both queues. These staff members for the "Service" and "Sales" areas have different skill levels and are to be assigned calls on the basis of their respective skills.
- The queues must be reachable directly during business hours from 09:00 to 17:00 hours.

- If all members are busy or not available, callers are to be notified accordingly and have music played back to them. If no staff member is free, a caller should optionally be allowed to leave a callback request or to reach the Attendant by dialing specific digits. If no digit is dialed, the caller should be automatically placed back in the queue.
- During closed hours, callers are to hear an announcement indicating that they can record a voicemail with a callback request or optionally be forwarded to an emergency number.
- In the time from 8:00 to 9:00 hours, callers are to be greeted with a personal greeting and have the option of leaving a callback request or being connected to the operator.
- During the lunch break from 12:00 to 13:00 hours, an announcement is to be activated for each queue to offer callers the option of recording a message with a callback request
- Fallback solution: If the Linux server of OpenScape Office HX fails, the calls of all queues are to be accepted at defined workplaces.

**Linking a Queue with a UCD Group**

Before a queue can be configured, it must first be linked to a HiPath 3000 UCD group. The UCD group is a normal group that is converted to a UCD group by the assignment of a virtual address number.

The following figure shows the schematic sequence of an incoming call to group 440 (Service Department).



The UCD functionality is provided in the HiPath 3000 communication system by linking Group 440 with the virtual address number #201 in the call destination list. This information is stored in the SQL client and automatically transferred to the OpenScape Office database.

By setting up a queue with the call number 440 in the OpenScape Office Contact Center, a link to the UCD group 440 of the HiPath 3000 communication system is automatically established .

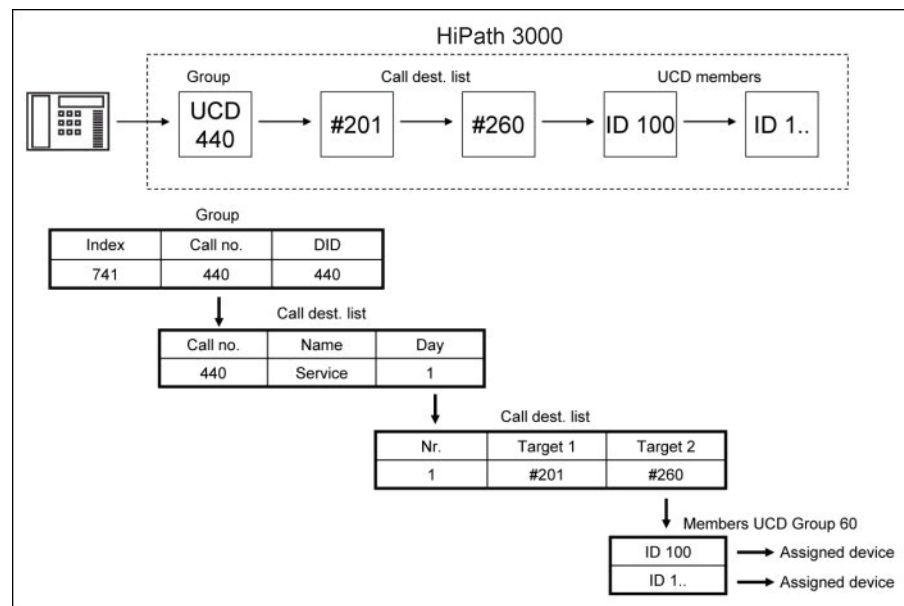
---

**INFO:** During the normal operation of the Contact Center, an agent cannot log into a queue by using a phone.

---

### Fallback Solution if the Linux Server of OpenScape Office HX Fails

The following figure shows the schematic sequence of an incoming call to group 440 (Service Department) when the Contact Center is not operational.



The UCD functionality is provided in the HiPath 3000 communication system by linking Group 440 with the virtual address number #201 in the call destination list.

Since no UCD agent IDs are assigned to the Group #201, the call is immediately forwarded to the Group #260.

Due to the assignment of UCD agent IDs in the UCD Group #260, agents can log into the UCD Group #260 from a telephone.

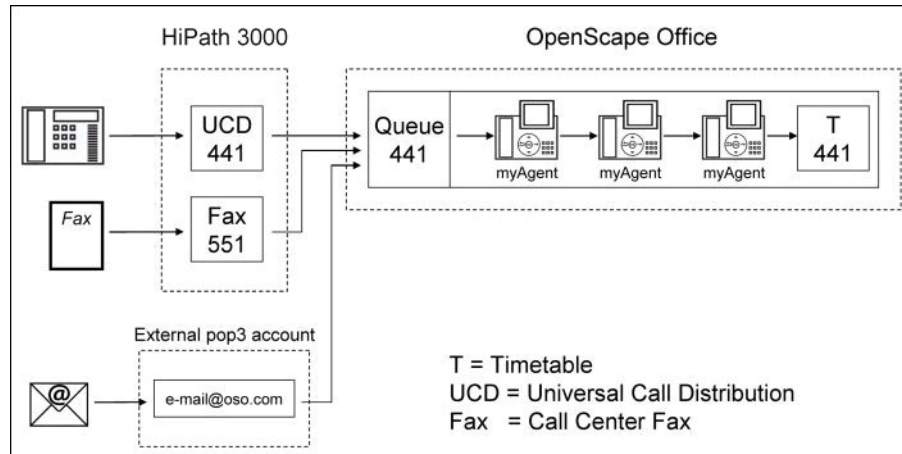
In the UCD group #260, the incoming calls are then forwarded to the phones of available agents.

When the Contact Center is back in operation, all incoming calls will only be processed in the group #201. No overflow to the UCD group #260 occurs.

This ensures that the phones of the agents logged into the UCD group #260 are only addressed in the event of a failure of the Contact Center and cannot intervene in the call distribution controlled by OpenScope Office.

### Queues without Announcements or Greetings

The following figure shows the schematic sequence for calls, faxes and e-mails received at a queue of the OpenScope Office Contact Center without any announcement prior to answering and without any greetings option.



A call to the UCD group 441 is accepted by the queue 441 of the OpenScope Office Contact Center. The call distribution to the available agents occurs immediately. If no agent accepts the call, the call is processed further by the schedule 441 (see *Schedule and Call Control Vector (CCV)*).

An incoming fax is accepted by the virtual station Fax 551 and handled by the queue 441 of the OpenScope Office Contact Center. The distribution to the available agents occurs immediately. If no agent accepts the fax, the fax remains in the queue and will be distributed later to an agent who becomes free.

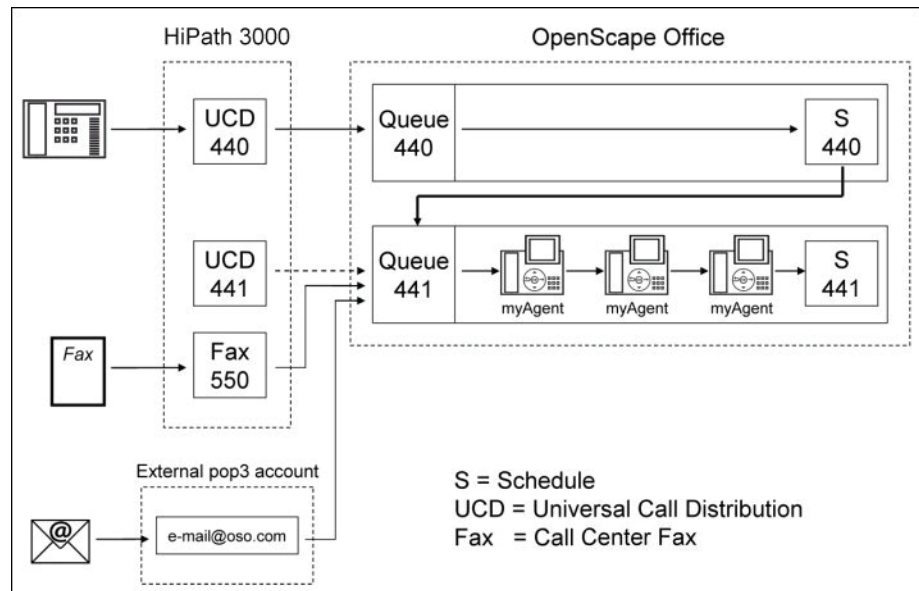
E-mails received on the external mail server are checked every 30 seconds by the internal e-mail client of the queue 441 of the OpenScope Office Contact Center. The e-mails are accepted by the queue 441 and immediately distributed to available agents. If no agent accepts the e-mail, the e-mail remains in the queue and will be distributed later to an agent who becomes free.

To use the e-mail function, a POP3 e-mail account is required on an external e-mail server. The Linux server of OpenScope Office HX does not provide e-mail accounts.

### Queues with Announcements or Greetings

The following figure shows the schematic sequence for calls, faxes and e-mails received at a queue of the OpenScope Office Contact Center with an announcement prior to answering or a greetings option.





A call to the UCD group 440 is accepted by the queue 440 of the OpenScope Office Contact Center. Since no agent is assigned to this queue, the call is immediately processed further via the schedule 440. This is where the greeting to the caller and the forwarding to queue 441 occurs.

The call is accepted through the queue 441 of the OpenScope Office Contact Center and distributed immediately to the available agents. If no agent accepts the call, the call is processed further by the schedule 441 (see *Schedule and Call Control Vector (CCV)*).

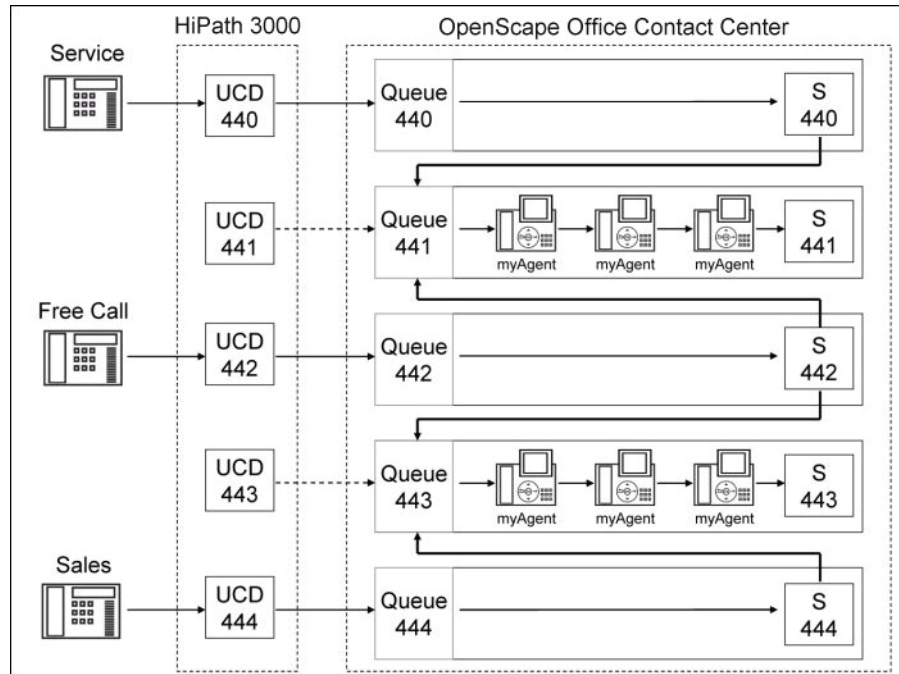
An incoming fax is accepted by the virtual station Fax 550 and handled by the queue 441 of the OpenScope Office Contact Center. The distribution to the available agents occurs immediately. If no agent accepts the fax, the fax remains in the queue and will be distributed later to an agent who becomes free.

E-mails received on the external mail server are checked every 30 seconds by the internal e-mail client of the queue 441 of the OpenScope Office Contact Center. The e-mails are accepted by the queue 441 and immediately distributed to available agents. If no agent accepts the e-mail, the e-mail remains in the queue and will be distributed later to an agent who becomes free.

To use the e-mail function, a POP3 e-mail account is required on an external e-mail server. The Linux server of OpenScope Office HX does not provide e-mail accounts.

### Concatenation of Multiple Queues

The following figure shows the schematic sequence for calls received at the Service, Free Call and Sales queues of the sample scenario for an OpenScope Office HX Contact Center.



A call to the UCD group 440 (Service Department) is accepted by the queue 440 of the OpenScape Office Contact Center. Since no agent is assigned to this queue, the call is immediately processed further via the schedule 440. This is where the greeting to the caller and the forwarding to queue 441 occurs.

The call is accepted through the queue 441 of the OpenScape Office Contact Center and distributed immediately to the available agents. If no agent accepts the call, the call is processed further by the schedule 441 (see *Schedule and Call Control Vector (CCV)*).

A call to the UCD group 442 (Free Call) is accepted by the queue 442 of the OpenScape Office Contact Center. Since no agent is assigned to this queue, the call is immediately processed further via the schedule 442. This is where the greeting to the caller and the manual selection of the queue (441 or 443) to which the caller wants to be forwarded occurs (see *Schedule and Call Control Vector (CCV)*).

A call to the UCD group 444 (Sales Department) is accepted by the queue 444 of the OpenScape Office Contact Center. Since no agent is assigned to this queue, the call is immediately processed further via the schedule 444. This is where the greeting to the caller and the forwarding to queue 443 occurs.

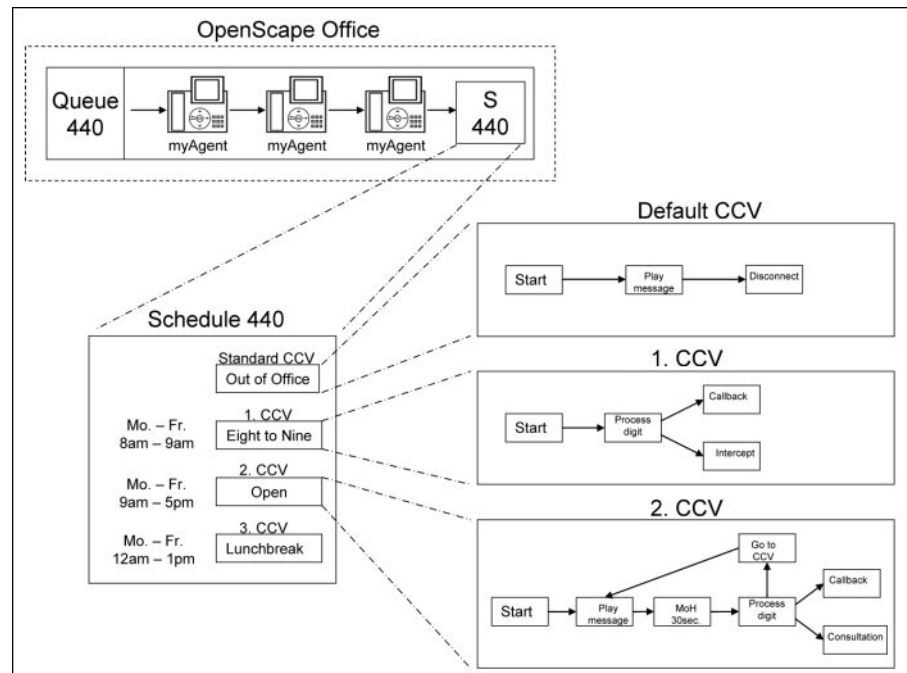
The call is accepted through the queue 443 of the OpenScope Office Contact Center and distributed immediately to the available agents. If no agent accepts the call, the call is processed further by the schedule 443 (see *Schedule and Call Control Vector (CCV)*).

**INFO:** The distribution of faxes and e-mails is not described in this example.

If an integration of faxes and e-mails is required, this occurs as described under *Queues without Announcements or Greetings*.

### Schedule and Call Control Vector (CCV)

The following figure shows the schematic sequence for calls received at a queue of the OpenScope Office Contact Center and their subsequent processing via a schedule.



If a call to a queue is not accepted by an agent, further processing always occurs via a schedule. This schedule and the rules contained in it (Call Control Vectors or CCVs) define how incoming calls are to be handled on specific dates and at specific times.

For each required time period within a schedule, a Call Control Vector (CCV) must be set up. If the functionality is the same on all days (24 hours/7 days), at least one default CCV is needed.

Example:

- **Default CCV Out of Office (entire week)**  
The call is answered with an announcement. The caller can optionally leave a callback request or reach the operator by dialing digits.

- **CCV Eight to Nine (Monday - Friday, 08:00 to 08:59 hours)**  
The call is answered with an announcement. The caller can optionally leave a callback request or reach the operator by dialing digits.
- **CCV Open (Monday - Friday, 09:00 hours to 17.00 hours)**  
The call is answered with an announcement, followed by Music on Hold for 30 seconds. The caller can optionally leave a callback request or reach the operator by dialing digits.

---

**INFO:** If a call is being processed by a CCV, and an agent of the associated queue becomes free, the call is forwarded immediately to the free agent.

---

### **Configuring the Sample Scenario**

The following actions must be performed for this sample scenario:

- **Preconfiguration using HiPath 3000 Manager E**
  - **Configure UCD groups**

The Contact Center uses the "Uniform Call Distribution (UCD)" feature of the HiPath 3000 communication system to distribute calls within a queue. A UCD group contains agents (subscribers) that belong to a work group and can be reached at a single phone number (UCD group call number). Using the UCD group call number, a queue is uniquely assigned to a UCD group.

In order to set up a UCD group, a hunt group (e.g., with the call number 440) must be first defined. This group must then be assigned a virtual address number (e.g., #201 for UCD group 1). The hunt group thus becomes a UCD group that can be called by dialing the call number 440.
  - **Configure the fallback solution**

For the present example, it is necessary to configure a further UCD group (fallback UCD group, which is the UCD group 60 in the example) and to define this UCD group as the call forwarding destination of all configured UCD groups. If a failure occurs in the Contact Center, all calls will be routed to the fallback UCD group 60. Agents who are assigned to this UCD group 60 via UCD agent IDs are automatically logged into this UCD group if they log in through myAgent. They can thus answer the calls for all queues.
  - **Configure the station numbers to be shown on the display of external subscribers**

For the present example, the Contact Center is to transmit a phone number for calls with external subscribers and show it on the phone display of the external party. To do this, a virtual station must be set up, and the station number to be transmitted must be assigned to it as a DID number.

- Transfer the settings  
The preconfigured settings must be transmitted to HiPath 3000.  
The initial transfer of the CDB from HiPath 3000 Manager E to HiPath 3000 is time- consuming, since the database of SQL server is completely rebuilt by OpenScape Office. For HiPath 3800, the transfer takes about 20 minutes, and for HiPath 3500, about 60 minutes. The other changes to the settings are transferred to the database of the SQL server faster.
- Configuration using OpenScape Office Assistant
  - Configure subscribers as agents  
For this example, six subscribers must be configured as agents.
  - Record individual announcements  
For this example, various announcements are to be recorded. This includes an announcement for situations when no agent is available, for example, or an announcement to inform callers about possible options (using **Process after digits**).
  - Load individual announcements  
For this example, the recorded announcements are to be loaded into the communication system.
  - Define schedules  
For each time interval within a schedule, rules (Call Control Vectors or CCVs) can be defined to determine how incoming calls are to be handled on specific days and at specific times.  
For this example, a Timetable schedule is to be defined for the two queues, Sales and Service. In addition, a second Free Call schedule is to be defined for the Free Call queue.  
For both schedules, the following rules must be defined:

Schedule	Rule (CCV)	
Timetable	Out of Office (outside business hours)	The rule is always applied by default, except at the times for which exceptions have been defined (default CCV).
	Eight to Nine (before business hours)	08:00 hours to 08:59 hours
	Open (during business hours)	09:00 hours to 17:00 hours
	Lunch Break	12:00 hours to 13:00 hours
Free Call	Free Call	24 Hours

- Adding three queues  
In this example, one queue is to be configured for the Service Department and one for Sales. A further queue (Free Call) is to be configured for free calls.
- Assign agents to queues  
For this example, three agents are to be assigned to the Service queue and three to the Sales queue.

More details on the configuration of all Contact Center functions can be found under the [Configuration Procedure](#).

## 12.6.3 Configuration Procedure

This section contains an overview of the actions to be performed when configuring the Contact Center.

- **Configure UCD groups**  
The queues of the Contact Center are essentially workgroups that are based on the UCD groups of the communication system. The UCD groups must be defined before the actual configuration of the Contact Center.
- **Configure a fallback solution**  
If the Contact Center is unavailable due to problems (crash, connection down, etc.) the "Uniform Call Distribution (UCD)" feature of the communication system is automatically used. This feature thus serves as the fallback solution for the Contact Center (see [Fallback solution](#)).
- **Configure subscribers as agents**
- **Record individual announcements for the Contact Center**
- **Load individual announcements for the Contact Center**
- **Add schedules**
- **Add queues**
- **Define target values for the Grade of Service**
- **Define the VIP caller priority**
- **Edit the VIP call list**
- **Define preferred agents**
- **Add Contact Center breaks**
- **Add wrap-up codes**
- **Assigning agents to queues**

## 12.7 Notes on Using the Contact Center

This section contains information about some special aspects and possible restrictions to be observed when using the Contact Center.

### 12.7.1 Using the Contact Center in a Communication System with IP Trunks and Outside Line

The external connections of the Contact Center can be made via both ISDN and IP telephony. It should be noted that the integration of IP telephony is only possible through certified Internet Telephony Service Providers (ITSPs). Analog CO trunks (MSI) are not supported through the Contact Center.

Information about the certified Internet Telephony Service Providers can be found in the expert wiki for telephones, communication systems and Unified Communications from Siemens Enterprise Communications (<http://wiki.siemens-enterprise.com>).

The following example for OpenScape Office MX describes the operation of the Contact Center using ISDN. This means that only ISDN trunks are used for external connections of agents.

For a Contact Center with OpenScape Office HX, the settings for the HiPath 3000 communication system (CON groups, CON Matrix) must be made using HiPath 3000 Manager E.

OpenScape Office MX uses CON groups (traffic restriction groups) to control which connections between stations (agents) and trunks are allowed or denied. All stations and CO trunks are assigned to CON group 3000 by default. All stations (agents) thus have unrestricted access to all trunks (including both inbound and outbound).

In order to ensure that the agents of the Contact Center only use ISDN trunks for external connections, the agents, IP trunks and the analog CO trunks must each be assigned to a separate CON group. The CON matrix can then be used to prevent connections between the CON group for agents with der CON group for IP trunks and the CON group for analog CO trunks.

---

#### **Related Topics**

- [CON Groups \(LX/MX\)](#)

## **12.7.2 Restrictions on Operating the Contact Center**

The operation of the Contact Center is subject to certain conditions. In addition, there are some restrictions on the use of system features by agents.

#### **Conditions for the Operation of the Contact Center**

The following conditions for the operation of the Contact Center must be taken into account:

- **Trunks**  
The Contact Center does not support analog trunks (MSI). All external connections of the Contact Center must be made via ISDN or IP telephony. It should be noted that the integration of IP telephony is only possible through certified Internet Telephony Service Providers (ITSPs).
- **Networking**  
In a networked scenario, all agents must be connected to the communication system in which the Contact Center is configured.

- **Agent telephones**  
Agents can use all system telephones (IP phones (HFA) such as OpenStage 40, for example) and DECT telephones. Note that only the DECT telephones that are currently released for operation with HiPath Cordless Office may be used.  
It is not possible to use analog, ISDN and SIP telephones here.  
Agents are not allowed to be members of a group (Group Call, Hunt Group) or a MULAP. This restriction also applies to system features used in combination with MULAPs, i.e., Team Configuration (Team Group), Executive/Secretary (Top Group) and Mobility Entry.
- **myAgent**  
myAgent should not be used simultaneously with other UC clients, since mutual interference with the presence status cannot be excluded (see [Notes on Using myAgent and UC Clients Simultaneously](#)). During normal operation of the Contact Center, agents use only myAgent to change their status (logged in, logged out, available, etc.).
- **Connecting applications via the CSTA interface**  
It is possible to connect applications via the CSTA interface, provided the following conditions are met:
  - The application should not produce any significant additional load on the CSTA interface.  
Consequently, the connection of unified communications or call distribution solutions, CTI power dialers or even CTI solutions with many intensively used individual CTI clients is not allowed.
  - The application must not control any agent telephones via the CSTA interface or set up any call forwarding for the agent telephones.  
Consequently, the connection of CTI applications for agents, rule assistants or personal assistants is not allowed.The connection of HiPath TAPI 120/170 has been basically approved. For the load of the communication system, the same conditions as for the connection of other applications via the CSTA interface apply. In connection with the Contact Center, HiPath TAPI 120/170 should preferably be used to connect CRM (Customer Relationship Management) or ERP (Enterprise Resource Planning) systems, provided they support TAPI.

### **Restrictions on Using System Features**

The following system features are not available to agents or are subject to restrictions. These features are, however, not mandatory for agents, since the allocation of calls is handled automatically by the Contact Center. The allocation depends on the set rules and the availability of agents.

- **Locked Features**  
As soon as a subscriber of the communication system is configured as an agent, the following features are no longer available.
  - Second call
  - Call waiting
  - Intrusion on an agent call (exception: agents with the authorization level of a Supervisor or Administrator)
  - Group Call



- Do Not Disturb (for logged in agents)
- Features that affect call routing

The following features could potentially change the call routing in the contact center and should therefore not be executed by agents.

  - Call forwarding

If a logged in agent activates call forwarding, a logout occurs.  
Call forwarding is disabled as soon as an agent logs into a queue.
  - Do Not Disturb

If a logged in agent activates Do Not Disturb via a UC client, an automatic logout occurs.  
Do not Disturb is disabled as soon as an agent logs into a queue.
  - Relocate

Relocating a telephone changes the logical assignment of the station numbers. The new station number assignment is only transmitted after restarting the Contact Center.
  - Night service

When setting up a night service in the communication system, it must be ensured that the configurations of the Contact Center-related parameters (agents, queues, etc.) for the day and night service are identical.
- Features that affect reports

Executing the following features from an agent telephone can lead to a distortion of the information in reports:

  - Call pickup of Contact Center calls by non-agents
  - Call transfers (e.g., via the Direct Station Select (DSS) key) of Contact Center calls to non-agents
  - Conferencing
  - Alternate (Toggle/Connect)
  - Parking

---

**INFO:** The "Consultation Hold" feature is transparent for the presentation of Contact Center calls in reports and can be used by agents, regardless of the consultation destination.

---
- Roles and functions not relevant for agents

The following functions are not relevant, since the "Call Waiting" feature (also called "camp on") is blocked for agents.

  - Attendant Console
  - Hotline destination

## 12.8 Notes on the Use of DECT Telephones (HiPath Cordless Office)

DECT telephones can be used as phones for contact center agents. However, the differences in the operating procedure as compared to corded phones must be taken into account.

### Prerequisites for the Use of DECT Telephones (HiPath Cordless Office)

- Only the DECT telephones that are currently released for operation with HiPath Cordless Office may be used.
- The area within which the contact center agents move about must provide a complete wireless coverage.
- The number of HiPath Cordless Office base stations must be such that enough B-channels are available for the DECT telephones of the contact center agents.
- As far as possible, a contact center agent should not leave the wireless range while logged into a queue of the contact center.

### Differences in the Operating Procedure as Compared to Coded Phones

- Logging into a queue of the contact center is only possible through myAgent.
- No messages such as **Available** or **Break**, for example, appear in the display of the DECT telephone.
- The control of a DECT telephone via myAgent (e.g., via the **Telephony bar** or the **myAgent Inbound Call** screen pop) is not possible.
- Incoming calls can only be accepted via the DECT telephone.
- Outbound calls must be initiated via the DECT telephone.

### Aspects to be considered when using DECT telephones (HiPath Cordless Office)

- Search time  
For an incoming call, the time required to find the DECT telephone may take several seconds (at worst up to 20 seconds) before a call is signaled on the DECT telephone. During the search time, the caller hears the ringing tone. The contact center evaluates this time as "pickup time". The actual pickup time by a contact center agent thus consists of the search time and the alert time (i.e., time until the call is answered).  
If a contact center agent leaves the wireless range with his or her DECT telephone, this may result in longer search times.
- DECT telephone cannot be found  
If a contact center call exceeds the prescribed time for a call to be answered by the agent (e.g., because the contact center agent is out of range), the agent is automatically logged out of the queue or queues involved. Logging in again is only possible through myAgent.

## 12.9 Reports

Reports are used to determine the current status of the Contact Center and to analyze the strengths and weaknesses of its associated components. This makes it possible to optimize the Contact Center configuration, for example, and to thus use the Contact Center resources more efficiently. The Contact Center provides users with real-time reports as well as historical reports.

### Real-time Reports

Real-time reports are continuously updated. They provide important information such as details on agent utilization, the grade of service, abandon rates and average processing times. Using these continually updated and filterable caller lists, the progress of a customer contact can be examined in stages. In addition, the activities of all agents can be reviewed. This information can be used for training purposes, for example, and for contact analysis and wrap-up activities.

Agents with the authorization level of a Supervisor or Administrator can be acoustically and visually informed when definable operating parameters are exceeded. Appropriate thresholds for each queue can be defined individually.

### Historical Reports

By selecting data elements and user-specific report parameters, historical reports can be set up quickly and retrieved in graphic or tabular form.

Using the myAgent application, more than 20 predefined report templates can be used for standard reports.

The optionally available myReports application expands the options for creating historical reports with over 100 predefined report templates. The report generation can be individually scheduled, and the prepared reports can be automatically sent at scheduled times in standard export formats to predefined e-mail addresses or stored at a location configured by the myReports administrator. Experienced users who are familiar with database structures can also use the BIRT (Business Intelligence and Reporting Tools) RCP Designer integrated in myReports to edit the predefined report templates and to create new templates.

---

**INFO:** Reports based on the call history stored in the communication system. The maximum retention period for the call history is 365 days (default setting). An administrator with the **Expert** profile can set the retention period for the call history on a system-wide basis.

Example: The retention period was set to 100 days. This means that only data that is up to 100 days old can be used for the preparation of reports.

---

### Data Protection

If the myReports administrator enabled data protection when configuring myReports, the last four digits of the phone numbers (CLI column) will be replaced by \*\*\*\* in all relevant reports.

If the subscriber has flagged his or her private number, mobile number, external number 1 and/or external number 2 as invisible, these phone numbers will not be displayed in all relevant reports.

## 12.9.1 Predefined Report Templates

myReports provides more than 100 predefined report templates for creating reports.

These templates are classified by subject area and assigned to the following report groups:

- **Agent Activity**
- **Agents**
- **CLI**
- **Call History**
- **Calls**
- **Fax / E-Mail**
- **Other**
- **Performance**
- **Queues**
- **User Presence Status**
- **Wrap-up Codes**

## 12.9.2 Report Designer

The Report Designer integrated in myReports can be used to design custom report templates.

The Report Designer is a separately started Open Source application (called the BIRT RCP Designer) for the professional creation of report templates. BIRT is an acronym for Business Intelligence and Reporting Tools.

myReports supports the BIRT RCP Designer through

- the predefined database connection,
- the integration of report templates used in myReports.
- a data transfer program for integrating newly created report templates in the Report Manager.

## 13 Mobility

OpenScope Office provides integrated mobility solutions for any business. This typically includes the integration of mobile phones/smartphones, the usage of Cordless and WLAN phones, etc., down to Desk Sharing and teleworking. Mobility includes Mobility on the road, Mobility in the office and Mobility at home.

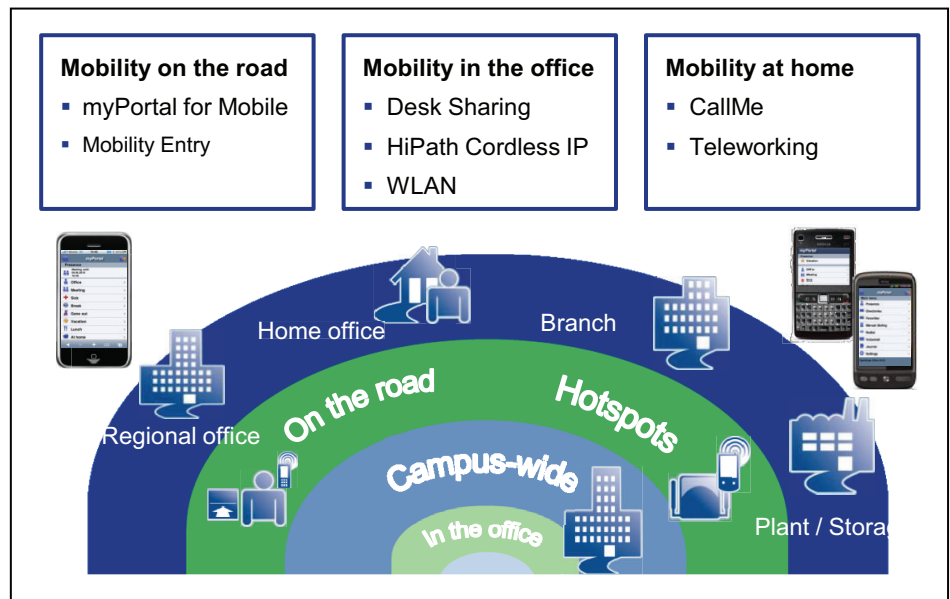
---

**INFO:** Further Mobility functions are offered through unified communications (see [Unified Communications](#)). For more information on teleworker connections via a VPN, see [Security](#).

---

### 13.1 Integrated Mobility Solution

The mobility solutions integrated in OpenScope Office provide efficient communication everywhere and with a wide variety of terminals. With myPortal for Mobile, OpenScope Office HX additionally supports the mobility solutions of HiPath 3000.



---

#### Related Topics

- [myPortal for Mobile](#)
- [Mobility Entry \(MX\)](#)
- [IP Mobility / Desk Sharing \(LX/MX\)](#)
- [CallMe Service](#)
- [Connecting Teleworkers via a VPN](#)

## 13.2 Mobility on the Road

Mobility on the road is achieved through the integration of mobile phones via myPortal for Mobile or Mobility Entry. The One Number Service (for myPortal for Mobile and Mobility Entry) enables a subscriber to be reached through a single phone number worldwide. Furthermore, with dual-mode telephony, additional cost savings can be achieved if the subscriber is within range of a WLAN.

The Mobility Entry client (Mobility client) and myPortal for Mobile are mutually exclusive, i.e., cannot be used simultaneously on the same mobile phone.

A maximum of 150 (OpenScape Office MX) or 500 (OpenScape Office LX/HX) mobile phones are supported.

---

### Related Topics

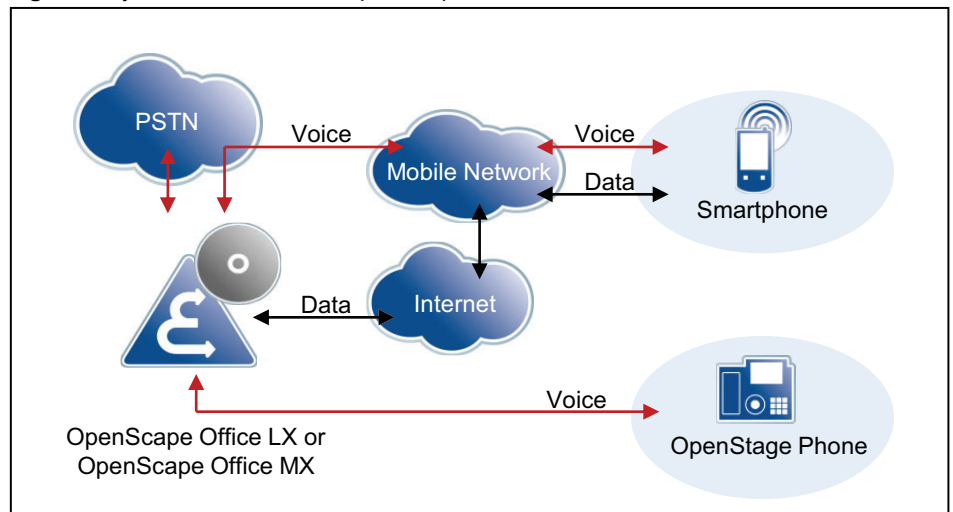
- [Mobility at Home \(LX/MX\)](#)

### 13.2.1 myPortal for Mobile

myPortal for Mobile integrates mobile phones into the communication system. This enables subscribers to access unified communications features analogously to myPortal for Desktop and myPortal for Outlook via the web browser of the mobile phone. Mobile phones can be integrated into the communication system with any phone numbers (e.g., the mobile phone number).

With myPortal for Mobile, the mobile phone controls the communication system via the web browser. myPortal for Mobile sets up a parallel data connection to the communication system, providing additional unified communications functions such as the Presence status, directories and journals. myPortal for Mobile can be used on both pure GSM mobile phones and dual-mode phones. In order to use myPortal for Mobile, a mobile phone contract with data option (flat rate recommended) is required.

**Figure:** myPortal for Mobile at OpenScape Office LX/MX



### Features of myPortal for Mobile

myPortal for Mobile provides the following features:

- Directories
- Favorites List
- Journal
- Presence status
- CallMe Service
- Voicemails

For a description of the unified communications features and myPortal, see [Unified Communications](#).

### CTI Features During a Call

myPortal for Mobile offers the following CTI features:

- Consultation
- Alternate (Toggle/Connect)
- Attendant
- Conferencing
- Disconnect

### Calling myPortal for Mobile

The mobile subscriber can now access myPortal for Mobile via the web browser of his or her mobile phone. The URL is `http://<IP address of the communication system>:8801` or `https://<IP address of the communication system>:8802`.

After a connection with the communication system has been successfully established, the login screen with the user name (= internal call number of the subscriber) and password (= password for myPortal) is displayed in the web browser.

### Dialing Methods of myPortal for Mobile

Mobile phone users can choose between different dialing methods for outbound calls. The following table shows the possible dialing methods for the OpenScape Office communication system:

Dialing mode	LX	MX	HX/HiPath 3000
Callback	yes	yes	yes
Call through	yes	yes	yes
SIP	yes	yes	no
Associated dialing, only for tablet PC	yes	yes	yes, for associated UP0 and HFA telephones no, for associated SIP phones
GSM	no	no	no

---

#### Related Topics

- [Integrated Mobility Solution](#)
- [One Number Service \(LX/MX\)](#)
- [Comparison between myPortal for Mobile and Mobility Entry](#)
- [Dependencies for myPortal for Mobile and Mobility Entry](#)

### 13.2.1.1 Prerequisites for myPortal for Mobile

In order to use myPortal for Mobile, the mobile phone must be equipped with the appropriate hardware and software.

The following requirements apply:



Client	Technical Data
myPortal for Mobile	<p>myPortal for Mobile is optimized for presentation on Apple's iPhone and can also be used with several other mobile phones. Depending on which device and operating system is used, the ease of use or function may be affected. The following requirements apply:</p> <ul style="list-style-type: none"> <li>• Touch screen (recommended for ease of use)</li> <li>• Display resolution of at least 240 * 320 pixels</li> <li>• Internet access</li> <li>• Web browser with JavaScript enabled</li> <li>• Support for the simultaneous transmission of voice and data through mobile phones and the mobile network</li> <li>• 3G data connection, for example, EDGE, UMTS, HSDPA (recommended for smooth service). GPRS can lead to slow page rendering.</li> <li>• Flat rate data plan (recommended for cost reasons), since data volumes of several 100 MB per month may be involved, depending on usage.</li> </ul>
myPortal for Mobile (for Tablet PC)	<p>myPortal for Mobile/Tablet PC is optimized for presentation on Apple's iPad and can also be used with several other tablet PCs. Depending on which device and operating system is used, the ease of use or function may be affected. The following requirements apply:</p> <ul style="list-style-type: none"> <li>• Touch screen (recommended for ease of use)</li> <li>• Display resolution of at least 800 * 480 pixels Recommended resolution: at least 1024 * 600 pixels</li> <li>• Internet access</li> <li>• Web browser with JavaScript enabled</li> <li>• 3G data connection, for example, EDGE, UMTS, HSDPA (recommended for smooth service). GPRS can lead to slow page rendering. Alternatively: a pure WLAN connection with a SIP client for telephony.</li> <li>• Flat rate data plan (recommended for cost reasons), since data volumes of several 100 MB per month may be involved, depending on usage.</li> </ul>

Depending on which device and operating system is used, the ease of use or function may be affected.

### **Operating systems and reference devices**

myPortal for Mobile works with numerous mobile phones and tablet PCs and has been optimized for the following operating systems and reference devices:

Operating system	Reference device
Apple iOS	<ul style="list-style-type: none"> <li>• Apple iPhone 3GS</li> <li>• Apple iPhone 4</li> <li>• Apple iPad</li> </ul>
Android	<ul style="list-style-type: none"> <li>• HTC Desire</li> <li>• Motorola Xoom</li> <li>• HTP Flyer</li> </ul>
Symbian	<ul style="list-style-type: none"> <li>• Nokia N97</li> <li>• Nokia C7-00</li> </ul>
BlackBerry OS	<ul style="list-style-type: none"> <li>• RIM Torch 9800</li> </ul>

Support is only provided if a reported problem with a reference device can be reproduced.

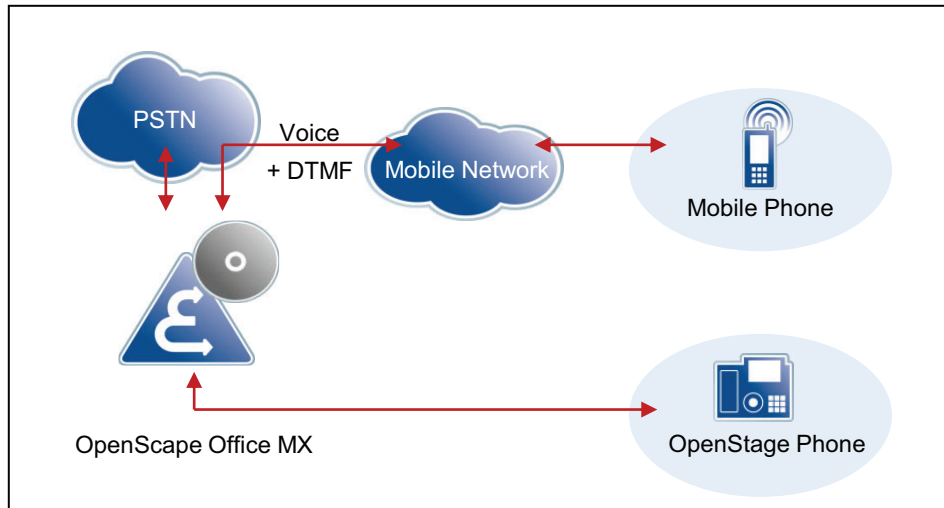
For more information on other devices, browsers and operating systems, refer to the Experts wiki at [http://wiki.siemens-enterprise.com/wiki/myPortal\\_for\\_Mobile](http://wiki.siemens-enterprise.com/wiki/myPortal_for_Mobile).

### 13.2.2 Mobility Entry (MX)

Mobility Entry enables mobile phones to be integrated in OpenScape Office MX. This provides subscribers with access to certain system features via mobile phones.

Mobility Entry enables subscribers to control voice connections using DTMF after dialing into OpenScape Office MX.

**Figure:** Mobility Entry at OpenScape Office MX



### Dialing Methods for Mobility Entry

Mobile phone users can choose between different dialing methods for outbound calls. The following table shows the possible dialing methods for the OpenScape Office communication system:

Dialing mode	LX	MX	HX/HiPath 3000
Callback	no	yes	yes
Call through	no	yes	yes

If a mobile phone subscriber at the communication system calls a special DID number with a callback, the call is automatically terminated before the connection is established, and a callback is executed immediately. After the callback, no further authorization is necessary. The mobile phone subscriber can conduct internal and external calls and also use all Mobility features via the communications system.

The prerequisites for a callback are as follows:

- The external number of the calling telephone must be registered and configured at the communication system. If not, the call is disconnected, and no callback is executed.
- The direct inward dialing number must be configured.
- Together with the call, the CLIP information, i.e., the external call number is transmitted.

### Features in a Dormant State

When accessing system features, the following generally applies:

- Dial the DISA call number
- Wait for the dial tone
- Dial the DTMF code

Function	DISA call number + DTMF code	Explanation
Dial a number	[station number]	Always include the CO access code (trunk code) when dialing an external destination number.
Program/delete call forwarding	*111+ [station number] or #11	When programming, enter the phone number for the call forwarding destination . Always include the CO access code (trunk code) when dialing an external destination number.
Activate/Deactivate Do Not Disturb	*97 or #97	Do Not Disturb is activated/deactivated (e.g., after working hours, when on vacation or for privacy).

Function	DISA call number + DTMF code	Explanation
Send message	*68 + [station number of internal station] + [digits 0 ... 9]	Enter the phone number of the internal station and dial a digit for the message. The info/message text is sent to the internal subscriber.
Reset all services	#0	The following services are reset: deleting call forwarding instructions and active callback requests, deactivating the do-not-disturb and station number suppression features.
Activate/Deactivate Station Number Suppression (CLIR)	*86 or #86	For subsequent calls, the phone number is suppressed or not suppressed.

### Features in Talk State

Function	DTMF code	Explanation
Consultation	[station number of second station]	Dial the number of the second subscriber. Always include the CO access code (trunk code) when dialing an external destination number.
Alternate (Toggle/Connect)	*2	
Conferencing	*3	
Disconnect and return to held call	*0	
Activate callback (delete in dormant state via #0)	*58	Activate the callback ("Callback on Busy" or "Callback on No Answer"). The callback is requested after the ringback or busy tone is played. Acknowledgement is provided by a positive or negative confirmation tone (no display).
Enabling DTMF suffix dialing	*53	The next DTMF code is forwarded "transparently", for example, to control a voicemail box or to dial into a Meet-Me conference.

---

### Related Topics

- [Integrated Mobility Solution](#)

## 13.2.3 Comparison between myPortal for Mobile and Mobility Entry

myPortal for Mobile and Mobility Entry (OpenScape Office MX only) support different features.

Feature	myPortal for Mobile	Mobility Entry (MX)
<b>General functions</b>		
Control of OpenScape Office LX	Control via web browser	(OpenScape Office LX cannot be controlled using DTMF)
Control of OpenScape Office MX/HX	Control via web browser	Mobile phone controls OpenScape Office MX/HX using DTMF (OpenScape Office HX via HiPath 3000)
Mobile phone contract with data option	Yes (flat rate recommended)	no
Countries where released	All countries	All countries The Mobility Client has only been released in DE (German), EN (English) and SV (Swedish)
Licensing	Included in Comfort Plus User license	Included in Comfort Plus User license
Parallel call signaling on system telephone and mobile phone (twinning)	yes	yes
Transfer of caller number to the mobile phone (if the network transmits external phone numbers as CLIP; CLIP no screening)	yes	yes
One Number Service (if the network transmits external numbers as CLIP, CLIP no Screening))	yes	yes
Do not Disturb / Disablable call forwarding	no	yes
Station number suppression, enableable/disablable	no	yes
Automatic identification of registered stations	yes	yes
Support for virtual stations	yes	yes
<b>Presence status, Journal, voicemail box</b>		
Change own presence status	yes	no
View presence status of other subscribers	yes	no
Journal	All, Missed, Answered, Inbound, Outbound	no
Common voicemail box	yes	yes

<b>Feature</b>	<b>myPortal for Mobile</b>	<b>Mobility Entry (MX)</b>
Query voicemail Box	yes	yes
Display received voicemail	Display new, retrieved and saved voicemails	no
<b>Dial</b>		
Access to contacts in mobile phone	no	yes
Contacts in the communication system	Personal contacts, internal and external directory, system directory	no
Favorites	yes	no
Manual dialing	yes	yes
Redialing	yes	no
Dial mode	Call-Through, Callback	Call-Through, Callback (only for OpenScape Office MX, OpenScape Office HX via HiPath 3000)
<b>During the call</b>		
Consultation	yes	yes
Alternate (Toggle/Connect)	yes	yes
Attendant	yes	yes
Conferencing	yes	yes
Callback on free and busy	no	yes
Call pickup from mobile phone to system telephone	yes	yes
Busy indicator also for calls at the mobile phone (with One Number Service)	yes	yes

---

**Related Topics**

- [myPortal for Mobile](#)

## 13.2.4 Dependencies for myPortal for Mobile and Mobility Entry

myPortal for Mobile and Mobility Entry have dependencies on other features (e.g., DISA).

The Mobility Entry client (Mobility client) and myPortal for Mobile are mutually exclusive, i.e., cannot be used simultaneously on the same mobile phone.

Dependency	myPortal for Mobile	Mobility Entry
DISA phone number	For the Mobile Callback dialing mode, the DISA phone number must be configured.	The mobile subscriber may only dial the DISA phone number via the communication system's ISDN lines (not via ITSP and not via analog trunks).
External destination phone number	Dialing external destination phone numbers by the mobile subscriber is controlled by the system because of the LCR configuration. Dialing can therefore be performed via the ISDN fixed network, analog fixed network or via ITSP.	
Activate CLIP No Screening	You cannot display a caller's number on the mobile station unless it was supplied unverified by the network provider.	
Mobile subscriber CLIP	The CLIP of the mobile subscriber must be transmitted to the communication system. This must be made available by the network provider.	
LCR Administration	As some network providers (fixed-network or ITSP) do not accept destination numbers with a separate international prefix, the system must delete this prefix from these destination numbers. This can be performed in least cost routing (LCR).	
B channels / External connections	The number of (network provider) B channels available in the exchange must be set depending on the connection duration or the number of mobile stations. Every incoming external call to a mobile subscriber requires two voice channels in the system. If there are not enough voice channels available, it may not be possible to reach a mobile subscriber, and the mobile subscriber may not be able to initiate any calls with the One Number Service.	
Emergency Numbers	When a mobile user dials an emergency number via the communication system, the location of his or her mobile phone cannot be identified. It is therefore advisable to dial an emergency number directly.	
Dialing internal station numbers	When dialing internal phone numbers in international format (e.g., 00049xxx100) at the mobile station, the PABX number of the system must be unique, and thus DID-capable. Otherwise, internal destinations are routed via the exchange, which can result in costs.	
Directory maintenance	To ensure that the called party can be reached when dialing from directories in all dialing modes, all external phone numbers should be entered in canonical format (e.g., +49 xxx 100).	-

Dependency	myPortal for Mobile	Mobility Entry
Firewall	A data channel is set up to the integrated web server of the communication system. Consequently, port forwarding to port 8801 (for http) and port 8802 (for https) must be configured in the firewall.	-
Data connection	It is advisable to sign a mobile phone contract with a flat-rate data plan. Users of volume rates should disable the "Auto Refresh" option in the settings of myPortal for Mobile.	-
Parallel connections	For some features, a simultaneous voice and data connection is required. This must be supported by both the mobile network providers and the mobile devices.	-
Connection setup from the communication system to mobile stations via	All feature types	ISDN lines (restricting the LCR class of service for mobile stations to the ISDN fixed network.)

---

**Related Topics**

- [myPortal for Mobile](#)

### 13.2.5 One Number Service (LX/MX)

The One Number Service (ONS) effectively makes mobile phones operate as fixed network extensions. This means that subscribers can be reached under one phone number world-wide and can identify themselves only by their respective fixed network numbers.

The mobile phone integration with the One Number Service offers a single phone number for the workplace (system telephone) and the mobile phone. The caller dials the system phone's number (fixed network). Outgoing calls from mobile phones are signaled to the called party with the fixed network number.

Calls can be signaled in parallel (twinning) at the system telephone and mobile phone and also be picked up alternatively at either the system telephone or the mobile phone.



If the call is accepted at the mobile phone, it can be picked up by the system telephone by pressing the DSS key (direct station select with the internal call number of the mobile phone). If the call is accepted at the system telephone, it can be likewise transferred to the mobile phone by pressing the DSS key.

Another advantage of the One Number Service is the system- and network-wide busy indicator for the mobile subscriber.

---

#### **Related Topics**

- [myPortal for Mobile](#)

### **13.2.6 Dual-Mode Telephony (LX/MX)**

Dual-mode mobile phones support both GSM/UMTS networks and WLAN networks. Registration at the communication system as a SIP station is possible over a WLAN.

If the dual-mode mobile phone is in the WLAN range, it is automatically called as a SIP station (SIP features). If it is outside the WLAN range, the dual-mode mobile phone is called via GSM/UMTS (i.e., Mobility Client functionality is available).

Automatic forwarding to the GSM phone number only works if the associated SIP station is entered in the system as a Mobility Entry station (mobile phone integration). This means that if the SIP station is registered, it is called as a SIP station, and if it is not registered, it is called via the GSM phone number assigned in the mobile phone integration configuration.

The following SIP features are supported:

- Making calls
- Placing a call on hold
- Call transfer
- Display of phone number and name
- Mailbox LED (Message Waiting Indication)
- Enabling Call Waiting

Calls on the company premises occur over the WLAN. As long as calls are made over the WLAN, no call charges are incurred on the mobile phone. Handover and roaming are supported within the WLAN range (if the wireless LAN infrastructure is designed for it), but not from WLAN to GSM, and vice versa.

### **13.2.7 Configuring myPortal for Mobile and Mobility Entry (LX/MX)**

myPortal for Mobile and Mobility Entry are configured with the **Mobile Phone Integration** wizard. The operating mode of mobile phones that have already been integrated can be changed in Expert mode.

Using the **Mobile Phone Integration** wizard, the administrator can:

- Set up the One Number Service

- Set up myPortal for Mobile
- Set up Mobility Entry
- Set up dual-mode phones

The mobile phone integration of GSM phones occurs via the virtual stations. The administrator assigns a mobile station to an internal station, thus creating a group consisting of the system telephone and the virtual station. Features are transferred to the mobile station in this way. Every station with a "Comfort Plus User" license can be assigned a maximum of one mobile station.

Mobile phones can be used as dual-mode phones for either myPortal for Mobile or Mobility Entry. myPortal for Desktop/Outlook and myPortal for Mobile cannot be used with GSM only. Please also refer to the released mobile phones in the respective sale information documents.

### **Operating Modes of Mobile Phones**

The following operating modes are implemented for mobile phones:

- **GSM only**  
Calls to the internal mobile call number are only signaled at the GSM mobile phone. If **GSM only** is set, the associated system telephone can no longer be called. **GSM only** can only be configured in Expert mode.
- **Twinning** (Default)  
Calls are signaled in parallel at the system telephone and the GSM mobile phone (twinning). The signaling occurs at the system telephone first and at the mobile phone a few seconds later.
- **Dual Mode**  
If the dual-mode mobile phone is reachable via the WLAN, the call is conducted via the WLAN. If the WLAN is not available, the call is made via GSM.

### **Saving the Login Data in Mobile Phones**

The user name and password of myPortal for Mobile can be stored in the mobile phones as a cookie in order to facilitate future logins. As an administrator, you can enable or disable this feature.

## **13.2.8 Configuring myPortal for Mobile and Mobility Entry (HX/HiPath 3000)**

For mobile phone integration, you will need to configure HiPath 3000 using HiPath 3000 Manager E.

The configuration of the mobile phone integration for HiPath 3000 occurs via the following steps:

- LCR configuration
- MULAP configuration
- Mobility configuration

## 13.2.9 DISA (MX)

DISA (Direct Inward System Access) allows authorized subscribers to use features of the communication system from outside, e.g., at the mobile phone using myPortal for Mobile (for mobile callback) and Mobility Entry.

Using DISA, a subscriber can also set up outgoing connections, both internal and external. Whenever a subscriber uses DISA, he or she must enter the password for the lock code. Certain features are then available as for internal use.

---

**INFO:** A mobile subscriber may only dial the DISA phone number via the communication system's ISDN lines (not via ITSP and not via analog trunks).

---

DISA supports the following features:

Feature	by the subscriber him/ herself	via associated services
Call forwarding on / off	x	x
Do not disturb on / off	x	x
Hunt group on / off	x	x
Advisory message on/off	x	x
Ringing group on / off	x	x
COS changeover on / off	x	x
Reset services	x	x
System Speed Dialing	x	–
Send message text	x	–
Night service on / off	x	–

The administrator specifies under which call number the stations can access DISA. The call number may be different for external and internal use. Internal means at some other "IP-networked" node.

The password to be entered by subscribers consists of the internal call number and the PIN for the lock code. After entering the password, subscribers must either press the # key or wait until the communication system has recognized their input, depending on the security mode that was set for DISA by the administrator.

The subscriber must log in again for further action via DISA.

## 13.3 Mobility in the Office (LX/MX)

Mobility in the office is achieved via Desk Sharing, Cordless Phones and WLAN phones. For Desk Sharing, IP Mobility (Mobile Logon and Flex Call) offers features for mobile users who want to use the phone at a different workplace just like their own phone.

### 13.3.1 IP Mobility / Desk Sharing (LX/MX)

With IP Mobility, multiple subscribers can share a system telephone and thus a workplace (Desk Sharing). IP mobility is supported through the Mobile Logon and Flex Call features.

Some of the typical use cases for IP mobility include:

- **Desk Sharing**  
With Desk Sharing (or Hot Desking), subscribers have no fixed workplace and no fixed office phone. IP Mobility enables multiple mobile subscribers of the communication system to share an office workplace and/or the phone. The subscriber simply logs in at the workplace phone where he or she happens to be currently working.
- **Teleworking**  
A subscriber uses the same login ID and password in the office and at home. When a subscriber logs in from home, his or her system telephone in the office receives a so-called non-mobile number. Consequently, other colleagues can use this system telephone.

The following features can be used for IP Mobility:

- Speaker call (paging)
- Conferencing
- Override
- Alternate (Toggle/Connect)
- Parking
- Consultation
- Transfer
- Call pickup
- Do Not Disturb
- Call forwarding
- Send message (message waiting)
- Callback
- Station number suppression
- Ringing group on

---

#### **Related Topics**

- [Integrated Mobility Solution](#)
- [Mobility at Home \(LX/MX\)](#)

### 13.3.1.1 Mobile Logon (LX/MX)

Mobile Logon enables a system telephone to be temporarily used by other subscribers as if that phone were their own phones. Mobile Logon enables multiple subscribers to share a system telephone as thus a workplace (Desk Sharing).

After the mobile login, the station number of the logged in subscriber is transferred to the used system telephone. The used system telephone can no longer be reached under its original station number. If the subscriber logs in at another system telephone, his or her station number is transferred to that new system telephone. When the user logs out (Logout), the system phone automatically logs back on with its own non-mobile number.

One of the following steps must be performed at the system phone to activate the feature:

- Enter code for "mobile logon" + number of mobile station + optional password/PIN (For details on codes, see [Codes for Activating and Deactivating Features \(LX/MX\)](#).)

When using phones with different numbers of function keys, the transfer of key layouts may be subject to restrictions.

---

**INFO:** When using Mobile Logon, an additional license (Comfort User or Comfort Plus User) is required for each mobile phone number.

---

### 13.3.1.2 Flex Call/Mobile PIN (LX/MX)

Flex Call (Mobile PIN) enables a system telephone to be temporarily used by other subscribers for the next outbound call as if that phone were their own phones.

Flex Call includes this subscriber's phone number, name, toll restriction, and call detail recording.

The phone being used cannot be reached at its own station number if Flex call is enabled. This status is reverted at the end of the call.

To enable Flex Call, an individual code lock must have been assigned for the mobile subscriber.

One of the following steps must be performed at the system phone to activate the feature:

- OpenStage: Service Menu > PIN and Class of Service > Flex Call + Mobile phone number + Lock code of mobile subscriber
- Code for Flex Call + Mobile phone number + Lock code of mobile subscriber (For codes, see [Codes for Activating and Deactivating Features \(LX/MX\)](#))

### 13.3.2 HiPath Cordless IP (LX/MX)

With HiPath Cordless IP, DECT is also available in voice-over-IP infrastructures. The connection to the communication systems occurs via SIP. This enables DECT radio cells to complement SIP-enabled voice-over-IP systems perfectly as a basis for mobile communication solutions.

More information on HiPath Cordless IP can be found in the relevant documentation.

### 13.3.3 WLAN Phones and Access Points (LX/MX)

WLAN phones and dual-mode telephones enable mobile communications. These phones can be integrated in already existing WLAN infrastructures. With WLAN Access Points, you can build wireless networks and use the same infrastructure for voice and data services. It is only recommended that only high-performance WLAN Access Points (e.g., from Enterasys) be used.

### 13.3.4 WLAN Requirements (LX/MX)

When using a WLAN, it is important to ensure that the basic requirements for Voice-over-WLAN are satisfied. To implement the wireless portion of the network, a site survey may need to be conducted.

Decision-making aids:

- Smaller installations with up to three APs can be effectively assessed during a site visit or by studying the floor plans. It is not generally necessary to perform a site survey in this scenario.
- Site surveys should always be performed for installations with more than four APs. This applies specially to installations extending across multiple buildings or floors within buildings.
- A site survey is required irrespective of the number of APs in scenarios involving an RF-intensive environment or if you want the solution to operate alongside preexisting WLAN systems.

---

**INFO:** For more information on the LAN telephony requirements, see [LAN Telephony Requirements \(LX/MX\)](#).

---

## 13.4 Mobility at Home (LX/MX)

Mobility at home is achieved through unified communications features such as CallMe and Teleworking. Teleworking is supported by IP Mobility (Mobile Logon) and the connection of teleworkers via a VPN. In addition, mobility at home is supported by the same features as for mobility on the move (mobile phone integration and One Number Service).

For a description of the unified communications features, see [Unified Communications](#).

For a description of IP Mobility, see [IP Mobility / Desk Sharing \(LX/MX\)](#).

For a description of the connection of teleworkers via a VPN, see [Connecting Teleworkers via a VPN](#).

---

### Related Topics

- [CallMe Service](#)
- [IP Mobility / Desk Sharing \(LX/MX\)](#)
- [Connecting Teleworkers via a VPN](#)
- [Mobility on the Road](#)

## 14 Security

The term security includes not only the security in a data network with secure access by users (via a VPN and secure administration using SSL) and with restricted system access (through firewalls, IP and MAC address filtering and a DMZ), but also the security against unauthorized access at telephones (e.g., telephone locks).

### Security Checklist

The aspect of secure communications has been taken into account in the default settings of OpenScape Office MX. During the initial setup, the functions and settings may need to be adapted to the specific situation of the customer, and additional provisions may have to be made in the customer environment. In order to raise the awareness of security risks and to implement suitable measures to counteract them, a security checklist is provided in the product documentation. It is urgently recommended that this checklist be discussed with the customer during the initial setup and that all implemented measures be carefully documented.

### 14.1 VPN (Virtual Private Network) (MX)

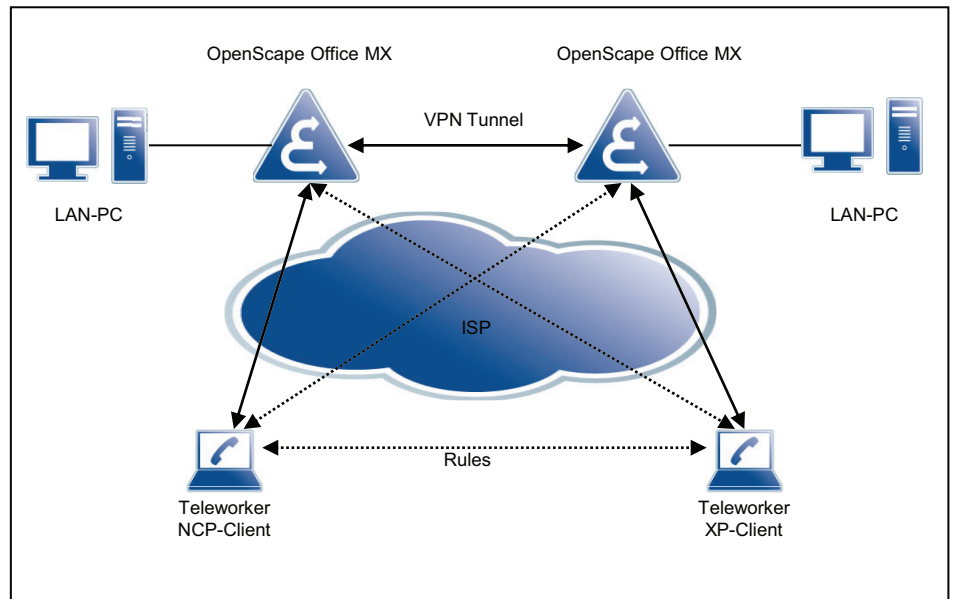
A virtual private network (VPN) is a PC network used to transport private data in a public network (such as the Internet). It therefore transfers data securely over an insecure network. Data is transmitted in encrypted format.

VPN offers you:

- Secure connection via an unprotected medium (Internet)
- Protection of confidential data against manipulation
- Secure business processes
- Reliable integration of external partners in the corporate network
- Access to corporate information for field service



## Overview of a VPN



To ensure secure communications, VPN works as follows: A tunnel is created between the communication peers as if one of the stations had called the other station. In this instance, tunnel configuration is subject to authentication and authorization. The actual data is transferred following tunnel configuration.

A VPN can be set up between (at least) two computers or networks (tunnel endpoints).

Two types of networking exist:

- Site-to-Site VPN  
This type of networking performs encryption between two VPN gateways; data is transferred unencrypted within the LANs.
- End-to-Site VPN  
Remote access VPN (remote access by mobile teleworkers)

### System-Specific Information

The VPN parameters are principally administered via the VPN wizard.

Note that the connection to the communication system must be a secure SSL connection using OpenSwan or OpenSSL.

**Dependencies**

Topic	Dependency
DynDNS	If you change an IP address in the VPN, OpenScape Office MX updates the host-name-specific data (IP address) in the DynDNS.
DNS	Every VPN partner can resolve the host name/IP address via the standard DNS protocol. All DNS names (such as host name) must be fully qualified domain names (FQDN). Connections via IPSec tunnels are not possible while the IP address is being updated via DNS.

**14.1.1 LAN Requirements for a VPN (MX)**

To ensure the quality of the voice and data transmissions, the networks being used and the communication system must satisfy certain requirements for the LAN. Due to encryption, in particular, more bandwidth than for other networks must be planned.

In the following examples and in the tables, the encryption mode "ESP Tunnel Mode with Authentication" is used as a basis. This mode offers the highest security for site-to-site VPNs.

**Structure of an encrypted voice packet:**

Protocol	Bytes	
ESP Trailer	12	
ESP Padding	varies (y)	encrypted
ESP Padding Header	2	encrypted
Voice Payload	varies (x)	encrypted
RTP	12	encrypted
UDP	8	encrypted
IP (original)	20	encrypted
ESP header	8 + iv	
IP (tunnel)	20	
802.1Q VLAN Tagging	4	
MAC (incl. Preamble, FCS)	26	
<b>Total</b>	<b>112 + iv + x + y</b>	

**Length of the ESP Header**

The length of the ESP header depends on the encryption algorithm used.

Required for Cipher Block Chaining. The ESP header contains an initialization vector (IV). The length of the IV is identical to the length of the cipher block.

**Padding**

Padding is required, since the encryption algorithm is based on cipher block chaining. This means that the entire encrypted portion of the packet (original IP/UDP/ RTP header + voice payload+ESP header padding) must correspond to an integral multiple of the cipher block length.

Block length of the encryption algorithm:

Encryption Algorithm	Block length	Length of the initialization vector
AES	16 bytes (128 bit)	16 bytes (128 bit)
DES	8 bytes (64 bit)	8 bytes (64 bit)
3DES	8 bytes (64 bit)	8 bytes (64 bit)

Calculation of the required padding bytes for voice packets:

$$(42 + x + y) \text{ (bytes)} = N \times (0 \text{ or } 16 \text{ (bytes)}) \text{ (N integer)}$$

**Bandwidth calculation for the AES encryption algorithm:**

Codec	Packet parameters	Sample size (ms)	Payload (bytes)	Padding (Bytes)	Ethernet packet length (bytes)	Payload / Packet overhead ration	Ethernet load (incl.) header (kbps)
G.711	20	20	160	6	294	75%	117.6
G.711	30	30	240	6	372	50%	99.2
G.711	40	40	320	6	454	38%	90.8
G.711	60	60	480	6	614	25%	81.9
G.729A	1	20	20	2	150	600%	60.0
G.729A	2	40	40	6	182	300%	36.4
G.729A	3	60	60	2	198	200%	26.4

**Bandwidth calculation for the DES/3DES encryption algorithm:**

Codec	Packet parameters	Sample size (ms)	Payload (bytes)	Padding (Bytes)	Ethernet packet length (bytes)	Payload / Packet overhead ration	Ethernet load (incl.) header (kbps)
G.711	20	20	160	6	286	75%	114.4
G.711	30	30	240	6	366	50%	97.6
G.711	40	40	320	6	446	38%	89.2
G.711	60	60	480	6	606	25%	80.8

## Security

VPN (Virtual Private Network) (MX)

Codec	Packet parameters	Sample size (ms)	Payload (bytes)	Padding (Bytes)	Ethernet packet length (bytes)	Payload / Packet overhead ration	Ethernet load (incl.) header (kbps)
G.729A	1	20	20	2	142	600%	56.8
G.729A	2	40	40	14	166	300%	33.2
G.729A	3	60	60	10	182	200%	24.3

### Bandwidth calculation for transporting the Fax payload with T.38

The bandwidth calculation for the encrypted transport of the fax payload follows the same scheme as the encrypted transport of the voice payload. The only difference is that the Fax payload is directly encapsulated in a UDP frame and not in an RTP frame, so the RTP header must be removed from the above formulae for the voice payload.

Encrypted packet length:

$$(100 + iv + x + y) \text{ (bytes)}$$

Calculation of the required number of padding bytes for Fax payload packets:

$$(30 + x + y) \text{ (bytes)} = N \times (8 \text{ or } 16 \text{ (bytes)}) \text{ (N integer)}$$

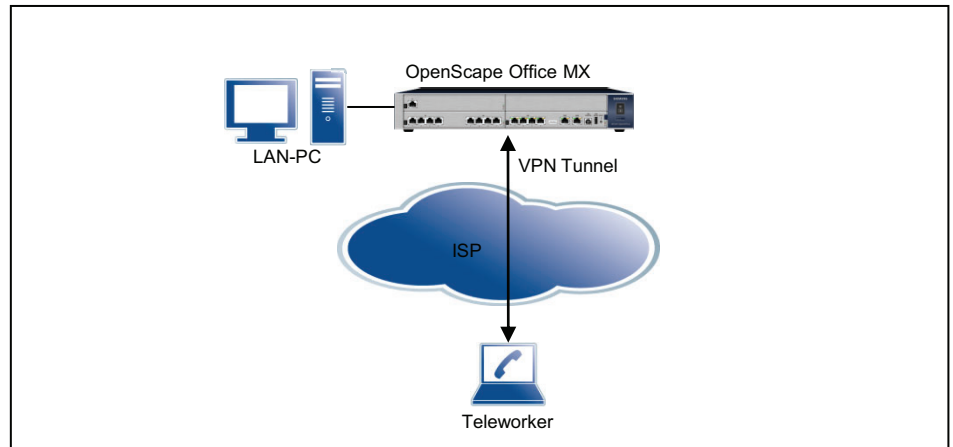
### Bandwidth for T.38 Fax (Redundancy 2)

Encryption Algorithm	Sample size (ms)	Payload y (bytes)	Padding x (bytes)	Ethernet packet length (bytes)	Payload packet (overhead in percent)	Ethernet load (incl.) header (kbps)
DES / 3DES	30	169	1	278	64%	74.1
AES	30	169	9	294	74%	78.3

## 14.1.2 Connecting Teleworkers via a VPN

Teleworkers can be connected to the OpenScape Office MX via a secure VPN connection.

### Stand-alone System with Integration of Teleworkers via a VPN



OpenScape Office MX provides integrated VPN functionality (configured using OpenScape Office Assistant). A maximum of 10 teleworker workplaces can be connected via a VPN per OpenScape Office MX. The following VPN clients have been released for OpenScape Office MX: Microsoft Windows XP client, NCP client, Shrew Soft client.

The following import and export options are available to transfer teleworkers from one communication system to another:

- Exporting Teleworker Data from the System
  - You can combine all teleworker data (that is saved on your system) for transfer to another system. Teleworker data refers here to all data for configuring the IPSec client on the teleworker PC.
  - The teleworker data is made available in the form of text files: for Windows XP clients, in the form of .bat files, for the NCP client as .ini files and for the ShrewSoft client as .vpn files.

---

**INFO:** Diacritical characters such as umlauts or accents are not handled in this file. Blanks are replaced by underscores.

---

#### Status Indicator of the VPN Wizard

In all overviews of the VPN wizard, a status indicator appears in the last column of the list. If the VPN is not active, a red bar is displayed; if it is active, a green check mark appears.

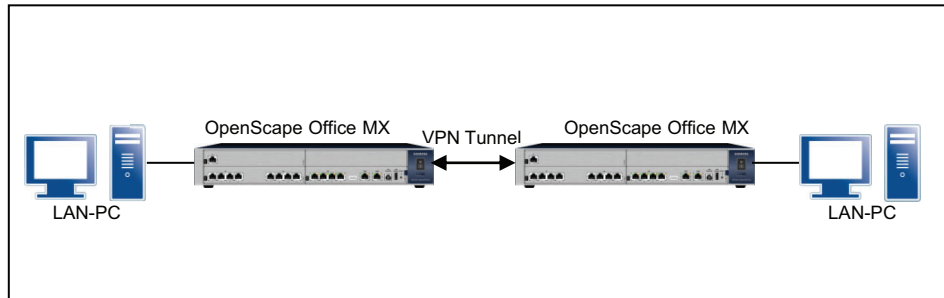
#### VPN with OpenScape Office LX

With OpenScape Office LX, the VPN is terminated via an external router. The description of external applications is not part of this documentation.

### 14.1.3 Networking Communication Systems via a VPN (MX)

Multiple OpenScape Office MX systems can be securely networked with one another via a VPN.

#### Networking via VPN



You can optionally configure the networking of multiple systems on one communication system and then export that configuration and import it on all other systems.

The distinction between the own system and the local systems occurs through the detection of the own DynDNS name or (when using fixed IP addresses) through the own Internet address.

- Export Topology Data from System
  - You can combine all the data about the setup of your system and prepare it for export to another system.
- Importing Topology Data into a System
  - You can import all the data about the setup of some other system as a file and use it for your own system.

The key (password) for these import and export options is freely selectable and should be provided to any other administrator who may want to import these settings.

#### Status Indicator of the VPN Wizard

In all overviews of the VPN wizard, a status indicator appears in the last column of the list. If the VPN is not active, a red bar is displayed; if it is active, a green check mark appears.

### 14.1.4 VPN - Security Mechanisms (MX)

In VPN, the encryption of data occurs via different security mechanisms such as IPSec tunneling, Security Associations and authentication methods (peer-to-peer, digital signatures).

## **IPSec Tunnels**

IPSec is used to encrypt data and can generally be implemented with and without tunnels. IPSec is an option for implementing VPN. You can encrypt the entire IP packet here with the IP header: this occurs in tunnel mode.

Tunnels must always be configured for both VPN peers.

IPSec supports the automatic key management system, Internet Key Exchange (IKE). This is a standard that is integrated in IPSec.

## **Security Associations SA**

A security association (SA) is an agreement between two communicating units in computer networks. It describes how the two parties will use security services to communicate securely with each other.

VPN connections always require three security associations (SA), negotiated in two phases:

- Phase 1 - Generating the IKE SA  
One for the initial mutual authentication and for exchanging the session keys (IKE-SA)
- Phase 2 - Negotiating the payload SAs  
One for each direction in the connection for payload traffic once established (payload SAs)

## **IKE SA**

The IKE protocol has essentially two different tasks. Start by creating a protocol used exclusively by the IKE protocol (IKE-SA). The existing IKE-SA is then used for secure negotiation of all further SAs (payload SA) for the transmission of payload data. IKE therefore operates in the two consecutive phases:

When setting up a call between VPN partners, various parameters must be negotiated (such as how often a key is regenerated or which encryption procedures are used). These parameters are stored and administered in IKE SAs.

## **Payload SA**

IKE phase 2 is used to negotiate all security parameters for the payload SAs between the VPN partners.

You always have to configure two SAs for transmission and receipt.

The following steps are essentially performed:

- Negotiating the algorithms for encryption and authentication
- Negotiating the security protocols used (ESP and AH)
- Negotiating the security protocol operating mode
- Negotiating the SA lifetime
- Defining the key material

**Authentication**

Peer-to-peer communication in VPN. The following two types of authentication are possible for VPN peers:

- Pre-shared keys  
Pre-shared keys are also mostly used for VPN. A key pair is configured for both VPN partners for this. These keys form a "hash value" which is verified by the relevant partners for authentication purposes.
- Digital signatures  
Every VPN partner is assigned a certificate. For successful authentication, the VPN peers at both tunnel endpoints must check the digital signature of their peer against a trusted CA.

**System-Specific Information**

The VPN parameters are generally administered for OpenScape Office MX via the wizard.

Note that the administrator connection to OpenScape Office MX must run via a secure connection with SSL.

- Security Associations SA  
OpenScape Office MX supports Oakley groups 1, 2, and 5
- IPsec  
OpenScape Office MX uses the IPsec tunnel mode with ESP (Encapsulating Security Payload). ESP is an IPsec protocol that guarantees packet encryption, packet integrity as well as packet authenticity
- Payload SA  
OpenScape Office MX supports the encryption algorithms DES, 3DES, and AES  
Of all the known groups of MAC algorithms (MAC=Message Authentication Code) for authenticating data origin and data integrity, OpenScape Office MX supports HMAC-SHA1 and HMAC-MD5.
- Recommended operating modes
  - IKE in "Main Mode" with Perfect Forward Secrecy
  - Hash function with SHA-1
  - Authentication with certificates (DSA and RSA)
  - Encryption with AES (up to 256 bits)
  - Support for dynamic public IP addresses via virtual IP addresses or DynDNS updating mechanisms for teleworker PCs



## Dependencies

Topic	Dependency
DynDNS	If you change an IP address in the VPN, OpenScape Office MX updates the host-name-specific data (IP address) in the DynDNS.
DNS	Every VPN partner can resolve the host name/IP address via the standard DNS protocol. All DNS names (such as host name) must be fully qualified domain names (FQDN). Connections via IPSec tunnels are not possible while the IP address is being updated via DNS.

### 14.1.5 VPN - Certificates (MX)

A certificate binds a specific public key to a specific VPN client. In this case, the client can be both a client of OpenScape Office MX and a teleworker. This unique combination of public key and VPN client provides the basis for authentication.

#### Certificates and certificate authority

Certificates are digitally signed and generated by a certificate authority (CA). IPSec accepts a certificate if it is issued by a trusted certificate authority.

In a simple VPN environment, the definition of an individual certificate authority may be sufficient; this CA operates as a trusted master certificate authority for the entire VPN and uses its self-signed CA certification for identification at all VPN clients.

Every VPN client needs one of the certificates issued by this CA.

Certificates based on the X.509 standard (the most widely used standard today) include the following main elements:

- information about the identity of the certificate owner
- the public key of the certificate owner,
- information about the CA that signed the certificate (a serial number, the validity period, information about the identity of the CA, and the digital signature of the CA)

#### Lightweight CA

A Lightweight CA function helps with certification in environments where the customer is not already using a PKI. A Lightweight CA offers the following options:

- creating public/private key pairs
- signing and generating corresponding certificates
- saving key pairs with associated certificates in files

In cryptographic terms, a PKI (public key infrastructure) is a system for generating, distributing, and verifying digital certificates.

**Certificate revocation lists (CRL)**

A critical situation occurs when a certificate has become known (or if this is suspected), and this certificate is hence no longer trustworthy for the peer authentication. In this case, the certificate authority must revoke the certificate and the revocation must be signaled to all peers as soon as possible. A remote peer's attempt to authenticate its identity using a revoked certificate is denied.

Basically, a CRL is a list of all revoked certificates. CRLs always have to be generated by the CA where the certificates originate.

A CRL contains the following main elements:

- a list of all revoked certificates; the certificates are identified by serial numbers
- the publication date for the next CRL updated (specifies the time to live for the CRL)
- information about the CA that generated the certificate (information on the identity of the CA and the digital signature of the CA)

The administrator must manually update and distribute the CRLs at regular intervals.

**System-Specific Information**

Authentication is performed on the basis of cryptographic algorithms with public keys. OpenScape Office MX supports RSA as the algorithm for cryptography with public keys. OpenScape Office only supports certificates that correspond to the X.509 standard.

OpenScape Office MX always operates as a VPN client for authentication.

- **Lightweight CA**  
OpenScape Office MX offers restricted CA functionality (Lightweight CA). The administrator provides the key material for OpenScape Office MX by manually importing private/public key pairs and certificates via the SSL-secured administration connection for all communication partners involved
- **CRL**  
In OpenScape Office, CRLs (certificate revocation lists) are used to revoke certificates. The CRL is imported into OpenScape Office by the administrator via an SSL-protected connection.

**14.1.6 VPN - Clients (MX)**

In order to connect teleworkers securely to a company network, the connection is implemented using a VPN. This is done by configuring the teleworker PCs as NCP clients or via the Microsoft Windows XP client software.

**NCP Client**

NCP clients can be used in any VPN environments with IPsec. This is significant if access is required from a remote PC to VPN gateways of different manufacturers or if a central VPN gateway from a third-party vendor is already

installed in the company network. In the case of a branch office network, the NCP Secure Enterprise Gateway can be used with other VPN gateways on the basis of IPSec connections.

The NCP client is not free, but in contrast to the Microsoft client software, it offers the benefits of a graphical user interface and a status indicator for the connection.

#### **Microsoft Windows XP Client**

The built-in client software of Microsoft Windows XP can also be used to securely connect individual teleworker PCs via the Internet. The client software is included in Windows XP, so no additional costs for software are involved.

All data transmitted between the firewall, the VPN server and the clients is encrypted.

#### **Shrew Soft VPN Client**

The Shrew Soft VPN Client is an open source and free VPN client with a graphical user interface that supports version 2.1.5 and hybrid authentication.

The Shrew Soft VPN client includes, among other things, ISAKMP, Xauth and RSA support, AES, Blowfish and 3DES encryption protocols, and numerous other features that are usually found only in professional solutions.

#### **System-Specific Information**

- LAN infrastructure with multiple subnets  
If VPN is to be used for a LAN infrastructure with multiple subnets, it is necessary to create rules for these subnets. These rules cannot be created via wizards, but must be configured in Expert mode.
- Tunnel in Tunnel  
With OpenScape Office MX, it is not possible create a second VPN tunnel through an already existing VPN tunnel.

### **14.1.6.1 NCP Client Settings (MX)**

To configure an NCP client for a VPN connection to OpenScape Office MX, you will need to make the following settings as an administrator:

#### **Basic Settings**

- Profile name  
freely selectable; use of meaningful names recommended
- Connection type  
VPN to IPSec peer
- Connection medium  
In accordance with the Internet connection used  
e.g., LAN (over IP) or xDSL (PPPoE)

## Security

### VPN (Virtual Private Network) (MX)

#### Dialing into network

No configuration required.

#### HTTP Login

No configuration required.

#### Modem

No configuration required.

#### Line Management

- Call setup  
automatic or manual  
Timeout = 0

---

**INFO:** This ensures the connection is not cleared due to idle time!

---

- Prioritizing Voice over IP (VoIP)  
Set check mark
- EAP Authentication  
No configuration required
- HTTP authentication  
No configuration required

#### IPSec Settings

- Gateway = IP address or DNS name of OpenScape Office MX  
OpenScape Office MX can be reached via the Internet under this IP address or DNS name  
Designation in the VPN wizard: **IP Address/DynDNS Name**
- IKE Policy = Unattended Mode
- IPSec Policy = Unattended Mode
- Exchange Mode = Main Mode
- PFS Group = DH Group 2 (1024 bits)
- Validity / Duration
  - IKE Policy: 000:00:07:00 (7 minutes)
  - IPSec Policy: 000:00:08:00 (8 minutes)
- Editor  
No configuration required

#### Advanced IPSec Options

No configuration required

### Identity

- Type = IP address  
ID = IP address of the teleworker PC (see also: Assigning IP addresses)  
Use Pre-shared key  
Set check mark  
Shared Secret = This is the password for the VPN connection  
Designation in the VPN wizard: **PreShared Secret**
- Extended Authentication (XAUTH)  
not used, no configuration required

### IP address assignment

- Assign IP address manually  
IP address = IP address of the teleworker PC  
Designation in the VPN wizard: **IP Address/DynDNS Name**
- DNS / WINS  
Set check mark
- DNS server = IP address of the OpenScape Office MX  
Designation in the VPN wizard: **Local IP Subnet Address (LAN)**

### VPN - IP Networks

No configuration required.

### Certificate check

No configuration required

### Link Firewall

- Activate Stateful Inspection:  
for existing connection
- Allow only communication in the tunnel:  
Set check mark

## 14.1.6.2 Microsoft Windows XP Client Settings (MX)

In order to configure the Microsoft Windows XP client software for a VPN connection to OpenScape Office MX, you will need to make some special settings as an administrator.

### Prerequisites

- Microsoft Windows XP with SP2
- PC account with administrator rights
- Install the Windows XP, Service Pack 2 support tools  
You will need *Ipseccmd.exe* to manage and monitor IPSec policies on a Windows XP computer.  
It is important that you select a complete installation!

## Security

### VPN (Virtual Private Network) (MX)

- Connection into the Internet via
  - DSL modem or
  - DSL router

#### VPN Connection Data

- VPN data
  - IP address / DNS name of OpenScape Office MX
  - PreShared Secret of the VPN connection
  - locale IP subnet address (LAN)
- IP address / DNS name of the Microsoft Windows PC

#### Configuring the VPN Connection

It is recommended that you create two batch files to simplify enabling and disabling the VPN connection.

- config\_start.bat

```
ipseccmd -w REG -p "PolicyName" -y
ipseccmd -w REG -p "PolicyName" -r "RuleOut" -t TunnelAddrRemote -f
0=*-n
ESP(MD5,3DES)420PFS2 -a PRESHARE:"presared key" -1p -1k 480S
ipseccmd -w REG -p "PolicyName" -r "Rulein" -t TunnelAddrLocal -f * =0 -n
ESP(MD5,3DES)420SPFS2 -a PRESHARE:"presared key" -1p -k 480S
ipseccmd -w REG -p "PolicyName" -x
```
- stop\_vpn.bat

```
ipseccmd -w REG -p "PolicyName" -y
```

#### Parameters

- **-p PolicyName**  
Unique name of the policy  
The name of the teleworker, as stored in the VPN wizard, could be used here, for example.
- **-t TunnelAddrRemote**  
Tunnel endpoint: IP address or DNS name of OpenScape Office MX  
OpenScape Office MX can be reached via the Internet under this IP address or DNS name.  
Designation in the VPN wizard: **IP Address/DynDNS Name**
- **-t TunnelAddrLocal**  
Tunnel endpoint: IP address or DNS name of the teleworker PC  
The teleworker PC can be reached via the Internet under this IP address or DNS name.  
Designation in the VPN wizard: **IP Address/DynDNS Name**

---

**INFO:** If the teleworker PC connects to the Internet via a DSL modem and has a dynamic IP address assignment from the ISP, then TunnelAddrLocal must be a DNS name. To do this, the

appropriate software for updating the IP address must be installed, and a DynDNS service (e.g., via dyndns.org) must be set up.

If the teleworker connects to the Internet via a DSL router, then TunnelAddrLocal is an IP address. The IP address depends on the configuration of the DSL router.

---

- **-a PRESHARE: preshared key**  
This is the password for the VPN connection  
Designation in the VPN wizard: **PreShared Secret**

### Configuring Internet Access

If the teleworker is to be provided with Internet access during the VPN connection, then an additional DNS server must be entered manually on the teleworker PC or DSL router.

The IP address of OpenScape Office MX (Designation in the VPN wizard: **Local IP Subnet Address (LAN)**) must be entered as the additional DNS server.

- DSL modem  
The automatic assignment of the DNS server address must be replaced by a manual assignment (Properties the TCP/IP Internet Protocol).
  - DNS server address: DNS server of the ISP (Provider)
  - DNS server address: IP address of OpenScape Office MX  
Designation in the VPN wizard: **Local IP Subnet Address (LAN)**
- DSL router  
Configuring the Second DNS Server Address in the Router

---

**INFO:** If this is not possible, then the automatic assignment of the DNS server address must be replaced by a manual assignment (Properties the TCP/IP Internet Protocol).

---

- DNS server address: IP address of the router
- DNS server address: IP address of OpenScape Office MX  
Designation in the VPN wizard: **Local IP Subnet Address (LAN)**

### Setting up the VPN Connection

- Set up connection to the Internet
- Call config\_start.bat
- Start applications

### Clearing the VPN connection

- Call stop\_vpn.bat

### Notes

- If a parameter contains blanks, the parameter must be enclosed within single quotes.

## Security

### VPN (Virtual Private Network) (MX)

- The parameter and parameter data must be delimited by a blank. (e.g., -p Teleworker)
- Every **ipseccmd** must be in a separate line. The line breaks in the examples are due to printing restrictions.
- **ipseccmd /?** can be used to view the complete help for the command

#### 14.1.7 VPN Services (MX)

You can manage services via the Configured Services function. Configured services become active services only on activation.

#### 14.1.8 VPN - Tunnel (MX)

Tunnel is the term used to describe the transportation of encrypted data packets to a defined endpoint. Active tunnels become configured tunnels when the configuration is enabled. A maximum of 256 tunnels can be set up per gateway.

#### 14.1.9 VPN - Rules (MX)

Rules define how IP packets are to be handled. The rule action *Pass* means that the IP packet is to be transported further (passed through). The rule action *Deny* means that the IP packet will not be transported further (i.e., will be ignored). You can also select whether or not the IP packet will use an encrypted VPN tunnel.

The communication system can manage 640 rules, of which 6 rules are preset (default rules) and 634 are free for allocation.

#### 14.1.10 PKI Servers (MX)

The PKI server designates a server that can issue, distribute and verify digital certificates. The certificates issued within a PKI (Public Key Infrastructure) are used to protect communications.

#### 14.1.11 Upgrading a VPN Configuration from V3.2 to V3.3 (MX)

A complete migration of the VPN configuration of OpenScape Office V3.2 to OpenScape Office V3.3 is not possible due to the structure of OpenSSL and OpenSwan.



### **Differences Between V3.3 and V3.2 with Respect to VPN Clients:**

- Certificates that were created with Safenet LWCA cannot be used with OpenSSL.  
This is due to the fact that various fields that were not evaluated by Safenet such as the "Subject Alternative Name", for example, are mandatory fields for OpenSSL.
- The length of the pre-shared keys in OpenSSL must be 20 characters (or more).
- Different scheme for VPN rules
- Different configuration parameters for teleworkers  
For OpenSSL, the Gateway LAN network address must be configured in the Teleworker client software.

## **14.2 Firewall (LX/MX)**

A firewall is a system of software and hardware components that restricts access to different networks in order to implement a security concept.

Firewalls are installed at the interfaces between individual networks and control the data flow between the sub-segments to prevent unwanted data traffic and only allow the desired traffic. Firewall are most frequently used to control traffic between a local network (LAN) and the Internet.

Accordingly, the firewall has two essential tasks:

- Suppressing unwanted data traffic from external PC systems to the protected area
- Suppressing unwanted data traffic from the protected area to external systems

In comparison to a straightforward IP address filter, the protection offered by a firewall is achieved through finer-grained access control, for example, by filtering protocols, port numbers, and names.

### **System-Specific Information**

OpenScape Office protects your internetwork through integrated security functions. Different functionality is offered by OpenScape Office LX and OpenScape Office MX for this purpose.

OpenScape Office LX provides the following features:

- Port firewall

OpenScape Office MX provides the following features:

- Port firewall
- NAT (Network Address Translation) on the WAN port
- Expression filter (web filter)
- Intrusion Detection System (IDS)

- MAC and IP address filtering

## 14.2.1 Ports and Services (LX/MX)

Ports and/or services are mandatory for communication via the protocols TCP and UDP because they allow multiple applications to exchange data simultaneously over a single connection. Ports are also used to assign data segments to the correct services.

The term firewall is generally understood as a port firewall (i.e., the blocking of individual services, or ports). The port firewall refers only to the WAN port of OpenScape Office MX, if the communication system provides Internet access. With OpenScape Office LX, a port firewall can be enabled on any (or every) LAN connection. OpenScape Office MX has additional access restrictions such as the MAC and IP address filter, for example.

A port firewall can have two operating states:

- The firewall is turned off, i.e., all ports/services on OpenScape Office LX and OpenScape Office MX are accessible.
- The firewall is turned on, i.e., all connections to all ports/services are stopped.

With OpenScape Office MX, the firewall on the WAN port is enabled in order to protect the internal network (LAN ports) against attacks from the Internet. If certain ports/services need to be accessible from the Internet anyhow (e.g., for a web server), they must be explicitly released (see Opening Ports). All ports/services for the functionality of OpenScape Office MX are automatically released on the LAN port (into the internal network).

OpenScape Office LX has only one LAN port (into the internal customer network) and is protected from the Internet by other components/routers in the customer network. In addition, the internal Linux firewall is enabled. To provide the required functionality, all ports/services must be enabled (to allow the phones to communicate with OpenScape Office LX, for example). This is done automatically, but the administrator can disable individual services

### Port Numbers

Port numbers can accept values between 0 and 65535 which is how they are assigned to the different applications. The ports between 0 and 1023 are referred to as 'well-known ports' and are permanently assigned by the IANA (Internet Assigned Numbers Authority). A list of these ports can be found under <http://www.iana.org/assignments/port-numbers>.

'Registered ports' lie between ports 1024 and 49151. Application vendors can have ports registered as required for their proprietary protocols. The advantage of this kind of registration is that an application can be identified on the basis of the port number as soon as it is entered in the IANA.

The remaining ports from 49152 through 65535 are known as 'dynamic' or 'private ports'. These can be set variably because they are not registered and therefore do not belong to an application.

Disabling specific ports in the communication system's firewall reduces the number of network attack points and blocks unwanted services (such as FTP at ports 20 and 21). You can also do the opposite and block all ports apart from those that are actually needed. This procedure significantly improves network security.

### 14.2.1.1 Port Administration and Port Forwarding (MX)

Port administration can be used to change some of the ports used by the communication system itself. This makes it easier to control the communication between OpenScape Office MX and the firewall of the customer in a network, for example.

If changes are to be made at the port administration, these changes must generally be made in all components (phones, systems, etc.) simultaneously in order to retain functionality.

### 14.2.1.2 Opening Ports (MX)

In contrast to port administration, opening ports has a different significance: if the system sets up the Internet access (e.g., via the WAN port), then, by default, the only communication allowed is from within the internal network (i.e., from the corporate network or the communication system itself) to the Internet and the associated response packets. Requests initiated from the Internet are blocked. This security setting can be bypassed by opening the port selectively to operate a Web server on the network, for example.

---

**NOTICE:** If OpenScape Office is used as an Internet router, port 5060 must be closed (default setting). For Internet telephony via an ITSP, OpenScape Office opens the relevant ports and keeps them open.

Port 5060 must likewise be closed if an external router or firewall is being used. OpenScape Office is responsible for opening this port (if required).

---

### 14.2.2 URL Blocker (MX)

A URL blocker can be used to restrict the access to the Internet. The URL filter list contains the web sites which are to be blocked by the OpenScape Office MX.

You can load a preset URL filter list from the communication system and edit it with a text editor of your choice. You can then copy the edited URL filter list back to the communication system.

The URL blocker can operate in two different modes, the transparent and proxy mode and the proxy mode.

### **Transparent and Proxy Mode**

Transparent and proxy mode means that no settings must be made in the web browsers on the client PCs. All http packets (to TCP port: 80) are filtered by the URL blocker. Disadvantage: If a web server that should be blocked is running on some other TCP port than 80, it will bypass the URL blocker.

### **Proxy Mode**

Proxy mode means that OpenScape Office MX must be entered as the proxy server under the proxy settings of the web browser on the client PC. To do this, the IP address of OpenScape Office MX must be entered and, in addition, 3128 must be specified as the destination port.

If the customer network has its own proxy server, the proxy server of OpenScape Office MX should be disabled.

### **Log File**

As an administrator, you can have a log file created by the communication system. This log file contains all pages that were called by users and blocked by URL filters.

## **14.2.3 Expression Filter (Web Filter) (MX)**

An expression filter (web filter) is used to restrict access to the Internet by systematically searching through web contents. If an Internet page contains an expression (word or combination of words) that is registered in a predefined expression list, this page will be blocked by the system.

The expression list is interpreted by the URL Blocker as a list of regular expressions. In other words, it is possible to define not only individual keywords, but also combinations of words.

You can load a preset expression filter list from the communication system and edit it with any text editor of your choice. You can then copy the edited expression filter list back to the communication system.

## **14.2.4 Intrusion Detection System (IDS) (MX)**

An Intrusion Detection System (IDS) is a service (hardware and/or software) for detecting attacks on a PC system or a PC network. The IDS primarily serves systems that are connected to the Internet. When deployed correctly, the IDS and firewall complement one another and thus increase the security of networks.

There are basically two procedures for intrusion detection: comparison against known attack signatures and what is known as statistical analysis. Most IDSs operate with filters and signatures that describe specific attack patterns. The disadvantage of this procedure is that only known attacks are recognized.

The entire process is split into three steps. Intrusions are detected by sensors that collect log data (HIDS) or network traffic data (NIDS). In the course of sample recognition, the IDS verifies and processes the collected data and compares it with examples from the sample database. An "intrusion alert" is triggered if an event matches one of the patterns. This alert can take various different forms. It may be just an e-mail or text message that is delivered to the administrator or, depending on the functional scope, it may block or isolate the would-be intruder.

---

**NOTICE:** OpenScope Office MX is shipped with IDS disabled. IDS should only be activated if there are grounds for suspicion, since the complex processes involved take a toll on performance.

---

### **System-Specific Information**

OpenScope Office MX uses the IDS of BASE (Base Analysis and Security Engine). The related online helps can be found in Expert mode under Telephony Server / Intrusion Detection.

The IDs can be turned on or off by an administrator using the Firewall / Intrusion Detection System wizard.

## **14.2.5 Services Administration (LX)**

The Linux-internal firewall is enabled by default, which prevents access to OpenScope Office LX by "outsiders". OpenScope Office LX does, however, also provide services (e.g., the telephony service) that require open ports (services). After the installation of OpenScope Office LX, these required ports/services must therefore be opened in the firewall.

---

**NOTICE:** Note that the blocking of services that are used by OpenScope Office LX can lead to a degradation and/or failure in the functionality of OpenScope Office LX.

---

## **14.3 MAC and IP Address Filtering (MX)**

MAC and IP address filtering protect OpenScope Office MX against unauthorized access.

Only PCs with IP addresses that are released in combination with the relevant unique MAC address via this security function are granted access authorization. If the IP and MAC addresses do not match those of the specified combination, access is denied

When IP address filtering is active, access via an unprotected network is restricted for the IP addresses released.

**System-Specific Information**

OpenScape Office MX has only a single IP address in the corporate network (customer network). Consequently, even with multiple components, OpenScape Office MX behaves like a single system

You can configure additional addresses internally and at other interfaces (accessed via the corporate network; DMZ and WAN).

## 14.4 Secure Administration (MX)

The Secure Socket Layer SSL and the Admin Log provide for secure administration of OpenScape Office MX. SSL authorizes transmission channels using certificates, and the Admin Log enables all changes made at the communication system to be tracked.

### 14.4.1 SSL (Secure Socket Layer) (MX)

SSL (Secure Sockets Layer) enables the secure administration of OpenScape Office MX. The data cannot be read or manipulated from unauthorized locations. Transfer paths are authenticated by means of certificates. You can generate and administer certificates.

SSL supports the following security services:

- Authenticity (the communication partner is who he says he is)
- Trustworthiness (the data cannot be read by a third party)
- Integrity (the data was received in the same condition as it was sent)

These security services demand prior agreement on the security mechanism used and the exchange of cryptographic keys. These two tasks are performed in the course of connection setup.

SSL uses certificates and keys to guarantee secure data transmission.

**CRL (Certificate Revocation List)**

Certificate Revocation Lists (CRL) are files containing a list of blocked certificates, their serial number, and their blocking data. A CRL list also contains the name of the party who issued the certificate revocation list and the next authentication time.

**CDP (Certificate Distribution Point)**

The CRL Distribution Point is the directory (location) where the current versions of the CRLs are located (for example, <http://sectestcal.microsoft.com/ErtEnvoll/SecTestCAL.crl>).

**System-Specific Information**

Client/server communication in SSL-based administration.

The server uses the certificates generated or imported by the SSL function for authentication at the client. Such certificates can be imported into the browser as trusted certificates to avoid warning messages in the browser when connecting to the SSL server.

## 14.4.2 Admin Log (MX)

The Admin log enables you to track what changes were made to the OpenScape Office MX communication system and by whom and when.

## 14.5 Security at the Phone

Security at the phone is enabled via a system telephone lock (with which the administrator block various functions) and by individual telephone locks (with which users can lock their phones).

### 14.5.1 Central Lock Code, COS Changeover (LX/MX)

The central lock code enables an authorized subscriber to set an extensive lock on most of the phone functions for all stations. Only the following features are still available: internal calls, system speed dialing and conference with internal subscribers. This lock code can be deactivated by the locked subscribers themselves or by the attendant console.

You do not need the PIN for the phone where you want to activate or deactivate the lock code.

#### **System-Specific Information**

If the lock code is active, class of service (COS) 1, i.e., outward restricted trunk access, applies by default.

The authorized station is the "first" IP station.

### 14.5.2 Individual Lock Code (Locking the Phone) (LX/MX)

If the individual telephone lock is set for a phone, external calls cannot be conducted from that phone, and the user settings cannot be modified.

Emergency numbers can be dialed even if the phone is locked.

You can still conduct internal calls.

Incoming calls can be redirected to internal subscribers.

## Security

### Signaling and Payload Encryption (SPE) (LX/MX)

A locked telephone only supports features that do not require external dialing. The System Speed Dialing feature is the exception to this rule.

To remind subscribers that the station is locked, the phone receives a steady tone (special dial tone). In addition, on phones equipped with a display, the message "Unlock Phone" appears.

#### System-Specific Information

Subscribers can lock their phones via a key or code after entering their personal lock codes and then unlock the phone again as required.

First, the phone lock code must be configured. The phone lock code is set to 00000 by default for all phones and can be set individually. To do this, the must be unlocked. The phone lock code must always be 5 digits. Only digits 0-9 are allowed. If the subscriber has forgotten the phone lock code, he or she can have it reset to the default value 00000 by an authorized user (always the first station in the system or the administrator using OpenScape Office Assistant).

## 14.6 Signaling and Payload Encryption (SPE) (LX/MX)

SPE is a security feature for the transmission of signaling and payload data to and from the communication system and between system phones. The feature is based on an asymmetrical encryption mechanism in which public and private keys are used.

---

**NOTICE:** The use of Signaling and Payload Encryption is only possible within the context of project -specific releases.

---

Encryption of signaling and payload data:

- Signaling encryption: The signal transmission between the gateway and clients is encrypted with a 128-bit key. The TLS protocol with AES encryption is used for the transmission. The same mechanism (TLS, AES) is used for IP networking.
- Payload encryption: The payload or voice data is transmitted using the Secure Real-time Transport Protocol (SRTP). They are likewise encrypted with a 128-bit key (AES). SRTP is also used for IP Trunking. The procedure for exchanging the key for SRTP is known as Multimedia Internet Keying (MIKEY).

For SPE, the individual system telephones and communication systems involved must be able to uniquely identify one another. This is done through certificates containing private or public keys.

The keys and certificates are distributed by the DLS server. The DLS server scans all connected devices with addresses using Auto-SPE. The devices approved for SPE are flagged manually; the DLS then sends the keys or certificates securely to them.



Depending on requirements, the security settings for evaluating the certificates and encrypting the data streams can be enabled or disabled. This increases or decreases the security of the encryption.

---

**NOTICE:** In order to use SPE, the optiPoint 410/420 and WL2 telephones must be removed, since they do not support SPE.

---

An encrypted connection only exists in a direct connection between two system telephones and not for consultation connections or conferences.

Due to the increased resource requirements when SPE is activated, some restrictions apply to the GMSA gateway module. For this gateway module, either a maximum of 3 S0 ports and 4 a/b interfaces or 4 S0 ports and 2 a/b interfaces may be used.

### **Salt Key Procedure**

A "Salt" refers to a random value (e.g., time), which is included along with the password in the generation function, and thus individualizes the result. This makes it possible to use the same password for different purposes and still obtain a different key (Salt Key) in each case. An attacker could therefore not possibly know whether it is always the same basic password or different passwords.

### **SRTCP Encryption**

SRTCP (Secure Real-time Transport Control Protocol) is an extension of the SRTP protocol and implements the security of control data. The extension consists of three additional fields: an SRTCP index, an encryption flag and an authentication tag.

## **14.7 Samba Share (LX/MX)**

The hard disk of OpenScape Office LX/MX makes a portion of the hard disk capacity available for file storage. This area can also be used by Microsoft Windows-based operating systems for file sharing on the internal network and is called a file share or SAMBA share.

Switching off the SAMBA share for security reasons results in restrictions on the following features:

- The online help for the OpenScape Office clients can no longer be invoked.
- The Samba Share cannot be used as a backup medium.
- The installation files for OpenScape Office client updates can no longer be made available via the Samba Share.

If a Samba Share is active, you can also specify write protection for this area, so all users are restricted to read-only access.

In the basic installation of OpenScape Office LX/MX, the system setting of the Samba share is enabled, i.e., the share is not write-protected.

## 14.8 SIP Attack Protection

The so-called SIP attacks represent a new form of attacks on communications systems via IP telephony. Such attacks may occur either from the LAN or via the Internet (through badly configured routers). Protection against SIP attacks is provided through password-protected SIP access.

The following rules should be applicable for any SIP subscriber access:

- Active authentication
- A qualified password that
  - is between 8 and 20 characters in length
  - includes one or more uppercase letters (A to Z)
  - includes one or more lowercase letters (A to Z)
  - includes one or more digits (0 to 9),
  - includes one or more special characters (e.g.: %),
  - does not have more than 3 repeated characters
- Definition of a SIP station ID that differs from the station number.

When a new SIP station is set up, authentication is activated by default, and a random password is generated. Since this random password is not known, it must be changed by the administrator.

With OpenScape Office LX and OpenScape Office MX, the appropriate settings are made via the "Central Telephony" wizard.

With OpenScape Office HX, the settings are made via Manager E and administered by HiPath 3000.

During system startup, the password list is checked, and an entry is made in the EventLog (Event Viewer) if a SIP station is configured without a password.

---

**NOTICE:** If OpenScape Office is used as an Internet router, port 5060 must be closed (default setting). For Internet telephony via an ITSP, OpenScape Office opens the relevant ports and keeps them open.

Port 5060 must likewise be closed if an external router or firewall is being used. OpenScape Office is responsible for opening this port (if required).

---

## 15 Networking OpenScape Office

OpenScape Office enables the networking of OpenScape Office MX, OpenScape Office LX and OpenScape Office HX. In this network-wide unified communications solution, subscribers can now use features such as the presence status, voicemail, conferencing and much more in exactly the same way as was originally possible with only a single OpenScape Office communication system.

Supplemented with a comprehensive set of features in the area of voice networking, medium-size companies now have access to a solution that offers a rich portfolio of features that was primarily reserved only for large-scale customers in the past.

Besides the homogeneous networking of OpenScape Office communication systems, it is now also possible to integrate existing HiPath 3000 systems or networks in a pure (hybrid) voice network.

Configuring an IP network is a complex task and should only be performed by experienced service technicians.

---

**NOTICE:** Closed numbering is assumed for all three networking scenarios described here, i.e., the dial plan of the internal station numbers must be unique.

---

### 15.1 Network Plan

Before configuring an internetwork, a network plan should first be created after consulting with the customer.

The network plan should include the following data:

- Node ID (node number) and the associated IP addresses
- Dial Plan

#### Upgrading from OpenScape Office V2 to OpenScape Office V3

For an existing internetwork of OpenScape Office Version 2, an update to Version 3 can be performed without any issues. The network is operating normally.

However, if you want to use the features of Version 3 (such as the automatic synchronization of phone numbers, etc.), you will need to deconfigure the internetwork and reconfigure it in Version 3.

---

**NOTICE:** The V3 wizard for the networking of V3 can likewise not be used!

---

## 15.1.1 Homogeneous and Heterogeneous Networks

In general, a distinction is made in networking between homogeneous (where all components belong to a single systems family) and heterogeneous networks (with different components).

### Homogeneous (Native) Network

A homogeneous (native) network consists of components of the OpenScape Office systems family (OpenScape Office LX and OpenScape Office MX).

### Heterogeneous (Hybrid) Network

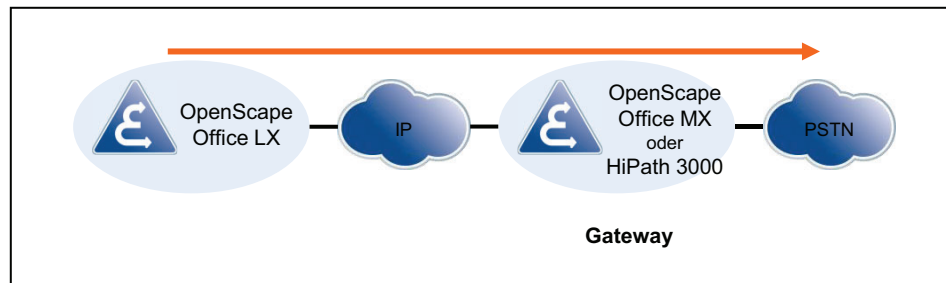
A heterogeneous (hybrid) network consists of components of the OpenScape Office systems family and a HiPath 3000 (from the HiPath systems family), for example.

## 15.1.2 Single and Multi-Gateway

A distinction is made in networking between a single and multi-gateway network, depending on whether only a single gateway or multiple gateways are used.

### Single Gateway

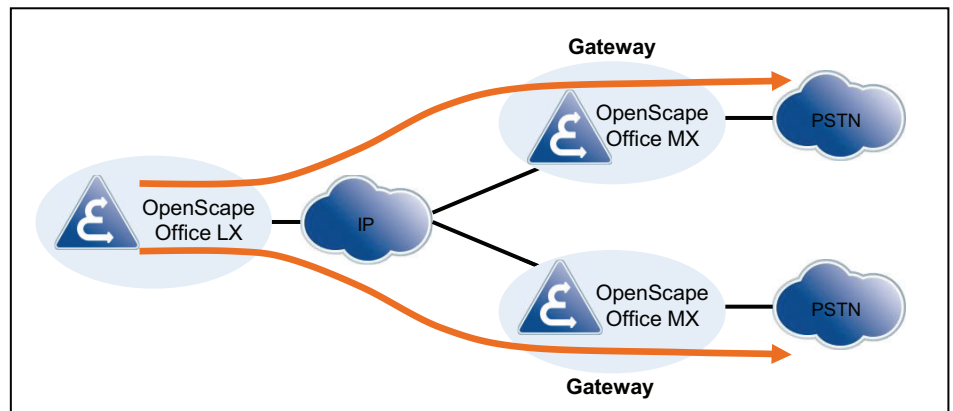
In the case of a single-gateway network, calls are routed via a single gateway.



- Supported if there are one or more OpenScape Office LX systems in the network.
- The IP stations are connected to different communication systems.
- OpenScape Office MX or HiPath 3000 can be used as a gateway.

### Multi-Gateway

In the case of a multi-gateway network, calls are routed via several different OpenScape Office MX gateways.



- There is only one PSTN Provider and one CO station number per gateway.
- The stations of the different locations are registered at a central system (OpenScape Office LX).
- Every station of the OpenScape Office LX is assigned a specific gateway (OpenScape Office MX).
- There should only be a single OpenScape Office LX in the network.
- OpenScape Office LX and OpenScape Office MX are in the same time zone and in the same country (same country code).
- There is only one CO access code worldwide.
- ISDN and analog stations can be locally set up on the gateways.

### 15.1.3 Removing a Node from the Internetwork

If a node is to be removed from the internetwork, it must first be ensured that the node is no longer available. Otherwise, the node will independently attempt to register itself again in the network.

#### Procedure

The deletion of a node occurs via the Networking wizard, where all nodes involved must always be removed.

If only one of the nodes involved is deleted, data will continue to be transferred from one OpenScape Office to another and thus produce inconsistencies in the internal directory, i.e., the users will not appear in the user directory and will therefore be unable to use myPortal for Desktop.

- Interrupt all paths (routing) to the nodes to be removed
- Administration of the internetwork
- Remove all nodes in the Networking wizard  
Enter "No network" for the slave node involved and remove the master node from the registration list.

## 15.2 Network-wide Features

A distinction is made in the network-wide features of OpenScape Office between the features of UC clients and the voice features. The central intercept position is also a network-wide feature for intercepting calls that cannot be assigned.

### 15.2.1 Network-wide Features of UC Clients

The following table shows an overview of the network-wide features of the UC clients and the interworking with HiPath 3000 (when HiPath 3000 is used as a gateway).

#### myPortal for Desktop

Unified Communication Features	Pure LX/MX network	Mixed LX/MX/HX/HiPath network	
		LX/MX/HX power supply	Interworking with HiPath 3000 3000 (without HX)
Directories	Personal directory	Personal directory	Internal subscribers of the HP3000 can be integrated via the external offline directory.
	Internal directory, netwide	Internal directory, netwide across LX-MX-HX	
	External directory (local via .CSV import in each case; local search)	External directory (local via .CSV import in each case; local search)	
	External offline directory (central, via LDAP)	External offline directory (central, via LDAP)	
Favorites list	Internal MX-LX subscribers and external subscribers	Internal LX-MX-LX subscribers and external subscribers (incl. HiPath 3000)	Internal subscribers of the HiPath 3000 can be integrated via the external directory or the external offline directory.
Journal	Open, All Calls, Missed, Answered, Internal, External, Inbound, Outbound, Scheduled	Open, All Calls, Missed, Answered, Internal, External, Inbound, Outbound, Scheduled	Calls into the HiPath 3000 network are displayed in the journal.

Unified Communication Features	Pure LX/MX network	Mixed LX/MX/HX/HiPath network	
		LX/MX/HX power supply	Interworking with HiPath 3000 3000 (without HX)
Screen pops	Incoming call	Incoming call	
	Outgoing call	Outgoing call	
	New VoiceMail	New VoiceMail	
	Change of own Presence status	Change of own Presence status	
	Open personal contact for inbound call	Open personal contact for inbound call	
	Open an e-mail	Open an e-mail	
	Schedule calls	Schedule calls	
Live Recording	Yes	Yes	Calls with HiPath 3000 subscribers can be recorded live.
Presence status	Yes	Yes	Yes
Busy status	Yes	Yes	Yes
CallMe Service	Yes	Yes	Yes
Status-based call forwarding	Yes	Yes	MX-LX subscribers can use status-based destinations of HiPath 3000.
Personal and Central AutoAttendant	Yes	Yes	Yes
Instant Messaging	Yes	Yes	Yes
Multi-user chat	Yes	Yes	MX-LX subscribers cannot include any HiPath 3000 subscribers.
Voicemail for voice messages and faxes	Yes	Yes	MX-LX subscribers can receive both from HiPath 3000 subscribers.
Voicemails	Yes	Yes	MX-LX subscribers can forward voicemails (independently of the subscriber) by e-mail.
Fax (incoming and outgoing)	Yes	Yes	MX-LX subscribers can receive and send faxes from and to HiPath 3000

**Networking OpenScape Office**  
Network-wide Features

Unified Communication Features	Pure LX/MX network	Mixed LX/MX/HX/HiPath network	
		LX/MX/HX power supply	Interworking with HiPath 3000 3000 (without HX)
Computer Telephony Integration CTI	Yes	Yes	Yes, local at the HiPath 3000 nodes
Conferences	Yes	LX/MX subscribers can be a master or slave in a conference. HX subscribers can only be slaves and cannot control a conference.	MX-LX and HiPath 3000 do not mutually see any presence status.
Desktop Dialer	Yes	Yes	No

**myPortal for Outlook**

Unified Communication Features	Pure LX/MX network	Mixed LX/MX/HX/HiPath network	
		LX/MX/HX power supply	Interworking with HiPath 3000 3000 (without HX)
Directories	Internal directory, netwide	Internal directory, netwide across LX-MX-HX	
	External directory (local via .CSV import in each case; local search)	External directory (local via .CSV import in each case; local search)	
	External offline directory (central, via LDAP)	External offline directory (central, via LDAP)	
Favorites list	Internal MX-LX subscribers and external subscribers	Internal LX-MX-LX subscribers and external subscribers (including HiPath 3000)	Internal subscribers of the HP3000 can be integrated via the external offline directory.
Journal	Open, All Calls, Missed, Answered, Internal, External, Inbound, Outbound, Scheduled	Open, All Calls, Missed, Answered, Internal, External, Inbound, Outbound, Scheduled	Calls into the HiPath 3000 network are displayed in the journal
Screen pops	Incoming call	Incoming call	
	Outgoing call	Outgoing call	
	New VoiceMail	New VoiceMail	
	Change of own Presence status	Change of own Presence status	
	Open personal contact for inbound call	Open personal contact for inbound call	
	Open an e-mail	Open an e-mail	
	Schedule calls	Schedule calls	
Live Recording	Yes	Yes	Calls with HiPath 3000 subscribers can be recorded live.



Unified Communication Features	Pure LX/MX network	Mixed LX/MX/HX/HiPath network	
		LX/MX/HX power supply	Interworking with HiPath 3000 3000 (without HX)
Presence status	yes	Yes	MX-LX and HiPath 3000 do not mutually see any presence status.
Busy status	Yes	Yes	MX-LX and HiPath 3000 do not mutually see any busy status.
CallMe Service	Yes	Yes	MX-LX subscribers can route calls to HiPath 3000.
Status-based call forwarding	Yes	Yes	MX-LX subscribers can use status-based destinations of HiPath 3000.
Personal and Central AutoAttendant	Yes	Yes	AutoAttendant can address HiPath 3000 subscribers.
Instant Messaging	Yes	Yes	MX-LX and HiPath 3000 cannot mutually send and receive instant messages.
Multi-user chat	Yes	Yes	MX-LX subscribers cannot include any HiPath 3000 subscribers.
Voicemail for voice messages and faxes	Yes	Yes	MX-LX subscribers can receive both from HiPath 3000 subscribers.
Voicemails	Yes	Yes	MX-LX subscribers can forward voicemails (independently of the subscriber) by e-mail.
Fax (incoming and outgoing)	Yes	Yes	MX-LX subscribers can receive and send faxes from and to HiPath 3000
Computer Telephony Integration CTI	Yes	Yes	Yes, local at the HiPath 3000 nodes
Conferences	Yes	LX/MX subscribers can be a master or slave in a conference. HX subscribers can only be slaves and cannot control a conference.	MX-LX and HiPath 3000 do not mutually see any presence status.
Desktop Dialer	Yes	Yes	No

**myAttendant**

Unified Communication Features	Pure LX/MX network	Mixed LX/MX/HX/HiPath network	
		LX/MX/HX power supply	Interworking with HiPath 3000 3000 (without HX)
Convenient call handling	Yes	Yes	Standard Attendant functions for HiPath 3000 such as automatic recall, intercept, display of forwarding station, no mutually visible busy indication
Directories	Personal directory	Personal directory	Internal subscribers of the HiPath 3000 can be integrated via the external directory or the external offline directory.
	Internal directory, netwide	Internal directory, netwide across LX-MX-HX	
	External directory (local via .CSV import in each case; local search)	External directory (local via .CSV import in each case; local search)	
	External offline directory (central, via LDAP)	External offline directory (central, via LDAP)	
Search in internal directory	Yes	Yes	No
Subscriber Management	Yes	Yes	No
Journal	Open, All Calls, Missed, Answered, Internal, External, Inbound, Outbound, Scheduled	Open, All Calls, Missed, Answered, Internal, External, Inbound, Outbound, Scheduled	Internal subscribers of the HiPath 3000 can be integrated via the external directory or the external offline directory.
Message Center	No	No	No
View presence status	Yes	Yes	No
Change presence status for subscriber	Yes	Yes	No
Live Recording	Yes	Yes	Calls with HiPath 3000 subscribers can be recorded live.
Multi-user chat	Yes	Yes	No
Screen pops	Incoming call; answering the incoming call	Yes	
Send instant messages	Yes	Yes	No

**myPortal for Mobile**

Unified Communication Features	Pure LX/MX network	Mixed LX/MX/HX/HiPath network	
		LX/MX/HX power supply	Interworking with HiPath 3000 3000 (without HX)
Directories	Internal directory with network-wide presence status	Internal directory with network-wide presence status	Internal subscribers of HiPath 3000 can be integrated via personal contacts.
	Personal contacts	Personal contacts	
	System directory (phone book)	System directory (phone book)	
	External offline directory (central, via LDAP)	External offline directory (central, via LDAP)	
Favorites List	Internal and external subscribers	Internal and external subscribers	Internal subscribers of HiPath 3000 can be integrated via personal contacts.
Journal	Incoming calls, outgoing calls, manual dialing, redialing	Incoming calls, outgoing calls, manual dialing, redialing	Calls into HiPath 3000 are displayed in the journal.
Voicemail Box	Yes	Yes	Not for HiPath 3000
Presence status	Yes	Yes	No

**myPortal for OpenStage**

Unified Communication Features	Pure LX/MX network	Mixed LX/MX/HX/HiPath network	
		LX/MX/HX power supply	Interworking with HiPath 3000 3000 (without HX)
Presence status	Yes	Yes	Not for HiPath 3000
Voicemail Box	Yes	Yes	No

**myAgent**

Unified Communication Features	Pure LX/MX network	Mixed LX/MX/HX/HiPath network	
		LX/MX/HX power supply	Interworking with HiPath 3000 3000 (without HX)
All features	Local connection of myAgent clients and Contact Center options per OpenScape Office LX/MX/HX network node. Contact Center solutions across multiple locations can be implemented via remote stations or VPN connections of subscribers.	No, locally via external Call Center solutions for the HiPath 3000 network segment	

**myReports**

Unified Communication Features	Pure LX/MX network	Mixed LX/MX/HX/HiPath network	
		LX/MX/HX power supply	Interworking with HiPath 3000 3000 (without HX)
All features	Local connection of myAgent clients and Contact Center options per OpenScape Office LX/MX/HX network node. Contact Center solutions across multiple locations can be implemented via remote stations or VPN connections of subscribers.	No, locally via external Call Center solutions for the HiPath 3000 network segment	

**15.2.2 Network-wide Voice Features**

For networking via the SIP-Q protocol, the following voice features are supported for OpenScape Office and HiPath 3000.

Feature	SIP-Q (IP Network)
Basic call	Yes
Callback on busy	Yes
Callback on RNA	Yes
Override	Yes
Call waiting	Yes
Second call	Yes
Calling Line Identification Presentation (CLIP)	Yes
Calling Line Identification Restriction (CLIR)	Yes
Connected Line ID Presentation (COLP)	Yes
Connected Line ID Restriction (COLR)	Yes
Calling / Connected Name Identification Presentation (CNIP)	Yes
Calling / Connected Name Identification Restriction (CNIR)	Yes
Do Not Disturb	Yes
Call forwarding	Yes
Call Forwarding on Busy	Yes
Call Forwarding on RNA	Yes
Call Deflection	Yes
Advice of Charge at Call Setup	No

Feature	SIP-Q (IP Network)
Advice of Charge during Call	Yes
Advice of Charge at the end of the call	Yes
Path optimization	Yes
Rerouting	No
Message Waiting Indication / Info	Yes
Trace call	Yes
Placing a call on hold	Yes
Alternate (Toggle/Connect)	Yes
Transfer	Yes
Conferencing	Yes
Automatic Recall	Yes
Calling for Help	Yes
Intercept	Yes
Private Numbering Plan (PNP)	No
Call pickup	No
Hunt Group	Yes
SPE (except for conferencing and applications)	Yes

### 15.2.3 Central Intercept Position in the Internetwork (LX/MX)

The communication system allows incoming calls that cannot be assigned to a station or answered to be diverted to a defined intercept position in the internetwork to ensure that no calls are lost.

If the central intercept position in the internetwork is configured using ISDN, then the functionality is identical to the functionality without networking; see [Intercept](#).

In conjunction with an ITSP Central Office, the central intercept position is subject to some restrictions, since every node essentially has its own ITSP:

- The ITSP intercept criteria apply only to each respective node.
- The intercepts "on RNA", "on Device Busy", "on Incomplete", "on Invalid", and "on Unanswered Recall" work.
- The intercept types "on Invalid" and "on Incomplete" do not work with the ITSP.
- Incomplete or invalid telephone numbers are returned to the ITSP with a busy signal.

If a central intercept position is to be used in an internetwork, virtual stations must be configured in each node. These virtual stations are permanently diverted via the internetwork to the myAttendant user.

Example for an ITSP CO: ITSP PABX number is 0211-23456789 + ITSP DID number; the number 0211-23456789-0 is publicly announced as the central number of the communication system.

- Station 100 is myAttendant with its own ITSP DID number 100 and a virtual station 199 with the ITSP DID number "0".
- In the ITSP mapping list of each node, the ITSP DID number "0" is assigned to the own virtual station.
- Under **Incoming Calls/Call Forwarding**, the virtual stations are referred to station 100.  
First destination: own virtual station  
Second destination: station 100 in the destination node  
Call time 5 seconds

For better identification of calls, it is recommended that the virtual stations of all nodes be provided with their call number (DID) and a name (e.g., company) via the myAttendant application (under **Setup/myAttendant/DIDs**). This enables a more detailed identification of the caller in the **Active Calls** window of myAttendant.

## 15.3 Licensing an Internetwork

For a networked communication system, either central or local licensing can be selected.

If central licensing is used, the slave nodes are automatically connected with the central license agent of the master node when running the **Network** wizard.

---

**INFO:** In mixed/heterogeneous networks, HiPath 3000 and OpenScape Office HX must be licensed separately.

---

For more information, see [Licensing](#).

## 15.4 Networking Requirements

To ensure the quality of the voice transmission, the IP networks being used and the communication system must meet certain requirements. The voice quality and voice communication reliability always depend on the network technology in use.

### Network Parameters, LAN and WAN Requirements

Parameters	Minimum requirement	Notes
Delay (one way)	50 ms	
Round Trip Delay	100 ms	
Jitter	20 ms	For good voice quality, the jitter must not be greater than 20 ms.
Packet Loss	3 %	For fax or modem transmissions over G.711, the packet loss should not exceed 0.05 % (e.g., for a connection via AP11xx).
Consecutive Packet Loss	3 with G.711, 1 with G.723.1	The loss in voice quality, as opposed to the packet loss, is greater with G.723.1 than with G.711. The minimum requirements apply to the default setting of 1.

#### Recommendation for Calculating Bandwidth

- A bandwidth of at least 256 kbps (in both the sending and receiving direction) is required on the internetwork.
- The bandwidth calculation should be based on a maximum of 50% for the voice portion with respect to the total bandwidth. In other words, in the case of a 1 Mbit WAN, for example, a maximum of 500 kbps should be calculated for voice. With the G.711 codec, for example, that would be a maximum of 5 IP trunks.
- Regardless thereof, the network properties with respect to QoS, delay, packet loss, etc., must also be taken into account.

## 15.4.1 LAN Networking Requirements

To ensure the quality of the voice and data transmissions, the IP networks being used and the communication system must meet certain requirements for the LAN.

#### LAN requirements

The data network must be of the Ethernet type:

- The recommended cable is a Cat.5 cable (screened/unscreened multi-element cables characterized up to 100 MHz for horizontal and building backbone cables as per EN 50288).
- Support for QoS: IEEE. 802.1p, DiffServ (RFC 2474).
- All active LAN ports must support 100 / 1000 MBit/sec. and full duplex communications.

Every communication system must be connected via a switch or a dedicated port of a router. Hubs and repeaters are not supported.

The VoIP- application should be connected via a separate VLAN to minimize collisions with other transmissions. If all involved devices support VLAN (in accordance with IEEE802.1q), all VoIP traffic can be placed in a separate VLAN.

**Payload Connections with RTP (Real-time Transport Protocol) in a LAN Environment**

The required bandwidth for voice transmissions in an IP network can be calculated with the help of the following table:

Codec type	Packet parameters	Sample size (ms)	Payload (bytes)	Ethernet packet length (bytes)	Payload packet (overhead in percent)	Ethernet load (incl.) header (kbps)
G.711	20	20	160	230	44%	92
G.711	30	30	240	310	29%	82.7
G.711	40	40	320	390	22%	78
G.711	60	60	480	550	15%	73.3
G.729A	1	20	20	90	350%	36
G.729A	2	40	40	110	175%	22
G.729A	3	60	60	130	117%	17.3
RTCP		5000		280		0.4

The load in the LAN is calculated for one direction. Double the bandwidth is required for both directions. If these codecs are used, the bandwidth requirements are reduced, depending on the scope of the idle periods for voice signals.

The calculation includes VLAN tagging in accordance IEEE 802 1q. Without VLAN tagging, the packet length is shorter by 4 bytes.

The overhead is calculated as follows:

Protocol	Bytes
RTP Header	12
UDP Header	8
IP Header	20
802.1Q VLAN Tagging	4
MAC (incl. Preamble, FCS)	26
Total	70

Control payload connection with parallel RTCP:

Report type	Report interval (sec)	Average Ethernet packet size (bytes)	Ethernet load, incl. header (kbps)
Sender report	5	140	0.2
Recipient report	5	140	0.2
Total	0.4		



Payload transport in a T.38 LAN environment:

	Sample size (ms)	Payload (bytes)	Ethernet packet length (bytes)	Payload packet (overhead in percent)	Ethernet load (incl. header) (kbps)
T.38	30	169	227	34%	60.5

Payload Connections with SRTP (Real-time Transport Protocol) in a LAN Environment:

Codec type	Sample size (ms)	Payload (bytes)	Ethernet packet length (bytes)	SRTP Ethernet packet length (kbps)	RTP Ethernet packet length (kbps)	Additional bandwidth for SRTP (%)
G.711	20	160	244	97.6	92	6.1
G.711	30	240	324	86.4	82.4	4.5
G.711	40	320	404	80.8	78	3.6
G.711	60	480	564	75.2	73.3	2.5
G.729A	20	20	104	41.6	36	15.6
G.729A	40	40	124	24.8	22	12.7
G.729A	60	60	144	19.2	17.3	10.8

The thumb rule for calculating the required bandwidth for n parallel VoIP connections with G.711 (one frame per RTP packet) is as follows:

$$\text{Bandwidth WAN} = n \times (180 \text{ Kbps Voice Payload} + 0.4 \text{ RTPC})$$

## 15.4.2 WAN Networking Requirements

To ensure the quality of the voice and data transmission, the IP networks being used and the communication system must meet certain requirements for the WAN.

### WAN Requirements

The following requirements apply if IP telephony is implemented in internal IP networks connected via WAN:

- The internal IP networks (LANs) must each be connected to the Internet via a WAN port with a fixed IP address.
- The bandwidth required for the calls must always be available for both uploads and downloads.
- The number of simultaneous WAN-based IP phone connections is limited by the bandwidth and the audio codecs used. Given the same bandwidth, more phone connections can be established if an Audio Codec with high compression is used.
- OpenScope Office MX does not come with an integrated modem; in other words, an external modem is required (e.g., a DSL modem).

The following constraints apply to IP telephony via ITSP (Internet Telephony Service Providers):

- Voice quality restrictions can occur at ports that are not QoS-compliant (generally, ADSL ports). Good voice quality is achieved by reserving a non-QoS-compliant Internet connection exclusively for voice connections to the ITSP.
- The router used must support QoS functions and broadband control mechanisms to guarantee good voice quality.

**The following values are calculated for Payload connections with RTP (Realtime Transport Protocol) in a WAN environment:**

Codec type	Packet parameters	Sample size (ms)	Payload (bytes)	Packet length (bytes)	Payload packet (overhead in percent)	WAN load (kbps)	Packet length with compr. Header (bytes)	WAN load with compr. Header (bytes)
G.711	20	20	160	206	29%	82.4	-	-
G.711	30	30	240	286	19%	76,3,7	-	-
G.711	40	40	320	366	14%	73.2	-	-
G.711	60	60	480	526	10%	70,1,3	-	-
G.729A	1	20	20	66	230%	26.4	28	11.2
G.729A	2	40	40	86	115%	17.2	48	9.6
G.729A	3	60	60	106	77%	14.1	68	9.1
RTCP	-	5000	-	230	-	0.4	-	0.4

Payload Transport in T.38 WAN Environment:

	Sample size (ms)	Payload (bytes)	Packet length (bytes)	Payload packet (overhead in percent)	Ethernet load (incl.) header (kbps)
T.38 (Redundancy 2)	30	169	203	20%	54.1

The WAN load is calculated for a route. Since WAN channels usually include channels in both directions, this is equivalent to the required bandwidth for an ISDN channel, for example.

The overhead is calculated as follows:

Protocol	Bytes
RTP Header	12
UDP Header	8
IP Header	20
PPP	6
Total	46
Compressed Header	8

For RTP/UDP/IP header compression, a "compressed header" is usually used. In addition, a full header (46 bytes) is transmitted every 5 seconds.

The thumb rule for calculating the required bandwidth for n parallel VoIP connections with G.711 (one frame per RTP packet) is as follows:

$$\text{Bandwidth WAN} = n \times (82 \text{ Kbps Voice Payload} + 0.4 \text{ RTPC})$$

### 15.4.3 Dial Plan in the Network

The dial plan is an important prerequisite for networking. The complexity of the internetwork configuration depends on the dial plan.

#### Closed numbering

In the case of closed numbering, a station in the internetwork is uniquely identified by the station number. Each station in the internetwork can reach another station by directly dialing its station number.

The advantage of closed numbering is that you do not have to dial a node number to reach another station in another networked communication system.

**Table:** Examples of closed numbering

	Node 1	Node 2	Node 3	Node 4
Phone Numbers	100	200	300	400
	101	201	301	401
	102	202	302	402
	103	203	303	403
	104	204	304	404

#### Transfer of Existing Customer Networks with Open Numbering Plan into OpenScape Office

In open numbering, a station is uniquely identified by the node number and the station number. Users of different communication systems (nodes) in the internetwork can thus have the same station number.

With open numbering, the station's node number must always be dialed in addition to the phone number. Phone number ranges can be used more than once for this, and multiple phone numbers can be used.

**Table:** Example of open numbering at HiPath 3000:

	Node 1	Node 2	Node 3	Node 4
Node number (PABX number)	95	96	97	98
Phone Numbers	100	100	100	100
	101	101	101	101
	102	102	102	102
	103	103	103	103
	104	104	104	104

---

**NOTICE:** OpenScape Office supports only closed numbering. Existing customer networks with open numbering must be adapted.

---

In an open internetwork comprising multiple HiPath 3000 systems with one connected OpenScape Office HX each, the dial plan must be converted to a closed numbering plan if the OpenScape Office HX systems are also to be networked. It is only then that features such as the presence status and instant messaging will be available.

## 15.5 Path Optimization (Path Replacement)

Path optimization (also called path replacement) helps to avoid the dual seizure of IP trunks for networked communication systems.

When multiple OpenScape Office systems are networked, the following problem could occur, for example: First, let us assume that subscriber A calls subscriber B who, in turn, has forwarded all calls to subscriber C. Subscribers A and C are in the same network node, but subscriber B is on a different network node. Consequently, the call with call forwarding initially seizes two trunks between the two network nodes. To avoid this dual seizure, path optimization must be enabled.

---

**NOTICE:** The system flag for the path optimization must be enabled for all networked OpenScape Office systems.

---

The path optimization is performed:

- After the connection setup (not in the ringing phase!)
- After transfer scenarios
- After call forwarding and CFNA (call forwarding-no answer)

The path optimization is not performed:

- When a ringing group or group call is involved
- For conferences
- If some other feature is enabled when executing the path optimization, the optimization is aborted.

The IP trunks of HiPath 3000 used for OpenScape Office HX must be configured only in route 8. Starting with HiPath 3000 V9, path optimization also occurs for the IP trunks of route 8.

---

**NOTICE:** The path optimization for OpenScape Office HX is configured via HiPath 3000 Manager E.

---

## 15.6 Networking Scenarios

A distinction is essentially made between five networking scenarios here:

- Multiple OpenScape Office MX systems
- Multiple OpenScape Office HX systems
- OpenScape Office LX/MX/HX (single gateway)
- OpenScape Office LX/MX (multi-gateway)
- OpenScape Office LX/MX with HiPath 3000 (where HiPath 3000 functions as a gateway)

---

**NOTICE:** Closed numbering is assumed for all three scenarios described here, i.e., the dial plan of the internal station numbers must be unique.

---

Call charge details can only be retrieved per network node, but not across nodes.

---

**NOTICE:** It is not possible to use an ITSP across nodes. This means that the SIP trunks of a node can only be used by the local stations of that node.

---

### 15.6.1 General Information

This section provides information on general requirements and helpful tips regarding all networking scenarios.

#### Networking OpenScape Office with HiPath 3000

In an internetwork of OpenScape Office and HiPath 3000, all the HiPath 3000 and HG 1500 communication systems involved must have at least Version V8, Minor Release 5.4. Earlier versions do not support hybrid (heterogeneous ) networks.

You should also check the configuration for the voice gateway of the HG 1500 and change the following settings if required:

- Node Monitoring: ICMP
- Disable the node monitoring for every OpenScape Office LX/MX
- Set the LAN protocol for every OpenScape Office LX/MX to SIPQ.

In general, all node and routing tables should be created on the OpenScape Office master. These settings can then be transferred to all HG 1500 systems without any problems by using the Export function.

### Automatic updates for CAR tables of the HG 1500 in HiPath 3000

The following requirements must be satisfied to automatically update the CAR tables in a network of OpenScape Office and HiPath 3000 communication systems:

- OpenScape Office Assistant  
The check box **Automatic update of CAR tables in corresponding HiPath 3000 / HXG** must be selected and the **OSO Access Call Number** must be configured in the **Networking** wizard of the master system.
- HiPath 3000 Manager E  
For each HiPath 3000, the **OSO Access Call Number** must be configured under the **System Settings**. This number is then displayed in the CAR tables of the HG 1500 with a reference to the respective HiPath 3000 node ID.

---

**NOTICE:** If an automatic update of the CAR tables to be activated, then the contents of the CAR tables of all HG 1500 boards involved must be deleted to avoid collisions.

---

### Networking and Accounting

- The costs by cause principle applies, i.e., call charge records are stored in the communication system which caused the charges. For example, if a subscriber in the OpenScape Office LX makes a trunk call that is routed through a gateway, then the charge record is generated in the OpenScape Office LX and not in the gateway.
- In general, no call charge records are generated for internal network connections, i.e., calls from node to node are not recorded.
- Calls initially conducted from node A generate call charge data in node A. After a transfer of the call to node B, the call charges are generated in node B.

### DSS Keys on optiPoint Attendant Available Across all Nodes

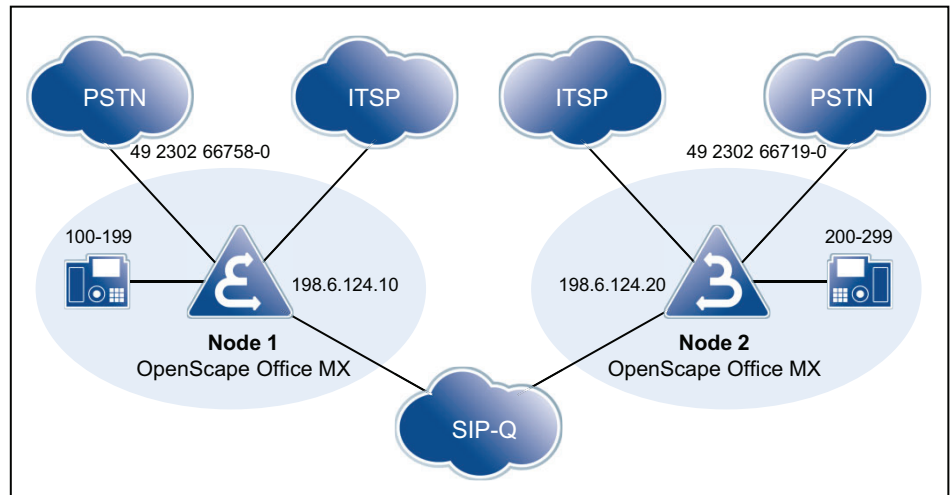
- In Version 3.2, DSS keys on optiPoint Attendant could be used only in the local node. As of Version 3.3, DSS keys can be used across nodes. As a prerequisite, an OpenScape Office MX or OpenScape Office LX must exist in the internetwork.
- If a HiPath 3000 exists in the internetwork, this functionality will only be available in conjunction with OpenScape Office HX.

### Restrictions and Dependencies

- For all types of networking, the servers and clients must be in the same time zone.
- Multi-gateway networks have only been released within a country.
- For OpenScape Office MX networks, no connection via an ITSP (SIP Provider) is basically supported.

## 15.6.2 Scenario 1: Networking Multiple OpenScape Office MX Systems

Up to 8 OpenScape Office MX communication systems can be networked, provided the dial plan is unique.



For OpenScape Office MX networks, no connection via an ITSP (SIP Provider) is basically supported.

Maximum configuration	
Maximum number of nodes	8
Maximum number of stations in the network	1000

**NOTICE:** Larger networks can be configured on a project-specific basis (via OSIRIS).

### Network-wide Features for an Internetwork of Multiple OpenScape Office MX Systems

myPortal	
Voicemail (Recording, Notification, Retrieval)	Netwide
Presence	Netwide
Busy status	Netwide
Internal directory / Favorites	Netwide
External directory	Local via .CSV import in each case
Search in external directories of other network nodes	Not possible
External offline directory	Central, via LDAP

<b>myAttendant</b>	
Attendant functions (automatic recall, intercept, display of forwarding station, ...)	Netwide
Instant Messaging	Netwide
Voicemail (Recording, Notification, Retrieval)	Netwide
Presence	Netwide
Busy status	Netwide
Internal directory	Netwide
External directory	Local via .CSV import in each case
Search in external directories of other network nodes	Not possible
External offline directory	Central, via LDAP
Check voicemails of other subscribers (only if the subscriber has activated this feature)	Local, i.e., not by subscribers on other nodes

<b>myAgent (Contact Center)</b>	
Agents	Must be in the same network node
Agent status	Local
Incoming ACD calls	Via local PSTN trunks, SIP Providers and SIP-Q trunks
Voicemail (Recording, Notification, Retrieval)	Netwide
Presence	Netwide
Internal directory / Favorites	Netwide
External directory	Local via .CSV import in each case
Search in external directories of other network nodes	Not possible

<b>Central AutoAttendant</b>	
Dialing call numbers (by the caller)	CCV scripts enable the targeted dialing of stations in the network. The possible destinations are all call numbers of the internal directory
Dialing call numbers (preconfigured by the administrator)	Any destinations can be entered by the administrator in CCV scripts and dialed by the caller with a single-digit selection.
<b>External applications</b>	
Teledata Office	Netwide
TAPI 170	Netwide
TAPI 120	With CMD, network-wide; without CMD, local
CallBridge IP	Local
External CSTA applications	Netwide, i.e., the CSTA application uses ONE CSTA link at ONE system to communicate with the entire network



SIP Provider	Local
PSTN Provider	Local or decentralized connections to the individual network nodes
<b>Bandwidth requirements</b>	
For HFA, SIP clients	No bandwidth control
<b>Administration</b>	Network-wide using wizards, Expert mode

### 15.6.3 Configuring Scenario 1

The configuration of scenario 2 explains the steps required to set up networking with the help of an example.

#### Prerequisites:

- A network plan is available. The network plan was used to ensure that every internal call number in the internetwork is only used once for closed numbering. Different station number lengths are allowed. DID station numbers may occur more than once (e.g., the CO station numbers 49 2302 66758 100 and 49 2302 66719 100 have the same DID No. 100).

---

**NOTICE:** The station numbers may need to be adapted. An open numbering scheme is not implemented!

---

- The IP network has been configured, and all nodes can be mutually pinged successfully
- All nodes have been upgraded to the same software version

Call forwarding across nodes: For incoming calls over IP trunks, which have already been forwarded, no further forwardings to the voicemail box are executed. This is because no unique assignment to the voicemail box can otherwise be made

If cross-node deputy rules (referral extensions) are required, this must be set up via the profiles of the OpenScape Office stations or ringing groups. The corresponding cross-node calls are not signaled as forwarded in this case, but as DSS (direct station selection) calls. Call forwardings of the deputy are therefore forwarded to the voicemail box

#### Setting up the Location Data for Node 1

Node 1	
G.-Location Country	49
G.-Location Local Network	2302
G.-Location System	66758

Node 1		
International Prefix		00
National Prefix		0
<b>Routes</b>		
ISDN	Trunk code	0
Networking	2nd trunk code	0
<b>Routing parameters</b>		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 1 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

#### Overview of Entries in the LCR for Node 1

Dial Plan		Route table			Dial Rule		
Name	Dialed digits	Route	Dedicated Gateway	Gateway ID	Dial Rule	Procedure	Type
Node 2 Internat	0C004923026 6719-Z	Networking	Mandatory	2	D492302667 19E3A	Corp. Network	International
Node 2 NAT	0C023026671 9-Z						
Node 2 Strn.	0C66719-Z						
CO	0CZ	ISDN	No		A	Main network supplier	Unknown
Various	-Z	Networking	No		A	Corp. Network	Unknown

#### Setting up the Location Data for Node 2

Node 2		
G-Location Country		49
G-Location Local Network		2302
G-Location System		66719
International Prefix		00
National Prefix		0
<b>Routes</b>		
ISDN	Trunk code	0
Networking	2nd trunk code	0

Node 2		
<b>Routing parameters</b>		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 2 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

#### Overview of Entries in the LCR for Node 2

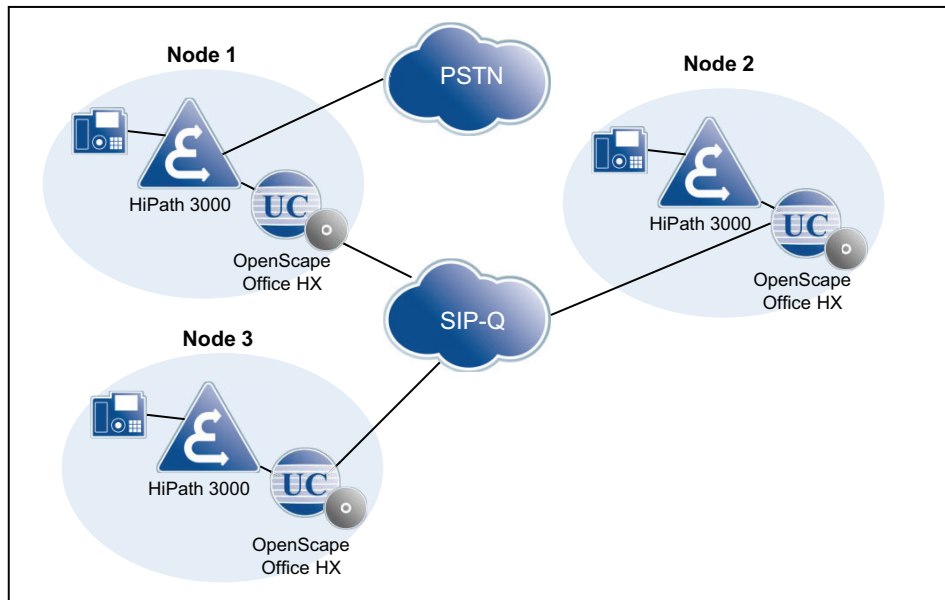
Dial Plan		Route table			Dial Rule		
Name	Dialed digits	Route	Dedicated Gateway	Gateway ID	Dial Rule	Procedure	Type
Node 1 Internat	0C0049230266758-Z	Networking	Mandatory	1	D49230266758E3A	Corp. Network	International
Node 1 NAT	0C0230266758-Z						
Node 1 Stn.	0C66758-Z						
CO	0CZ	ISDN	No		A	Main network supplier	Unknown
Various	-Z	Networking	No		A	Corp. Network	Unknown

#### Procedure to Set up Networking:

1. Configure the basic installation for node 1 (master)
2. Configuring Networking for Node 1
3. Configure the basic installation for node 2 (slave)
4. Configuring Networking for Node 2
5. Verify the networking function for the master
6. Check routes and routing parameters (master)
7. Check routes and routing parameters (Trk. Grp. 64) (master)
8. Configure LCR for networking (master)
9. Check routes and routing parameters (Slave)
10. Configure LCR for networking (slave)

### 15.6.4 Scenario 2: Networking Multiple OpenScape Office HX Systems

Up to 32 HiPath 3000 communication systems can be networked together, and one OpenScape Office HX can be connected to each HiPath 3000. The dial plan must be unique.



All OpenScape Office HX systems are interlinked, thus enabling the complete set of OpenScape Office applications to be used on a network-wide basis.

One OpenScape Office HX is configured as the master. All IP addresses of the networked OpenScape Office HX systems are stored in the master. The network functions are controlled solely by the OpenScape Office HX (or the appropriate application), without any involvement of the HiPath 3000.

The list of OpenScape Office IP addresses is automatically synchronized.

In general, any OpenScape Office HX can be configured as the master. However, there can always be only a single master in an internetwork.

Maximum configuration	
Maximum number of HiPath 3000 systems	32
Maximum number of OpenScape Office HX systems in the network (one HiPath 3000 must be deducted per OpenScape Office HX, for example, with 4 OpenScape Office HX systems in the internetwork, up to 60 HiPath 3000 systems are still possible)	8
Maximum number of stations in the network (project-specific).	1000

### Network-wide Features for an Internetwork of Multiple OpenScape Office HX Systems

myPortal	
Voicemail (Recording, Notification, Retrieval)	Netwide
Presence	Netwide
Busy status	Netwide
Internal directory / Favorites	Netwide

<b>myPortal</b>	
External directory	Local via .CSV import in each case
Search in external directories of other network nodes	Not possible
External offline directory	Central, via LDAP

<b>myAttendant</b>	
Attendant functions (automatic recall, intercept, display of forwarding station, ...)	Netwide
Instant Messaging	Netwide
Voicemail (Recording, Notification, Retrieval)	Netwide
Presence	Netwide
Busy status	Netwide
Internal directory	Netwide
External directory	Local via .CSV import in each case
Search in external directories of other network nodes	Not possible
External offline directory	Central, via LDAP
Check voicemails of other subscribers (only if the subscriber has activated this feature)	Local, i.e., not by subscribers on other nodes

<b>myAgent (Contact Center)</b>	
Agents	Must be in the same network node
Agent status	Local
Incoming ACD calls	Via local PSTN trunks, SIP Providers and SIP-Q trunks
Voicemail (Recording, Notification, Retrieval)	Netwide
Presence	Netwide
Internal directory / Favorites	Netwide
External directory	Local via .CSV import in each case
Search in external directories of other network nodes	Not possible

<b>Central AutoAttendant</b>	
Dialing call numbers (by the caller)	CCV scripts enable the targeted dialing of stations in the network. The possible destinations are all call numbers of the internal directory
Dialing call numbers (preconfigured by the administrator)	Any destinations can be entered by the administrator in CCV scripts and dialed by the caller with a single-digit selection.
<b>External applications</b>	
Teledata Office	Netwide
TAPI 170	Netwide

TAPI 120	With CMD, network-wide; without CMD, local
CallBridge IP	Local
External CSTA applications	Netwide, i.e., the CSTA application uses ONE CSTA link at ONE system to communicate with the entire network
SIP Provider	Local
PSTN Provider	Local or decentralized connections to the individual network nodes
<b>Bandwidth requirements</b>	
For HFA, SIP clients	No bandwidth control
<b>Administration</b>	
	Network-wide using wizards, Expert mode

## 15.6.5 Configuring Scenario 2

The configuration of scenario 2 explains the steps required to set up a network of multiple OpenScape Office HX systems with the help of an example

### Prerequisites:

- The HiPath 3000 communication systems are already networked. See also the HiPath 3000 Service Manual and configuration examples.

---

**NOTICE:** The station numbers may need to be adapted. An open numbering scheme is not implemented!

---

- The associated HG 1500s are configured.
- At each HiPath 3000, a local OpenScape Office HX is already installed and configured.
- At each HiPath 3000, the **Networked CTI-Domain** flag is set.  
For more information, see *OpenScape Office V3, Administrator documentation*, *Installing OpenScape Office HX*

Call forwarding across nodes: For incoming calls over IP trunks, which have already been forwarded, no further forwardings to the voicemail box are executed. This is because no unique assignment to the voicemail box can otherwise be made

If cross-node deputy rules (referral extensions) are required, this must be set up via the profiles of the OpenScape Office stations or ringing groups. The corresponding cross-node calls are not signaled as forwarded in this case, but as DSS (direct station selection) calls. Call forwardings of the deputy are therefore forwarded to the voicemail box

Configuration for Node 1	
Node ID	6
HiPath 3000 IP address	198.6.126.250
HG 1500 IP address	198.6.126.251
OpenScape Office HX IP address	198.6.126.222
Dial Plan	100 - 199

Configuration for Node 2	
Node ID	5
HiPath 3000 IP address	198.6.128.230
HG 1500 IP address	198.6.128.231
OpenScape Office HX IP address	198.6.128.243
Dial Plan	200 - 299

Configuration for Node 3	
Node ID	4
HiPath 3000 IP address	198.6.128.12
HG 1500 IP address	198.6.128.13
OpenScape Office HX IP address	198.6.128.9
Dial Plan	300 - 399

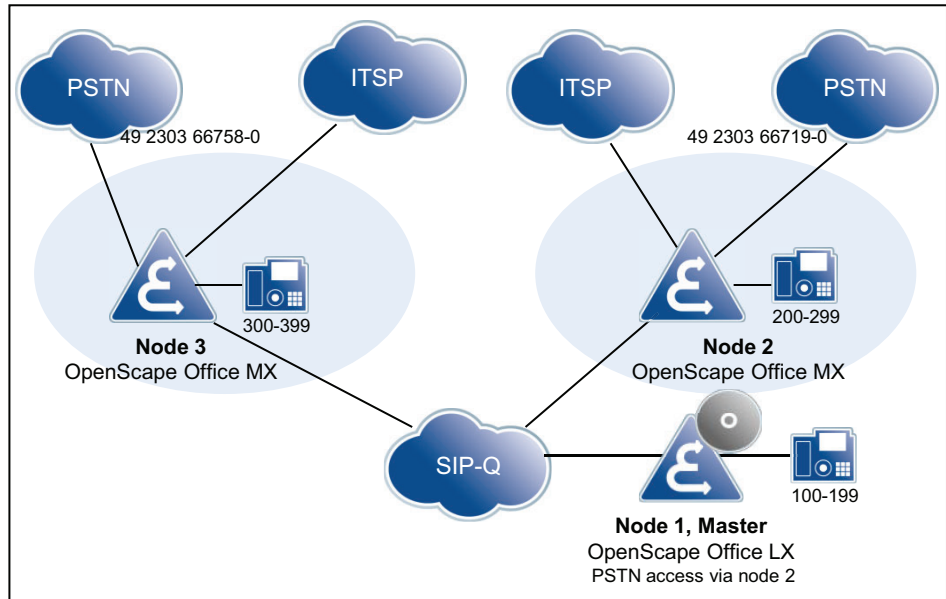
### 15.6.6 Scenario 3: Networking of OpenScape Office LX and OpenScape Office MX (Single Gateway)

Multiple OpenScape Office LX, OpenScape Office MX and OpenScape Office HX communication systems can be networked with one another. All IP stations of OpenScape Office LX are assigned to a specific gateway. The dial plan must be unique.

---

**NOTICE:** Call pickup groups and MULAPs can only be configured for stations connected to the same node.

---



Maximum configuration	
Maximum number of nodes	8
Maximum number of stations (OpenScape Office LX)	500
Maximum number of stations (OpenScape Office MX)	150
Maximum number of stations (OpenScape Office HX)	
Maximum number of stations in the network	1000

**NOTICE:** Larger networks can be configured on a project-specific basis (via OSIRIS).

### Network-wide Features for an Internetwork of Multiple OpenScape Office LX/MX/HX Systems

myPortal / myPortal for Outlook	OSO MX	OSO LX
Voicemail (Recording, Notification, Retrieval)	Netwide	
Presence	Netwide	
Busy status	Netwide	
Internal directory / Favorites	Netwide	
External directory	Local via .CSV import in each case	
Search in external directories of other network nodes	Not possible	
External offline directory	Central, via LDAP	



myAttendant	OSO MX	OSO LX
Attendant functions (automatic recall, intercept, display of forwarding station, ...)	Netwide	
Instant Messaging	Netwide	
Voicemail (Recording, Notification, Retrieval)	Netwide	
Presence	Netwide	
Busy status	Netwide	
Internal directory	Netwide	
External directory	Local via .CSV import in each case	
Search in external directories of other network nodes	Not possible	
External offline directory	Central, via LDAP	
Check voicemails of other subscribers	Local, i.e., not by subscribers on other nodes	

myAgent	OSO MX	OSO LX
Agents	Must be in the same network node	
Agent status	Local	
Incoming ACD calls	Via local PSTN trunks (not LX), SIP Providers and SIP-Q trunks	
Voicemail (Recording, Notification, Retrieval)	Netwide	
Presence	Netwide	
Internal directory / Favorites	Netwide	
External directory	Local via .CSV import in each case	
Search in external directories of other network nodes	Not possible	

Central AutoAttendant	
Dialing call numbers (by the caller)	CCV scripts enable the targeted dialing of stations in the network. The possible destinations are all call numbers of the internal directory
Dialing call numbers (preconfigured by the administrator)	Any destinations can be entered by the administrator in CCV scripts and dialed by the caller with a single-digit selection.
External TAPI applications	
Teledata Office	Netwide
TAPI 170	Netwide
TAPI 120	With CMD, network-wide; without CMD, local
CallBridge IP	Local

External CSTA applications	Netwide, i.e., the CSTA application uses ONE CSTA link at ONE system to communicate with the entire network	
SIP Provider	Local	
PSTN Provider	Local; network nodes without local PSTN trunks are reached via SIP-Q trunks of other nodes.	
Stations survivability when node fails	No	Yes, for OpenScape Office LX and HX, when OpenScape Office MX is used as a gateway
<b>Bandwidth requirements</b>		
For SIP-Q calls	See section on "Networking Requirements"	
For HFA, SIP clients	No bandwidth control	
<b>Administration</b>	Network-wide using wizards, Expert mode	
<b>CAR table generation</b>	Automatic update of the CAR table ( HiPath 3000, HG 1500) via the Networking wizard. The number of the voicemail box (voicemail call number ) is configured in CAR as a network node.	

### 15.6.7 Configuring Scenario 3

The configuration of scenario 3 explains the steps required to set up networking with the help of an example.

**Prerequisites:**

- A network plan is available. The network plan was used to ensure that every internal call number in the internetwork is only used once for closed numbering. Different station number lengths are allowed. DID station numbers may occur more than once (e.g., the CO station numbers 49 2302 66758 100 and 49 2302 66719 100 have the same DID No. 100).

---

**NOTICE:** The station numbers may need to be adapted. An open numbering scheme is not implemented!

---

- The IP network has been configured, and all nodes can be mutually pinged successfully
- All nodes have been upgraded to the same software version

Call forwarding across nodes: For incoming calls over IP trunks, which have already been forwarded, no further forwardings to the voicemail box are executed. This is because no unique assignment to the voicemail box can otherwise be made

If cross-node deputy rules (referral extensions) are required, this must be set up via the profiles of the OpenScape Office stations or ringing groups. The corresponding cross-node calls are not signaled as forwarded in this case, but as DSS (direct station selection) calls. Call forwardings of the deputy are therefore forwarded to the voicemail box.

## Using the Grace Period in an Internetwork

---

**NOTICE:** In an internetwork in which the grace period is being used, the CLA of OpenScape Office must always as be used as the central CLA!

---

Due to the different amounts of the upper limits, two different grace period files are required for OpenScape Office MX and OpenScape Office LX. The grace period file for OpenScape Office LX includes the MX base in addition to the LX base for networking scenarios.

In this scenario, whenever an OpenScape Office MX requests a license from a CLA of the OpenScape Office LX during the grace period, the limits of the OpenScape Office LX are used.

By contrast, if the CLA of the OpenScape Office MX were to be used instead, NO grace period would be granted to any requesting OpenScape Office LX, since no basis for OpenScape Office LX is included in this file.

### Setting up the Location Data for Node 1, OpenScape Office LX

Node 1		
G.-Location Country		49
G.-Location Local Network		2302
G.-Location System		66719
International Prefix		00
National Prefix		0
<b>Routes</b>		
Trk. Grp 1	Trunk code	0
Networking	2nd trunk code	0
<b>Routing parameters</b>		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 1 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

### Overview of Entries in the LCR for Node 1

Dial Plan		Route table			Dial Rule		
Name	Dialed digits	Route	Dedicated Gateway	Gateway ID	Dial Rule	Procedure	Type
Node 2 Internat	0C0049230266719-2Z	Networking	Mandatory	2	D49230266719E3A	Corp. Network	International
Node 2 NAT	0C0230266719-2Z						
Node 2 Strn.	0C66719-2Z						
Node 3 Internat	0C0049230266758-3Z	Networking	Mandatory	3	D49230266758E3A	Corp. Network	International
Node 3 NAT	0C0230266758-3Z						
Node 3 Strn.	0C66758-3Z						
CO	0CZ	Networking	Mandatory	2	E1A	Main network supplier	Unknown
Various	-Z	Networking	No		A	Corp. Network	Unknown

### Setting up the Location Data for Node 2, OpenScape Office MX

Node 2		
G.-Location Country		49
G.-Location Local Network		2302
G.-Location System		66719
International Prefix		00
National Prefix		0
<b>Routes</b>		
ISDN	Trunk code	0
Networking	2nd trunk code	0
<b>Routing parameters</b>		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 2 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

### Overview of Entries in the LCR for Node 2

Dial Plan		Route table			Dial Rule		
Name	Dialed digits	Route	Dedicated Gateway	Gateway ID	Dial Rule	Procedure	Type
Node 1 Internat	0C004923026 6719-1Z	Networking	Mandatory	1	D492302667 19E3A	Corp. Network	International
Node 1 NAT	0C023026671 9-1Z						
Node 1 Stn.	0C66719-1Z						
Node 3 Internat	0C004923026 6758-3Z	Networking	Mandatory	3	D492302667 58E3A	Corp. Network	International
Node 3 NAT	0C023026675 8-3Z						
Node 3 Stn.	0C66758-3Z						
CO	0CZ	ISDN	No		A	Main network supplier	Unknown
Various	-Z	Networking	No		A	Corp. Network	Unknown

### Setting up the Location Data for Node 3, OpenScape Office MX

Node 3		
G-Location Country		49
G-Location Local Network		2302
G-Location System		66758
International Prefix		00
National Prefix		0
<b>Routes</b>		
ISDN	Trunk code	0
Networking	2nd trunk code	0
<b>Routing parameters</b>		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 3 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

### Overview of Entries in the LCR for Node 3

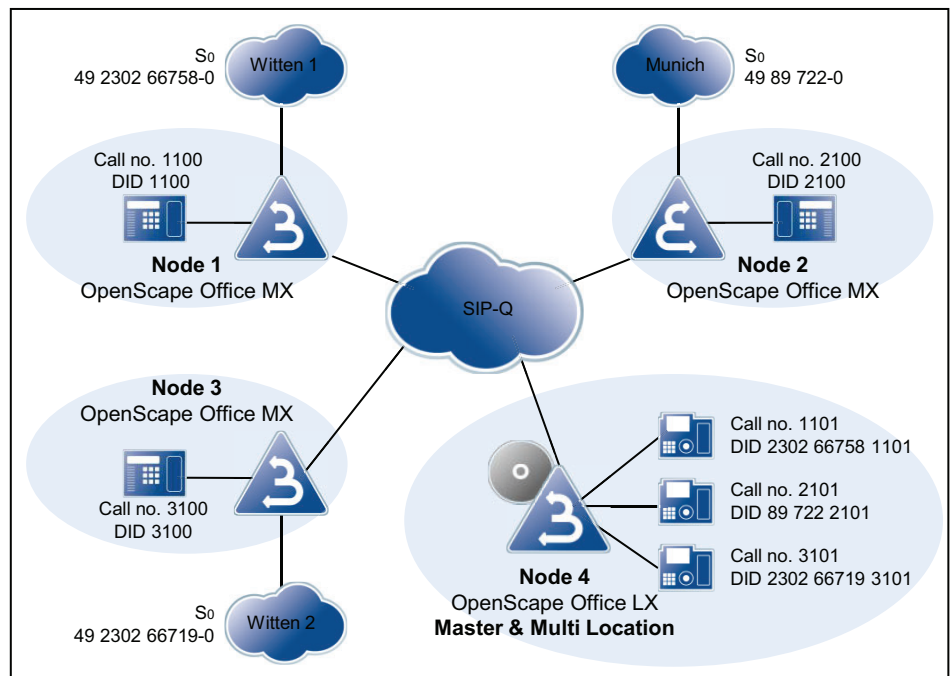
Dial Plan		Route table			Dial Rule		
Name	Dialed digits	Route	Dedicated Gateway	Gateway ID	Dial Rule	Procedure	Type
Node 1 Internat	0C0049230266719-Z	Networking	Mandatory	1	D49230266719E3A	Corp. Network	International
Node 1 NAT	0C0230266719-1Z						
Node 1 Stn.	0C66719-1Z						
Node 2 Internat	0C0049230266719-2Z	Networking	Mandatory	2	D49230266719E3A	Corp. Network	International
Node 2 NAT	0C0230266719-2Z						
Node 2 Stn.	0C66719-2Z						
CO	0CZ	ISDN	No		A	Main network supplier	Unknown
Various	-Z	Networking	No		A	Corp. Network	Unknown

#### Procedure to Set up Networking:

1. Configure the basic installation for node 1 (master)
2. Configuring Networking for Node 1
3. Configure the basic installation for node 2 (slave)
4. Configuring Networking for Node 2
5. Configure the basic installation for node 3 (slave)
6. Configure networking for node 3 (slave)
7. Verify the networking function for the master
8. Configure LCR for networking (node 1, master)
9. Configure LCR for networking (node 2)
10. Configure routes and routing parameters (node 3)
11. Configure routes and routing parameters (Trk. Grp. 64) (Node 3)
12. Configure LCR for networking (node 3)

## 15.6.8 Scenario 4: Networking Multiple OpenScape Office MX Systems with one OpenScape Office LX (Multi- Gateway)

Multiple OpenScape Office MX communication systems and one OpenScape Office LX can be networked with one another. All IP stations must be connected to the OpenScape Office LX. Each IP station of OpenScape Office LX is assigned to a specific gateway. The dial plan must be unique.



A multi-gateway network has only been released for cases where the network is located within one country.

Maximum configuration	
Maximum number of nodes	8
Maximum number of stations (OpenScape Office LX)	500
Maximum number of stations (OpenScape Office MX)	150
Maximum number of stations in the network	1000

**NOTICE:** Larger networks can be configured on a project-specific basis (via OSIRIS).

### Network-wide Features for an Internetwork of Multiple OpenScape Office MX and OpenScape Office LX Systems

myPortal / myPortal for Outlook	OSO MX	OSO LX
Voicemail (Recording, Notification, Retrieval)	Netwide	
Presence	Netwide	
Busy status	Netwide	
Internal directory / Favorites	Netwide	

**Networking OpenScape Office**  
Networking Scenarios

<b>myPortal / myPortal for Outlook</b>	<b>OSO MX</b>	<b>OSO LX</b>
External directory	Local via .CSV import in each case	
Search in external directories of other network nodes	Not possible	
External offline directory	Central, via LDAP	

<b>myAttendant</b>	<b>OSO MX</b>	<b>OSO LX</b>
Attendant functions (automatic recall, intercept, display of forwarding station, ...)	Netwide	
Instant Messaging	Netwide	
Voicemail (Recording, Notification, Retrieval)	Netwide	
Presence	Netwide	
Busy status	Netwide	
Internal directory	Netwide	
External directory	Local via .CSV import in each case	
Search in external directories of other network nodes	Not possible	
External offline directory	Central, via LDAP	
Check voicemails of other subscribers	Local, i.e., not by subscribers on other nodes	

<b>myAgent</b>	<b>OSO MX</b>	<b>OSO LX</b>
Agents	Must be in the same network node	
Agent status	Local	
Incoming ACD calls	Via local PSTN trunks (not LX), SIP Providers and SIP-Q trunks	
Voicemail (Recording, Notification, Retrieval)	Netwide	
Presence	Netwide	
Internal directory / Favorites	Netwide	
External directory	Local via .CSV import in each case	
Search in external directories of other network nodes	Not possible	

<b>Central AutoAttendant</b>		
Dialing call numbers (by the caller)	CCV scripts enable the targeted dialing of stations in the network. The possible destinations are all call numbers of the internal directory	
Dialing call numbers (preconfigured by the administrator)	Any destinations can be entered by the administrator in CCV scripts and dialed by the caller with a single-digit selection.	
<b>External TAPI applications</b>		



Teledata Office	Netwide	
TAPI 170	Netwide	
TAPI 120	With CMD, network-wide; without CMD, local	
CallBridge IP	Local	
External CSTA applications	Netwide, i.e., the CSTA application uses ONE CSTA link at ONE system to communicate with the entire network	
SIP Provider	Local	
PSTN Provider	Local; network nodes without local PSTN trunks are reached via SIP-Q trunks of other nodes.	
Stations survivability when node fails	No	Yes, for OpenScape Office LX, when OpenScape Office MX is used as a gateway
<b>Bandwidth requirements</b>		
For SIP-Q calls	See section on "Networking Requirements"	
For HFA, SIP clients	No bandwidth control	
<b>Administration</b>	Network-wide using wizards, Expert mode	

## 15.6.9 Configuring Scenario 4

The configuration of scenario 3 explains the steps required to set up a multi-gateway network with the help of an example.

### Prerequisites:

- A network plan is available. The network plan was used to ensure that every internal call number in the internetwork is only used once for closed numbering. Different station number lengths are allowed. DID station numbers may occur more than once

---

**NOTICE:** The station numbers may need to be adapted. An open numbering scheme is not implemented!

---

- The IP network has been configured, and all nodes can be mutually pinged successfully
- All nodes have been upgraded to the same software version
- At each HiPath 3000, the **Networked CTI-Domain** flag is set.  
For more information, see *OpenScape Office V3, Administrator documentation*, *Installing OpenScape Office HX*

Call forwarding across nodes: For incoming calls over IP trunks, which have already been forwarded, no further forwardings to the voicemail box are executed. This is because no unique assignment to the voicemail box can otherwise be made

If cross-node deputy rules (referral extensions) are required, this must be set up via the profiles of the OpenScape Office stations or ringing groups. The corresponding cross-node calls are not signaled as forwarded in this case, but as DSS (direct station selection) calls. Call forwardings of the deputy are therefore forwarded to the voicemail box

**Setting up the Location Data for Node 1**

Node 1		
G.-Location Country		49
G.-Location Local Network		2302
G.-Location System		66758
International Prefix		00
National Prefix		0
<b>Routes</b>		
ISDN	Trunk code	0
Networking	2nd trunk code	0
<b>Routing parameters</b>		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 1 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

**Overview of Entries in the LCR for Node 1**

Dial Plan		Route table			Dial Rule		
Name	Dialed digits	Route	Dedicated Gateway	Gateway ID	Dial Rule	Procedure	Type
Node 2 Internat	0C004989722-Z	Networking	Mandatory	2	D4989722E3A	Corp. Network	International
Node 2 NAT	0C089722-Z						
Node 2 Stn.	0C722-Z						
Node 3 Internat	0C0049230266719-Z	Networking	Mandatory	3	D49230266719E3A	Corp. Network	International
Node 3 NAT	0C0230266719-Z						
Node 3 Stn.	0C66719-Z						
Node 4 Internat	0C0049230266758-Z	Networking	NO		D230266758E3A	Corp. Network	National
Node 4 NAT	0C0230266758-Z						
Node 4 Stn.	0C66758-Z						

Dial Plan		Route table			Dial Rule		
Name	Dialed digits	Route	Dedicated Gateway	Gateway ID	Dial Rule	Procedure	Type
Various	-Z	Networking	No		BA	Corp. Network	Unknown
CO International	0C0049-Z	ISDN	No		D0E3A	Main network supplier	Unknown
CO	0CZ	ISDN	No		A	Main network supplier	Unknown

### Setting up the Location Data for Node 2

Node 2		
G-Location Country		49
G-Location Local Network		89
G-Location System		722
International Prefix		00
National Prefix		0
<b>Routes</b>		
ISDN	Trunk code	0
Networking	2nd trunk code	0
<b>Routing parameters</b>		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 2 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

### Overview of Entries in the LCR for Node 2

Dial Plan		Route table			Dial Rule		
Name	Dialed digits	Route	Dedicated Gateway	Gateway ID	Dial Rule	Procedure	Type
Node 1 Internat	0C00492302667 58-Z	Networking	Mandatory	1	D492302667 E3A	Corp. Network	International
Node 1 NAT	0C0230266758-Z						
Node 1 Stn.	0C66758-Z						

Dial Plan		Route table			Dial Rule		
Name	Dialed digits	Route	Dedicated Gateway	Gateway ID	Dial Rule	Procedure	Type
Node 3 Internat	0C0049230266719-Z	Networking	Mandatory	3	D49230266719E3A	Corp. Network	International
Node 3 NAT	0C0230266719-Z						
Node 3 Strn.	0C66719-Z						
Node 4 Internat	0C004989722-Z	Networking	NO		D89722E3A	Corp. Network	National
Node 4 NAT	0C089722-Z						
Node 4 Strn.	0C722-Z						
Various	-Z	Networking	No		BA	Corp. Network	Unknown
CO International	0C0049-Z	ISDN	No		D0E3A	Main network supplier	Unknown
CO	0CZ	ISDN	No		A	Main network supplier	Unknown

### Setting up the Location Data for Node 3

Node 3		
G.-Location Country	49	
G.-Location Local Network	2302	
G.-Location System	66719	
International Prefix	00	
National Prefix	0	
<b>Routes</b>		
ISDN	Trunk code	0
Networking	2nd trunk code	0
<b>Routing parameters</b>		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 3 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

### Overview of Entries in the LCR for Node 3

Dial Plan		Route table			Dial Rule		
Name	Dialed digits	Route	Dedicated Gateway	Gateway ID	Dial Rule	Procedure	Type
Node 1 Internat	0C0049230266758-Z	Networking	Mandatory	1	D49230266758E3A	Corp. Network	International
Node 1 NAT	0C0230266758-Z						
Node 1 Stn.	0C66758-Z						
Node 2 Internat	0C004989722-Z	Networking	Mandatory	2	D4989722E3A	Corp. Network	International
Node 2 NAT	0C089722-Z						
Node 2 Stn.	0C722-Z						
Node 4 Internat	0C004989230266719-Z	Networking	No		D230266719E3A	Corp. Network	National
Node 4 NAT	0C0230266719-Z						
Node 4 Stn.	0C66719-Z						
Various	-Z	Networking	No		BA	Corp. Network	Unknown
CO International	0C0049-Z	ISDN	No		D0E3A	Main network supplier	Unknown
CO	0CZ	ISDN	No		A	Main network supplier	Unknown

### Setting up the Location Data for Node 4

Associate location data with a dummy CO trunk (Trk. Grp. 1) incl. CO access code = 0 and Type = CO, since node 4 has no direct connection to a Central Office.

#### Node 4, dummy CO trunk

Node 4		
G.-Location Country		49
G.-Location Local Network		
G.-Location System		
International Prefix		00
National Prefix		0
<b>Routes</b>		
ISDN	Trunk code	0
Networking	2nd trunk code	0
<b>Routing parameters</b>		

Node 4		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 1 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

#### Node 4, Networking Route

Node 4		
G.-Location Country		
G.-Location Local Network		
G.-Location System		
International Prefix		00
National Prefix		0
<b>Routes</b>		
ISDN	Trunk code	0
Networking	2nd trunk code	0
<b>Routing parameters</b>		
Route	No. and type, outgoing	RNR type
Networking	National	Int/DID
ISDN	(No change in entry)	DID

#### Overview of Entries in the LCR for Node 4

Dial Plan		Route table			Dial Rule		
Name	Dialed digits	Route	Dedicated Gateway	Gateway ID	Dial Rule	Procedure	Type
Node 1 Internat	0C0049230266758-Z	Networking	Mandatory	1	D49230266758E3A	Corp. Network	International
Node 1 NAT	0C0230266758-Z						
Node 1 Stn.	0C66758-Z						
Node 2 Internat	0C004989722-Z	Networking	Mandatory	2	D4989722E3A	Corp. Network	International
Node 2 NAT	0C089722-Z						
Node 2 Stn.	0C722-Z						

Dial Plan		Route table			Dial Rule		
Name	Dialed digits	Route	Dedicated Gateway	Gateway ID	Dial Rule	Procedure	Type
Node 3 Internat	0C00498923026 6719-Z	Networking	Mandatory	3	D492302667 19E3A	Corp. Network	International
Node 3 NAT	0C0230266719-Z						
Node 3 Stn.	0C66719-Z						
Various	-Z	Networking	NO		A	Corp. Network	Unknown
CO	0CZ	Networking	MULTI- GATEWAY	1	E1A	Main network supplier	Unknown

**Procedure to Set up Networking:**

1. Configure the basic installation for node 4 (master)
2. Configure networking for node 4 (master)
3. Configure the basic installation for node 1 (slave)
4. Configure networking for node 1 (slave)
5. Configure the basic installation for node 2 (slave)
6. Configure networking for node 2 (slave)
7. Configure the basic installation for node 3 (slave)
8. Configure networking for node 3 (slave)
9. Verify the networking function for the master
10. Configure a multi-gateway for node 4 (master)
11. Configure routes and routing parameters (node 1, slave)
12. Configure LCR for networking (node 1, slave)
13. Configure routes and routing parameters (node 2, slave)
14. Configure LCR for networking (node 2, slave)
15. Configure routes and routing parameters (node 3, slave)
16. Configure LCR for networking (node 3, slave)
17. Configure routes and routing parameters (node 4, master)
18. Configure LCR for networking (node 4, master)

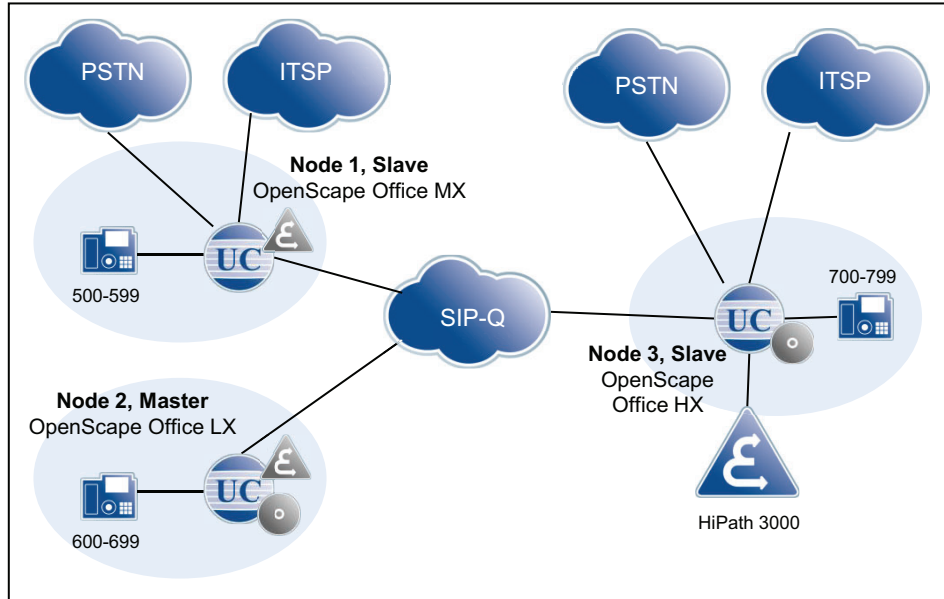
### 15.6.10 Scenario 5: Networking OpenScape Office LX/MX/HX and HiPath 3000

OpenScape Office MX, OpenScape Office LX and HiPath 3000 with OpenScape Office HX can be networked. To do this, the dial plan must be unique in the network, and either the HiPath 3000 or OpenScape Office LX must be used as a gateway for OpenScape Office MX.

---

**NOTICE:** Call pickup groups and MULAPs can only be configured for stations connected to the same node.

---



**Prerequisites:**

---

**NOTICE:** The station numbers of HiPath 3000 may need to be adapted. Open numbering is not supported for networking with HiPath 3000!

---

- The associated HG 1500s are configured.
- A local OpenScape Office HX is already installed and configured at the HiPath 3000.

Configuration for Node 1 (OpenScape Office MX), Slave	
Node ID	1
OpenScape Office MX, IP address	198.6.128.244
Dial Plan	500 - 599

Configuration for Node 2 (OpenScape Office LX), Master	
Node ID	2
OpenScape Office LX, IP address	198.6.128.245
Dial Plan	600 - 699



<b>Configuration for Node 3 (OpenScape Office HX), Slave</b>	
Node ID	3
HiPath 3000 IP address	198.6.128.230
HG 1500 IP address	198.6.128.231
OpenScape Office HX IP address	198.6.128.247
Dial Plan	700 - 799

## 15.7 Synchronization Status in the Internetwork

In an internetwork, the synchronization status is displayed in the Admin Portal, and the registration status of each node is indicated by colored buttons.

### Display of the Synchronization Status

Display	Color	Meaning for the master	Meaning for the slave
Synchronization status (display on the home page of the Admin Portal)	Red	-	The IP address of the master node is configured, but the slave system could not register. The slave tries to register with the master at cyclical intervals.
	Yellow	-	The slave is registered with the master, but the call numbers are not consistent in the internetwork. This may occur after a backup/restore or after the first registration.
	Green	If a node is configured as the master, the status appears as green.	
Registration status of the individual nodes (displayed in the Network>Node View dialog)	Red	The slave is configured, but the system has never registered.	The slave is configured, but the system has never registered.
	Green	The system is already registered. HiPath 3000 systems are always green, since they do not require registration.	The system is already registered. HiPath 3000 systems are always green, since they do not require registration.
Alive (displayed in the dialog Network>Node View)	Red	Node-specific view of the internetwork: all nodes that are marked in red cannot be reached. The reasons may be network problems or a failure in the communication system. This display also shows the status of the HiPath 3000 nodes.	
	Green	The (external) node can be reached via the network. The own node is always shown in green.	

## 15.7.1 Manual Synchronization in the Internetwork

If the automatic synchronization of the configured call numbers and names (internal or DID numbers) has not been completed in the other systems of an internetwork, a manual synchronization can be initiated.

The synchronization process only transfers changes in the configuration.

If the status indicator in the Admin Portal appears as "red", the Synchronization button can be pressed to try and manually synchronize the data with the master.

In cases where already configured systems in the network can no longer make calls, the potential cause for the problem must be found elsewhere. If the Alive status of individual nodes appears as "red", this indicates network problems or other reasons why the node cannot be reached in the network. In such cases, activating the Synchronization button will not improve the situation.

### Master

When activated on the master node, the slave nodes are requested to update the phone numbers and names of the system from the master.

### Slave

When activated on a slave node, the station numbers and names of the system are updated on the master. At the same time, the slave node is registered again at the master node.

## 15.8 Survivability (Only LX)

Survivability is the capability of a network to maintain service continuity in the presence of faults within the network. Survivability mechanisms to protect and restore a connection have been implemented for OpenScape Office LX to avoid service interruptions.

If an OpenScape Office MX is networked with OpenScape Office LX, and a network node fails, the subscriber at the LX system is rerouted to a stable network node of the OpenScape Office MX system. This provides continuity for basic telephony; however, the features of applications such as myPortal will be temporarily unavailable.

The time for switching to the standby system can last up to 30 minutes.

If the OpenScape Office LX fails, an attempt is first made to reach it again for a fixed time period (10 minutes; cannot be changed). It is only when this time has expired that the phones intended for this purpose are registered at the OpenScape Office MX. The current statuses of the registered phones can be viewed in Expert Mode > Diagnosis Logs.

The survivability settings are configured at the OpenStage telephones. If OpenScape Office LX fails, the phones will initially try to reach it again several times. A time-out or how often the phone tries to log in again can be configured via "System Redundancy" setting on the Administration menu of the telephones.

The default setting for the timeout is 30 seconds with one retry. After that, the telephones register at the standby gateway of OpenScape Office MX. The automatic registration back at the OpenScape Office LX is also configured at the OpenStage telephones.

The following prerequisites must be satisfied for this survivability functionality:

- A sufficient number of free ports must be available at the OpenScape Office MX for the phones connected to the OpenScape Office LX that need to be "saved" when a network node fails.
- These free ports at the OpenScape Office MX must not have any name and call number assigned to them. They must be configured and licensed as system telephones.

---

**NOTICE:** The survivability function can only be set up at the master node, since the **Secondary Gateway** parameter (which is needed for it) can only be set up there. Consequently, in cases where there are multiple OpenScape Office LX systems in an internetwork, only a single OpenScape Office LX can use survivability.

---

## 16 Application Connectivity

Application connectivity is supported by the system, e.g., with XMPP and Application Launcher.

### 16.1 XMPP

XMPP (Extensible Messaging and Presence Protocol) is an Internet standard for XML routing and is used mainly for instant messaging. XMPP enables the integration of external communication partners for instant messaging and the mapping between the presence status and the XMPP status.

XMPP is supported for the following clients:

- myPortal for Desktop
- myPortal for Outlook
- myAttendant

An external XMPP communication partner may be a Google Talk user, for example. The integrated Openfire XMPP server is externally addressed via port 5269 by default. The connections to other XMPP servers can be secured with TLS, provided they support TLS. Port 5222 is used to communicate internally with clients. The ports must be opened in the appropriate firewall. XMPP is disabled in the system by default and can be configured by the administrator. The required configuration of XMPP in each client can be performed by the subscriber. External XMPP gateway servers are not supported. XMPP IDs of external communication partners must conform to the pattern `xmpp:john.public@oso.example-for-a-domain.com` and may be present at the following locations:

- external directory
- External offline directory (LDAP)
- Personal directory (myPortal for Desktop)
- Outlook contacts (myPortal for Outlook)  
IM address field
- Favorites

---

#### Related Topics

- [Instant Messaging](#)

### 16.2 Application Launcher

Application Launcher is a Java-based Windows application for the call-related control of other applications on client PCs. Application Launcher can be used in a CRM system, for example, to automatically open the contact form for each caller.

Application Launcher provides the following features:

- Looking up call-related information on a phone number in either the Directory Service or in system directories
- Configurable screen pops for incoming calls with call-related information and buttons for user actions
- Launching Windows applications or web applications for incoming and outgoing calls
- Transfer of call-related information to applications (e.g., phone number, name of the caller, customer ID)

---

#### **Related Topics**

- [Service Center - Download Center](#)

## **16.2.1 Prerequisites for Application Launcher**

In order to use Application Launcher, the client PC must be equipped with the appropriate hardware and software.

#### **Operating System**

Application Launcher can be used in combination with the following operating systems:

- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows XP

Local administration rights on a client PC are required for the installation, but not for automatic updates.

#### **Windows Update**

The PCs always need the current status of all available updates, including Service Packs.

#### **Additional Software**

Sun Java >= 1.6.x (see **Service Center > Download Center**)

#### **Web Services for Mobile Phones**

Web services for mobile phones has been enabled in the system for the system connection. The ports configured in the system must be open in the firewalls on the LAN and the client PCs.

#### **Directory Service**

If Application Launcher is to use the data from the Directory Service, the Directory Service must be configured in the system. The port configured for this in the system must be open in the firewalls on the LAN and the client PCs.

---

**Related Topics**

- [Configuring myPortal for Mobile and Mobility Entry \(LX/MX\)](#)
- [OpenScape Office Directory Service](#)

## **16.2.2 Profile with Configuration Data for Application Launcher**

A profile with configuration data for Application Launcher enables the easy and fast configuration of Application Launcher on all client PCs.

The profile contains all the configuration data, except for the system connection and the user data. As soon as Application Launcher has been fully configured for an initial user, as an administrator, you can make that profile with the Application Launcher configuration data available in the communication system. All other users can then perform the configuration of Application Launcher by importing this profile.

## 17 Auxiliary Equipment

Auxiliary equipment consists of external devices (such as a fax device or door opener) that are connected to the interfaces of the communication system. Using an IP-enabled camera, the video surveillance solution Gate View can be deployed.

### 17.1 Fax Devices and Fax Servers (MX)

The system supports fax devices and fax servers at a/b interfaces and at S<sub>0</sub> or S<sub>2M</sub> interfaces (ISDN).

#### Info on Receiving a Fax

The a/b or ISDN port must be configured as Fax. An incoming fax message on an external device can be signaled by an LED.

#### Availability in the System with Previous Fax Numbers

Since it is not possible to forward an analog fax device to a fax number in the system, the following workaround exists: The previous fax number is configured in the system and receives the incoming fax messages. For the analog fax device, a port is configured with the previous number as the CLIP. The Configurable CLIP check box must be selected for this purpose. Outbound fax messages from the fax device show the previous number as the sender, unless sent to internal recipients. Internal stations see the internal number of the fax device.

#### Fax Servers

Fax servers can be connected via S<sub>0</sub> (GMS/GMSA module) or S<sub>2M</sub> (GME module) interfaces as follows:

- All S<sub>0</sub> trunks of a Fax server must be connected to the same GMS/GMSA module. Consequently, up to 8 B channels are available for a Fax server. Additional Fax servers (again with 8 B channels each) can be connected via further GMS/GMSA modules.
- S<sub>2M</sub> Fax servers must support the QSIG protocol. The pure "ISDN CO mode" is not supported by the GME module.

#### Sending Fax Messages with Fritz!Fax

In order to send fax messages with Fritz!Fax via the S<sub>0</sub> interface, the S<sub>0</sub> station must be configured as the station type Fax.

#### System-Specific Information

Every GMAA gateway module allows the connection of two parallel analog fax devices.

## 17.2 Entrance Telephone and Door Opener (MX)

Doorbell activation is signaled as a call at a specified phone (ring destination). A voice connection is set up if the subscriber accepts the call. The ring destination user can then activate the door opener on his or her phone.

The call is intercepted if the entrance telephone ring destination is not reachable. If the intercept destination is not free either, a system search is performed across all system phones.

---

**INFO:** The night service is ignored when signaling a door call.

---

Configuration options:

- **Door opener:**  
The door opener is configured via an a/b (T/R) interface and the entrance telephone must be connected via an adapter. The subscriber can then open the door by simply pressing a button on the phone during the connection with the ring destination.
- **DTMF:**  
This setting specifies whether the door opener is activated by a DTMF transmitter (DTMF: dual-tone multifrequency), that is, if the ring destination can open the door with DTMF suffix-dialing.
- **Call Forwarding (CF):**  
This specifies whether the call from the entrance telephone should be forwarded to an external call forwarding destination.

## 17.3 OpenStage Gate View

OpenStage Gate View is a user-friendly entry-level security solution that presents real-time video images on your OpenStage telephone, PC or - when on the road - the iPhone.

This enables you to monitor your entrance area and to control and provide secure access to your corporate premises.

The most important operating steps for users of OpenStage Gateview at an OpenStage 60, an iPhone or a web client are explained in the document *Quick Reference Guide*(Ref.No. A31003-P1120-U100-\*-19).

### 17.3.1 Legal Framework

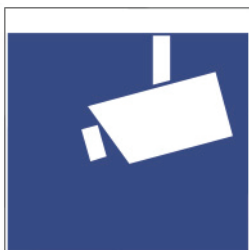
Video surveillance refers to the monitoring of locations with optical electronic equipment and is also known as "optical room surveillance system". When using video surveillance, the applicable country-specific regulations and laws must be observed.



### Country-specific Legal Situation

The legal framework for video surveillance in publicly accessible areas varies among countries. You should therefore check the legal situation in your own country.

Areas monitored through video surveillance may need to be identified by a symbol. A corresponding symbol is usually supplied by the camera manufacturer and may look something like this:



## 17.3.2 Components

The usage of OpenStage Gate View requires three components: *Source*, *Processing* and *Presentation*. All components are connected through a local area network.

### Source

The video source provides the video signal. Cameras from different manufacturers can be used as the source. Depending on the camera-type, a video converter is additionally required.

- IP cameras
- Analog cameras (in combination with composite/IP converter)
- Entrance telephones with integrated camera

The interface for processing the video signal is always an IP video stream.

If a commercial network camera is used as a video source, a LAN with Power over Ethernet (PoE) may be required to connect the camera in some circumstances.

### Processing

To process the video signal, the appropriate server software is required. Depending on which communication system is used, the server may be maintained separately on a plug PC or integrated in the communication system.

- HiPath 3000  
A separate Plug PC is required (reference number: S30122-X8001-X83).
- OpenScape Office MX/LX/HX  
As of Version V3R3, the server software is already integrated in these communication systems. No additional hardware for processing the video signal is required.

### **Presentation**

The presentation can occur on different devices. The following devices are intended for presenting the video signal.

- Devices der OpenStage Systems Family as of Version V2R0.48.0.
  - OpenStage 60 HFA
  - Octophon 660 HFA
- iPhone  
Using the iPhone App *OpenStage Gate View*, available in the Apple AppStore.
- Web Browsers  
Presentation within the web-based administration software *Video Surveillance System* or as Web Client.

The recording of the video signal at the server can be controlled from some devices.

## **17.3.3 Function Overview**

By using an OpenStage 60/80 HFA telephone, Openstage Gate View makes it possible to offer a powerful combination of the best voice quality, video transmission, and door opener functionality on one device.

[Image of overview ???]

### **Features and benefits**

- Video recording on network drive (OpenScape Office) or USB stick (Plug PC).
- Different displays of multiple video signals on OpenStage telephones, mobile phones (iPhone app) or web clients.
- Simple, password-protected administration via web-based, multilingual interface.
- Flexible licensing concept.
- Integrates into already existing investments (equipment and infrastructure).

### **Capacity Limits**

Depending on the platform on which the server software is running, a different number of cameras and devices can be used for the display.

- Plug PC:
  - 1 camera
  - 2 OpenStage telephones
  - 1 iPhone or web client
- OpenScape Office MX:
  - 2 cameras
  - 10 OpenStage telephones
  - 10 iPhones or web clients
- OpenScape Office LX/HX:
  - 8 cameras

- 20 OpenStage telephones
- 10 iPhones or web clients

In addition, the maximum number of usable cameras depends on the licenses procured. In this context, a license corresponds to one camera.

## 17.3.4 Menu

This section provides an overview of the menu of the administration software and describes how to set up individual features and parameters.

An overview of the menu functions is shown below.

### **Overview**

Displays detailed information about each installed camera with editing options.

### **Surveillance**

Displays the video image for each installed camera.

### **Recording**

Enables the configuration of various parameters used to record the video image.

### **Status**

Displays information about the hardware and software of the OpenStage Gate View system.

### **Administration**

- **Maintenance**  
Enables the deletion of software and user data.
- **Recording Configuration**  
Enables the configuration of the recording device (recorder) and the recording mode.
- **Entrance Telephone (Door Opener)**  
Enables the configuration of an entrance telephone with assignment of camera and telephone.
- **User Management**  
Provides information and settings options for users, profiles and sessions.
- **Cameras**
  - **Installed Cameras**  
Shows all installed cameras as a list.
  - **Add Camera (Auto Discovery)**  
Displays a list of all detected cameras to automatically install a camera.
  - **Add Camera (Manual)**  
Enables the manual installation of a camera.

- [Name of the camera]:  
Displays detailed information on the selected camera with editing options.
- **Telephones**
  - **Installed Phones**  
Shows all installed phones as a list.
  - **Add Phone (Auto Discovery)**  
Displays a list of all detected phones to automatically install a phone.
  - **Add Phone (Manual)**  
Enables the manual installation of a phone.
  - [Name of the telephone]  
Displays detailed information on the selected phone with editing options.
- **Log**
  - **View Log**  
Displays the current log file with download option.
  - **Download Log**  
Downloads the current log file.

### 17.3.5 Initial Setup of OpenStage Gate View

In order to set up the camera and display device, some minimal configuration is required at the OpenStage Gate View server. The setup is usually completed within a few minutes. Depending on the LAN infrastructure and the components used, additional installation steps may be required.

- First, a camera and a phone are assigned to the server configuration.
- After this, an OpenStage 60 telephone receives the software required to present the video image and is configured to operate the video function.

If the automatic detection of the camera or OpenStage 60 telephone fails, you also have the option to manually add these devices to the configuration.

### 17.3.6 OpenStage Gate View Video Recording

OpenStage Gate View enables you to record a video and review it later at any time and as often as desired.

#### **Recorder / Storage Location**

If you are using OpenStage Gate View with the OpenScape Office MX/LX/HX communication system, the recordings will be stored on a network drive.

When using a Plug PC (e.g., with a HiPath 3000), the recordings are stored on a USB memory stick that is inserted into the plug PC.

Both the storage location and the file name of the recording can be set up.

### Quality and Quantity of the Recording Data

Recordings can be created in varying quality. Recordings with high quality take up more space than low quality recordings.

To limit the space used on storage media for the recording, the maximum duration of the recording can be set in advance.

## 17.3.7 OpenStage Gate View User Management

As an administrator, you can enable the customized usage of OpenStage Gate View by optionally setting up further users in addition to the default user **admin**.

With these personal user accounts, you can not only obtain a better overview as an administrator, but also implement more security in the use of OpenStage Gate View:

- Each user has a personal account with a user name and password.
- You can temporarily block users.
- You can enforce password changes.
- You can view the session data of users with their respective IP addresses and the time of last use and can optionally end active sessions.
- Using the log file, you can review past activities of different users.

You can create any number of users, edit user data and remove users from the configuration permanently.

## 17.3.8 OpenStage Gate View Server Administration

As an administrator, you should keep track of the extensive server data and delete the information that is no longer required.

- You can view both the version number of the installed server software as well as the maximum number of devices and licenses.
- You can optionally delete phone and user data permanently.
- You can view the log data of the OpenStage Gate View server and download it.

## 17.3.9 OpenStage Gate View Customizations

Most administration tasks have been automated in order to minimize the customized settings that need to be made manually. However, due to the large number of different LAN configurations, it may be necessary to make some individual settings by hand.

- You can add and remove a camera to and from configuration manually.
- You can add and remove a telephone to and from configuration manually.
- On an OpenScape Office system, you can disable the entire OpenStage Gate View server.

### **Adding a Camera Manually**

Many different camera types have already been stored with the appropriate access data. In such cases, only the camera type needs to be selected, and the IP address adjusted if required.

If the camera is not included in the list, the required access parameters, i.e., the camera IP, port, user name and password can also be entered as a URL. The format usually looks like this:

```
http://<user-name>:<password>@<camera-IP>:<port>
```

## 18 Accounting (LX/MX)

Accounting offers call detail recording, the display of call charges and call duration, as well as cost control and accounting tools.

### 18.1 Call Detail Recording (LX/MX)

Call Detail Recording offers Call Detail Recording Central (CDRC) and Account Codes.

#### 18.1.1 Call Detail Recording Central (LX/MX)

The system can also record the call charge details for all calls of its own system and transfer this information to a PC for evaluation (Call Detail Recording Central, CDRC).

For every completed call and/or every incoming call, a call detail record is created. The call detail records are not numbered. A separate call detail record is recorded for a new call segment (for example, as a result of transferring or forwarding to another subscriber). In the case of networked systems, the call detail record is saved at the system which caused the charges. Charges for internal network connections are not recorded.

The administrator can activate the following options:

- Compressed output (no padding with blanks)
- Suppress last four digits  
The last four digits of the destination are suppressed.
- Log incoming calls
- Call Duration
- On Ringing  
Start logging on beginning the call
- Output MSN  
The used MSN is logged.
- Decimal format
- Display amounts instead of units
- Outgoing without connection

For example, this gives the calling party proof that the destination station did not accept the attempted call (marked in the output log with the call time 00:00:00). This option applies to ISDN connections and to all subscribers.

Recording is not performed for

- premature termination of the call attempt.
- call attempts that are not allowed (LCR, denied lists).

If call charges accrue before the call is set up (as occurs in Austria, for instance), these are recorded, irrespective of whether or not "Outgoing without connection" is set.

Call Detail Recording Central takes connections via QSIG trunks into account only if a trunk code has been configured for them.

The system can display the call charge data using HTTPS in a web browser (compressed or uncompressed output format) or transfer it to a LAN TCP client. (Compressed Output Format)

You can evaluate the call details with the application TeleData Office V4.0.

Call charge pulses are converted into monetary amounts using the call charge factor that is set by the administrator as the currency amount per call charge unit/pulse.

**Compressed Output Format**

A call detail record in the compressed output format contains the following fields delimited by |, i.e., without blanks.

Field position	Length	Description
1	8	Date (at end of call)
2	8	Time (at end of call)
3	3	Number of seized trunk
4	16	Internal station number
5	8	Duration of incoming call
6	8	Duration of call
7	Max. 25	DID call number
8	11	Call charge pulse/amount
9	2	Additional information (such as incoming call, outgoing call, transferred call, conference, DISA, call setup charges)
10	Max. 11	Acc. code
11	Max. 11	Only for a point-to-multipoint connection: used MSN
12	6	LCR access code, CO access code
13	2	LCR route used, dial rule
14		Additional data in U.S.: <ul style="list-style-type: none"> <li>• PRI Nodal Service</li> <li>• PRI WATS band</li> <li>• PRI Carrier Identification Code</li> </ul>

Examples of call detail records:

- Outgoing call:  
 31.03.08|14:18:02|3|107||00:00:02|820609|0.06|2|||0|1|
- Incoming call:  
 31.03.08|14:09:51|3|107|00:02|00:00:00|820635||1||||



### Uncompressed Output Format

Unavailable information and missing characters are replaced by blanks. The uncompressed output format is particularly suitable for printing and is only available for output via HTTPS.

Field position	Character position, Length	Description	Alignment
1	1-8 (8)	Date (at end of call): DD.MM.YY  (DD = day: value range 01 ... 31, MM = month: value range 01 ... 12, YY = year: value range 00 ... 99)	Left
2	9-16 (8)	Time at the end of a call segment or an unanswered incoming call: hh:mm:ss a  (hh = hours: value range 00 ... 23, mm = minutes: value range 00 ... 59, ss = seconds: value range 00 ... 59)	Left
3	17-19 (3)	Trunk: trunk number  Value range 1 ... 250	Right
4	20-25 (6)	Stations: internal station number, value range 0000000 ... 9999999.  For unanswered calls, this is the last station called (e.g., a hunt group, call forwarding, call forwarding—no answer). For group calls, this is the last station entered. For answered calls, the station that accepted the call is shown. A programmed SNO prefix (with networking only) is not output.  If the internal numbering was converted to a maximum 7-digit numbering plan, the converted station number is output.  The internal station number may be preceded by a max. 7-digit node number. If the total resulting from the node number and the station number is greater than seven, only the last seven digits of the number are output.	Right
5	26-30 (5)	Ring duration of an incoming external call: mm:ss  (mm = minutes: value range 00 - 59, ss = seconds: value range 00 - 59)  The display occurs for all incoming calls, provided the output of the ring duration has been configured in the system. If a counter overflow occurs (duration > 59:59), "59:59" is output. A change in date or time during system operation can result in this situation.  In the case of an incoming call to a busy station, the ring duration is "00:00".	Left
6	31-38 (8)	Duration of the call or call segment: hh:mm:ss  (hh = hours: value range 00 ... 23, mm = minutes: value range 00 ... 59, ss = seconds: value range 00 ... 59)  If a connection has not been established for an incoming call, 8 blanks are output here. If a counter overflow occurs (duration > 23:59:59), "23:59:59" is output.	Left



Field position	Character position, Length	Description	Alignment
9	75-76 (2)	<p>Information element: additional information</p> <p>Value range: 0 - 9</p> <p>Meaning:</p> <ul style="list-style-type: none"> <li>• 1 = Incoming connection (Voice / 3.1 kHz Audio Call)</li> <li>• 2 = Outgoing connection (Voice / 3.1 kHz Audio Call)</li> <li>• 3 = Incoming connection (Other Services)</li> <li>• 4 = Outgoing connection (Other Services)</li> <li>• 5 = Incoming connection, routed</li> <li>• 6 = Outgoing connection, routed</li> <li>• 7 = int/ext/ext conference with incoming connection / transit through external transfer</li> <li>• 8 = Conference with outgoing connection / Transit through external transfer</li> <li>• 9 = Outgoing connection via call forwarding to external destination</li> <li>• 0 = Call information (caller list) is output immediately on receiving an incoming call (the output can be suppressed). This can be used, for instance, for a database search from a PC. In cases where multiple stations are called, a separate line is output for each individual station (without ring duration, call duration, call charge information).</li> <li>• +20 = Offset as a code for call setup charges (connection setup without call duration)</li> <li>• +30 = Offset as a code for a follow-up data record in the case of <ul style="list-style-type: none"> <li>– a call duration &gt; 24 h.</li> <li>– contiguous call segments with the same line/station number (e.g., after transferring a call or clearing a conference).</li> </ul> </li> <li>• +40 = Offset for a data record with transit code (by an extension in the subsystem). Can occur in combination with offset +30.</li> <li>• +50 = Offset as a code for DISA calls</li> <li>• +70 = combination of offsets +30 and +40</li> </ul>	Right

Field position	Character position, Length	Description	Alignment
17	109-112 (2)	Only in the case of a non-activated extended data set: End of Line control character (Carriage Return CR, Line Feed LF)	-
18	113-137 (25)	For activated extended data set: Dialed or received station number (if available): nnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnn  (n = dialed or received character: value range 0 ... 9)  The output occurs for incoming and outgoing calls, if activated.  For outgoing calls, the station number actually sent to the Exchange (following LCR conversion if required) is displayed.  For incoming calls, the internal station number for the desired station, i.e., the first station dialed, is displayed.	Left
19	138-139 (2)	End of Line control character (Carriage Return CR, Line Feed LF)	-

### 18.1.2 Enabling or Disabling Call Detail Recording (LX/MX)

The **Call Detail Recording** wizard can be used to activate or deactivate the central recording of call charges and to configure account codes.

### 18.1.3 Account Codes (LX/MX)

Account codes (Acc. code) enable call charges or other connection data to be evaluated on an account-specific basis

ACCT is used in combination with Call Detail Recording Central (CDRC) and is available to all subscribers.

The subscriber can enter an ACCT at the phone before or after dialing. It is not possible to dial from a client with ACCT enabled.

An ACCT entered during a conference with external stations is assigned to all participating calls and trunks.

The administrator can set whether an ACCT should be saved for redialing.

The personal directory (also called a phonebook) can save the code for the ACCT feature + an ACCT + a phone number together in one entry:

#### **ACCT Input Procedure**

The administrator defines the ACCT input procedure in the LCR dial plan:

- **Mandatory**  
The ACCT must be entered before setting up the connection (before or after seizing a route).
- **Optional**  
The ACCT may optionally be entered before setting up the connection. IP phone clients support input during a call, including incoming calls.

#### **ACCT Checking Procedure**

The system can check the validity of an ACCT entered for the following types:

- **List verification**  
Only predefined ACCTs are valid. After a valid ACCT has been entered, the subscriber can immediately continue dialing. The system rejects an invalid ACCT. "Incorrect entry" appears on the display and a negative confirmation tone is output.
- **Check number of characters**  
All ACCTs that are theoretically possible with the configured number of digits are valid. After a valid ACCT has been entered by the subscriber, he or she can immediately continue dialing.
- **No Check**  
The validity of the ACCT is not checked. ACCTs with less than 11 digits must be separated from the other digits dialed by the subscriber with "#". For ISDN phones, this variant always requires a 11-digit account code; otherwise, no dialing occurs.

If the subscriber determines during a call that the assigned ACCT is not correct, he or she can enter some other ACCT. The system will overwrite the currently set account code. Central call detail recording sends a call detail record after every segment. therefore, previously completed call segments will be identified with the old account code number.

## **18.2 Display of Call Charges and Call Duration (LX/MX)**

The call charges and call duration can be shown on the display of system telephones in various ways.

### **18.2.1 Advice of Charges at Station (LX/MX)**

The system can display call detail information about the current external call as a currency amount (GESp) on the phone's display.

The amount is added up in call charge memory. A call charge factor is used to calculate the currency amount on the basis of the call charge units/pulses received by the network provider. The network provider must support the Advice Of Charge (AOC) feature.

The call detail information can be transmitted at the following times:

## Accounting (LX/MX)

### Display of Call Charges and Call Duration (LX/MX)

- On starting the call and possibly during the call (AOC-S)
- During the call (AOC-D)
- At the end of the call (AOC-E)

At the end of the call, the display shows the final charges for the completed call for about 5 seconds, provided the subscriber has not started some other action.

Call charges for the current call are always displayed when toggling.

If a call is returned as a recall in the case of an unscreened transfer, the overall amount is displayed and calculated.

A subscriber to whom a call is transferred will only see and be charged for the relevant amount from that point in time during the call.

The call charge factor is set by the administrator as a currency amount (including any necessary surcharges) for each call charge unit/pulse.

## 18.2.2 Call Duration Display on Telephone (LX/MX)

The system can show the duration of outgoing and incoming external calls on the phone's display.

The format is HH:MM:SS.

### System-Specific Information

The feature is a system-wide option (default: disabled).

If the elapsed time display is disabled, the phone's display shows the PSTN's call detail information instead. If there is no call detail information available, the display shows the caller's number (if known).

## 18.2.3 Call-Charge Display with Currency (not for U.S.) (LX/MX)

The system can display the currency amount transmitted for the current external connection by the network provider on the display of the telephone.

The amount is added up in call charge memory. The network provider must support the transfer of currency amounts with the Advice Of Charge (AOC-D or AOC-S) feature.

The currency amount can basically be transferred at the following times:

- on starting the call and possibly during the call (AOC-S)
- during the call (AOC-D)

### System-Specific Information

The administrator can avoid inaccuracies in recording connection data via the "Computing accuracy" parameter. The computing accuracy determines:

- the number of decimal digits for evaluating the connection data (minimum currency amount),

- the maximum number of currency amounts added up in memory (maximum total currency amount).

The set computing accuracy must not be lower than that of the ISDN. If the maximum of three decimal places is insufficient, the system automatically rounds up the number to the next unit. Values here include.

Computing accuracy	Minimum currency amount	Maximum currency amount
No decimal digits	1	around 4.3 billion
1 decimal digit	0.1	around 430 million
2 decimal digits (e.g., for Euro)	0.01	around 43 million
3 decimal digits (e.g., for British pounds sterling)	0.001	about 4.3 million

## 18.3 Cost Control (LX/MX)

Cost control is offered by the features Expensive Connection Route Advisory and Toll Fraud Monitoring.

### 18.3.1 Expensive Connection Route Advisory (LX/MX)

If the System is currently unable to reach a call destination via the least-cost routing path, it can notify the subscriber of the use of an expensive connection path via an advisory signal.

The subscriber can thus decide whether or not to conduct the call at that time despite the expensive connection path. The advisory signal may occur as follows:

- Text in the display
- Tone
- Text in the display and tone

The system issues an advisory message for the expensive connection path if a corresponding warning has been configured in the routing table and if the system is not using the route of index 1 of the routing table.

The advisory message is only displayed on the screen if no name is configured for the associated dial rule. If a name is configured, it is displayed.

## **18.3.2 Toll Fraud Monitoring (LX/MX)**

The system can monitor connections to detect possible occurrences of toll fraud (Toll Fraud Monitoring). Monitoring is performed for connections that arrive via a trunk and then leave via a trunk. The first IP station issues a signal when you exceed an arbitrary connection duration set and lets you clear down the call.

Monitoring is disabled by default.

## **18.4 Accounting Tools (LX/MX)**

Accounting tools are provided by Accounting Manager and Teledata Office.

### **18.4.1 Accounting Manager (LX/MX)**

Accounting Manager is a Windows application for retrieving call charge data via HTTPS and evaluating this data using tables and graphics.

Accounting Manager ships with its own documentation. Accounting Manager retrieves the call charge data of only one respective node. You can also use Accounting Manager to test the Call Charges interface. You can download Accounting Manager in the **Service Center** of OpenScape Office Assistant. Accounting Manager requires local administration rights and the activation of TLS 1.0 in Microsoft Internet Explorer.

### **18.4.2 Teledata Office (LX/MX)**

Teledata Office combines cost management in the telecommunications area with the analysis of communications traffic. Teledata Office is a Windows application for the professional evaluation of the call charge data.



# 19 Maintenance

OpenScape Office offers several maintenance options. This includes changing the telephony settings, backing up and restoring the configuration data, updating the software with updates and upgrades and restarting/reloading functions. In addition, appropriate functions to determine status and for monitoring and maintenance are available. Remote access to OpenScape Office is possible via different Remote Services.

## 19.1 Telephony Configuration

The communication system offers various configuration options for telephony, e.g., date and time, SNTP, customized display, and Music on Hold.

### 19.1.1 Date and Time (LX/MX)

The communication system features a system clock with date and time. This system time is shown in myPortal for Desktop and on every terminal's display.

You can define the basic system time or update it as follows:

- via a time server using SNTP
- via an ISDN trunk through an outgoing call
- by a manual setting

System-specific settings are not possible for the system time after activating an SNTP server.

The time displayed on the terminals may differ from the system time if ever an SNTP server cannot be reached.

A system time manually set after system startup is always overwritten by ISDN time information the first time an outgoing ISDN call is made, provided the network provider transmits this information. If the difference between the system time manually set and the ISDN time information in a live system is between 2 and 70 minutes, the ISDN time information is applied. Otherwise, the system time manually set is maintained.

The administrator can select one of the following formats to display the date on the terminal. The format is additionally dependent on the type of phone:

Date format	OpenStage	OptiPoint 410, OptiPoint 420
Europe	Tue 20.11.07	20. NOV 07

Date format	OpenStage	OptiPoint 410, OptiPoint 420
USA	Tue 11/20/07	Tue NOV 20.07
International1	Tue 20.11.07	Tue 20 NOV 07
International2	Tue 20.11.07	TUE 20.11.07

If you inadvertently set a date before 2007 as an administrator, you will subsequently no longer be able to access OpenScape Office Assistant. This will only be possible after a restart, which resets the date to 01.01.2007.

## 19.1.2 SNTP (LX/MX)

SNTP (Simple Network Time Protocol) is a simplified version of NTP (Network Time Protocol), a standard for synchronizing date and time via packet-based communication networks.

Your system needs a connection to an NTP server to synchronize date and time. This connection can occur in your local network or on the Internet. A number of different NTP servers are available on the Internet; you can select one that is located in your time zone. Note the conditions of use for the relevant server and, if necessary, request permission.

## 19.1.3 Telephone Logos

System telephones with a display show the logo as a background of the Telephony User Interface (TUI).

As an administrator, you can import, assign or delete phone logos for system telephones with a display. Different types of system telephones may use different phone logos.

---

### Related Topics

- [Updating System Telephones](#)

## 19.1.4 Customized Display ( LX/MX)

A customized display enables the company name, for example, to be displayed on the phone in the idle state.

### System-Specific Information

The feature can be used with the following telephones:

- optiPoint 410/420
- optiPoint WL2 professional

Only the right portion (max. 18 characters) of the second display line, which displays "OpenScape" by default, can be changed. The text lines up with the left part of the date if the length of the text allows it:

```
16:30          FR 29.FEB 08          123456 Post Office Hotel>
```

## 19.1.5 Flexible Menus (LX/MX)

Flexible menus allow you to customize the menu items shown on the display of system telephones.

As an administrator, you can select the menu items to be shown or hidden individually.

## 19.1.6 Music on Hold (LX/MX)

The communication system can play back Music on Hold (MOH) to waiting subscribers during switching operations. Callers hear MOH while in the hold state, parked state or transfer state. This also applies to callers in the call distribution queue.

As an administrator, you can transfer audio files with Music on Hold from your PC to the communication system for use as:

- alternative internal music
- additional CON group-specific music on hold

### Music On Hold

The administrator can configure the following functions:

- Music on hold with ringing tone (ringback):  
The subscriber on hold first hears the MOH melody during the consultation. After the party on hold is transferred to the destination, the ring tone is heard instead of the music on hold.
- Music on hold without ringing tone (ringback):  
The held party will hear MOH until the called party answers the call.
- No music on hold:  
The held party hears nothing (silence). The caller hears the ringback tone in the event of an unscreened transfer for an external call.

### CON group-specific music on hold

As an administrator, you can configure music on hold independently for each of the 16 CON groups. The communication system generally uses the music on hold of the CON group of the respective subscriber who initiated the hold or parked the call. If a CON group does not have any music on hold assigned to it, the internal music on hold is used for the group.

## 19.1.7 Music on Hold / Announcements Wizard (LX/MX)

The **Music on Hold / Announcements** wizard can be used to transfer audio files to the communication system and to configure announcements and music on hold.

## 19.1.8 Announcements (LX/MX)

The communication system allows on-hold announcements to be activated for callers before answering a call and also when using call distribution and DTMF direct inward dialing. Announcement equipment can be connected to an a/b interface for this. You can also replace the MOH melody in certain situations by an announcement, for example, if a party is placed on hold or if a subscriber is busy or being routed.

The administrator can configure internal announcements for single or continuous playback.

The administrator can transfer additional audio files with announcements from the PC to the communication system.

An external announcement device must behave like a station, i.e., announce itself, play the announcement and switch the call (enter consultation hold, dial and hang up).

## 19.1.9 User to User Signaling (LX/MX)

The communication system enables the transparent transmission of messages between stations (user to user signaling, UUS). UUS1 is supported for information exchange in control messages for connection setup and cleardown.

In the case of a point-to-multipoint connection, it is important to ensure that only one device transmits a message to an incoming call.

## 19.1.10 Voice Channel Signaling Security (LX/MX)

The communication system offers a security mechanism that can be set up by the administrator to prevent undesirable tone injections into the voice channel. No override is possible for a connection protected by this method. Every station configured as a Fax device automatically has this signaling security mechanism.

Recalls are deferred until the extension is free again.

Stations on-hold always have signaling security.

### 19.1.11 Time Parameters (LX/MX)

The communication system offers the administrator options for setting various time parameters such as the "length of callback" or the "timer for automatic redial".

The time parameters are preset in the communication system and should normally not be changed. The time duration for a time parameter is determined by the set base (e.g., 1 sec) multiplied by the set factor (e.g., 10), which produces 10 sec., for example.

### 19.1.12 Controlling Centrex Features (LX/MX)

To control Centrex features, the dial tones for \* and # must be transmitted to the ISDN and ITSP.

As an administrator, you can activate or deactivate this feature.

The input of a code must occur in the dialing state (e.g., after entering the trunk code). The input always begins with \* or #, followed by a digit or digit combination, and ends with #.

## 19.2 Backup and Restore

The configuration data of OpenScape Office can be backed up and restored.

The configuration data of OpenScape Office is saved in a backup set. Every backup creates a separate backup set. Backups can be created manually immediately or scheduled for automatic execution at specific times.

It is strongly recommended to regularly back up the configuration data as backup sets.

Different backup media can be used to store the backup sets (such as the local hard disk of OpenScape Office, a network drive or USB media, for example).

#### Backup Directory on Hard Disk (MX)

The configuration data of OpenScape Office can be saved in a separate partition on the hard disk of OpenScape Office MX in the backup directory. This backup directory is already provided as the standard archive "Hard Disk". The backup directory can be set up as a network drive, e.g., \\<IP address of OpenScape Office MX>\backup. All backups stored there can thus be saved with a customer-specific backup system.

#### File Share (MX)

The hard disk of OpenScape Office MX makes a portion of the hard disk capacity available for file storage. This area can also be used by Microsoft Windows-based operating systems for file sharing on the internal network and is called a file share

or SAMBA share. The files stored on this file share are not saved by the Backup&Restore concept of OpenScape Office MX, however, and must hence be backed up with the customer's own backup system.

### Backup Sets for Diagnostic Purposes

"Smaller" backup sets containing diagnostic data for Service Support can be created for diagnostic purposes. In contrast to normal backup sets, significantly smaller data amounts are produced for this purpose and can thus be easily sent with an e-mail, for example. Diagnostics backup sets include, among other things, the configuration data of the communication system and the UC Suite. Voicemails, fax messages and announcements are not included.

---

### Related Topics

- [Configuration Data for Diagnostics](#)

## 19.2.1 Backup Sets

The configuration data of the communication system is saved in a backup set.

If the number of backup sets saved exceeds the set value, the oldest backup sets are deleted.

### Backup Set Data

The following data for a backup set is presented:

- **Archive name:** Name of the backup set
- **Size:** Size of the backup set in bytes
- **Creation date:** Date on which the backup set was created.
- **Comment:** Comment that was specified when creating the backup set (optional).

Backup sets that have been grayed out cannot be restored.

## 19.2.2 Backup Media

The backup sets are stored on the selected backup media.

The following backup media can be used for the backup:

- Local hard disk of the communication system
- Inserted USB storage device
- FTP/FTPS servers
- Network Drive
- Client PC using HTTP (only possible with immediate backup)

For every backup medium, the maximum number of backup sets to be stored in the directory can be specified.

### USB Storage Device

To use a USB storage device (e.g., a USB hard disk or flash drive) for backup, the USB device must be inserted and available for the backup. In addition, the USB device must be formatted with FAT-32. USB media formatted with NTFS are read-only. Note that if multiple partitions exist, only the first partition can be used for the backup!

If a bootable USB device is used for the backup, this USB device must be safely removed after the backup.

Only for OpenScape Office MX: The USB device must be inserted in the USB server port of OpenScape Office MX. For multibox systems, the USB device may only be connected to the USB server port of the central box, since the USB server ports of the expansion boxes are not active.

### FTP/FTPS servers and network drives

FTP/FTPS servers and network drives can be added, edited or deleted as new media. FTP/FTPS servers and network drives may also be specified more than once if different directories on them are used. SSL/TLS is supported as the encrypted file transfer protocol (FTPS).

In order to back up the configuration data, the user must have write permission for the root directory of an FTP/FTPS server. To back up to a network drive, users only need write permission for the desired directory.

If the transmission speed to the FTPS server is too low, there may be a malfunction in the backup. If this occurs, the backup must be restarted.

## 19.2.3 Immediate Backup

The configuration data can be immediately backed up manually.

In order to enable fast and easy backups, the standard archives **Hard Disk** and **USB Device** have been created for backing up to the hard disk of the communication system or a USB medium, respectively.

The name of the backup set is assigned automatically during the backup. It includes, among other things, the date on which the backup was performed. If desired, a comment can be optionally added to identify a backup set more easily prior to a subsequent restore.

It is not advisable to create a backup using HTTPS, since the saved backup set cannot be restored using HTTPS. To do this, the backup set would need to be first copied to another supported medium.

---

### Related Topics

- [Upgrading from OpenScape Office V2 LX/MX to OpenScape Office V3 LX/MX](#)

## 19.2.4 Scheduled Backup

You can use a schedule to automatically back up configuration data. The time, frequency and location of the automatic backup is configurable.

The scheduled data backup can be scheduled for a fixed time daily or weekly and then started automatically. This "backup job" can be created for an internal or external backup medium. It is not possible to configure multiple backup jobs.

It is not advisable to create a backup using HTTPS, since the saved backup set cannot be restored using HTTPS. To do this, the backup set would need to be first copied to another supported medium.

---

**INFO:** After updating to V1 R4 or upgrading to V2, the backup jobs created earlier are lost. Previously created backup sets are only displayed again after recreating the backup paths.

---

---

### Related Topics

- [Upgrading from OpenScape Office V2 LX/MX to OpenScape Office V3 LX/MX](#)

## 19.2.5 Restore

The restoration of configuration data must be performed manually using the backup sets.

All the supported media can be used to restore data; however, it is not possible to restore a backup set using HTTPS. To do this, the backup set must be first copied to another supported medium.

---

**INFO:** After upgrading to V3, no V2 backup can be restored, since this would likewise result in inconsistent data. These V2 backups cannot be selected for a restore.

---

## 19.3 Updates and Upgrades

Updates provide the latest software available for the system components within a version. Upgrades, by contrast, replace an older version of the software with a newer version.

Updates and upgrades are performed with OpenScape Office Assistant. The version of the installed software is displayed on the start page of OpenScape Office Assistant. If more recent software updates are available, this is indicated there.

The following system components are updated:



- Software of the communication system, including the following:
  - Software of OpenScape Office
  - Software for the OpenScape Office Applications
  - Software of OpenScape Office Assistant
  - Documentation
- Software for system telephones (updates can also be performed individually)

The software update should be performed outside the business hours of the customer, since the communication system and/or the system telephones are restarted, and existing calls are dropped.

The software for the OpenScape Office applications is updated together with the software of the communication system. If a more recent software version is available, users of the OpenScape Office applications are notified via an Auto-Update message that an update is available and can be installed.

The software can be updated via the Internet web server, an internal web server or directly via image files. The software update can be optionally started immediately or by defining the times for the software transfer and software activation independently.

### **Updating via a Web Server**

In order to perform a software update via a web server, the Internet web server of OpenScape Office is accessed by default.

However, it is also possible to use an internal web server for updates (see [Using an Internal Web Server](#)).

The system checks for the presence of new software updates after automatically setting up a connection to the web server. For new software updates, the starting time for the software transfer and for the software activation are can be selected. In the case of slow connections to the web server, it must be ensured that the software has been completely transferred to the communication system before starting the activation. To be on the safe side when performing updates via the internal web server, a time gap of at least 60 minutes or more should be maintained between the start of the software transfer and the specified time for its activation.

After the image file has been transferred from the Download area of the web server to the communication system, the software just needs to be activated. Following a restart, the newly loaded software will be active.

### **Updating via an Image File**

To update system components, compressed image files containing the software of the system components are required. These image files can be downloaded from the OpenScape Office Internet web server and should be independently stored in an internal directory or on an internal web server. A separate image file is required for the communication system and for each system telephone type, and these files must be loaded into the communication system.

The following types of image files are available:

- **tgz**: for the software of the communication system. The tgz file contains a tar file. The tar file must be unpacked from the tgz file with a decompressor such as WinZip or 7-zip, for example. The tgz file is offered for download because a check can be performed to determine whether or not the file is corrupted when downloading the software from the server.
- **tar**: for the software of the communication system. It contains the packed files for each system component.
- **app**: for the software of the system telephone.

The following options are available for loading the image file to the communication system:

- Loading the image file via the internal web server  
The image file is located on an internal web server. Access is possible via HTTP or HTTPS.
- Loading the image file directly from a directory on the internal network  
The image file is located in a directory on a PC in the internal network.

### 19.3.1 Using an Internal Web Server

The software can be updated via an internal web server.

The current image files must be stored on the internal web server. In addition, the access data of the internal web server must be entered in OpenScape Office Assistant. This change can only be performed by an administrator with the **Expert** profile. After the access data of the web server has been entered, this will be set as the default for all future updates of OpenScape Office. In other words, the internal web server will now be used instead of the Internet web server.

### 19.3.2 Updating OpenScape Office

On updating OpenScape Office, the software of OpenScape Office and that of the system telephones are updated concurrently. A full update of all system components can thus be quickly and easily performed.

OpenScape Office can be updated by an administrator with the **Advanced** or **Expert** profile.

### 19.3.3 Updating System Telephones

The software of the system telephones can be loaded together with the software of the communication system via a web server or a single image file on the communication system. A separate image file is available for each system telephone type. The phone software can be transferred to all system telephones associated with this type or to just a single system telephone.

The update of the system telephone software can only be performed by an administrator with the **Expert** profile.

If some specific phone software (image file) is flagged as the default, the corresponding image will be automatically transferred to any system telephone associated with this type whenever that phone logs into the system for the first time.

---

**Related Topics**

- [Telephone Logos](#)

### 19.3.4 Software Status

The software status provides information on the current software version, whether a more recent version is available for an update and whether a new software version is being loaded into the system.

### 19.3.5 Upgrading from OpenScape Office V2 LX/MX to OpenScape Office V3 LX/MX

An "Upgrade" updates the OpenScape Office LX/MX V2 version to the new OpenScape Office LX/MX V3 version. The system components as well as the UC clients are upgraded. The upgrade is a pure software upgrade. No new hardware or software prerequisites are involved.

---

**INFO:** The number of mobile stations has been increased from 50 to 150 in the V3 version. To enable this, the number of virtual stations had to be reduced from 80 to 70.

---

#### Prerequisites

- The communication system and the UC clients are currently running the software version V2 Rx.x.x.
- The upgrade license *OpenScape Office V3 Upgrade* has been procured.

#### Steps to be Performed

1. **Back up data from V2**

Before the upgrade from V2 to V3 is performed, the current data of V2 must be backed up to an external medium (USB or network).

2. **Perform the full update to V3**

The full update updates the communication system and the OpenScape Office clients to the current version 3.

You can perform the Full Update by two methods:

- Via a web server: the image file is downloaded from either the Internet web server or an internal web server.
  - Via an image file: The image file is stored on the local PC or in the internal network.
3. **Activate the upgrade license**  
After the upgrade to V3, the communication system remains fully operational for a period of 30 days even without the upgrade license (grace period). The upgrade license must be activated within this time period.

---

**INFO:** After a successful upgrade from V2 to V3, a data backup should be performed.

---

4. **Assign Comfort Plus User licenses to IP stations**  
During the upgrade to V3, 15 Comfort User licenses from the OpenScape Office MX V2 basic package are converted to Comfort Plus User licenses. After the upgrade, assign the Comfort Plus User licenses to the 15 IP stations with the Comfort User licenses.
5. **Update the Factory Default Image (Golden Image)**  
After the upgrade to V3, the factory default image (golden image) must be updated. When a factory reset is performed on the communication system, the current factory default image is loaded. If the factory default image is not updated, the image of V2 is loaded.

---

**Related Topics**

- [Immediate Backup](#)
- [Scheduled Backup](#)
- [Licensing](#)

## 19.3.6 Upgrading from OpenScape Office HX V2 to OpenScape Office V3 HX

An "Upgrade" updates the OpenScape Office HX V2 version to the new OpenScape Office V3 HX version. The system components as well as the UC clients are upgraded. The upgrade from HiPath 3000 V8 to HiPath 3000 V9 is mandatory.

HiPath 3000 V8 can also be upgraded to HiPath 3000 V9 without an upgrade license. However, only OpenScape Office HX V2 can then be used. OpenScape Office V3 HX can only be operated on HiPath 3000 systems that have been upgraded to HiPath 3000 V9 with an upgrade license. The licensing occurs with HiPath 3000 Manager E.

**Prerequisites**

- OpenScape Office and the UC clients are currently running the software version V2 Rx.x.x.
- HiPath 3000 in Version V8.x

- HiPath 3000 Manager E is installed on the admin PC in the required version V9 R1.x.x, and the admin PC and is connected to the HiPath 3000 V8.
- The upgrade license to HiPath 3000 V9 and OpenScape Office V3 R2 HX has been acquired.
- A more recent CLA (e.g., V1 R20.1.2) is located on the admin PC with HiPath 3000 Manager E.

### Steps to be Performed

In order to upgrade OpenScape Office HX to the V3 version and HiPath 3000 to V9, the following steps must be performed in the specified order:

1. **Back up data from OpenScape Office HX V2**  
Before upgrading from V2 to V3, the OpenScape Office HX V2 data must be backed up to an external medium (USB or network).
2. **Clear the connection between HiPath 3000 and OpenScape Office HX**  
In order to ensure that no data of HiPath 3000 is written to the SQL database of the Linux server of OpenScape Office HX during the update, the connection between the HiPath 3000 and the Linux server, incl. OpenScape Office HX, must be cleared.
3. **Upgrade HiPath 3000 V8 to HiPath 3000 V9**  
In order to upgrade the HiPath 3000 communication system to Version 9, the HG 1500 must be first upgraded to V9, and the CDB must then be converted to Version 9. Finally, the software of the HiPath 3000 must be updated.
4. **Update licenses**  
A new HiPath 3000 V9 license file including the OpenScape Office V3 HX licenses must be imported into the CLA and loaded into the HiPath 3000 using HiPath 3000 Manager E.
5. **Configure IP trunks for OpenScape Office HX**  
For all IP trunks to the OpenScape Office HX, the **Ext. H.323** entry must be changed to **Ext. SIP**.
6. **Install SLES 11**  
Older SUSE Linux Enterprise Server versions (e.g.: SLES 10) are no longer supported. Consequently, the new version SLES 11 SP1 (32 bit) must be installed.
7. **Install OpenScape Office V3**  
After the Linux installation has completed successfully, the UC Suite OpenScape Office V3 must be installed on the Linux server.
8. **Restore data from OpenScape Office HX V2**  
The data from OpenScape Office HX V2 must be restored in the new OpenScape Office V3 HX.
9. **Restore the connection between HiPath 3000 and OpenScape Office HX**  
The connection between the HiPath 3000 and the Linux server of OpenScape Office HX must be restored after the upgrade so that the data from HiPath 3000 can be written back to the SQL database on the Linux server of OpenScape Office HX.

## Maintenance

Restart, Reload, Shutdown, Factory Reset

### 19.3.7 Upgrading UC Clients from V2 to V3

When upgrading to V3, new software for the UC clients is made available on the hard disk of the communication system. The administrator must make the new installation files available to the users of the UC clients. The users must manually uninstall and reinstall the UC clients on their PCs via the Control Panel. Local administrator rights are required for this purpose. The supported operating system versions and the special aspects to be considered for the installation are described in the `Readme_first` file included with the install files. When upgrading the UC clients, all personal settings and data are retained.

## 19.4 Restart, Reload, Shutdown, Factory Reset

You can use the associated wizards to initiate a Restart or Reload of OpenScape Office and for a controlled shutdown of OpenScape Office MX. In addition, a restart of the UC Suite (integrated applications) and of the Web Services can be initiated. A Factory Reset can be used to revert OpenScape Office MX to its default factory state.

### 19.4.1 Restarting OpenScape Office

The **Restart** wizard can be used to initiate a controlled restart of OpenScape Office.

The following differences must be observed:

- OpenScape Office LX and OpenScape Office MX  
A controlled restart of the communication system occurs. The communication system will be operational again after the startup.  
The startup time depends on system configuration and the OpenScape Office networking scenario.
- OpenScape Office HX  
A controlled restart of the OpenScape Office portion and the UC Suite (integrated applications) occurs. The UC Suite will be operational again after the startup.

During a restart, all active applications such as myPortal for Desktop and myPortal for Outlook, for example, are disconnected. After the startup, all connections are automatically set up again.

### 19.4.2 Reloading OpenScape Office

The **Reload** wizard can be used to initiate a reload of OpenScape Office.

The following differences must be observed:

- OpenScape Office LX and OpenScape Office MX  
The communication system is reloaded. After the subsequent startup, the communication system will be in its default state.
  - All country and customer-specific settings were deleted (system country code = Germany).
  - The communication system has the default IP address 192.168.1.2 and the internal IP range 192.168.2.xxx.
  - The licensing is retained.
  - In a multibox system, the configuration of the system boxes is retained. The system box configured as a central box continues to function as a central box. The system boxes configured as expansion box 1 and 2 continue to function as expansion box 1 and 2.The startup time depends on system configuration and the OpenScape Office networking scenario.
- OpenScape Office HX  
The OpenScape Office portion is reloaded. After the subsequent startup, the OpenScape Office portion will be in its default state.
  - All custom (i.e., customer-specific) settings of the OpenScape Office portion (e.g., the User Directory) were deleted.
  - The licensing is retained.

### 19.4.3 Restarting the UC Suite

The **Restart Application** wizard can be used by an administrator to initiate a controlled restart of the UC Suite (integrated applications).

During a restart of the UC Suite, all active applications such as myPortal for Desktop and myPortal for Outlook, for example, are disconnected. After the startup, all connections are automatically set up again.

### 19.4.4 Restarting the Web Services

The **Restart Web Services** wizard can be used by an administrator to initiate a controlled restart of the Web Services.

During a restart of the Web Services, the myPortal Web Services are restarted. Existing sessions of the myPortal for Mobile and myPortal for OpenStage clients are terminated.

In addition, the XMPP server integrated in the communication system is likewise restarted.

### 19.4.5 Shutting Down the OpenScape Office MX Communication System

The **Shut down** wizard can be used to initiate a controlled shutdown of the OpenScape Office MX communication system.

## Maintenance

Restart, Reload, Shutdown, Factory Reset

On completing the shutdown, the blue LEDs of all motherboards light up (operating state "Shutdown"), and the communication system can be turned off (On/Off switch of all system boxes at position "0").

### 19.4.6 Factory Reset of the OpenScape Office MX Communication System

A Factory Reset reverts the OpenScape Office MX communication system to the default factory state.

The following must be observed after a Factory Reset:

- All system boxes belonging to the communication system will be in the default factory state. For all system boxes belonging to the communication system, the factory default image will have been activated. The initial startup procedure must then be performed for each system box. In addition, multibox systems must be fully configured again.
- No previous country- and customized settings will be available.
- The communication system will be in an unlicensed state.

#### Factory Default Image (Golden Image)

Every OpenScape Office MX system box is shipped with a Factory Default Image (Golden Image). This image file contains a defined version of the software for the communication system and defined versions of the software for the system telephones.

### 19.4.7 System Behavior after Pressing the On/Off Switch (MX)

This section describes the system behavior in OpenScape Office MX one-box and multibox systems when you press the On/Off switch.

---

**INFO:** An OpenScape Office MX system box may only be turned off with the On/Off switch in emergencies.

---

#### One-box System

Activity	Effects
Deactivation and reactivation with the On/Off Switch	In other words, the communication system is deactivated and reactivated in an undefined state.  The communication system will be operational again after the startup.

---

**INFO:** The effect of pressing the on/off switch is similar to powering down and restarting a PC.

---



### Multibox System

Activity	Effects on		
	Central box (CB)	Expansion box 1 EB1	Expansion box 2 EB2 (if present)
Deactivation and reactivation of the central box with the On/Off switch	The CB is deactivated and reactivated in an undefined state.  The CB will be operational again after the startup.	A controlled shutdown is performed for EB1: all services (e.g., UC Suite) are stopped, and all current data is backed up ("Reset" operating mode).  EB1 waits till the CB has restarted. After the startup, the multibox system goes back into service.	A controlled shutdown is performed for EB2: all processes are stopped, and all current data is backed up ("Reset" operating mode).  EB2 waits till the CB has restarted. After the startup, the multibox system goes back into service.
Deactivation and reactivation of expansion box 1 with the On/Off switch	The gateway modules in EB1 and EB2 (if present) can no longer be reached.  The applications running on EB1 (e.g., conference, UC Suite) may be subject to certain feature restrictions.	EB1 is deactivated and reactivated in an undefined state.  The EB1 will be operational again after the startup.	A controlled shutdown is performed for EB2: all processes are stopped, and all current data is backed up ("Reset" operating mode).  EB2 waits till EB1 has restarted. The multibox system goes back in service after the startup.
Deactivation and reactivation of expansion box 2 (if present) with the On/Off switch	The gateway modules in EB2 can no longer be reached.	No effects	EB2 is deactivated and reactivated in an undefined state.  The EB2, and thus the multibox system, will be operational again after the startup.

---

**INFO:** The effect of pressing the on/off switch is similar to powering down and restarting a PC.

---

## 19.4.8 System Behavior after Unlocking the Module Release Latch of the Motherboard (MX)

This section describes the system behavior in OpenScape Office MX one-box and multibox systems when you unlock the module release latch of the motherboard.

**Maintenance**

Restart, Reload, Shutdown, Factory Reset

**One-box System**

Activity	Effects
Unlock the module release latch of the motherboard	A controlled shutdown is performed for EB2: all services are stopped, and all current data is backed up.  On completing the shutdown, the blue LED of the motherboard lights up (operating state "Shutdown"), and the communication system can be turned off (On/Off switch at position "0").

**Multibox System**

Activity	Effects on		
	Central box (CB)	Expansion box 1 EB1	Expansion box 2 EB2 (if present)
Unlock the module release latch of the motherboard in the central box	A controlled shutdown is performed for CB: all services are stopped and all current data is backed up ("Shutdown" operating mode).	EB1 performs a restart.  EB1 waits till the CB has restarted. After the startup, the multibox system goes back into service.	The EB2 performs a restart.  EB2 waits till the CB has restarted. After the startup, the multibox system goes back into service.
Unlock the module release latch of the motherboard in expansion box 1	No effects	A controlled shutdown is performed for EB1: all services (e.g., UC Suite) are stopped, and all current data is backed up ("Shutdown" operating mode).	The EB2 performs a restart.  EB2 will be operational again after the startup.
Unlock the module release latch of the motherboard in expansion box 2 (if present)	No effects	No effects	A controlled shutdown is performed for EB2: all processes are stopped, and all current data is backed up ("Shutdown" operating mode).

---

**INFO:** If the communication system state is "Shutdown" (the blue LED is lit on all motherboards associated with the communication system), the system can be powered down (all On/Off switches in "0" position).

---

**19.4.9 System Behavior after Initiating a Reset via the Reset Switch (MX)**

This section describes the system behavior in OpenScape Office MX one-box and multibox systems when you initiate a reset (restart) via the Reset switch.

---

**INFO:** The Reset (Restart) switch must only be used to reset (restart) the system box in emergencies.

---

### One-box System

Activity	Effects
Press the Reset switch < 10 sec.	The communication system undergoes a controlled restart (reboot).  The communication system will be operational again after the startup.

---

**INFO:** The effect of pressing the Reset switch is similar to pressing the Reset button on a PC.

---

### Multibox System

Activity	Effects on		
	Central box (CB)	Expansion box 1 EB1	Expansion box 2 EB2 (if present)
Press the Reset switch on the central box for < 10 sec.	The CB undergoes a controlled restart (reboot). All services are stopped, and the current data is backed up.  The CB will be operational again after the startup.	A controlled shutdown is performed for EB1: all services (e.g., UC Suite) are stopped, and all current data is backed up ("Reset" operating mode).  EB1 waits till the CB has restarted. After the startup, the multibox system goes back into service.	A controlled shutdown is performed for EB2: all processes are stopped, and all current data is backed up ("Reset" operating mode).  EB2 waits till the CB has restarted. After the startup, the multibox system goes back into service.
Press the Reset switch on expansion box 1 for < 10 sec.	No effects	EB1 undergoes a controlled restart (reboot).  The EB1 will be operational again after the startup.	A controlled shutdown is performed for EB2: all processes are stopped, and all current data is backed up ("Reset" operating mode).  EB2 waits till EB1 has restarted. The multibox system goes back in service after the startup.
Press the Reset switch on expansion box 2 (if present) for < 10 sec.	No effects	No effects	EB2 undergoes a controlled restart (reboot).  The EB2, and thus the multibox system, will be operational again after the startup.

---

**INFO:** The effect of pressing the Reset switch is similar to pressing the Reset button on a PC.

---

## Maintenance

Restart, Reload, Shutdown, Factory Reset

### 19.4.10 System Behavior after Initiating a Reload via the Reset Switch (MX)

This section describes the system behavior in OpenScope Office MX one-box and multibox systems when you initiate a reload via the Reset switch.

#### One-box System

Activity	Effects
Press the Reset switch > 10 sec.	A reload is initiated on the communication system.  After the startup, the one-box system will be in its default state. All country and customer-specific settings were deleted (system country code = Germany). The default IP address of the communication system is 192.168.1.2.

---

**INFO:** After the basic settings have been configured using the **Initial Installation** wizard, country- and customer-specific data backups can be reloaded. For more detailed information on the procedure, see [Restore](#).

---

#### Multibox System

Activity	Effects on		
	Central box (CB)	Expansion box 1 EB1	Expansion box 2 EB2 (if present)
Press the Reset switch on the central box for > 10 sec.	A reload is initiated on the central box.  The multibox system is deconfigured, and all system boxes revert to their initial default state.	A reload is initiated on EB1.  The multibox system is deconfigured, and all system boxes revert to their initial default state.	A reload is initiated on EB2.  The multibox system is deconfigured, and all system boxes revert to their initial default state.
Press the Reset switch on expansion box 1 for > 10 sec.	A reload is initiated on the central box.  The multibox system is deconfigured, and all system boxes revert to their initial default state.		
Press the Reset switch on expansion box 2 (if present) for > 10 sec.			

---

**INFO:** In order to put the multibox system back into service, an initial configuration of the multibox system must be performed. For more detailed information on the procedure, see [Multibox Systems](#).

---

## 19.5 Inventory Management

The term Inventory Management refers to the process for determining the current status of the OpenScape Office MX and OpenScape Office LX communication systems and the hardware configuration of the OpenScape Office MX communication system.

### 19.5.1 System Status (LX/MX)

The current status of the OpenScape Office MX and OpenScape Office LX communication systems can be determined by an administrator with OpenScape Office Assistant. The following information can be retrieved: status of the network and interfaces, stations, connection setup, ITSPs, VPNs, the current dial plan and the IP addresses.

#### Network Status (MX)

The network status enables information to be retrieved on

- the current status of a networked OpenScape Office MX communication system.

In the case of a faulty network, information on the cause of the error is displayed. An error message appears, for example, when using the WAN interface to connect a network node, since such usage of the WAN interface is not allowed.

For more detailed information on networking, see [Networking OpenScape Office](#).

- the current status of various interfaces of the OpenScape Office MX communication system.

Details on the following interfaces can be retrieved:

**Maintenance**  
Inventory Management

Interface (port)	Displayed information	Motherboard / Gateway module
LAN interface 1 (ADMIN)	IP address: IP address of the communication system	Motherboard
LAN interface 2 (OUT)	Subnet mask: subnet mask of the communication system	
LAN interface 3 (IN)	MAC address: MAC address of the associated motherboard	
LAN interface 4 (UPLINK)	Max. data packet size (bytes): maximum packet size in bytes that was selected for this interface.  IEEE802.1p/q Tagging: Yes (Quality of Service (QoS) is used.) / No (QoS is not used.)  LAN port: number of this LAN port  Interface is active: yes / no  Ethernet Link Mode: mode (full duplex, half duplex or automatic) and speed that was selected for this interface.	
DMZ interface	Interface is active: yes / no  IP address: IP address of the communication system for the DMZ (Demilitarized Zone)  Subnet mask: subnet mask of the communication system for the DMZ  MAC address: MAC address of the associated motherboard for the DMZ  Ethernet Link Mode: mode (full duplex, half duplex or automatic) and speed that was selected for this interface.  Max. data packet size (bytes): maximum packet size in bytes that was selected for this interface.	Motherboard

Interface (port)	Displayed information	Motherboard / Gateway module
WAN port Description. Part 1 of 3	DSL at WAN port directly (= activated WAN port): The WAN is used as: DSL MAC address: MAC address of the associated motherboard for the WAN Connection Status: Active / Not active / Waiting for activity Dynamic, local IP address: IP address that was assigned by your ISP for Internet access. Dynamic IP address of partner: IP address of the server of your ISP Domain Name Server 1: IP address of the first DNS server Domain Name Server 2: IP address of the second DNS server Online time (hours:minutes:seconds): duration of the connection to the ISP Terminated pppd daemons: Number of terminated daemons Connection forcing packet: number of data packets transmitted Transfer statistic: number of inbound and outbound bytes and packets	Motherboard



Interface (port)	Displayed information	Motherboard / Gateway module
WAN port Description. Part 2 of 3	<p>TCP/IP at WAN Port via an external router (= activated WAN port):</p> <p>The WAN is used as: LAN connection type TCP/IP</p> <p>Interface is active: yes</p> <p>IP address: IP address of the communication system</p> <p>Subnet mask: subnet mask of the communication system</p> <p>MAC address: MAC address of the associated motherboard for the WAN</p> <p>Ethernet Link Mode: mode (full duplex, half duplex or automatic) and speed that was selected for this interface.</p> <p>Max. data packet size (bytes): maximum packet size in bytes that was selected for this interface.</p> <p>Network Address Translation (NAT): Yes (NAT (for IP addresses) is used.) / No (NAT is not used.)</p> <p>Bandwidth control for voice connections: setting (No, Upload only or Upload and Download) that was selected for this interface.</p> <p>Bandwidth of connection (Kbps): bandwidth that was selected for this interface.</p> <p>Bandwidth used for voice/fax (%): percentage value that was selected for this interface (proportion of bandwidth to be reserved for voice and fax connections).</p> <p>IEEE802.1p/q Tagging: Yes (Quality of Service (QoS) is used.) / No (QoS is not used.)</p>	Motherboard
WAN port Description. Part 3 of 3	<p>TCP/IP at WAN port via an external router (= activated WAN port):</p> <p>The WAN is used as: not configured or deactivated</p>	Motherboard

<b>Interface (port)</b>	<b>Displayed information</b>	<b>Motherboard / Gateway module</b>
S <sub>0</sub> interface 1 S <sub>0</sub> interface 2 S <sub>0</sub> interface 3 S <sub>0</sub> interface 4	B channels: number of maximum possible B channels and currently seized B channels  DSP: number of maximum possible DSPs and currently seized DSPs	GMS and GMSA Gateway Modules
S2M interface	B channels: number of maximum possible B channels and currently seized B channels  DSP: number of maximum possible DSPs and currently seized DSPs	Gateway Module GME
T1 Interface	B channels: number of maximum possible B channels and currently seized B channels  DSP: number of maximum possible DSPs and currently seized DSPs	Gateway Module GMT

**Station status**

The station status enables the following information on the configured stations to be retrieved:

- Phone Number
- Name
- Device type
- IP address
- MAC Address
- Current SW version
- HW version
- Status (On/Off)

**Status of the Connection Setup (MX)**

The dial-up network status enables information on existing connections to PSTN partners (i.e., Public Switched Telephone Network partners such as public or home telecommunications networks, for example) to be retrieved.

**ITSP Status**

The ITSP status enables information on the current status of preconfigured and any possibly added Internet Telephony Service Providers (ITSPs) to be retrieved. In addition, it shows which stations were set up for which ITSP.

The status of each ITSP is indicated by the color of the associated rectangle (green = OK, gray = not activated/configured, orange = at least one of the stations was not properly configured).

**VPN Status (MX)**

The VPN status enables information on the configured VPN tunnels to be retrieved:

### Dial Plan

The current dial plan (also called a numbering plan) of the communication system is displayed.

The dial plan contains all the station numbers and direct inward dialing numbers and codes currently defined in the communication system.

For more information, see [Dial Plan](#) and [Codes for Activating and Deactivating Features \(LX/MX\)](#).

### Overview of IP Addresses (MX)

The IP addresses configured in the OpenScape Office MX communication system are displayed.

In addition, the overview also shows with which wizards and which menus in Expert mode the IP addresses can be configured.

## 19.5.2 Inventory

The Inventory enables an administrator to retrieve information on the hardware and software of OpenScape Office MX and the software of OpenScape Office LX and OpenScape Office HX.

### OpenScape Office MX

The following details can be retrieved for every system box belonging to the OpenScape Office MX communication system:

- System box X  
Among other things, the following information is displayed: MAC address, IP address, host name, operating system version and software version.
- Hard Disk Information  
Details on memory amounts, including the available and used memory.
- Gateway Modules  
Among other things, the following information is displayed: slot no., type, serial number, software version and status of all inserted gateway modules.
- Applications  
All applications and their respective statuses are displayed.

In addition, the allocation of call numbers to the motherboards and gateway modules belonging to the communication system can be retrieved.

### OpenScape Office LX and OpenScape Office HX

The following details can be retrieved:

- Software  
Among other things, the following information is displayed: MAC address, IP address, host name and software version.
- Hard Disk Information  
Details on memory amounts, including the available and used memory.

## Maintenance

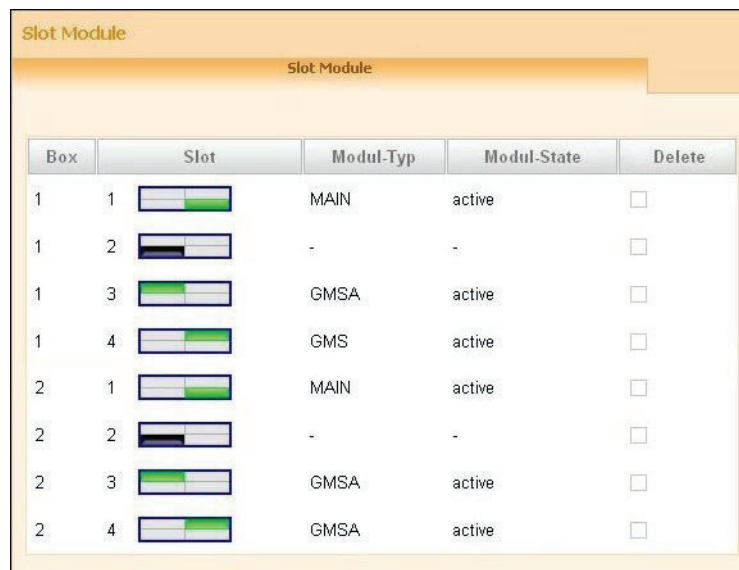
### Automatic Actions ( LX/MX)

- Applications  
All applications and their respective statuses are displayed.

## 19.5.3 Hardware Configuration (MX)

The hardware configuration of the OpenScape Office MX communication system is identified by the number of system boxes and motherboards and by the gateway modules plugged in.

The following layout is used for the hardware configuration in OpenScape Office Assistant.



Box	Slot	Modul-Typ	Modul-State	Delete
1	1	MAIN	active	<input type="checkbox"/>
1	2	-	-	<input type="checkbox"/>
1	3	GMSA	active	<input type="checkbox"/>
1	4	GMS	active	<input type="checkbox"/>
2	1	MAIN	active	<input type="checkbox"/>
2	2	-	-	<input type="checkbox"/>
2	3	GMSA	active	<input type="checkbox"/>
2	4	GMSA	active	<input type="checkbox"/>

The example shown illustrates the hardware configuration in a two-box system.

The central box (box 1) is equipped with a motherboard (slot 1: module type: MAIN) and two gateway modules (slot 3: module type: GMSA and slot 4: module type: GMS). Slot 2 is empty.

The expansion box (box 2) is equipped with a motherboard (slot 1: module type: MAIN) and two gateway modules (slot 3: module type: GMSA and slot 4: module type: GMSA). Slot 2 is empty.

## 19.6 Automatic Actions ( LX/MX)

This function can be used to define actions to be executed once or at regular intervals. These actions are then executed automatically by the communication system at the set time.

## 19.6.1 Garbage Collection Automatic Action

The automatic action Garbage Collection enables an automatic garbage collection to be performed on the communication system.

The color of the list item displayed in the menu tree indicates the status of the action (green = action activated, red = action not activated).

**Start/Stop Action** can be used to enable or start an inactive action (red list item) and to disable or stop an active action (green bullet point).

The automatic action Garbage Collection is disabled by default.

## 19.6.2 DLS Notification Automatic Action

The automatic action DLS Notification can be used to initiate an automatic login at an external DLS server on starting up the communication system.

The color of the list item displayed in the menu tree indicates the status of the action (green = action activated, red = action not activated).

**Start/Stop Action** can be used to enable or start an inactive action (red list item) and to disable or stop an active action (green bullet point).

The automatic action DLS Notification is disabled by default.

## 19.7 Monitoring and Maintenance of OpenScape Office

OpenScape Office offers different functions for monitoring the current status of the system and for finding and resolving errors.

### 19.7.1 Checking the Network Connection (MX)

The network connection between the OpenScape Office MX communication system and the target address can be checked by using an ICMP (Internet Control Message Protocol) request.

Echo request packets can be sent via both the **Ping** and **Traceroute** functions. The corresponding echo reply messages are displayed together with the round-trip times.

The **Traceroute** function sends echo request packets with various incremental TTL (Time-To-Live) values.

## 19.7.2 SNMP (Simple Network Management Protocol) (LX/MX)

The Simple Network Management Protocol (SNMP) is a network protocol which can be used to monitor and operate networking components (such as routers, servers, switches, printers, PCs) from a central station (management console). The protocol controls communication between the monitored components and the monitoring station.

SNMP describes the structure of data packets that can be sent and the communication procedure. SNMP was designed so that all network-capable devices can be included in monitoring. SNMP-based network management tasks include

- monitoring networking components,
- performing remote control and remote configuration of networking components,
- error detection and notification.

Devices known as "agents" are used for monitoring. These are utilities that run directly on monitored components. These utilities are able to record the status of components, make settings, and trigger actions. SNMP allows the central management console to communicate with the agents over a network.

### Management Information Databases (MIB)

The volume of data that can be administered via SNMP is defined in MIBs (Management Information Base). MIBs are data models that describe the networking components to be administered in an established manner. The OpenScape Office MX MIB can be downloaded via the OpenScape Office Assistant (service center).

OpenScape Office MX has a separate SNMP agent that allows access to various system data that is stored in its MIB or Management Information Base. The MIB provides basic system information, status information, event-related data, and information on installed hardware (slots) and configured connections (ports).

SNMP supports the central monitoring and administration of networking components, including OpenScape Office MX itself. It is possible to

- address the OpenScape Office MX over the TCP/IP protocol.
- access data over external management applications.
- perform remote maintenance activities.
- visualize the operating status of OpenScape Office MX.
- transmit service-specific errors (Traps).

### Communities

Access to the SNMP data (MIBs) is governed by communities. A distinction is made here between read, write, and Trap communities. Each community has a specific IP address.

To enable read access to SNMP data (MIBs) on a PC, for example, the IP address of this PC must be entered in the list of read communities. To enable read and write access, the IP address must be entered in the list of write communities.

Trap Communities are used to manage the recipients of error messages (traps).

### Traps

When problems occur in OpenScape Office MX, traps are generated to indicate errors and failures. The following types of traps are available:

- System traps = System errors that require immediate action for recovery.
- Performance Traps = Information on performance problems that do not require corrective action.

Traps are classified by their effects and can be retrieved by an administrator with the **Expert** profile using the OpenScape Office Assistant. A list of all traps received is displayed with the following information:

Table column	Meaning
VarBind1 (Severity)	Trap effect classes The following entries are possible: Critical: Error Message. This error causes problems. Major: error message. This error could cause problems. Minor: error message. The error has no problematic consequences. Warning: report of a possibly problematic procedure or status, but not an error message. Deleted Information: plain status messages, no error messages. Intermediate status Other traps
VarBind2 (Name)	Trap name
Generic Name	General Description such as Enterprise Specific, for example
Specific Name	Trap type (1 = software, 2 = hardware)
Enterprise	–
Time	Time of error
Index	List number

Trap display is updated every 30 seconds. Traps are sorted in the sequence of occurrence.

Trap details can be displayed by clicking a trap name.

## 19.7.3 Manual Actions

Many different logs (diagnostics data and diagnosis logs) can be loaded via manual actions.

**Maintenance**

Monitoring and Maintenance of OpenScape Office

Administrators with the **Advanced** profile can load diagnostic data (diagnosis logs) by using the **Trace** wizard.

Administrators with the **Expert** profile can load diagnostic data (diagnosis logs) in **Expert mode**.

The following logs can be loaded:

Protocol	Explanation	Application case
Trace log	Standard trace file, if trace profiles have been activated. A selection can be made between the following options: <ul style="list-style-type: none"> <li>• <b>Complete Trace Log</b>: The full set of trace log files is downloaded.</li> <li>• <b>Log from Today</b>: The trace log files of the current day (as of 00:00 hours) are downloaded.</li> <li>• <b>Own Selection: From: XXX To: YYY</b>: The trace log files of the selected time period are downloaded.</li> </ul>	No special application
Event Log Only for OpenScape Office LX/MX	Actions/events of the communication system (Reset, On/Off, etc.)	No special application
Admin Log (also called Admin Protocol) Only for OpenScape Office LX/MX	Messages about administration processes at the communication system (login attempts, etc.)	No special application
License Protocols Only for OpenScape Office LX/MX	Messages about the communication system components that require licenses	Problems with licensing (the license file cannot be activated, and so on)
Customer Trace Only for OpenScape Office LX/MX	Messages for the customer trace are provided in a more detailed format than in the trace log, for example (remote login, ITSP login, etc.).	No special application
Framework Protocol Only for OpenScape Office LX/MX	Messages of OpenScapeOffice Assistant	Problems with licensing, backup, restore or with OpenScape Office Assistant.
Diagnosis Protocol Only for OpenScape Office LX/MX	Diagnosis logs of the communication system (FP/LDH)	System crash or uncontrolled shutdown of the communication system
Slot module protocols Only for OpenScape Office MX	Messages of the individual slot modules	Problems with gateway modules (gateway module does not start up properly, crashes, etc.)



Protocol	Explanation	Application case
OpenScape Office Protocols  Only for OpenScape Office LX/MX	<p>Messages of the UC Suite of the communication system (UC Suite, CSP and MEB logs)</p> <p>A selection can be made between the following options:</p> <ul style="list-style-type: none"> <li>• <b>Complete Trace Log:</b> All UC Suite, CSP and MEB log files are downloaded.</li> <li>• <b>Log from Today:</b> The UC Suite, CSP and MEB log files of the current day (as of 00:00 hours) are downloaded.</li> <li>• <b>Own Selection: From: XXX To: YYY:</b> The UC Suite, CSP and MEB log files of the selected time period are downloaded.</li> </ul> <p>All log files are archived together in a compressed file. The following file naming conventions apply to the OpenScape Office logs: UC Suite log files = vs_yyyy_mm_dd.log, CSP log files = cspttrace_yyyy_mm_dd.log, MEB log files = mebtrace_yyyy_mm_dd.log.</p>	Problems with the UC Suite and/or the client (myPortal for Desktop, myAttendant, etc. )
Application Protocols  Only for OpenScape Office LX/MX	<p>Messages of the application side of the communication system (for example, CSP protocols)</p> <p>An administrator with the <b>Expert</b> profile can select between the following options in <b>Expert Mode</b>:</p> <ul style="list-style-type: none"> <li>• <b>Complete Trace Log:</b> All log files are downloaded</li> <li>• <b>From: xxx To: YYY:</b> The log files of the selected time period are downloaded.</li> </ul> <p>All log files are archived together in a compressed file.</p>	Problems with the application side of the communication system
System Diagnosis Logs  Only for OpenScape Office LX/MX	Diagnosis logs of the communication system	No special application
PPP Logs  Only for OpenScape Office LX/MX	Messages for the Point-to-Point Protocol	Problems with Dial-In or Dial-Out connections
CoreLog Protocol	CoreLogs are created for resets, etc. (e.g., memory dumps at a PC).	System crash or uncontrolled shutdown of OpenScape Office

After the desired logs have been selected, a compressed file is created and stored in a specified directory.

### 19.7.4 Traces (LX/MX)

Traces can be used to record the execution of individual program steps and their results during the execution of a program. In combination with further diagnostics data, an incorrectly executing program can be traced back to the source of the error. The individual traces to be recorded and their respective levels of detail are configured via the trace profiles and trace components.

## Maintenance

### Monitoring and Maintenance of OpenScape Office

---

**INFO:** Activating traces can have a negative impact on system performance and must hence only be performed by experienced administrators and only after consulting with the responsible Service Support.

The console trace, in particular, requires substantial system resources and thus has an adverse effect on the performance of the communication system.

---

## Networking

In order to diagnose networked communication systems, the trace data of each individual node must be collected separately. It is not possible to acquire the trace data of networked communication systems centrally.

### Trace Format Configuration

The Trace Format Configuration function can be used by an administrator with the **Expert** profile to define which header data is to be included in the trace output and how the trace data is to be formatted.

Header data for the trace output (all options are activated in the default setting):

- Global Trace Header Format Settings  
If this option is enabled, the options for the following header data can be activated or deactivated.
- Subsystem ID
- Task Name
- Task ID
- Time
- Module Name
- Line Number

#### Formatting the Trace Data

- Full formatting with parameter expansion (default) = large data volume, normal trace performance. Default setting
- Limited formatting (message types binary, special X-Tracer format) = medium data volume, fast trace performance.
- Limited formatting (expansion of basic data types only) = low data volume, very trace performance.
- Performance optimized trace without parameter expansion = very low data volume, extremely fast trace performance.

---

**INFO:** Note that adding more trace header data and extensive trace data formatting will decrease the overall trace performance.

---

### Trace output interfaces

This function enables an administrator with the **Expert** profile to define the interfaces for the trace output.

Trace output interface	Explanation	Default setting
File Trace	<p><b>Switch File Trace On</b></p> <p>Trace messages are entered into a log file.</p> <p>The following settings apply when the option is enabled:</p> <p><b>Max. Trace Quota (kByte):</b> 2097152 (Max. size of the trace memory)</p> <p><b>Policy to handle reach of max. quota.</b> You can choose between <b>Wrap Around (delete oldest file)</b> and <b>Stop temporarily the file trace.</b></p> <p><b>Time between creation of new trace files (sec):</b> 900</p> <p><b>Time period for which trace files are available:</b> The actual time period is specified.</p>	Activated
Trace via LAN	<p><b>Switch Trace via LAN On</b></p> <p>Trace messages are transmitted via the LAN interface.</p> <p>The following setting applies when the option is enabled: <b>Timer value</b> = 25 sec. (delay period until data is transmitted.)</p>	Not activated

### Trace log

If the trace output interface Switch File Trace On is enabled, the resulting log files can be transferred by an administrator with the **Expert** profile to a PC or deleted.

### Digital Loopback

This function can be used by an administrator with the **Expert** profile to enable loopbacks for the B channels of the S<sub>0</sub>, S<sub>2M</sub> and T1 interfaces of existing gateway modules, if any.

### Event Viewer / Customer Trace Log

The **Event Viewer** wizard can be used by an administrator with the **Advanced** profile to start the event display (customer trace) In addition, the customer trace log file can be copied to a PC or deleted.

The following functions, which can be started using the wizard, are described here:

- *Displaying or Editing Event and Customer Trace Logs*
- *Downloading or Opening the Event Log / Customer Trace Log*
- *Clearing the Event Log / Customer Trace Log*

## Maintenance

### Monitoring and Maintenance of OpenScape Office

Administrators with the **Expert** profile can start displaying the customer trace log file in **Expert mode**. In addition, the customer trace log file can be copied to a PC or deleted.

### Call Monitoring

The Call Monitoring function can be used by an administrator with the **Expert** profile to monitor the connection setup and clear-down of the trunk and station interfaces (ports) of the communication system.

After selecting the desired port and starting the trace, the individual events are logged. Every event is logged with a sequential number, the time, the call number involved and the affected port. In addition, the state of the event is entered.

Possible entries in the State: column:

State	Explanation
Idle	Port is idle.
Call Initiated	Port is ready.
Overlap Sending	External sending of digits
Outgoing Call Proc	End of dialing
Call request	Waiting for ALERT.
Call Present	Port is ringing.
Active	Port is in talk state
Hold	Port is on Hold.
Disconnect Indication	Request to disconnect an active call
Direct	Port is in Speaker call/Direct answering mode.
Intrusion	Override is enabled at the port
Call Back A	Callback: Station A
Call Back B	Callback: Station B
Busy	Port is busy.
Error	Port is in Error state
Disconnect PI	Wait for Disconnect from PI (Progress Indicator)
Sensor	Signal was sent by Sensor
Conference Master	Conference Master
Paging	Port is in process of using Paging
Help Dial	Associated dialing is used at the port.
Remote	Trunk port is used for remote administration or DISA.
ACD	Universal Call Distribution
Call Monitor	Call monitoring is used at the port.
Unknown State	Unknown Status

Possible entries in the Event column:

Event	Explanation
Setup	Trunk: incoming or outgoing seizure
Setup Ackn	Trunk: seizure acknowledgment
Info	Trunk: Info (Number Digits)
Call Proc	Trunk: unevaluated end-of dialing
Progress	Trunk: additional info for call setup
Alert	Trunk: evaluated end-of dialing
Connect	Trunk: connection of B channel
Connect Ackn	Trunk: acknowledgement of connecting B-channel
Disconnect	Trunk: request for disconnect
Release	Trunk: acknowledgement of disconnect
Release Compl	Trunk: connection released
Monitor On	Trunk/Station: start call monitoring.
Monitor Off	Trunk/Station: end call monitoring.
Off Hook	Station: handset goes off hook
On Hook	Station: handset goes on hook
Digit	Station: digits are dialed

The Call Monitoring log file can be converted to a readable format via the ISDN message decoder. The ISDN message decoder can be downloaded from the **Service Center** of OpenScape Office Assistant.

### H.323 Stack Trace

This function can be used by an administrator with the **Expert** profile to set the H.323 Stack Trace Configuration. The level of detail for the trace can be defined via trace levels (0 = lowest level of detail to 4 = maximum level of detail). The following settings can be selected for the H.323 stack trace output:

Trace output interface	Explanation	Default setting
Console Trace	<p><b>Switch Console Trace On</b></p> <p>H.323 Stack Trace messages are output on the console.</p>	Not activated
File Trace	<p><b>Switch File Trace On</b></p> <p>H.323 Stack Trace messages are written to a log file.</p> <p>The following settings apply when the option is enabled:</p> <p>Max. size of the trace buffer = 50000 bytes (amount of data stored in the buffer.)</p> <p>Max. size of the trace file = 1000000 bytes (maximum size of the log file.)</p> <p>Trace Timer = 60 sec. (delay period until data is written to the log file.)</p>	Not activated

By activating and/or deactivating H.323 modules, you can define for which components of the H.323 stack trace the process and status information is to be recorded. The status of each H.323 module is indicated by the color of the associated bullet point (green = H.323 module active, red = H.323 module inactive).

The H.323 Stack Trace log can be transmitted to a PC or deleted.

**Trace Profiles**

Trace profiles define what data is to be recorded and at what level of detail. Trace components are assigned to a trace profile. This allows you to specify for which system components the process and status information should be logged by the trace profile.

Predefined trace profiles are also provided. In addition, an administrator with the **Expert** profile can also create his or her own profiles. When you start a trace profile, logging is activated via this profile. When you stop the profile, logging is deactivated.

- Administrators with the **Advanced** profile can start and/or stop trace profiles by using the **Trace** wizard. The status of every trace profile is indicated by the color of the associated list item (green = trace profile active, red = trace profile not active). **Start/Stop** can be used to enable or start an inactive trace component (red bullet point) and to disable or stop an active trace component (green bullet point).

**Load Trace** is used to transfer the generated log files to a PC or open them.

**Delete Trace** is used to delete the generated log files.

The following functions, which can be started using the wizard, are described here:

- *Downloading Traces / Trace Logs*
- *Clearing Traces / Trace Logs*

- *How to Display all Trace Profiles*
- *Starting a Trace Profile*
- *Stopping a Trace Profile*
- *Downloading Diagnostics Data / Diagnosis Logs*
- Administrators with the **Expert** profile can collectively stop all trace profiles and selectively start and/or stop individual trace profiles in **Expert mode**. In the menu tree display, the color of the list item indicates the status of the trace profile (green = trace profile is activated, red = trace profile is not activated). **Start/Stop Trace Profile** can be used to enable or start an inactive trace component (red bullet point) and to disable or stop an active trace component (green bullet point).  
By selecting **Display Trace Profile** you can view the details of the desired trace profile: This includes the profile name, details about write protection and the status of the profile, as well as information on when, i.e., for which problems, this trace profile should be used. In addition, you can see which trace components belong to the trace profile.

Trace Profile	Application case
Analog_subscriber_and_trunks Only for OpenScape Office MX	Failed functions of analog stations or analog trunks
Charging_data	Wrong or missing charge data.
Default	Trace profile with the factory default settings
DHCP Only for OpenScape Office MX	New LAN components do not get IP addresses
Display_problems	Missing, incorrect or delayed display on screens of the connected phones.
External_CSTA_application	Interrupted function between communication system and external application.
Gateway_modules Only for OpenScape Office MX	Gateway modules are not put into service. Gateway modules are not in service. The gateway module status is not displayed correctly in OpenScape Office Assistant.
Integrated_voicemail_faxmail	Voicemail not installed. Wrong greetings when forwarded to voicemail. No voicemail recording possible after greetings. Voice recording was interrupted. No notification about new message. Fax was not received in the fax box. Fax was received in the wrong fax box. Fax transmission was interrupted.
License_download	Licenses cannot be loaded from the License server. License file cannot be loaded and applied.

**Maintenance**

## Monitoring and Maintenance of OpenScape Office

Trace Profile	Application case
Licensees	Licensed components are not interpreting licenses correctly. Licensed functions are working incorrectly or do not work at all. Licenses were lost.
Network_DMZ Only for OpenScape Office MX	No access to DMZ
Network_LAN	No access to LAN.
Network_WAN Only for OpenScape Office MX	No access to the WAN (e.g., DSL).
RAS_or_Internet_access Only for OpenScape Office MX	No RAS or Internet connection. RAS or Internet connection was dropped.
SIP_connections	SIP phones or Access Points cannot register or lose registration. SIP Phones cannot be called. No registration at the ITSP possible. Cannot make calls to ITSP. Calls from ITSP are not signaled at phones. DTMF signals cannot be sent or received over ITSP connection. Faxes cannot be transmitted or received over the ITSP connection.
Voice_fax_connection	Missing or garbled voice or fax connection. Wrong display. False LED signals. Interrupted calls or faxes. No Music On Hold User cannot make or answer call. Call not ringing at phone. No dial tone.
VPN Only for OpenScape Office MX	No access via VPN. The VPN connection was interrupted.
Web-based management	Login at OpenScape Office Assistant not possible. Configuration data not applied. Configuration data lost at second invocation of a web page.



## Trace Components

Trace components can be used to record the process and status information of individual components of the communication system.

All trace components can be stopped together and started or stopped individually by an administrator with the **Expert** profile. Starting and stopping a trace component activates and deactivates the recording. The level of detail for the trace can be defined via trace levels (0 = lowest level of detail to 9 = maximum level of detail).

The color of the list item displayed in the menu tree indicates the status of the trace component (green = trace component activated, red = trace component not activated). **Start/Stop Trace Component** can be used to enable or start an inactive trace component (red bullet point) and to disable or stop an active trace component (green bullet point).

A Trace Component display shows the subsystem name, the trace component index, the set trace level, the status information and whether or not the trace component is currently active. If a trace component needs to be edited, apart from changing the trace level, the trace component can also be started or stopped.

## TCP Dump

A TCP dump is used for monitoring and evaluating data traffic in an IP network.

An appropriate application is required for the diagnosis of the TCP dump files.

TCP dumps are often used to

- generate a LAN trace for a short period of time (e.g., for a reproducible error image).
- allow authorized service technicians to remotely access a LAN trace, for example via SSDP.

Advantages over RPCAP daemon: remote access is possible, so trace files do not have to be sent by e-mail

Disadvantages compared to RPCAP daemon: long-term traces are not meaningful; limited storage space, no capture filter can be set, more complex handling for several individual traces

## RPCAP (Remote Packet Capture) Daemon

An RPCAP daemon is used for monitoring and evaluating data traffic in an IP network.

The RPCAP daemon enables external applications to remotely access the TCP/IP packets on the LAN interfaces of the communication system.

An RPCAP a daemon is often used for long-term traces, since the trace files are stored on a PC and not in the communication system.

Advantages over TCP dump: faster and easier to use, long-term traces possible, number and/or size of the trace files can be freely selected, trace of internal LAN possible

Disadvantages compared to TCP dump: double network traffic and therefore increased load on the LAN interfaces of the communication system, special opening of ports needed (firewall)

## 19.7.5 Events (LX/MX)

Events provide information about communication system deficiencies. All events are written to a log file that is restricted in size. A new file is created if the maximum file size is exceeded. Up to seven files can be created.

Depending on the setting in the reaction table and the problem class, events may generate an SNMP trap, trigger an e-mail and/or start or stop trace monitoring. The event log (Event Viewer) can be evaluated, configured, and saved via OpenScape Office Assistant.

To interpret the event log file, you must download and extract the file with OpenScape Office Assistant. The file can then be opened, edited and printed using any text editor. Once the event log file has been transferred, the file can be deleted from the communication system's memory.

Events that can trigger actions are defined by the following properties:

- Event code:  
Identifies an event such as `MSG_ADMIN_LOGGED_OUT` = Logout information of an administrator.
- Event type:  
The following different types exist:
  - Information: plain status messages, no error messages.
  - Warning: report of a possibly problematic procedure or status, but not an error message.
  - Minor: error message. The error has no problematic consequences.
  - Major: error message. This error could cause problems.
  - Critical: Error Message. This error causes problems.
  - Cleared: error message. The error was already corrected by the communication system.
  - Indeterminate: error message. The cause of the error cannot be accurately determined.
- Event text  
Some event texts contain variable data. These are identified in the following manner:
  - %s: character string
  - %u: positive or negative decimal number
  - %f: floating point number
  - %p: indicator (memory address)
  - %x: hexadecimal number (with lower-case letters)
  - %X: hexadecimal number (with upper-case letters)
  - %C: single character

- %d and %l: positive decimal number

### **Reaction Table**

For each possible event, the Reaction Table can be used by an administrator with the **Expert** profile to independently define what action is to be taken when that event occurs.

You can set whether an SNMP trap should be sent, whether the communication system should be restarted, whether the e-mail should be sent, and whether a trace profile should be started or stopped. If the event is assigned a trace profile, the name of this profile is shown.

### **E-mail Settings**

These settings can be made by an administrator with the **Expert** profile to define how e-mails are sent when an event occurs.

### **Diagnosis Logs**

The communication system logs certain process-specific actions in diagnosis logs. These log files can be evaluated for diagnostic purposes by an administrator with the **Expert** profile.

## **19.7.6 Configuration Data for Diagnostics**

"Smaller" backup sets containing diagnostic data for Service Support can be created for diagnostic purposes. In contrast to normal backup sets, significantly smaller data amounts are produced for this purpose and can thus be easily sent with an e-mail, for example.

Diagnostics backup sets include, among other things, the configuration data of the communication system and the UC Suite (integrated applications). Voicemails, fax messages and announcements are not included.

The following media can be used to save backup sets for diagnostics:

- **USB Device**

The data can be backed up to a connected USB drive or a connected USB stick, for example.

---

**NOTICE:** If a USB hard disk, a partition thereof, or a USB stick is to be used for the backup, it must be formatted with FAT 32. USB media formatted with NTFS are read-only. Note that if multiple partitions exist, only the first partition can be used for the backup. If a bootable USB device is used for the backup, this USB device must be safely removed after the backup.

---

## Maintenance

### Monitoring and Maintaining the UC Suite

- **HTTP**

The data can be backed up using HTTPS to a Web server on the Internet or intranet.

---

**INFO:** It is not possible to create a backup on the hard disk of the communication system.

---

---

#### Related Topics

- [Backup and Restore](#)

## 19.8 Monitoring and Maintaining the UC Suite

The OpenScape Office Assistant administration tool, which is integrated in OpenScape Office, offers an administrator with the **Expert** profile numerous functions for monitoring and maintaining the UC Suite (i.e., the integrated applications).

### 19.8.1 Logging

The execution of the UC Suite (integrated applications) is monitored internally by the system. **System Logging** can be used to set whether logs should be created. In addition, a log of the activities of the UC Suite (e.g., the start of an application) is maintained in **Client Logs**.

#### System Logging

The following system logs can be enabled or disabled:

System log	Default setting
Log Trace Messages (Verbose)	Not activated

The results of the enabled system log are written daily to a log file with the designation `vs-yyyy-mm-dd.log` (e.g., `vs-2010-08-16.log`) and stored in the communication system under `/var/system/trace_log/vsl/log`.

---

**INFO:** The analysis of these log files can only be performed by Development.

---

## Client Logs

**Client Logs** are the log files of the UC Suite (integrated applications). For each application (myPortal for Desktop, myAttendant, etc.) and station (user), a separate directory is created, and the relevant log files are stored in it. The logs record the activities of a subscriber such as starting the application, outgoing and incoming calls, etc.

The path in which the `CC-Logs` directory with the directories for the individual applications is to be stored can be defined. You can also select whether the directory is to be stored on every client PC or on a central PC or server on the network.

By default, the `CC-Logs` directory is stored in the following path:

`<Drive>:\Documents and Settings/<PC User Name>/CC-Logs`

The retention period for **Client Logs** is 5 days. No changes are possible.

The logging of the UC Suite activities in **Client Logs** is enabled by default. Administrators with the **Advanced** profile can disable logging on a station-specific basis by using the **User Directory** wizard. An administrator with the **Expert** profile can disable logging on a station-specific basis in **Expert Mode**.

An administrator with the **Advanced** profile can use the **Trace** wizard to download the client logs (log files) of the applications (myPortal for Desktop, myAttendant, etc.) used by the internal subscribers.

An administrator with the **Expert** profile can use the **Expert mode** wizard to download the client logs (log files) of the applications (myPortal for Desktop, myAttendant, etc.) used by the internal subscribers.

## 19.8.2 Notification

**E-mail notifications** can be sent to the entered **Recipients** to provide advance warnings about critical disk usage levels for the hard disk, for example, or about errors.

The sending of e-mails can be linked to the following **conditions**:

Conditions	Default setting
Send Critical Messages	Activated
Send Crash Notifications	Activated

In addition, you can define how many of the last lines of a log file should be included with the sent e-mail.

The Send Critical Messages and Send Crash Notifications settings should be enabled and thus sent. These messages warn the entered recipients about a potential problem that needs to be reported to the responsible Service Support.

## 19.8.3 Maintenance

Retention periods for messages, calls information in the Call Journal and for log files can be defined via the Maintenance.

You can also set at what time daily the deletion of messages, call information in the call journal and log files for which the set retention periods have expired is to occur. The default setting is 2:00 a.m.

For more information on **Message Maintenance**, see [Voicemail Box](#).

For more information on **Calls Information Maintenance**, see [Journal](#).

During **Log File Maintenance**, the log files for which the set retention periods have expired are deleted. The default setting for the retention period for log files is 10 days.

## 19.9 Remote Services

Different Remote Services provide remote access to the communication system and the connected components to authorized service technicians. This reduces the cost of maintenance activities, while still providing users with on-site support in solving their problems.

### 19.9.1 Remote Access (MX)

Remote access can be used by authorized service technicians to access the OpenScape Office MX communication system via an ISDN or Internet connection. This ensures that support is available when solving administration tasks or performing troubleshooting.

You must enable remote access to activate remote access to the communication system. The following access methods are possible:

- Access via ISDN connection  
To dial in via ISDN, the service technician needs a valid direct inward dialing phone number (**MSN/DID Number**) for the communication system.  
Note that for remote access via an ISDN connection, longer waiting times may be experienced due to the limited transmission speed.

- Access via Internet connection  
To dial in via the Internet, the service technician needs a special port (**Port Number**) to access the communication system. Port number 10099 is specified by default.  
When using an external router, port forwarding of the port number must be set up in the external router for remote access to the communication system.

---

**INFO:** The port number for Internet access to the communication system must not be blocked by a possible firewall on the PC of the service technician. Port number selection should therefore be coordinated with the service technician.

---

You must disable remote access to block remote access to the communication system.

---

**NOTICE:** To prevent unauthorized access to the communication system, remote access must be turned off on completing the remote administration.

---

## 19.9.2 SSDP (Smart Services Delivery Platform)

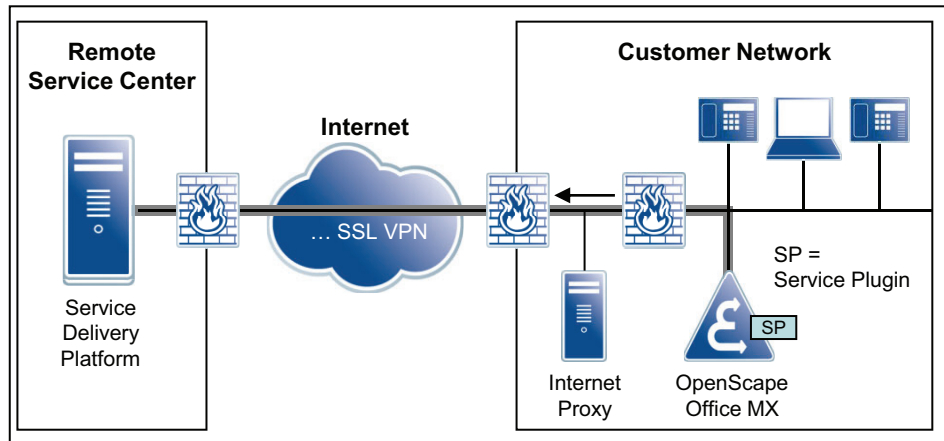
SSDP is the new Internet-based platform for Remote Services from Siemens Enterprise Communications GmbH & Co. KG. In contrast to SIRA (Secured Infrastructure for Remote Access), SSDP does not require any expensive and slow dial-up connections and cumbersome configurations of VPN connections. Apart from the significantly higher bandwidth, SSDP also guarantees greater security.

SSPD offers the following major advantages in combination with OpenScape Office:

- Maximum security through outbound Internet connection  
The entire remote connection setup is always initiated by the communication system. This means that the firewall of the customer network must only allow one HTTP connection to a single address in the Remote Service Center. Under normal circumstances, no changes to the security policy or firewall of the customer are required, so high security for the customer network is effectively guaranteed.  
with SSDP, the administrator of the communication system retains control over the remote connection by simply enabling and disabling access.
- High bandwidth  
Due to the broadband Internet connection, diagnostics data can be transmitted much faster, thus increasing the quality of service.
- Simple and cost-effective setup  
The software of the communication system already includes a so-called Service Plugin for SSDP. On setting up the communication system, an automatic registration at the Remote Service Center occurs.

- Future-proof  
The Smart Services Delivery Platform is the basis for future (value-added) services such as automated backups, reporting and monitoring, for example.

**Figure:** Smart Services Delivery Platform – Overview of OpenScope Office MX



SSDP supports all the usual Web Services Standards, including the Hypertext Transfer Protocol (HTTP), Simple Object Access Protocol (SOAP) and Extensible Markup Language (XML).

All components of the Smart Services Delivery Platform have been certified by the SSL (Secure Sockets Layer) certification authority VeriSign. Communications between the customer side and the Remote Service Center are always secured using 128-bit SSL encryption.

By entering the appropriate code, the customer controls the activation and deactivation of a VPN connection for remote service via a system telephone.

### Activation and Deactivation

You have the following options for activating and deactivating the SSDP Service Plugin:

- Using the **Activate/Deactivate Service Plugin** wizard
- Entering the appropriate code via a system telephone  
For security reasons, the PIN configured in the communication system must be entered for the activation and deactivation via a system telephone. The configuration of this PIN is performed by an administrator with the **Advanced** profile.

---

**IMPORTANT:** The PIN applies to the activation/deactivation of both the remote service via VPN as well as the SSDP Service Plugin via a system telephone.

---



### 19.9.3 Remote Service via VPN (MX)

VPN connections provide a suitable mechanism for ensuring that the high bandwidth requirements for remote service and the increased security demands of customers can be met. By entering the appropriate code, the customer controls the activation and deactivation of a VPN connection for remote service via a system telephone.

As a prerequisite, the remote service via VPN requires the configuration of an inactive VPN connection (VPN tunnel) from the communication system of the customer to a Remote Service Center. The **Enable Remote Service via VPN** flag, which can be activated via a service code, ensures that only VPN connections for the remote service can be enabled or disabled via codes.

For security reasons, the PIN configured in the communication system must be entered for the activation and deactivation via a system telephone. The configuration of this PIN is performed by an administrator with the **Advanced** profile.

---

**IMPORTANT:** The PIN applies to the activation/deactivation of both the remote service via VPN as well as the SSDP Service Plugin via a system telephone.

---

### 19.9.4 PIN for Activating and Deactivating the Remote Service via VPN and the SSDP Service Plugin

The activation and deactivation of the remote service via VPN and of the SSDP Service Plugin are PIN-protected.

The PIN configured in the communication system must be entered for the activation and deactivation via a system telephone. The configuration of this PIN is performed by an administrator with the **Advanced** profile.

---

**IMPORTANT:** The PIN applies to the activation/deactivation of both the remote service via VPN as well as the SSDP Service Plugin via a system telephone.

---

### 19.9.5 Online User ( LX/MX)

The Online User enables the remote control, verification and monitoring of OpenStage telephones via a Windows PC. The behavior of an OpenStage telephone is recreated via the Online User on the PC.

In order to communicate with an OpenStage phone, the phone software must have a so-called dongle key.

The following entries must be made via the Online User in order to access an OpenStage telephone:

- OpenStage phone type
- IP address of the OpenStage telephone
- Administrator password of the OpenStage telephone

Details on using the Online User can be obtained from the following documentation: *OpenStage HUSIM Phone Tester User Guide*. Access to this document is available via the intranet portal for technical product documentation at [http://apps.g-dms.com:8081/techdoc/search\\_en.htm](http://apps.g-dms.com:8081/techdoc/search_en.htm).

## 20 Appendix

This appendix contains reference information such as the supported languages, standards, configuration limits and capacities, Euro-ISDN features, codes for enabling and disabling features, feature codes using DTMF and the IP protocols and port numbers used.

### 20.1 Languages Supported

Several different language variants are available for the various target groups such as subscribers, customer administrators, administrators and service technicians.

These languages will be released as part of the country-specific introduction.

		de	en	cs	da	es	fi	fr	hr	hu	it	nl	no	pl	pt	ru	sv	tr
OpenScape Office	myAgent	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	myAttendant																	
	myPortal for Desktop																	
	myPortal for Mobile																	
	myPortal for OpenStage																	
	myPortal for Outlook																	
	myReports	X	X	X	-	X	X	X	-	-	X	X	-	X	X	X	-	-
TUI (Telephone User Interface)		X	X	-	X	X	X	X	X	X	X	X	X	X	X	X	X	X
OpenScape Office Assistant (the language can be set at login.)		X	X	-	-	X	-	X	-	-	X	-	-	-	X	-	-	-

---

**INFO:** A Russian Windows operating system is required in order to use the Russian user interface of myPortal for Outlook.

---

The following language codes (ISO 639-1) are used for the abbreviations in the table:

- de = German
- en = English
- cs = Czech
- da = Danish
- es = Spanish
- fi = Finnish
- fr = French
- hr = Croatian
- hu = Hungarian

- it = Italian
- nl = Dutch
- no = Norwegian
- pl = Polish
- pt = Portuguese
- ru = Russian
- sv = Swedish
- tr = Turkish

## **20.2 Supported Standards (LX/MX)**

### **Ethernet**

- RFC 894 Ethernet II Encapsulation
- IEEE 802.1Q Virtual LANs
- IEEE 802.2 Logical Link Control
- IEEE 802.3u 100BASE-T
- IEEE 802.3X Full Duplex Operation

### **IP Routing**

- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 2822 Internet Message Format
- RFC 826 ARP
- RFC 2131 DHCP
- RFC 1918 IP Addressing
- RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
- RFC 1334 PPP Authentication Protocols
- RFC 1618 PPP over ISDN
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 1877 PPP Internet Protocol Control Protocol
- RFC 1990 The PPP Multilink Protocol (MP)
- RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE)
- RFC 3544 IP Header Compression over PPP

### **NAT**

- RFC 2663 NAT

### **IPSec**

- RFC 2401 Security Architecture for IP
- RFC 2402 AH - IP Authentication Header
- RFC 2403 IPsec Authentication - MD5
- RFC 2404 IPsec Authentication - SHA-1
- RFC 2405 IPsec Encryption - DES
- RFC 2406 ESP - IPsec encryption
- RFC 2407 IPsec DOI
- RFC 2408 ISAKMP
- RFC 2409 IKE
- RFC 2410 IPsec encryption - NULL
- RFC 2411 IP Security Document Roadmap
- RFC 2412 OAKLEY

### **SNMP**

- RFC 1213 MIB-II

### **QoS**

- IEEE 802.1p Priority Tagging
- RFC 1349 Type of Service in the IP Suite
- RFC 2475 An Architecture for Differentiated Services
- RFC 2597 Assured Forwarding PHB Group
- RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)

### **Services**

- RFC 2597 Assured Forwarding PHB Group
- RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)

### **Codecs**

- G.711
- G.729

### **VoIP over SIP**

- RFC 2198 RTP Payload for Redundant Audio Data
- RFC 2327 SDP Session Description Protocol
- RFC 2617 HTTP Authentication: Basic and Digest Access Authentication
- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 3261 SIP Session Initiation Protocol
- RFC 3262 Provisional Response Acknowledgement (PRACK) Early Media
- RFC 3263 SIP Locating Servers

- RFC 3264 An Offer/Answer Model with the Session Description Protocol
- RFC 3310 HTTP Digest Authentication
- RFC 3311 Session Initiation Protocol (SIP) UPDATE Method
- RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
- RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3489 STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 3515 The Session Initiation Protocol (SIP) Refer Method
- RFC 3550 RTP: Transport Protocol for Real-Time Applications
- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control
- RFC 3581 An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
- RFC 3891 The Session Initiation Protocol (SIP) Replaces Header

**XMPP**

- RFC 3920 Extensible Messaging and Presence Protocol (XMPP): Core
- RFC 3921 Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence

**Other**

- RFC 959 FTP
- RFC 1305 NTPv3
- RFC 1951 DEFLATE

## 20.3 Configuration Limits and Capacities

The configuration limits and capacities described here are based on system-specific maximum values and the maximum values for a network.

The maximum values refer to

- the hardware capacity limits of OpenScape Office MX.
- the system-specific capacity limits of OpenScape Office LX and OpenScape Office MX.
- the software capacities of OpenScape Office LX, OpenScape Office MX, OpenScape Office HX and a network.

**Hardware Capacity Limits of OpenScape Office MX**

System Box	Maximum configuration
OpenScape Office MX System Box	3

Gateway module	Interfaces	B channels
GMS (not for U.S. and Canada)	4 S <sub>0</sub> ports for the ISDN trunk connection or ISDN station connection	8
GMSA (not for U.S. and Canada)	4 S <sub>0</sub> ports for the ISDN trunk connection or ISDN station connection and 4 a/b interfaces for the analog station connection	8 + 4 <sup>1</sup>
GME (not for U.S. and Canada)	1 S <sub>2M</sub> interface for the ISDN Primary Rate Interface	30
GMT (for U.S. and Canada only)	1 T1 interface for the ISDN Primary Rate Interface	24
GMAA	4 a/b interfaces for the analog trunk connection and 2 a/b interfaces for the analog station connection	4 + 2
GMAL	8 a/b interfaces for the analog station connection	8

<sup>1</sup> Due to the increased demand for resources on enabling Signaling and Payload Encryption (SPE), the following restriction applies to a GMSA gateway module. For this gateway module, either a maximum of 3 S<sub>0</sub> ports and 4 a/b interfaces or 4 S<sub>0</sub> ports and 2 a/b interfaces may be used.

### System-specific Capacity Limits of OpenScope Office LX and OpenScope Office MX

Stations		Maximum configuration	
		OpenScope Office LX	OpenScope Office MX
IP stations:			
	Total of system phones, SIP stations, adapters, WLANs per communication system	500, of which 2 are reserved for remote and server access	150, of which 2 are reserved for remote and server access
TDM stations:			
	ISDN stations (S <sub>0</sub> stations) per communication system	ISDN stations via gateway	48 S <sub>0</sub> stations can be configured (at max. 36 S <sub>0</sub> ports: 3 boxes x 3 slots x 4 S <sub>0</sub> ports each)
	Analog stations per communication system	Analog stations via adapters or via gateway	72 (3 system boxes with 3 X GMAL each and further analog stations via adapters)
Mobility Stations:			
	Mobility Entry: stations per communication system	–	150 <sup>1</sup>
	myPortal for Mobile/Tablet: stations per communication system	200	100 <sup>1</sup>
Sum total of all IP, TDM and Mobility stations		500	150 per communication system, 50 per system box
Virtual stations (freely configurable)		70	70

<sup>1</sup> The total number of Mobility stations must not exceed 150.

**Appendix**  
Configuration Limits and Capacities

Trunks	Maximum configuration	
	OpenScope Office LX	OpenScope Office MX
Total of all trunks per communication system	220 (IP trunks) ISDN and analog trunks via gateway	220 (IP, ISDN and analog trunks)
<b>Info for OpenScope Office MX:</b>		
A total of up to 220 IP, ISDN and analog trunks can be used, without exceeding a maximum number of 120 IP trunks. By default, 30 channels are reserved for the UC Suite.		
By default, 120 trunks (channels) are preconfigured.		
Examples for the maximum configuration:		
<ul style="list-style-type: none"> <li>8 x GME gateway modules = 8 x 30 channels = 240 ISDN trunks As a prerequisite for using 240 ISDN trunks, the channels reserved for the UC Suite must be reduced from 30 to 10!</li> <li>9 x GMT gateway modules = 9 x 24 channels = 216 T1 analog trunks + 20 IP trunks As a prerequisite for using 236 trunks (216 analog trunks + 20 IP trunks), the channels reserved for the UC Suite must be reduced from 30 to 14!</li> <li>5 x GME gateway modules = 5 x 30 channels = 150 ISDN trunks + 90 IP trunks As a prerequisite for using 240 trunks (150 ISDN trunks + 90 IP trunks), the channels reserved for the UC Suite must be reduced from 30 to 10!</li> </ul>		

Administration	Maximum configuration	
	OpenScope Office LX	OpenScope Office MX
User profiles	3 (Basic, Advanced, Expert)	3 (Basic, Advanced, Expert)
Simultaneous administrator accesses	5, but only one has write access	5, but only one has write access

**Software Capacities of OpenScope Office LX, OpenScope Office MX, OpenScope Office HX and a Network**

The specifications in the Network column refer to a network of OpenScope Office LX, OpenScope Office MX and OpenScope Office HX with a total of 1000 subscribers. The following abbreviations are used:

- : Not applicable / relevant
- =: The capacity of each individual networked communication system applies, regardless of the network size.
- +: The maximum configuration of the network is equal to the total capacities of the networked communication systems.

Topic: Connection to Service Provider	Maximum configuration			
	OpenScope Office LX	OpenScope Office MX	OpenScope Office HX	Networking
ITSP (Internet Telephony Service Provider) connection:				
ITSP trunks per communication system	128	32	-	=
Simultaneously activated ITSPs per communication system	4	4	-	=



Topic: Stations		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
Classes of Service:					
	Classes of Service per communication system	15	15	–	=
Station numbers:					
	Digits per station number	16 (default setting = 3)	16 (default setting = 3)	–	=

Topic: Unified Communications		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
	myAttendant	20 (license-dependent)	20 (license-dependent)	20 (license-dependent)	+
	myPortal for Desktop	500 (license-dependent)	150 (license-dependent)	500 (license-dependent)	1000 <sup>1</sup>
	myPortal for Outlook	500 (license-dependent)	150 (license-dependent)	500 (license-dependent)	1000 <sup>1</sup>
AutoAttendant:					
	Personal AutoAttendant	Available for every user of myPortal for Desktop and myPortal for Outlook	Available for every user of myPortal for Desktop and myPortal for Outlook	Available for every user of myPortal for Desktop and myPortal for Outlook	=
	Central AutoAttendant	1	1	1	=
Call journal (myPortal for Desktop and myPortal for Outlook):					
	Archiving duration in the UC clients	30 days (default setting = 30 days)	30 days (default setting = 30 days)	30 days (default setting = 30 days)	–
	Archiving duration in the communication system	365 days (default setting = 30 days)	365 days (default setting = 30 days)	365 days (default setting = 30 days)	–
	Call journal entries	Unrestricted	Unrestricted	Unrestricted	–
Recording calls/conferences: <sup>2</sup>					
	Recording length per call/conference	Limited by the length of the call/conference	Limited by the length of the call/conference	Limited by the length of the call (only call recording possible)	–
Application-controlled conferences:					

**Appendix**

Configuration Limits and Capacities

Topic: Unified Communications		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
	Simultaneous conferences per communication system	5	5	–	–
	Participants per conference	16	16	–	–
	External participants per conference	15	15	–	–
	Conference channels	40	20	–	–
External database connectivity (LDAP, SQL, etc.):					
	External database connections per communication system	10	10	10	=
	Simultaneous LDAP accesses via system phones per communication system	20	20	–	=
	LDAP connection via OpenStage 60, 60 G, 80, 80 G	One LDAP connection possible per telephone	One LDAP connection possible per telephone	–	–
	LDAP usage via UC clients (myAttendant, myPortal for Desktop, etc.)	Every client can use the central LDAP connection of the communication system	Every client can use the central LDAP connection of the communication system	Every client can use the central LDAP connection of the communication system	–
	SQL usage via UC clients (myAttendant, myPortal for Desktop, etc.)	Every client can use the central SQL connection of the communication system	Every client can use the central SQL connection of the communication system	Every client can use the central SQL connection of the communication system	–
Voicemail box: <sup>2</sup>					
	Voicemail boxes per communication system	500	150	Depending on the communication system of the HiPath 3000 systems family	=
	Recording length	15 minutes per call (1 minute of voice corresponds to approx. 1 MB of storage space)	15 minutes per call (1 minute of voice corresponds to approx. 1 MB of storage space)	15 minutes per call (1 minute of voice corresponds to approx. 1 MB of storage space)	=
	Simultaneous calls (incoming and outgoing)	30	30	30	=
Fax box: <sup>2</sup>					

Topic: Unified Communications		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
	Fax boxes per communication system	500	150	250 (depending on the communication system of the HiPath 3000 systems family)	=
	Fax length in pages	500 (1 standard fax (2 DIN A4 pages) corresponds to approx. 48 KB of storage space)	500 (1 standard fax (2 DIN A4 pages) corresponds to approx. 48 KB of storage space)	500 (1 standard fax (2 DIN A4 pages) corresponds to approx. 48 KB of storage space)	=
	Faxes to be simultaneously sent and received	2	2	2	=
	Merge fax recipients	Unrestricted	Unrestricted	Unrestricted	–
	Fax box groups per communication system	20	20	30	=
	Stations per fax box group	10	10	10	–
Announcements: <sup>2</sup>					
	Announcements per UC Suite subscriber	1 greeting announcement, 1 name announcement, 1 presence status based announcement and 1 announcement for the personal AutoAttendant	1 greeting announcement, 1 name announcement, 1 presence status based announcement and 1 announcement for the personal AutoAttendant	1 greeting announcement, 1 name announcement, 1 presence status based announcement and 1 announcement for the personal AutoAttendant	=
Presence status:					
	Status per UC Suite subscriber	9	9	9	=
	Voicemail announcements per presence status	1	1	1	=
	Forwarding destinations per presence status	6	6	6	=
Multi-user chat:					
	Internal communication partner	Unrestricted	Unrestricted	Unrestricted	+
	External XMPP communication partner	1	1	1	=

1 The maximum total number of myPortal for Desktop and myPortal for Outlook users is 1000.

## Appendix

### Configuration Limits and Capacities

2 The total recording duration for voice announcements, voicemails, recorded voice calls and faxes depends on the hard disk capacity in the communication system. There are no individual limits per subscriber.

80 GB hard disk: approx. 8000 minutes in total (corresponds to approx. 8 GB of storage space on the hard disk)

160 GB hard disk: approx. 16000 minutes in total (corresponds to approx. 16 GB of storage space on the hard disk)

250 GB hard disk: approx. 40000 minutes in total (corresponds to approx. 40 GB of storage space on the hard disk)

Topic: Functions at the Telephone		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
Caller list:					
	Caller lists per communication system	650	650	–	+
	Entries per caller list	10	10	–	–
	Saved digits per entry	25-digit phone number and seizure code	25-digit phone number and seizure code	–	=
Direct station select keys (DSS keys):					
	Key modules per communication system	250	250	–	+
	Key modules per telephone	2	2	–	–
	Keys per key module	12 with OpenStage Key Module / 18 with OpenStage Key Module 15	12 with OpenStage Key Module / 18 with OpenStage Key Module 15	–	–
	Busy Lamp Fields (BLF) per communication system	12	12	–	+
	Keys per Busy Lamp Field	90	90	–	–
Individual Speed Dialing (ISD):					
	Entries in the KWI pool per communication system	2000	2000	–	+
	Entries per station	10	10	–	–
	Digits per entry	25-digit phone number and seizure code	25-digit phone number and seizure code	–	–
System Speed Dialing (SSD):					
	Entries per communication system	1000	1000	–	1000
	Length of the Name entry	16	16	–	–
	Digits per entry	25-digit phone number and seizure code	25-digit phone number and seizure code	–	–
Redialing:					

Topic: Functions at the Telephone		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
Entries per telephone with display	3 for optiPoint 410, 420 and OpenStage 20 E, 20, 20 G, 40, 40 G / 10 for OpenStage 15. In OpenStage 60, 60 G, 80 and 80 G, a maximum of 30 entries per "Answered", "Missed" and "Dialed" call list can be used.	3 for optiPoint 410, 420 and OpenStage 20 E, 20, 20 G, 40, 40 G / 10 for OpenStage 15. In OpenStage 60, 60 G, 80 and 80 G, a maximum of 30 entries per "Answered", "Missed" and "Dialed" call list can be used.	–	–	
Entries per telephone without display	1	1	–	–	
Saved digits per entry	25-digit phone number and seizure code	25-digit phone number and seizure code	–	–	
<b>Call Waiting / Call Waiting Tone:</b>					
Waiting callers per telephone	16	16	–	–	
<b>Parking:</b>					
Park positions per communication system	10	10	–	–	
<b>Callback calls:</b>					
Callback entries per communication system	64	64	–	–	
Callback entries per telephone	5	5	–	–	
<b>Advisory Messages / Message Texts:</b>					
Advisory messages per communication system	250	250	–	–	
Message texts per communication system	150	150	–	–	
Configurable advisory messages / message texts per communication system	10 + 10	10 + 10	–	–	
Length of a configurable advisory message / message text	24	24	–	–	
Received advisory messages / message texts per telephone with display	5	5	–	–	
Received advisory messages / message texts per telephone without display	1	1	–	–	
<b>Ringing group on:</b>					
Stations included	5	5	–	–	
<b>Call Forwarding (CF):</b>					

## Appendix

### Configuration Limits and Capacities

Topic: Functions at the Telephone		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
	Entries per communication system	500	500	–	+
	FWD destinations per telephone	4	4	–	–
	Digits per external CFW destination	25-digit phone number and seizure code	25-digit phone number and seizure code	–	–
	Chained FWD destinations	5	5	–	–
System-controlled conferences:					
	Simultaneous conferences per communication system	6	6	–	–
	Participants per conference	8	8	–	–
	External participants per conference	7	7	–	–
	Conference channels	20	20	–	–
Entrance Telephone/Door Opener:					
	Connections via a/b interfaces per communication system	–	4	–	–
	Digits per code entry	–	5	–	–
Trunk queuing:					
	Simultaneous entries per communication system	–	10	–	–

Topic: Working in a Team (Groups)		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
Call pickup groups:					
	Call pickup groups per communication system	32	32	–	+
	Stations per call pickup group	32	32	–	=
Group calls, hunt groups, Basic MULAPs, Executive MULAPs, Team groups, Top groups and voicemail groups:					

Topic: Working in a Team (Groups)		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
	Total of group calls, hunt groups, Basic MULAPs, Executive MULAPs and voicemail groups per communication system	310	310	–	+
	Total number of Team groups and Top groups per communication system	500	150	–	+
	Sunscribers per group call, hunt group, Basic MULAP	20	20	–	–
	Subscribers per Executive MULAP, Team group, Top group	10	10	–	–
	Stations per voicemail group	20	20	–	–
	MULAP keys per telephone	10	10	–	–
Fax box groups:					
	Fax box groups per communication system: see				
UCD groups:					
	UCD groups per communication system	60	60	–	+
	Announcements per UCD group	7	7	–	–
	Priority levels per UCD group	10	10	–	–
	Queued calls per UCD group	30	30	–	–
UCD agents:					
	UCD agent IDs per communication system	150	150	–	–
	Simultaneously active UCD agents per communication system	64	64	–	+
Announcements for UCD:					
	Number of callers, per communication system, for whom an announcement can be simultaneously played	8	8	–	+

Topic: Call Routing		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
Toll restriction:					

**Appendix**  
Configuration Limits and Capacities

Topic: Call Routing		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
	Allowed lists	6	6	–	=
	Denied lists	6	6	–	=
	Allowed list, short (10 entries)	5	5	–	=
	Allowed list, long (100 entries)	1	1	–	=
	Short Denied list (10 entries)	5	5	–	=
	Long Denied list (50 entries)	5	5	–	=
	Number of characters in list entries	25	25	–	=
Least Cost Routing LCR):					
	Dialed/Verified digits	24	24	–	–
	Dial Plans	1000	1000	–	=
	Route tables	254	254	–	=
	Routes per routing table	16	16	–	–
	Dial rules per route	254	254	–	–
	Digits per dial rule	40	40	–	–
Night service:					
	Authorized stations per communication system	1	1	–	–
E911 Emergency Call Service (for the U.S. only):					
	Digits per LIN (Location Identification Number)	16	16	–	=
Hotline after Timeout / Hotline:					
	Hotline destinations per communication system	6	6	–	+
CON groups:					
	CON groups per communication system	16	16	–	=

Topic: Multimedia Contact Center		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
myAgent:					
	Licensable agents	64	64	64	+
	Simultaneously active agents	64	10 per one-box system / 64 pro multibox system	64	+



Topic: Multimedia Contact Center		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
myReports		1	1	1	+
Queues:					
	Queues per communication system	50	50	50	+

Topic: Mobility		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
Teleworker workplaces:					
	Teleworker workplaces via VPN per communication system	Possible via external router	10	–	+
	Teleworker workplaces via the UC Suite (CallMe service) per communication system	Available for every system telephone	Available for every system telephone	–	+
Mobility Stations:					
	Mobility Entry: stations per communication system	–	150 <sup>1</sup>	100 <sup>2</sup>	=
	myPortal for Mobile/Tablet: stations per communication system	200	100 <sup>1</sup>	100 <sup>2</sup>	=
HiPath Wireless Standalone Access Points:					
	HiPath Wireless Standalone APs per communication system	10	10	–	+

1 The total number of Mobility stations must not exceed 150.

2 The total number of Mobility stations must not exceed 100.

Topic: Security		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
VPN:					
	VPN tunnel	Possible via external VPN router	256	–	=
	VPN rules		640, of which 6 are reserved (for default rules), 634 free	–	=
Individual lock code:					
	Digits per phone lock code	5	5	–	–
	Allowed digits	0 through 9	0 through 9	–	–

## Appendix

### Configuration Limits and Capacities

Topic: Networking OpenScape Office <sup>1</sup>		Maximum configuration	
Networking of OpenScape Office LX and OpenScape Office MX:			
Networked communication systems (nodes)	8		
Stations in the network	1000		
Networking of OpenScape Office LX, OpenScape Office MX and OpenScape Office HX:			
Networked communication systems (nodes) <sup>2</sup>	64		
Stations in the network	1000		

1 Project-specific releases can be requested for networking requirements beyond the configuration limits listed here. Please also refer to the current Sales Release.

2 A total of up to 64 communication systems can be networked, of which a maximum of up to eight OpenScape Office LX, OpenScape Office MX and HiPath 3000 systems can be deployed with OpenScape Office HX. A maximum of four OpenScape Office LX and/or OpenScape Office MX communication systems can be integrated in an existing network with HiPath 5000 RSM (Real-Time Services Manager). The deployment of OpenScape Office HX is not possible.

Topic: Accounting		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
Call Detail Recording Central:					
Entries in the call data buffer per communication system	20000	20000	–	–	
Account Code (ACCT):					
Account code entries per communication system	1000	1000	–	–	
Verifiable digits per Acc. code	11	11	–	–	
Allowed digits	0 through 9	0 through 9	–	–	

Other Topics		Maximum configuration			
		OpenScape Office LX	OpenScape Office MX	OpenScape Office HX	Networking
CSTA:					
CSTA links via CSP per communication system	6 (license-dependent)	6 (license-dependent)	–	+	
CSTA monitoring points per communication system	1500	700	–	–	

## 20.4 Euro-ISDN Features (LX/MX)

The Euro-ISDN features can be used at every Euro-ISDN port if the available hardware (phone or ISDN card, for instance) is appropriately configured. The features are either available permanently in the Central Office or activated/deactivated with codes.

The availability of features depends on the network provider. Some of the named features are subject to charges.

Topic	Explanation
Multiple Subscriber Number (MSN)	Every point-to-multipoint connection can be assigned several phone numbers. The user can assign these phone numbers to the individual terminals directly at the terminals.
Calling Line Identification Presentation (CLIP)	The actual phone number is transmitted to the called station and appears, for example, on the phone's display or in the caller list if the call is not answered. Incorrect phone numbers cannot be transmitted. Direct inward dialing from TC systems cannot be checked, however. Phone number transmission can be suppressed on a case-by-case basis or for all calls.
Calling Line Identification Restriction (CLIR)	Phone number transmission can also be deactivated either permanently or on a case-by-case basis. If deactivated, phone numbers are only displayed at specially defined B stations (emergency help lines, police, fire department).
Malicious Call Identification (MCID)	The called party can have an anonymous caller traced by the attendant console, even if phone number transmission is deactivated. A charge is applied for this feature.
Terminal Portability (TP)	This feature lets you move the ISDN phone you are using and plug it into a different ISDN jack without interrupting an ongoing call. You must park the ongoing call before you move the ISDN phone.
Subaddressing (SUB)	This function is subject to an additional charge and can be used in addition to the normal phone number. Subaddressing lets you operate a dialable phone (for example, a program on the PC) depending on the caller.
User to User Signaling (UUS)	Information can be exchanged over the D channel during connection setup and clear-down. Transmission is possible in both directions.
Closed User Group (CUG)	If you activate this feature, no calls are possible outside the user group (apart from the emergency numbers 110 and 112). External callers can also be blocked.
Call Forwarding Busy (CFB)	This call forwarding variant routes calls on busy to an arbitrary available phone. Call forwarding is performed in the attendant console. This leaves both B channels free.
Call Forwarding Unconditional (CFU)	This call forwarding variant routes calls immediately to an arbitrary available phone. Call forwarding is performed in the attendant console. This leaves both B channels free.

## Appendix

### Features of the UC Clients that can be used with SIP Telephones

Topic	Explanation
Call Forwarding No Reply (CFNR)	This call forwarding variant routes calls after 20 seconds (if the destination cannot be reached) to an arbitrary available telephone. Call forwarding is performed in the attendant console. This leaves both B channels free.
Call waiting (CW)	A second caller is signaled during an ongoing connection. The caller meanwhile hears the ringback tone. The camp-on connection can be accepted, declined or simply ignored.
Toggle (Hold = Call Hold)	The Consultation feature lets you set up a second connection while another connection is already ongoing. Switching back and forth between two connections is known as toggling. The party on hold cannot overhear the other active call.
Three Party Service (3-PTY)	Two existing connections can be joined together. A three-party conference can be conducted by three subscribers.
Completion of Calls to Busy Subscriber (CCBS; automatic callback on busy)	You can activate this feature if a station called is busy. You hear a signal as soon as this station's port is free. The connection is cleared down by replacing the handset.
Advice of Charge (End) (AOCE)	You can program the application to display call charges at the end of a call. This does not take account of any discounts or tariffs.
Advice of Charge (During) (AOCD)	You can program the application to display call charges during a call. This does not take account of any discounts or tariffs.

---

#### Related Topics

- [Codes for Activating and Deactivating Features \(LX/MX\)](#)

## 20.5 Features of the UC Clients that can be used with SIP Telephones

The following features of the UC clients myAttendant, myPortal for Desktop and myPortal for Outlook can be used with SIP telephones.

The used SIP telephone must satisfy the following prerequisites:

- 3PCC as per RFC 3725 is supported.
- The "Call waiting" feature is supported.

- Do Not Disturb is disabled.  
Alternatively, for subscribers with SIP phones, DND can be activated in the communication system.

---

**INFO:** The full functionality of the features depends on the SIP phone used and cannot be guaranteed.

A successful test of the features was performed with OpenStage 15.

---

- Connection-/call-oriented features:
  - Make Call
  - Redirect call
  - Resume call
  - Application-controlled conference
  - Placing a call on hold
  - Alternate (Toggle/Connect)
  - Consultation
  - Disconnect
  - Transfer
- Phone-oriented features:
  - Do Not Disturb
  - Call forwarding

## 20.6 SIP Features Supported by OpenScape Office

The following SIP features are supported by OpenScape Office.

---

**INFO:** The full functionality of the features depends on the SIP phone used and cannot be guaranteed.

---

- Authentication  
Before using a SIP phone, the phone must be registered at the communication system using the configured call number. To protect against SIP attacks (SIP Attack Protection), authentication is strongly recommended.
- Basic call  
Both incoming and outgoing calls as well as late SDP connection setups are supported.
- Display of name and telephone number  
During the call setup, the name and number of the SIP phones involved appear on the display. As a prerequisite, the names must have already been configured in the communication system, and no restrictions (caller ID suppression of the caller and/or called party) should apply.  
SIP phones generally allow the configuration of a device name. However, instead of any device name that may have been configured, OpenScape Office always shows the name configured in the communication system.

## Appendix

### Codes for Activating and Deactivating Features (LX/MX)

- Call waiting  
The feature is disabled in the default setting of the communication system. Activation is possible on a station-specific basis using station flags.
- Call forwarding  
In general, SIP phones allow the configuration of call forwarding destinations. Call Forwarding on Busy (CFB), Call Forwarding Unconditional (CFU) and Call Forwarding No Reply (CFNR) are supported. It is important to ensure that the call forwarding configured in the SIP phone does not conflict with any other call forwarding that may have been configured in the communication system. For example, if call forwarding is configured in the SIP phone after 20 seconds, it would not be executed if the call forwarding configured in the communication system occurs after 15 seconds.
- Placing a call on hold, resuming a call and alternating between calls (toggle/connect)  
Placing a call on hold, resuming a call and alternating between calls (toggle/connect) are all supported. The communication system can play back Music on Hold (MOH) to subscribers on hold.
- Transfer  
Both blind transfers and consultation transfers (also called supervised transfers) are supported.
- Message Waiting Indication  
The signaling of new voice messages at the SIP phone is supported. The type of signaling depends on the phone being used (acoustic signaling using a special dial tone, optical signaling via a Mailbox key (if configured) and/or a display message).
- Different Call Signaling  
Different call signaling for internal and external calls and callbacks is supported. This requires the SIP telephone to be configured correctly.
- Video  
Video connections between the SIP phones of one OpenScape Office communication system or between the SIP phones of a homogeneous network of OpenScape Office communication systems are supported. Video connections to the ITSP are not possible.

## 20.7 Codes for Activating and Deactivating Features (LX/MX)

Users can activate and deactivate features on their respective phones by dialing certain codes.

The following tables contain the activation/deactivation codes for system phones (optiPoint 410, optiPoint 420, OpenStage), analog phones and ISDN phones.

In addition, it shows in which states of the phone a feature may or may not be activated or deactivated. The following abbreviations are used for this:

- RC = Ringer Cutoff
- RS = Ready State (after lifting the handset, for example)
- DI = Digit input state
- BS = Busy

- IC = Incoming Call
- OC = Outgoing Call
- TK = Talking

<b>Topic: Stations</b>					
<b>Feature</b>	<b>Code for</b>			<b>Not possible</b>	<b>Information / Notes</b>
	<b>System telephone</b>	<b>analog telephone</b>	<b>ISDN telephone</b>		
Key programming	*91 + XXX + YYY	–	–	IC, TK	XXX = Key to be programmed YYY = Call number or function code

<b>Topic: Unified Communications</b>					
<b>Feature</b>	<b>Code for</b>			<b>Not possible</b>	<b>Information / Notes</b>
	<b>System telephone</b>	<b>analog telephone</b>	<b>ISDN telephone</b>		
Initiate conference	*3	*3	723	–	Initiation from call state
End conference	#3	#3	733	RH, BR, DI, BS, IC, OC	

<b>Topic: Functions at the Telephone</b>					
<b>Feature</b>	<b>Code for</b>			<b>Not possible</b>	<b>Information / Notes</b>
	<b>System telephone</b>	<b>analog telephone</b>	<b>ISDN telephone</b>		
Enable advisory message (absence text)	*69 + XXX	*69 + XXX	7269 + XXX	BS, IC	XXX = Text number (0 = back at., 1 = on vacation till., 2 = traveling till., 3 = absent whole day, 4 = absent during afternoons, 5 = not reachable, 6 = home tel., 7 = representative., 8 = at time., 9 = am in room no.:)
Disable advisory message (absence text)	#69	#69	7369	BS, IC	
Accept call waiting	*55	*55	7255	–	
Allow call waiting (automatic)	*490	*490	72490	BS, IC	
Prevent call waiting (automatic)	#490	#490	73490	BS, IC	
Disable call waiting tone	*87	*87	7287	BS, IC	
Enable call waiting tone	#87	#87	7387	BS, IC	
Caller list: save call number	*82	–	–	RS, DI, IC	
Query caller list	#82	–	–	DI, IC, OC	

## Appendix

### Codes for Activating and Deactivating Features (LX/MX)

Topic: Functions at the Telephone					
Feature	Code for			Not possible	Information / Notes
	System telephone	analog telephone	ISDN telephone		
Do not disturb on	*97	*97	7297	BS, IC	
Do not disturb off	#97	#97	7397	BS, IC	
Directed call pickup	*59 + XXX	*59 + XXX	7259 + XXX	DI, BS, IC, OC	XXX = Station number of phone at which the call is signaled.
Call forwarding on	*11 + XXX + YYY	*11 + XXX + YYY	7211 + XXX + YYY	BS, IC	XXX = forwarding type (1 = all calls, 2 = only external calls, 3 = internal calls) YYY = Forwarding destination
Call forwarding off	#11	#11	7311	BS, IC	
Enable call forwarding after timeout	*12 + XXX	*12 + XXX	7212 + XXX	BS, IC	XXX = Forwarding destination
Disable call forwarding after timeout	#12	#12	7312	BS, IC	
Call forwarding on Out of Service On	*13 + XXX	*13 + XXX	7213 + XXX	BS, IC	XXX = Forwarding destination If the phone fails (due to an interruption in the line, for example), calls are forwarded to the selected destination (Call Forwarding Station Out Of Service CFSS).
Call forwarding on Out of Service Off	#13	#13	7313	BS, IC	
Associated Services	*83 + XXX + YYY	*83 + XXX + YYY	7283 + XXX + YYY	BS, IC	XXX = Station number of partner YYY = Code of feature (or service)
Override	*62	*62	7362	–	Only for authorized stations
Speaker call	*80 + XXX	*80 + XXX	–	DI, BS, IC, OC	XXX = Call number of destination
Direct answering on	*96	*96	–	–	
Direct answering off	#96	#96	–	–	
Save/edit individual speed-dial (ISD))	*92 + XXX + YYY	*92 + XXX + YYY	7292 + XXX + YYY	BS, IC	XXX = speed-dial numbers *0 to *9 (720 to 729 for ISDN phone) YYY = Call number of external destination
Dial speed-dial number	*7 + XXX	*7 + XXX	727 + XXX	BS, IC	XXX = individual speed-dial numbers *0 to *9 (720 To 729 for ISDN phone) or XXX = station (central) speed-dial numbers 000 ... 999
Reset features/services	#0	#0	730	BS, IC	
Alternate (Toggle/Connect)	*2	*2	722	–	



Topic: Functions at the Telephone					
Feature	Code for			Not possible	Information / Notes
	System telephone	analog telephone	ISDN telephone		
DTMF dialing	*53	*53	7253	RH, BR, DI, BS, IC, OC	DTMF signals can be transmitted during voice calls to control devices (e.g., answering machines or automatic information systems).
Microphone off (mute on)	*52	–	–	–	
Microphone on (mute off)	#52	–	–	–	
Send message text (info text)	*68 + XXX + YYY	*68 + XXX + YYY	7268 + XXX + YYY	BS, IC	XXX = Call number of destination YYY = Text number (0 = Request callback, 1 = Visitor waiting, 2 = Attention: appointment, 3 = Urgent call, 4 = Do not disturb, 5 = Pick up fax/telex, 6 = request dictation, 7 = Please come, 8 = Please bring coffee, 9 = Leaving office)
Message text (info text): check/delete/cancel sent texts	#68	#68	7368	BS, IC	
Park on	*56 + XXX	*56 + XXX	7256 + XXX	RH, BR	XXX = Park position 0 to 9
Retrieve call	#56 + XXX	#56 + XXX	7356 + XXX	DI, BS, IC, OC, TK	XXX = Park position 0 to 9
Save callback	*58	*58	–	RH, BR, DI, BS, RG, GS	
View/delete callback requests	#58	#58	–	RH, BR, DI, BS, RG, GS	
Enable station number suppression (temporary)	*86	*86	7286	BS, IC	
Disable station number suppression (temporary)	#86	#86	7386	BS, IC	
Assign call number	*41 + XXX + YYY	*41 + XXX + YYY	7241 + XXX + YYY	–	XXX = Direct inward dialing number YYY = Call number of destination You can assign a specific DID number to your phone before dialing a station number. This number will then appear on the display of the called party.
Ringing group on	*81 + XXX + YYY ...	*81 + XXX + YYY ...	7281 + XXX + YYY ...	BS, IC	XXX = Station number of a first phone YYY = Station number of a second phone You can have calls to your phone signaled acoustically at up to five additional phones.

## Appendix

### Codes for Activating and Deactivating Features (LX/MX)

Topic: Functions at the Telephone					
Feature	Code for			Not possible	Information / Notes
	System telephone	analog telephone	ISDN telephone		
Ringing group off	#81	#81	7381	BS, IC	
Ringer cutoff on	*98	–	–	BS, IC	
Ringer cutoff off	#98	–	–	BS, IC	
Trunk flash on analog trunk	*59	*59	–	–	<p>XXX = Code of feature (of service) and/or station number of internal destination</p> <p>In order to initiate ISDN-like features or services via analog lines of the network provider (e.g., consultation hold), you need to send a signal on the lines before dialing the code of the feature (or service).</p>
Language selection	*48 + XXX	–	–	–	<p>XXX = Language code</p> <p>You can change the language of display texts on your phone.</p>
Directory (phone book)	*54 + XXX + YYY	–	–	–	<p>XXX = directory (1 = internal directory, 2 = LDAP directory)</p> <p>YYY = Entry to be selected</p> <p>You have access to the internal directory and the LDAP directory (if configured).</p>
Door opener on	*89 + XXX + YYY	*89 + XXX + YYY	7289 + XXX + YYY	–	<p>XXX = Call number of entrance telephone</p> <p>YYY = 5-digit code for the door opener (default code = 00000)</p> <p>You can turn on the door opener so that visitors can open the door themselves by entering a 5-digit code (via a DTMF transmitter or an installed keypad, for example).</p> <p>Only for authorized stations</p>
Door opener off	#89 + XXX	#89 + XXX	7389 + XXX	–	<p>XXX = Call number of entrance telephone</p> <p>Only for authorized stations</p>
Press door opener	*61 + XXX	*61 + XXX	7261 + XXX	–	<p>XXX = Call number of the entrance telephone (only required to open the door without talking via the entrance telephone.)</p> <p>If an entrance telephone has been configured, you can use your phone to talk with the entrance telephone and to press the door opener.</p>
Retrieve external held call	*63 + XXX	*63 + XXX	7263 + XXX	–	XXX = Trunk code
Return to held call (exclusive hold off)	*0	*0	720	–	

<b>Topic: Working in a Team (Groups)</b>					
<b>Feature</b>	<b>Code for</b>			<b>Not possible</b>	<b>Information / Notes</b>
	<b>System telephone</b>	<b>analog telephone</b>	<b>ISDN telephone</b>		
Call forwarding MULAP trunk On	*501 + XXX + YYY + ZZZ	*501 + XXX + YYY + ZZZ	72501 + XXX + YYY + ZZZ	BS, IC	XXX = MULAP station number YYY = Forwarding type (1 = all calls, 2 = only external calls, 3 = internal calls) ZZZ = Forwarding destination Only for members of a team group, Executive / Secretary or Top group, Basic MULAP or Executive MULAP
Call forwarding MULAP trunk Off	#509	#509	73509	BS, IC	Only for members of a team group, Executive / Secretary or Top group, Basic MULAP or Executive MULAP
Group call on	*85	*85	7285	BS, IC	
Group call off	#85	#85	7385	BS, IC	
All group calls on	*85*	*85*	728572	BS, IC	
All group calls off	#85#	#85#	738573	BS, IC	
Ring transfer on	*502 + XXX	*502 + XXX	72502 + XXX	BS, IC	XXX = MULAP station number You can switch the signaling of incoming calls Only for members of an Executive / Secretary or Top group or Executive MULAP
Ring transfer off	#502 + XXX	#502 + XXX	73502 + XXX	BS, IC	
Hunt group on	*85	*85	7285	BS, IC	
Hunt group off	#85	#85	7385	BS, IC	
All hunt groups on	*85*	*85*	728572	BS, IC	
All hunt groups off	#85#	#85#	738573	BS, IC	
Pickup - group	*57	*57	7257	DI, BS, IC, OC	
Call distribution (UCD): login	*401 + XXX	*401 + XXX	72401 + XXX	BS, IC	XXX = Identification (ID) or agent (person responsible) Only for members of a UCD group
Call distribution (UCD): log out	#409	#409	73409	BS, IC	Only for logged in members of a UCD group
Call distribution (UCD): available	*402	*402	72402	BS, IC	Only for logged in members of a UCD group
Call distribution (UCD): not available	#402	#402	73402	BS, IC	Only for logged in members of a UCD group

## Appendix

### Codes for Activating and Deactivating Features (LX/MX)

Topic: Working in a Team (Groups)					
Feature	Code for			Not possible	Information / Notes
	System telephone	analog telephone	ISDN telephone		
Call distribution (UCD): wrap-up on	*403	*403	72403	BS, IC	Only for logged in members of a UCD group
Call distribution (UCD): wrap-up off	#403	#403	73403	BS, IC	Only for logged in members of a UCD group
Call distribution (UCD): night service on	*404 + XXX	*404 + XXX	72404 + XXX	BS, IC	XXX = Call number of night service destination Only for logged in members of a UCD group
Call distribution (UCD): night service off	#404	#404	73404	BS, IC	Only for logged in members of a UCD group
Call distribution (UCD): check number of calls in the queue	*405	*405	72405	BS, IC	Only for logged in members of a UCD group

Topic: Call Routing					
Feature	Code for			Not possible	Information / Notes
	System telephone	analog telephone	ISDN telephone		
Release trunk (emergency trunk access)	*43 + XXX	*43 + XXX	7243 + XXX	BS, IC	XXX = Trunk code Only for attendant
Night service on	*44 + XXX	*44 + XXX	7244 + XXX	BS, IC	XXX = * (= 72 for ISDN phone) (for forwarding to the default night service destination) or XXX = station number of temporary night service destination (for forwarding to a temporary night service destination) Only for authorized stations
Night answer off	#44	#44	7344	BS, IC	Only for authorized stations

<b>Topic: Mobility</b>					
<b>Feature</b>	<b>Code for</b>			<b>Not possible</b>	<b>Information / Notes</b>
	<b>System telephone</b>	<b>analog telephone</b>	<b>ISDN telephone</b>		
DISA internal	*47 + XXX + YYY + ZZZ	*47 + XXX + YYY + ZZZ	–	DI, BS, IC, OC	XXX = DISA number YYY = DISA station ZZZ = DISA service
Mobile PIN (Flex Call)	*508 + XXX + YYY	*508 + XXX + YYY	72508 + XXX + YYY	–	XXX = Call number of user YYY = Code of user's individual lock code
Activate Mobile User Logon (IP mobility)	*9419 + XXX + YYY	–	–		XXX = Mobile number YYY = Password
Deactivate Mobile User Logon (IP mobility)	#9419	–	–		

<b>Topic: Security</b>					
<b>Feature</b>	<b>Code for</b>			<b>Not possible</b>	<b>Information / Notes</b>
	<b>System telephone</b>	<b>analog telephone</b>	<b>ISDN telephone</b>		
Locking the phone (individual lock code)	*66 + XXX	*66 + XXX	7266 + XXX	BS, IC	XXX = Code
Unlocking the Phone (Individual Lock Code)	#66 + XXX	#66 + XXX	7366 + XXX	BS, IC	XXX = Code
Change code for individual lock code	*93 + XXX + YYY + YYY	*93 + XXX + YYY + YYY	7293 + XXX + YYY + YYY	BS, IC	XXX = old code YYY = new code
Lock another internal phone (central lock code)	*943 + XXX + *	*943 + XXX + *	72943 + XXX + 72	BS, IC	XXX = Station number of phone to be locked. Only for authorized stations
Unlock another internal phone (system lock code)	*943 + XXX + #	*943 + XXX + #	72943 + XXX + 73	BS, IC	XXX = Station number of phone to be unlocked. Only for authorized stations

## Appendix

### Codes for Activating and Deactivating Features (LX/MX)

Topic: Accounting					
Feature	Code for			Not possible	Information / Notes
	System telephone	analog telephone	ISDN telephone		
Call charges for own phone	*65	–	–	–	The call charges for the last chargeable call conducted are displayed first. After five seconds, the accrued call charges (total) are displayed.
Account code (ACCT) for cost accounting	*60 + XXX + # + YYY	*60 + XXX + # + YYY	7260 + XXX + 73 + YYY	DI, BS, IC, OC	XXX = Account code (ACCT) YYY = Call number of external destination

Topic: Maintenance					
Feature	Code for			Not possible	Information / Notes
	System telephone	analog telephone	ISDN telephone		
Associated dialing	*67 + XXX + YYY	*67 + XXX + YYY	7267 + XXX + YYY	DI, BS, IC, OC, TK	XXX = Station number of partner YYY = Call number of destination
Call Monitoring	*944 + XXX	–	–	DI, BS, IC, OC	XXX = Station number of internal destination  For selected countries only; only for authorized subscribers
Test phone	*940	*940	–	DI, BS, IC, OC, TK	You can test the operation of your phone.
Stop trace	*509	*509	72509	–	You can stop an active trace profile.
Enable remote service via VPN	*995 + XXX	–	–	DI, BS, IC, OC, TK	xxx = 4-digit code for activation and deactivation of the remote service via VPN and the SSDP Service Plugin
Disable remote service via VPN	#995 + XXX	–	–	DI, BS, IC, OC, TK	xxx = 4-digit code for activation and deactivation of the remote service via VPN and the SSDP Service Plugin
Enable the SSDP Service Plugin	*996 + XXX	–	–	DI, BS, IC, OC, TK	xxx = 4-digit code for activation and deactivation of the remote service via VPN and the SSDP Service Plugin
Disable the SSDP Service Plugin	#996 + XXX	–	–	DI, BS, IC, OC, TK	xxx = 4-digit code for activation and deactivation of the remote service via VPN and the SSDP Service Plugin

Other Features					
Feature	Code for			Not possible	Information / Notes
	System telephone	analog telephone	ISDN telephone		
Call forwarding in ISDN trunk on	*64	–	–	BS, IC	Only for authorized stations
Call forwarding in ISDN trunk off	#64	–	–	BS, IC	Only for authorized stations
Discreet call	*945 + XXX	*945 + XXX	72945 + XXX	DI, BS, IC, OC, TK	XXX = Call number of destination You can monitor an existing connection between two parties and provide one of them with instructions, without the other subscriber hearing this conversation. Only for authorized stations
Trace call	*84	*84	7284	–	
Telephone Data Service (TDS)	*42 + XXX	*42 + XXX	7242 + XXX	BS, IC	XXX = Code for the desired data service If configured, you can use your phone to control attached PCs or their programs, e.g., hotel services or information services.
Activate timed reminder	*46 + XXX	*46 + XXX	7246 + XXX	–	XXX = time, 4-digit (for example, 0905 for 9:05 hours (= 9.05 a.m.) or 1430 for 14:30 hours (= 2.30 p.m.) You can have your phone call you to remind you of appointments.
Deactivate timed reminder	#46 + XXX	#46 + XXX	7346 + XXX	–	
Communicate with PC applications via CSTA interface	*494 + XXX	–	–		XXX = application code If configured, you can communicate with PC applications by using your phone. You can send information to the application and receive information from the application on your phone display, for example.

---

### Related Topics

- [Euro-ISDN Features \(LX/MX\)](#)

## 20.8 IP Protocols and Port Numbers Used

The following lists provide details on the individual components of OpenScape Office and show which IP protocols and port numbers are required for their functionality. These port numbers may need to be opened when setting up a firewall. A distinction is made here between the server and client functions.

---

**Related Topics**

- [NAT \(MX\)](#)

## 20.8.1 IP Protocols and Port Numbers for Server Functions

The following server functionality is implemented in OpenScope Office.

### OpenScope Office MX System Administration

IF function	Protocol	Server port	Description	Configurable
AdminPortal (http)	TCP	443	AdminPortal	no
AdminPortal (http)	TCP	8100	Access to internal resources (URL blocker )	no
OSO application	TCP	8101	Autoupdate process, myReports	no
RemoteAdminAccess	TCP	10099	Remote access via the Internet	yes
Postmaster	TCP	5432	Database server	no
CLA	TCP	61740	Licensing: CLA service port for CLC, CSC and CLM (optional)	yes
CLA Auto Discovery	UDP	23232	Licensing: CLA Service Port for Auto Discovery of CLM	yes
DLI	TCP	18443	DLI	
DLSC	TCP	8084	Port for communication between gateway and DLS	no
DLSC	TCP	8084	Port for communication between gateway and DLS	no

### Support Functions

IF function	Protocol	Server port	Description	Configurable
FTP	TCP	21		no
DNS	UDP/TCP	53	DNS Server	no
DHCP	UDP	67	DHCP	no
DHCP Client	UDP	68	DHCP	no
NTP	UDP	123	Time server	no
SNMP (traps)	UDP	162	Transmit/Receive SNMP error messages	no
SNMP (Get/Set)	UDP	161	SNMP browser	no
SNMP (traps)	UDP	1024-65535	SNMP traps sent by OpenScope Office	no
TFTP	UDP	69	APS Transfer with TFTP	no



IF function	Protocol	Server port	Description	Configurable
SSH	TCP	22	SSH server for secure login and sftp for diagnostics, myReports (server)	no
AP Directory	UDP	3517	Process to find WLAN access points in the network The multicast IP address 224.0.1.178 is used for this purpose.	no
Rpc.mountd	TCP	791, 792	NFS	no
SyMoM	TCP	4708-4711	Connector for SOAP	no
Squid Proxy	TCP	3128	HTTP proxy port. Packets transmitted to this proxy port are handled by Squid. Squid is currently used only to provide the URL blocker function.	no
SQUID	UDP	3130		no
SQUID	UDP	3401		yes
SQUID	UDP	32771		yes
SQUID	UDP	32772		yes
Rpc.mountd	TCP	791, 792		yes

### H.323 Call Signaling

IF function	Protocol	Server port	Description	Configurable
H225 call signaling active	TCP	transient	Call signaling for H323 HFA telephones and H323-based trunking	yes
H225 secure call signaling active	TCP/TLS	transient	Secure call signaling for H323 HFA telephones and H323-based trunking	yes
H225 call signaling passive	TCP	1720	Call signaling for H323 HFA telephone and H323-based trunking	yes
H225 secure call signaling passive	TCP/TLS	1300	Secure call signaling for H323 HFA telephones and H323-based trunking	yes

**Appendix**

IP Protocols and Port Numbers Used

**SIP**

IF function	Protocol	Server port	Description	Configurable
SIPS	TCP/TLS	5061	Secure call signaling for SIPQ trunking	yes
SIP (Dynamic Ports)	TCP	transient		no
SIP	TCP/UDP	5060	Call signaling for SIP telephones and SIP-based trunking. Closed by default.	yes

---

**NOTICE:** If OpenScape Office is used as an Internet router, port 5060 must be closed (default setting). For Internet telephony via an ITSP, OpenScape Office opens the relevant ports and keeps them open.

Port 5060 must likewise be closed If an external router or firewall is being used. OpenScape Office is responsible for opening this port (if required).

---

**HFA**

IF function	Protocol	Server port	Description	Configurable
HFA	TCP	4060	Control of HFA clients (CorNet-TC server port)	yes
HFA secure	TCP/TLS	4061	CorNet-TC via TLS	yes

**Media Gateway RTP / T.38 payload**

A full range of media ports is available for OpenScape Office. The number of ports depends on the included interfaces and the configured applications.

The general MediaBasePort for OpenScape Office MX and OpenScape Office LX is 29100.

IF function	Calculation of the required port range	Number of ports	Min port	Max port	Description
MEB	1 MEB/box *3 boxes* (30 RTP + 30 T.38 + 30 RTCP) ports/MEB	270	29100	29369	RTP/RTCP and T.38 ports for MEB
Media Server	515	512	29370	29881	RTP/RTCP ports for MS (conferences, MOH)
Media Gateway	3 gateways/box *4 boxes* (32 RTP + 32 RTCP + 32 SRTP + 32 SRTCP)	1536	29882	31417	RTP/RTCP/SRTP/SRTCP and T.38 ports for slot modules
Internal RTP proxy port range (to the phones)	LX: 128 * (RTP + RTCP)	256	31418	31673	LX: RTP/RTCP port range for RTP proxy MX: RTP/RTCP port range for RTP proxy
	MX: 32 * (RTP + RTCP)	64		31481	

IF function	Calculation of the required port range	Number of ports	Min port	Max port	Description
External RTP proxy port range (to the SIP provider)	LX: 128 * (RTP + RTCP) MX: 32 * (RTP + RTCP)	256 64	31674 31866	31929	LX: RTP/RTCP port range for RTP proxy MX: RTP/RTCP port range for RTP proxy
Dummy RTP port	1 port	1	31930		This port is used in an "interim SDP answer"; packets sent to this port are dropped.
Total	Port range for media ports	2831	29100	31930	

### VPN

IF function	Protocol	Server port	Description	Configurable
ISAKMP	UDP	500	Internet Security Association and Key Management Protocol for IPsec	yes
Encapsulating Security Payload	ESP	-	IPsec protocol for encapsulated payload transport	no
NAT traversal (NAT-T)	UDP	4500	IPsec protocol for encapsulated payload transport. In contrast to ESP, NAT-T also works if there are NAT devices (e.g., routers) between the VPN partners. The need for NAT-T is automatically detected and enabled by the QuickSec IPsec Stack.	yes

### CSTA access

IF function	Protocol	Server port	Description	Configurable
CSTA	TCP	7003	CSTA Server Port	no
CSTA Service Provider	TCP	8800	IP port for all applications that want to connect to the CSP.	yes

### MediaExtensionBridge (MEB)

IF function	Protocol	Server port	Description	Configurable
MEB SIP	TCP	15060	(LX/MX): call signaling for SIPQ trunking	yes
MEB SIP	TCP	5060	HX: call signaling for SIPQ trunking	No

### IP Accounting

IF function	Protocol	Server port	Description	Configurable
Accounting Server	TCP	13042	Interface for IP accounting	no

## Appendix

### IP Protocols and Port Numbers Used

#### File and Print Server

IF function	Protocol	Server port	Description	Configurable
nmbd	UDP	137	NetBIOS name server for NetBIOS over IP naming services at clients	no
nmbd	UDP	138	NetBIOS name server for NetBIOS over IP naming services at clients	no
smbd	TCP	139	SambaDeamon - SAMBA (File) Share	no
smbd	TCP	445	SambaDeamon - SAMBA (File) Share	no
cupsd	UDP	631	Common Unix Printing System Daemon	no
cupsd	TCP	631	Common Unix Printing System Daemon	no
Print Server	TCP	9100	Print Server	no
Squid Proxy	TCP	3128	HTTP proxy port Required for the URL Blocker functionality.	no

#### WLAN Access Points

IF function	Protocol	Server port	Description	Configurable
AP Discovery	UDP	3517	Process to detect WLAN access points in the network The multicast IP address 224.0.1.178 is used for this purpose.	no

#### SSDP Internet-based platform for remote services

IF function	Protocol	Server port	Description	Configurable
SSDP	TCP	3011	Internet-based platform for remote services.	no

#### OpenScape Office Server

IF function	Protocol	Server port	Description	Configurable
VSL	HTTP/TCP	8770	VSL service port	no
vsld	TCP	8774	Directory Server	no
vsld	TCP	8775	Instant Messaging Server	no
vsld	TCP	8776	PIMP server	no
vsld	TCP	8777	Calendar Integration Server (Exchange Integration)	no
OSO - Multisite	TCP	8778	For multi-site connections	yes
OSO - User Portal	TCP/UDP	8779	For client connections. UDP is used for broadcasts for the auto-discovery of the server by clients (also multicast capable)	yes
vsld	TCP	18774	FastViewer	no
vsld	TCP	18775	IM server (PIMP server uplink port)	no

IF function	Protocol	Server port	Description	Configurable
myDbChecker	TCP	3465	myDbChecker for the scheduled printing and transmission of reports	no
OSO myReports	TCP	8101	Report Preview	no
JSFT	TCP	8771	Java Socket File Transfer (for myReports)	
JSFT	TCP	8772	Port required by internal JSFT server to avoid opening two instances at the same time (for myReports)	

### Diagnostics Tools

IF function	Protocol	Server port	Description	Configurable
Online Trace Port (LDH)	TCP	2048	Access for XTracer online trace tool (Route 99)	no
Online Trace Port (FP)	TCP	21965	Access for XTracer online trace tool	yes
rpcapd	TCP	2002	Remote pcap daemon to provide a remote access interface. This port is only open if this interface was activated via the management interface.	no
OpenScape Office Status Server	TCP	8808	Access to the OpenScape Office Status Client (/sbin/OsoStatus)	no

### XMPP Server / Openfire (integrated XMPP server)

IF function	Protocol	Server port	Description	Configurable
XMPP clients	TCP	5222	for XMPP client connections	no
XMPP Connection Manager	TCP	5262	for XMPP Connection Manager connections	no
XMPP server	TCP	5269	for XMPP server connections	no
Openfire Admin (http)	TCP	9090	for Openfire administration via http	no
Openfire Admin (https)	TCP	9091	for Openfire administration via https	no

### XMPP Service Provider

IF function	Protocol	Server port	Description	Configurable
IM / Mobile Connectivity	TCP	9093	Used for XMPP proxy	no

## Appendix

### IP Protocols and Port Numbers Used

#### Mobile Connectivity

IF function	Protocol	Server port	Description	Configurable
thin desktop clients	TCP	8801	Web Clients and OpenStage XML access; OpenScape Office Application Launcher (System Access Port)	no
thin mobile clients	TCP	8802	Web Clients access via HTTP; OpenScape Office Application Launcher (System Access Port, Default)	no

#### Lightweight Application Server

IF function	Protocol	Server port	Description	Configurable
HiWeb Service Provider	TCP	8603	for HiWeb Service Provider connections	no

#### LDAP server

IF function	Protocol	Server port	Description	Configurable
LDAP server	TCP	389	OpenScape Office Directory Service	no

#### Automatic CAR update

IF function	Protocol	Server port	Description	Configurable
CAR update registration port	TCP	12061	Registration port for Reg. Message of HG 1500	no
CAR update registration port	TCP	12063	Registration port for CarServer	no

## 20.8.2 IP Protocols and Port Numbers for Client Functions

The following client functionality is implemented in OpenScape Office. The corresponding server port is addressed by the client in the external system and may need to be opened in the firewall.

#### Client Functionality of OpenScape Office MX

Function	Protocol	Client port	Server port	Description
http client	TCP	1024-65535	80	Downloading of software and phone images
https client	TCP	1024-65535	443	Downloading of software and phone images
E-mail client	TCP	1024-65535	25	<b>OpenScape Office-&gt;ApplicationSuite-&gt;Server-&gt;Notifications</b>
SNMP trap	UDP	1024-65535	162	SNMP traps sent by OpenScape Office
LDAP clients	TCP	1024-65535	389	Central directory, PKI infrastructure

Function	Protocol	Client port	Server port	Description
DynDNS	TCP	1024-65535	2164	Dynamic DNS Client
SNTP	UDP	1024-65535	123	SNTP client in unicast operation (RFC2030); synchronization of the Simple Network Time Protocol
Central charging tool	TCP	1024-65535	443	Send call charge data to a configurable server. The IP address and port numbers are configurable in OpenScape Office MX
IPSEC / VPN / Application Launcher	TCP	1024-65535	389	CRLs are stored locally on the gateway or retrieved by an LDAP server using the LDAP protocol.
DNS client	UDP	1024-65535	53	DNS client or client side of a DNS relay agent
DNS client	TCP	1024-65535	53	DNS client or client side of a DNS relay agent
Online licensing	TCP/TLS	1024-65535	7790	Activate license online via License Management (CSCm->CLP)
Backup / Restore	TCP	1024-65535	20 - 21	Back up to an FTP server via FTP
Backup / Restore	TCP / TLS	1024-65535	22	Back up to an FTP server via SFTP
E-mail forwarding	TCP	1024-65535	25	Service Center
VoIP – SIP signaling	UDP	5060	5060	Registration and call signaling at the ITSP. Closed by default.
VoIP – H323 signaling	TCP	1024-65535	1720	H323-based call signaling for HFA and CorNet-IP/NQ trunking
STUN client	UDP		Configurable (e.g. 3478, 3479, 10000, 10001)	Used for calls to SIP Internet telephony service providers
DHCP Relay Agent	UDP	1024-65535	67	

## 20.9 Interface Ranges for Subscriber Lines (MX )

The following table provides the maximum possible lengths of subscriber lines at the OpenScape Office MX communication system.

The values apply under ideal conditions for the cables specified, that is, no coupling joints, etc. are permitted. Actual values can only be measured on site.

**Appendix**

Interface Ranges for Subscriber Lines (MX )

Gateway module	Interface		Cable	Maximum Loop Resistance	Maximum Line Length (Range)
GMAA	a/b interface for the analog station connection		Communication lines with a conductor diameter of 0.4 to 0.8 mm	Approx. 900 Ohm (including 300 Ohm terminal DC resistor)	Approx. 2000 m
GMAL	a/b interface for the analog station connection		Communication lines with a conductor diameter of 0.4 to 0.8 mm	Approx. 900 Ohm (including 300 Ohm terminal DC resistor)	Approx. 2000 m
GMS	S <sub>0</sub> interface for the ISDN station connection	ISDN S <sub>0</sub> point-to-point connection	J-Y (ST) 2x2x0.6 (The specified line lengths apply only to this cable type. Other cable types with a conductor diameter of at least 0.4 mm or greater may also be used.	Max. 6 dB, measured at 96 kHz with 100 Ohm terminators	Approx. 600 m
		Enhanced ISDN S <sub>0</sub> bus connection		Max. 4 dB, measured at 96 kHz with 100 Ohm terminators	Approx. 400 m
		ISDN S <sub>0</sub> bus connection		Max. 2 dB, measured at 96 kHz with 100 Ohm terminators	Approx. 120 m
		ISDN S <sub>0</sub> line jack unit for the phone		–	Approx. 10 m



Gateway module	Interface		Cable	Maximum Loop Resistance	Maximum Line Length (Range)
GMSA	a/b interface for the analog station connection		Communication lines with a conductor diameter of 0.4 to 0.8 mm	Approx. 90 Ohm	Approx. 2000 m
	S <sub>0</sub> interface for the ISDN station connection	ISDN S <sub>0</sub> point-to-point connection	J-Y (ST) 2x2x0.6 (The specified line lengths apply only to this cable type. Other cable types with a conductor diameter of at least 0.4 mm or greater may also be used.	Max. 6 dB, measured at 96 kHz with 100 Ohm terminators	Approx. 600 m
		Enhanced ISDN S <sub>0</sub> bus connection		Max. 4 dB, measured at 96 kHz with 100 Ohm terminators	Approx. 400 m
		ISDN S <sub>0</sub> bus connection		Max. 2 dB, measured at 96 kHz with 100 Ohm terminators	Approx. 120 m
		ISDN S <sub>0</sub> line jack unit for the phone		–	Approx. 10 m

## 20.10 Standards and Attenuation Values for Trunk Connections (MX )

The following tables provide the country-specific standards and attenuation values for trunk connections at the OpenScape Office MX communication system.

As a rule, trunk connections are installed by the provider and attenuation is measured and adjusted on site.

**Appendix**

Standards and Attenuation Values for Trunk Connections (MX )

**For Europe only: Standards and attenuation values for trunk connections**

Gateway module	Interface	Standards / Attenuation
GMAA	a/b interface for the analog trunk connection	<ul style="list-style-type: none"> <li>• 1TR110 1996/12 (technical description of the DTAG analog dialup line)</li> <li>• ETSI TS 103 021-1 2004/5 (General aspects)</li> <li>• ETSI TS 103 021-2 2004/11 (Basic transmission and protection of the network from harm)</li> <li>• ETSI TS 103 021-3 2003/9 (Basic Interworking with the PSTN)</li> <li>• ES 201 187 V1.1.1 1999/3 (Loop disconnect dialing)</li> <li>• EN 300 659-1 V1.3.1 2001/1 (Clip on-hook data transmission)</li> <li>• EN 300 659-2 V1.3.1 2001/1 (Clip off-hook data transmission)</li> <li>• FTZ 121TR8 Part 9 (16 kHz metering pulse detection)</li> <li>• Input level: -6 dBr, Output level: -1 dBr</li> <li>• <math>Z_{in} = 270 + 750//150 \text{ nF}</math></li> <li>• <math>Z_{\text{-Hybrid}} = 270 + 750//150 \text{ nF}</math></li> </ul>
GME	S <sub>2M</sub> interface for the ISDN Primary Rate Interface	<ul style="list-style-type: none"> <li>• TBR4/A1 1997 TE</li> <li>• TBR13 1996 Tie</li> <li>• EN 300 403 1999 TE EDSS1, Basic Call</li> <li>• EN 300 xxx TE EDSS1, Suppl. Services (1)</li> <li>• EN 300 172 2003 Tie QSIG, Basic Call</li> <li>• EN 300 239 2003 Tie QSIG, Generic Functions</li> </ul>
GMS	S <sub>0</sub> interface for the ISDN trunk connection	<ul style="list-style-type: none"> <li>• TBR3/A1 1997</li> </ul>
GMSA		<ul style="list-style-type: none"> <li>• EN 300 403 1999 TE EDSS1, Basic Call</li> <li>• EN 300 xxx TE EDSS1, Suppl. Services (1)</li> <li>• EN 300 172 2003 Tie QSIG, Basic Call</li> <li>• EN 300 239 2003 Tie QSIG, Generic Functions</li> </ul>

(1) List of Standards for Supplementary Services depending on implementation.

**For Australia only: Standards and attenuation values for trunk connections**

Gateway module	Interface	Standards / Attenuation
GMAA	a/b interface for the analog trunk connection	<ul style="list-style-type: none"> <li>• AS/ACIF S002:2001 (Analogue Interworking with PSTN)</li> <li>• AS/ACIF S003:2006 (DC, Ringing, Isolation, Transmission)</li> <li>• AS/ACIF S004:2006 (DC, Ringing, Isolation, Transmission)</li> <li>• Input level: –6 dBr, Output level: –1 dBr</li> <li>• <math>Z_{in} = 220 + 820//120 \text{ nF}</math></li> <li>• <math>Z\text{-Hybrid} = 220 + 820//120 \text{ nF}</math></li> </ul>
GME	$S_{2M}$ interface for the ISDN Primary Rate Interface	<ul style="list-style-type: none"> <li>• AS/ACIF S038:2001</li> <li>• AS/ACIF S016:2001 (Layer1, Jitter, Wander)</li> <li>• TBR4/A1 1997 TE</li> <li>• TBR13 1996 Tie</li> <li>• EN 300 403 1999 TE EDSS1, Basic Call</li> <li>• EN 300 xxx TE EDSS1, Suppl. Services (1)</li> <li>• EN 300 172 2003 Tie QSIG, Basic Call</li> <li>• EN 300 239 2003 Tie QSIG, Generic Functions</li> </ul>
GMS	$S_0$ interface for the ISDN trunk connection	<ul style="list-style-type: none"> <li>• AS/ACIF S031:2001 (Layer 1, 2, 3)</li> <li>• TBR3/A1 1997 TE</li> <li>• EN 300 403 1999 TE EDSS1, Basic Call</li> <li>• EN 300 xxx TE EDSS1, Suppl. Services (1)</li> <li>• EN 300 172 2003 Tie QSIG, Basic Call</li> <li>• EN 300 239 2003 Tie QSIG, Generic Functions</li> </ul>
GMSA		

(1) List of Standards for Supplementary Services depending on implementation.

**For South Africa only: Standards and attenuation values for trunk connections**

Gateway module	Interface	Standards / Attenuation
GMAA	a/b interface for the analog trunk connection	<ul style="list-style-type: none"> <li>• DPT-SWS-001 1996/11</li> <li>• ICASA TE-010 (Clip on-hook data transmission)</li> <li>• EN 300 659-1 V1.3.1 2001/1 (Clip on-hook data transmission)</li> <li>• Input level: –6 dBr, Output level: –1 dBr</li> <li>• <math>Z_{in} = 220 + 820//115 \text{ nF}</math></li> <li>• <math>Z\text{-Hybrid} = 220 + 820//115 \text{ nF}</math></li> </ul>

**Appendix**  
System Flags (LX/MX)

Gateway module	Interface	Standards / Attenuation
GME	S <sub>2M</sub> interface for the ISDN Primary Rate Interface	<ul style="list-style-type: none"> <li>• TBR4/A1 1997 TE</li> <li>• TBR13 1996 Tie</li> <li>• EN 300 403 1999 TE EDSS1, Basic Call</li> <li>• EN 300 xxx TE EDSS1, Suppl. Services (1)</li> <li>• EN 300 172 2003 Tie QSIG, Basic Call</li> <li>• EN 300 239 2003 Tie QSIG, Generic Functions</li> </ul>
GMS	S <sub>0</sub> interface for the ISDN trunk connection	<ul style="list-style-type: none"> <li>• TBR3/A1 1997 TE</li> <li>• EN 300 403 1999 TE EDSS1, Basic Call</li> <li>• EN 300 xxx TE EDSS1, Suppl. Services (1)</li> <li>• EN 300 172 2003 Tie QSIG, Basic Call</li> <li>• EN 300 239 2003 Tie QSIG, Generic Functions</li> </ul>
GMSA		

(1) List of Standards for Supplementary Services depending on implementation.

**For the U.S. and Canada only: Standards and attenuation values for trunk connections**

Gateway module	Interface	Standards / Attenuation
GMAA	a/b interface for the analog trunk connection	<ul style="list-style-type: none"> <li>• ANSI/TIA968-A-3 2004</li> <li>• ANSI/TIA-464-C-2002</li> <li>• ANSI/TIA-777-A (Caller-ID)</li> <li>• Input level: -3 dBr, Output level: +3 dBr</li> <li>• Z<sub>in</sub> = 600 Ohm</li> <li>• Z-Hybrid = 600 Ohm and 350 + 1000//210 nF</li> <li>• CS-03, Issue 8</li> </ul>
GMT	T1 interface for the ISDN Primary Rate Interface	<ul style="list-style-type: none"> <li>• ANSI/TIA-968-A-3 2004</li> <li>• ANSI/TIA-464-C 2002</li> <li>• CS-03, Issue 8</li> </ul>

## 20.11 System Flags (LX/MX)

By activating or deactivating system flags, an administrator with the **Expert** profile can enable or disable functions for subscribers on a system-wide basis.

The system flags listed in the table below are country-specific.

System flag	System flag enabled	System flag disabled	Default setting
Through-connection for external FWD on	<p>Calls forwarded to an external destination are put through immediately. The forwarding occurs regardless of whether an internal or external (MSI/ISDN) call is involved.</p> <p>If the call forwarding occurs via an ISDN trunk, and the external forwarding destination is located in another network (such as a GSM network, for example), the call setup from the ISDN Central Office is reported with the progress indicator Leaving ISDN. As of this point in time, the caller incurs connection charges.</p>	Calls forwarded to an external destination are not put through immediately.	Disabled
Call forwarding to main station interface permitted	Calls over analog trunks (MSI) follow the external call forwarding.	Calls over analog trunks (MSI) do not follow the external call forwarding.	Activated
Hunting to external call forwarding destination	If the external call forwarding destination cannot be reached, the call is forwarded to the next destination entered in the call destination list.	No call forwarding (CFNA) occurs.	Disabled
Conference tone	The participants of a conference are reminded that they are currently in a conference call by a special tone at intervals of 20 seconds.	No special conference tone is sent.	Disabled
Warning signal for call pickup groups	A call for a member of a call pickup group is signaled to the other group members with an optical signal (via the display). If the call is not answered within four call cycles (4 x 5 seconds), the other group members also receive a warning tone.	A call for a member of a call pickup group is signaled to the other group members only with an optical signal (via the display).	Activated
Increase volume for optiPoint/OpenStage terminals	optiPoint and OpenStage phones are switched to an alternative attenuation plan, which increases the volume.	The attenuation plan remains unchanged.	Disabled
Relocate allowed	System telephones can be physically relocated without changing the logical configuration (call number, name, key programming, etc.).	The physical relocation of system phones results in changes to the logical configuration.	Disabled
More than 1 external conference member	<p>Multiple external subscribers can attend in a conference.</p> <p>For details on the maximum possible external conference participants, see <a href="#">Configuration Limits and Capacities</a></p>	A maximum of one external participant can attend a conference.	Activated

**Appendix**  
System Flags (LX/MX)

System flag	System flag enabled	System flag disabled	Default setting
Trunk reservation, automatic	A subscriber can reserve a trunk in advance if there are no free trunks available (busy signal). The subscriber receives a recall as soon as this trunk becomes free and can then set up the external connection.	It is not possible to reserve a trunk.	Disabled
No. redial with a/c code	On redialing, any account code that was entered is also repeated in addition to the station number.	On redialing, only the entered station number is repeated. The account code must be entered manually.	Disabled
Use only default number for MSN	On an S <sub>0</sub> bus, MSNs (Multiple Subscriber Numbers) can only be created for already existing internal station numbers (to prevent any possible toll fraud).	On an S <sub>0</sub> bus, MSNs (Multiple Subscriber Numbers) can also be created for internal station numbers that do not exist.	Disabled
Path optimization	Path optimization is performed for networked communication systems.  <b>INFO:</b> The flag must be enabled for all communication systems belonging to a network.  Example for two networked systems (system 1 and system 2): For a call from subscriber A (system 1) to subscriber B (system 2) and subsequent call forwarding to subscriber C (system 1), two trunks are reserved. With path optimization, the connection from A to C is automatically switched over a single trunk.	No path optimization is performed.	Activated
DTMF automatic	After every successful connection setup, an automatic switchover to DTMF mode occurs. This enables answering machines to be checked remotely, for example.	No automatic switchover to DTMF mode occurs.	Activated
Broadcast with connection	The Speaker Call (Paging) function can be used to set up an internal connection without the called subscriber lifting the handset. On lifting the handset, the call becomes a normal two-party call.	The connection is cleared by replacing the handset.	Activated
Tone from CO	A connection is switched through to the Central Office or to a networked communication system even if no tone is sent from the peer.	A connection is switched through to the Central Office or to a networked communication system only if a tone is sent from the peer.	Disabled
Ringback protection	Ringbacks are triggered automatically.	Ringbacks are not triggered automatically.	Disabled

System flag	System flag enabled	System flag disabled	Default setting
Euro-impedance (for specific countries only)	<p>The following impedance values apply in Europe:</p> <ul style="list-style-type: none"> <li>• a/b interfaces for the analog station connection: <ul style="list-style-type: none"> <li>– Input impedance = 270 Ohms + 750 Ohms    150 nF</li> <li>– Second ringer impedance = 270 Ohms + 750 Ohms    150 nF</li> <li>– Relative Level A/D = 0 dBr</li> <li>– Relative Level D/A = -7 dBr</li> </ul> </li> <li>• a/b interfaces for the analog trunk connection: <ul style="list-style-type: none"> <li>– Input impedance = 270 Ohms + 750 Ohms    150 nF</li> <li>– Second ringer impedance = 270 Ohms + 750 Ohms    150 nF</li> <li>– Relative Level A/D = -6 dBr</li> <li>– Relative Level D/A = -1 dBr</li> </ul> </li> </ul>		Disabled
Different phonemail messages Day/Night	In a communication system with phonemail, different phonemail announcements can be activated for a station by transmitting different station numbers for that station to the phonemail. As a prerequisite, different call forwarding destinations for day and night modes must be configured for that station.	The station number of the called station is always transmitted to the phonemail.	Disabled
Display international / national code number	This flag is used to define the display format of system speed dialing (SSD) numbers for incoming calls for which no name is stored in the SSD memory.		Disabled
	<p>The complete phone number (PABX number + Direct Inward Dialing (DID) number, including the local area code and country code, if available) is shown on the display of the phone.</p> <p>Example: The SSD number 06671234 was set up without a name. Local area code = 02302, PABX number = 667, DID number = 1234. In the case of an incoming call from 6671234, the number 023026671234 appears on the display.</p>	<p>For incoming calls, the PABX number + DID number is displayed on the phone.</p> <p>Example: The SSD number 06671234 was set up without a name. Local area code = 02302, PABX number = 667, DID number = 1234. In the case of an incoming call from 6671234, the number 6671234 appears on the display.</p>	
Line change for direct call	This flag is used to define the behavior of a Direct Station Select (DSS) key during an active call on a MULAP trunk. Relevant for Team Configuration / Team Group, Executive/Secretary / Top Group, Basic MULAP, Executive MULAP.		Disabled (not for U.S. and Canada)
	On pressing a Direct Station Select (DSS) key, a line change is performed. The call is placed on hold and can only be resumed at this phone.	On pressing a Direct Station Select (DSS) key, a consultation hold is initiated.	Enabled (for U.S. and Canada only)

**Appendix**  
System Flags (LX/MX)

System flag	System flag enabled	System flag disabled	Default setting
Automatic redial	Automatic redialing is performed when a called subscriber is busy.  The time parameter <b>Timer for automatic redial</b> defines after how much time the redialing is activated.	No automatic redialing is performed.	Disabled
Node phone number for voicemail	For networked communication systems, this flag defines whether or not the node number must be supplied for the identification of one central or multiple decentralized voicemail server(s).		Disabled
	The node number must be supplied for the identification of the voicemail server or servers.	The node number need not be supplied for the identification of the voicemail server or servers.	
Call Pickup after automatic recall	This flag defines whether recalls and callbacks should also be signaled at other members of a call pickup group.		Disabled
	Recalls and callbacks are also signaled at other members of a call pickup group and can be accepted by them.	Recalls and callbacks are not signaled at other members of a call pickup group	
Configurable CLIP	Instead of the actual station number, the number entered under <b>Clip/Lin</b> is transmitted to the called external connection and presented on the display. If the <b>Clip/Lin</b> entry is empty, the station number is transmitted.	The station number is transmitted to the called external connection and presented on the display.	Activated
Caller list at destination in case of Forward Line	In case of a Forward Line Key (MULAP), incoming calls are entered in the caller list of the destination station.	In case of a Forward Line Key (MULAP), incoming calls are entered in the caller list of the desired station.	Disabled
Call forwarding after deflect call / single step transfer	If a subscriber has enabled call forwarding to an external destination (call deflection), the call is signaled at that destination. After the call forwarding time has expired, the call is signaled at the first destination entered in the call destination list and subsequently at the second destination, if any, and so on.  Example: For station A, a deflect call to station B was executed. The first destination entered in the call destination list of station B is station C, and the second destination is station D. In this case, the call will be signaled at station C first and then at station D, after the call forwarding time has expired.  <b>INFO:</b> The activation of this flag only makes sense if the flag <b>Follow call management in case of deflect call / single step transfer</b> is also activated.	If a subscriber has enabled call forwarding to an external destination (call deflection), the call is first signaled at that destination and subsequently at the first destination entered in the call destination list (after the call forwarding time has expired). Further destinations entered in the call destination list, if any, are not followed.  Example: For station A, a deflect call to station B was executed. The first destination entered in the call destination list of station B is station C, and the second destination is station D. In this case, the call is signaled at station C, but not forwarded to station D.	Activated



System flag	System flag enabled	System flag disabled	Default setting
Follow call management in case of deflect call / single step transfer	<p>If a subscriber has enabled call forwarding to an external destination (call deflection), the call is first signaled at that destination and subsequently at any further destination entered in the call destination list (after the call forwarding time has expired).</p> <p>Example: For station A, a deflect call to station B was executed. The first destination entered in the call destination list of station B is station C. After the call forwarding time has expired, the call is signaled at station C.</p>	<p>If a subscriber has enabled call forwarding to an external destination (call deflection), the call forwarding ends at that destination. Further destinations entered in the call destination list, if any, are not followed.</p> <p>Example: For station A, a deflect call to station B was executed. The first destination entered in the call destination list of station B is station C. In this case, the call is signaled at station B, but no forwarding to station C occurs.</p>	Activated
Calling number in pick-up groups / ringing groups / CFN / RNA	This flag defines whether the station number and name of a caller are to be displayed at all members of a call pickup group, all members included in a ringing group and at CFN (call forwarding) and CFNA (call forwarding on no answer) destinations.		Activated
	The station number and name are presented on the display.	The station number and name are not shown.	
SPE support	<p>The Signaling and Payload Encryption (SPE) feature is supported.</p> <p>The VoIP payload and signaling data streams to and from the communication system and between OpenStage system telephones are encrypted.</p> <p><b>Note:</b> Enabling the station parameter <b>Payload Security</b> is a prerequisite for the usage of SPE by a subscriber.</p>	<p>The Signaling and Payload Encryption (SPE) feature is not supported.</p> <p>No encryption of the VoIP payload and signaling data streams occurs.</p>	Disabled
SPE advisory tone	<p>When the system flag <b>SPE Support</b> is enabled, and an OpenStage 15, 20, 20 E or 20 G phone is used, subscribers are notified about an unencrypted connection by a beep tone in addition to the display.</p> <p>No beep tone is heard when using an OpenStage 40, 40 G, 60, 60 G, 80 or 80 G telephone. The status of the connection (encrypted/unencrypted) is permanently shown in the display.</p>	When the system flag <b>SPE Support</b> is enabled, subscribers are notified about an unencrypted connection only via the display.	Disabled
SIP Prov. to SIP Prov. transit	<p>This flag defines whether transit line connections are allowed for ITSP connections. A transit line connection occurs when two trunks of the same communication system are seized by a single call.</p> <p>Example: An external is forwarded to an internal station via an ITSP. The internal station then transfers the call again to an external destination via an ITSP. This results in a transit line connection within the communication system. Two trunks are occupied for the duration of the call.</p>		Disabled
	The resulting transit line connections are allowed.	Transit line connections are not possible.	

**Appendix**  
Station Flags (LX/MX)

System flag	System flag enabled	System flag disabled	Default setting	
Transparent dialing of * and # on trunk interfaces	<p>This flag defines whether it is possible to enable and disable Centrex features via IP trunks (ITSP) and ISDN trunks.</p> <p>Several providers offer Centrex (Central Office Exchange) features that can be enabled or disabled by using codes.</p> <p>The input of a code must occur in the dialing state (e.g., after entering the trunk code). The input always begins with "*" or "#". This must be followed by the actual code (digits 0 through 9) and terminated with "#". It is not possible to enable or disable Centrex features in the talk state.</p>		Disabled	
	Centrex features can be enabled or disabled via IP trunks (ITSP) and ISDN trunks.	Centrex features cannot be enabled or disabled via IP trunks (ITSP) and ISDN trunks.		
Transit permission:	<p>This flag defines which transit connections are allowed. Transit connections are call connections from external stations that are handled via the communication system. This may include connections to the CO as well as connections to networked communication systems.</p>			
	<p>Feature transit:</p> <p>Transit connections associated with specific features such as external call forwarding, call transfers and DISA applications, for example, are allowed. This applies regardless of whether tie trunk or trunk-to-trunk connections are involved.</p>	<p>Feature transit:</p> <p>Transit connections are not possible.</p>		Activated
	<p>Tie traffic transit:</p> <p>Transit connections in direct inward dialing for tie trunk connections (networked communication systems) are allowed.</p>	<p>Tie traffic transit:</p> <p>Transit connections in direct inward dialing for tie trunk connections (networked communication systems) are not possible.</p>		Activated
	<p>External traffic transit:</p> <p>Transit connections in direct inward dialing for trunk-to-trunk connections are allowed.</p>	<p>External traffic transit:</p> <p>Transit connections in direct inward dialing for trunk-to-trunk connections (networked communication systems) are not possible.</p>		Disabled

## 20.12 Station Flags (LX/MX)

By activating or deactivating station flags, an administrator with the **Expert** profile can enable or disable functions for subscribers on an individual basis.

The station flags listed in the table below depend on whether an IP station (IP client, SIP client), ISDN station, analog station, virtual station or a UC Suite station (users of the UC clients myAttendant, myPortal for Desktop, etc.) is involved.

Station flag	Station flag enabled	Station flag disabled	Default setting
Override class of service on	The subscriber can break into (i.e., override) an internal subscriber's ongoing connection. The subscribers involved are notified of the busy override by a warning tone and a display message.	The subscriber is not authorized to break into (i.e., override) an internal subscriber's ongoing connection.	Disabled
Override Do Not Disturb	When the subscriber calls a station for which Do Not Disturb has been activated, he or she can override the Do Not Disturb. After five seconds, the call is signaled at the called station.	The subscriber is not authorized to override the Do Not Disturb. Subscribers who call a station for which Do Not Disturb has been activated receive the busy tone.	Disabled
FWD external permitted	The subscriber can activate call forwarding to an external destination.  Charges incurred for the execution of an external call forwarding are allocated to the subscriber who activated the call forwarding.	The subscriber is not authorized to activate call forwarding to an external destination.	Activated
Prevention of voice calling off	The subscriber can be addressed directly. This enables an internal call to be set up without lifting the handset. The loudspeaker on the called station is activated automatically in the process.	The speaker call is signaled like a normal call.	Activated
DISA class of service	DISA (Direct Inward System Access) enables external subscribers to activate or deactivate functions of the communication system and set up outbound connections just like any other internal subscribers. This also includes activating and deactivating call forwarding, the Do Not Disturb feature and the lock code, for example.	The subscriber is not authorized to use DISA (Direct Inward System Access).	Disabled
Transit allowed via Hook-on	The subscriber can transfer an external call to another external subscriber by hanging up.  The subscriber is the conference controller and hangs up: if there are other internal subscribers still in the conference, the longest participating internal subscriber automatically becomes the conference controller. If there are only external participants remaining in the conference, the conference is terminated, and all connections are cleared.	The subscriber is not authorized to transfer external calls to other external subscribers by hanging up.  The subscriber is the conference controller and hangs up: the conference is terminated, and all connections are cleared.	Disabled
System telephone lock reset	The subscriber can reset the individual lock code of other internal subscribers to the default code.	The subscriber is not authorized to reset the individual lock code of other internal subscribers to the default code.	Disabled

**Appendix**  
Station Flags (LX/MX)

Station flag	Station flag enabled	Station flag disabled	Default setting
CLIP analog (only for analog stations)	The caller's phone number is shown on the phone display of the analog station. As a prerequisite, the analog phone of the subscriber must support CLIP (Calling Line Identification Presentation).	The caller's phone number is not shown on the phone display of the analog station.	Activated
MCID access	The subscriber can have malicious external callers identified via the ISDN Central Office. As a prerequisite, the "Trace call" (Malicious Call Identification, MCID) feature must have been applied for and activated by the network provider.  <b>Note:</b> After the "Trace call" feature has been activated by the network provider, the following must be noted: for each incoming call from the ISDN CO, the release of the connection to the called station is delayed for a specific timeout period after the caller hangs up. This timeout enables the called station to activate the "Trace call" feature. The ISDN trunk availability is somewhat reduced as a result.	The subscriber is not authorized to have malicious external callers identified via the ISDN Central Office.	Disabled
Entry in telephone directory	The name and call number of the subscriber is displayed in the system directory.	The name and call number of the subscriber is not displayed in the system directory.	Activated
Editing the Telephone Number	The subscriber can edit the digits of the call number entered via the keypad before the digit transmission. This requires a system phone with a display.	The subscriber cannot edit the digits of the call number entered via the keypad before the digit transmission.	Disabled
No group ringing on busy	The status of the station with group ringing programmed (i.e., the primary station) determines whether or not group ringing occurs: <ul style="list-style-type: none"> <li>• If the primary station is free: all stations included in the group are called immediately.</li> <li>• If call waiting is enabled at the primary station: all stations included in the group are called after a delay of 5 seconds.</li> <li>• If the primary station cannot receive a call or if call waiting is inactive: group ringing does not take place.</li> </ul>	All stations in the group are called immediately, regardless of the status of the primary station.	Disabled

Station flag	Station flag enabled	Station flag disabled	Default setting
Associated dialing/ services	<p>Associated dialing: The subscriber can dial a number on behalf of another internal subscriber as if that station itself were dialing.</p> <p>Associated services: The subscriber can control features on behalf of another internal subscriber as if that station itself were controlling these features. This includes activating and deactivating call forwarding, group ringing and the lock code, for example.</p>	The subscriber is not authorized to dial a number or control features on behalf of another internal subscriber.	Disabled
Call waiting rejection on	Subscribers who are conducting a call are not informed about other incoming calls via a call waiting tone or a display message.	Subscribers who are conducting a call are informed about other incoming calls via a call waiting tone or a display message.	Activated
Discreet call	The subscriber can discreetly join an existing voice call of another internal subscriber. He or she can silently monitor the call and speak with the internal subscriber without the other party hearing this conversation. This is only possible in the case of a two-party call. Discreet calling is not possible with consultation calls or conferences.	The subscriber is not authorized to discreetly join an ongoing connection of an internal subscriber.	Disabled
Discreet Call Lock	The subscriber cannot be called discreetly.	The subscriber can be called discreetly.	Disabled
Call Monitoring (for specific countries only)	<p>The subscriber can silently monitor (i.e., listen in on) the conversation of any internal subscriber. The microphone of the party listening in is automatically muted. The monitored subscriber is not notified via a signal tone or display message.</p> <p><b>Note:</b> Gaps in the conversation of up to two seconds may be encountered on starting and ending call monitoring.</p>	The subscriber is not authorized to silently monitor the conversation of another internal subscriber.	Disabled
Autom. connection, CSTA (only for OpenStage SIP telephones)	<p>When dialing or answering calls via myAttendant, myPortal for Desktop or myPortal for Outlook, speakerphone mode is activated on the associated SIP telephone.</p> <p><b>Note:</b> The details in the documentation for the SIP telephone must be observed. Additional settings may need to be made on the SIP telephone for the correct operation of this feature.</p>	When dialing via myAttendant, myPortal for Desktop or myPortal for Outlook, the associated SIP telephone is called. On lifting the handset, the call is set up to the dialed number.	Activated

## 21 Glossary

The glossary provides short explanations of the terms used (for instance, protocols and standards).

### 21.1 Glossary

The glossary provides short explanations of the terms used (for instance, protocols, standards).

#### **10BaseT, 100BaseT, 1000BaseT**

This refers to a specification (IEEE. 802.3i) for networks with 10 Mbps base band transmission over a symmetrical 100-Ohm four-wire cable. 100BaseT, on the other hand, is used for bandwidths of up to 100 Mbps and 1000BaseT for bandwidths of up to 1000 Mbps.

#### **AES (Advanced Encryption Standard)**

AES is a symmetric encryption system that was ratified by the National Institute of Standards and Technology as the successor to the earlier DES and 3DES Standards. It is used for VPN, for example.

#### **ADSL with dynamic IP address**

ADSL stands for Asymmetric Digital Subscriber Line and means that the bandwidths from the Internet (download, downstream) and to the Internet (upload, upstream) are different. The classic Internet telephony connection is ADSL. A dynamic IP address is sufficient if the web and mail services are provided by the Internet Service Provider.

#### **ADSL with fixed IP address**

ADSL stands for Asymmetric Digital Subscriber Line and means that the bandwidths from the Internet (download, downstream) and to the Internet (upload, upstream) are different. The classic Internet telephony connection is ADSL. ADSL with a fixed IP address is required if you want to run your own web and mail server on your site.

#### **AF-EF (Expedited Forwarding - Assured Forwarding)**

The codepoints AF and EF define the various priorities of IP packets for QOS (Quality of Service).

AF: guarantees minimum bandwidth for the data

EF: guarantees constant bandwidth for this data.

### **ARP (Address Resolution Protocol)**

The Address Resolution Protocol (ARP) is a network protocol that facilitates the assignment of network addresses to hardware addresses. Although it is not limited to Ethernet and IP protocols, it is almost exclusively used in conjunction with IP addressing in Ethernet networks.

### **Authentication**

Authentication is the verification of a person's or PC's identity. The check can be performed with a simple user name, for example, as well as with a fingerprint.

### **Authorization**

Authorization is a mechanism for granting rights, e.g., access rights in a data network.

### **B channel**

A B channel is the transmission path for the payload (voice, data) of an ISDN connection.

### **Busy Lamp Field (BLF)**

myPortal provides a so-called Busy Lamp Field (BLF) to display the call status of the specified subscribers.

### **Broadcast**

A broadcast is a message sent to everyone in a PC network. The message (i.e., a data packet) is transmitted from one point to all subscribers in the network. A broadcast is mainly used in a data network if the address of the message recipient is unknown.

### **CA (Certification Authority)**

The CA is an organization that issues certificates with digital signatures. Digital signatures are required for a VPN (Virtual Private Network), for example.

### **CAPI Interface (Common Application Programming Interface)**

CAPI is an ISDN-compliant standardized software interface. CAPI enables the development of ISDN software without requiring any knowledge about the manufacturer-specific ISDN hardware being used.

### **Centrex**

Centrex (Central Office Exchange) provides the functions of a telephone system via a PSTN or ITSP. This is also known as virtual telephone system, hosted PBX (Private Branch Exchange) or NetPBX.

### **CHAP (Challenge Handshake Authentication Protocol)**

CHAP is an authentication protocol used within the framework of the Point-to-Point protocol.

**COS (Classes Of Service)**

QoS is a procedure that ensures the transmission quality for data in IP networks.

**CLIP (Calling Line Identification Presentation)**

With station number transmission, the caller's phone number is displayed on the called party's station. The called party can therefore identify the caller before picking up the call.

**CLIR (Calling Line Identification Restriction)**

The caller suppresses the display of his or her call number on the called station. As a result, the called party cannot identify the caller before picking up the call.

**COLP (Connected Line Identification Presentation)**

With Connected Line Identification Presentation, the called party's number is displayed for the caller if the connection is successful.

**COLR (Connected Line Identification Restriction)**

With Connected Line Identification Restriction, the called party's number is not displayed for the caller, even if the caller activated COLP.

**Comfort User**

Comfort User is the standard user in OpenScape Office.

**Comfort Plus User**

The Comfort Plus User is the Advanced User of OpenScape Office. In contrast to the Comfort User, the Comfort Plus User can use more features (such as Fax, Mobility and Conferencing).

**CorNet**

CorNet is a protocol developed by Siemens for networking Hicom and HiPath communication systems. In contrast to the generally supported QSIG, all manufacturer-specific features of Hicom and HiPath systems are integrated in CorNet.

**CorNet-IP**

CorNet-IP is a protocol variant of CorNet that enables the cross-networking of systems or the connection of system telephones (such as optiPoint) over IP.

**CorNet-NQ**

A proprietary QSIG-based signaling protocol for interconnecting communication systems to one or more QSIG PBX systems.

**CSTA (Computer Supported Telecommunications Applications)**

CSTA is a protocol interface for applications that support the European Computer Manufacturers' Association (ECMA) standard. Telecommunication tasks are controlled and monitored using SIP via CSTA.



### **CSV (Character Separated Values)**

A CSV file is a text file for saving or exchanging simply structured data. CSV stands for Character Separated Values, Comma Separated Values or Colon Separated Values, since the individual values are delimited by a special separator character such as a comma or semicolon. CSV files must be available in ANSI/ASCII format.

### **CRL (Certificate Revocation List)**

A CRL or Certificate Revocation List is a list of all revoked certificates. CRLs always have to be generated by the certification authority where the certificates originate.

### **Delay**

A delay has two meanings in telecommunications:

- The delay by which an event is postponed.
- The time between the occurrence of an event and the appearance of a expected follow-on event.

### **Dedicated (Permanently Assigned) Gateway**

If a dedicated gateway is entered in the LCR for a route, then routing via this gateway is enforced. All contradictory rules are then invalid for the routing.

### **DHCP (Dynamic Host Configuration Protocol)**

DHCP is a procedure by which a PC is assigned a certain IP configuration (IP address, subnet mask, etc.) at startup.

### **DS (DiffServ, Differentiated Services)**

DS is a procedure for managing packets in data networks. The routing method for a specific data packet is specified as is a particular service level in regard to bandwidth, queuing theory, and packet discard decisions.

### **Diffie-Hellman algorithm**

The Diffie-Hellman algorithm is used for the exchange of keys in a VPN. The data produced by this algorithm is configured with a specific set of mathematical parameters. The key exchange only works properly if both subscribers use identical values for these parameters.

### **DLI (Deployment License Service Integrated)**

DLI enables the unattended installation and upgrading of IP system telephones.

### **DMZ (Demilitarized Zone)**

A demilitarized zone (DMZ) refers to a PC network that offers a number of security features for accessing connected network nodes (PCs, routers, etc.).

**DNS (Domain Name Service)**

Name resolution on the Internet and in the LAN. DNS translates the names of PCs or web pages into the relevant IP addresses.

**DSL (Digital Subscriber Line)**

DSL is a technological solution for providing high-bandwidth Internet access. Internet telephone bridges the gap between the provider's attendant and the customer's telephone jack.

**DSS (Direct Station Selection)**

The function keys on a telephone or add-on device can be programmed as Direct Station Select (DSS) keys. These are programmed with the phone number of an internal subscriber or a group for this. Pressing a DSS key initiates an immediate call to the programmed destination.

**DTMF (Dual Tone Multifrequency)**

See DTMF.

**EIM (Enterprise Instant Messaging)**

EIM is an Instant Messaging Service that runs on private servers in a company on platforms such as the Live Communications Server or Office Communications Server 2007 from Microsoft.

**Enterasys Switches**

Enterasys switches are produced by Enterasys Networks as secure network solutions. The stackable switches support QoS features and can classify and prioritize voice, video and data applications.

**ESP (Encapsulating Security Payload)**

ESP is an IPsec protocol that guarantees packet encryption, packet integrity as well as packet authenticity. The integrity and authentication check does not extend to the IP header. It is only performed for the actual data (payload).

**FoIP (Fax over IP)**

FoIP is a method for transmitting fax messages over an IP network.

**FTP**

The File Transfer Protocol (FTP) is a network protocol specified in RFC 959 for the transmission of data via TCP/IP networks.

**Functional Numbers**

Functional numbers (also called function codes) are MSN/DID numbers or pilot numbers, e.g., for parking, conferencing and the AutoAttendant. The functional numbers correspond to virtual stations. The functional numbers in an internetwork must be unique.

### **G.711**

G.711 is a standard for digitizing analog audio signals. It is used in classic fixed-network telephony (PCM technology). G.711 can also be used for voice encoding in VoIP.

### **G.723.1**

G.723.1 is also a standard for digitizing audio signals.

### **G.729AB**

G.729 is a codec for voice compression in digital signals and is used in IP telephony. G.729 is very CPU-intensive. Though only marginally inferior in terms of quality, G.729AB is a somewhat simplified version and therefore less CPU-intensive.

### **Gateway / Gateway Modules**

A gateway is the entrance and exit to a communications network, usually connecting two disparate traffic flows.

### **GSM (Global System for Mobile Communications)**

GSM is a standard for digital mobile networks that is primarily used for telephony, but also for line- and packet-switched data transmissions as well as short messages (SMS).

### **Handover**

The term handover designates the process in a mobile cellular communication network in which the mobile phone switches from one cell to another during a call or a data connection. The term is also used when switching between GSM and UMTS with a dual-mode mobile phone.

### **Hash value**

Hash or dispersion range values are usually scalable values from a subset of natural numbers. A hash value is also referred to as a "fingerprint" because it is a virtually unique identification of a quantity in much the same way as a fingerprint is a virtually unique identification of a person.

### **H.323**

H.323 designates a group of standards that define a variety of media types for packet networks. The standards cover voice, data, fax and video, and define how signals are to be converted from analog to digital and what signaling is to be used.

### **OpenScape Office Assistant**

OpenScape Office Assistant is used to administer the communication system. It provides all wizards for the quick support of administration tasks.

### **Hosted Services**

Hosted Services are traditional IT services such as e-mail, instant messaging (IM) and unified communications (UC), which are provided to a company by an Internet Provider from a remote site, thus eliminating the company's need to run and manage these services on their own servers on-site.

### **ICMP (Internet Control Message Protocol)**

ICMP is used in data networks for the exchange of information and error messages using the Internet Protocol IP.

### **IDS (Intrusion Detection System)**

IDS is a security system that monitors all incoming and outgoing network activities to identify possible security violations. These include both intrusion (attacks from outside the organization) and abuse (attacks from within the organization).

### **IEEE Standards**

IEEE Standards are a set of specifications defined by the Institute of Electrical and Electronic Engineers (IEEE) (such as Token Ring, Ethernet) to establish common networking standards among vendors.

### **IEEE. 802.1p**

IEEE. 802.1p is an IEEE standard for regulating the transport of data packets with different priorities in computer networks. The data packets are classified into priority classes from 1 to 7. The Standard only stipulates ascending priorities from 1 through 7, but does not deal with how the individual data packets should be handled.

### **IKE Protocol**

The IKE protocol has two different tasks. Start by creating an SA (Security Association) exclusively used by the IKE protocol (IKE-SA). The existing IKE-SA is then used for secure negotiation of all further SAs (payload SA) for the transmission of payload data.

### **IM (Instant Messaging)**

IM is a procedure for the real-time exchange of text messages over the Internet using computers, Pocket PCs and mobile phones. Modern IM services enable VoIP and video conferencing, file transfers and desktop application sharing.

### **IP PBX**

IP PBX is a communication system that supports both VoIP and normal voice connections over traditional phone lines.

### **IPSec**

IPSec is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks through the use of various security services and protocols.

### **ISP (Internet Service Provider)**

An ISP is a business that supplies Internet connectivity services to individuals, businesses, and other organizations. Some ISPs are large national or multinational corporations that offer access in many locations, while others are limited to a single city or region.

### **ITSP (Internet Telephony Service Provider)**

An ITSP is a business that supplies Internet connectivity services to individuals, businesses, and other organizations.

### **DP (Dial Pulsing)**

DP is the oldest signaling method used for automatic telephone switching. Today, DP has generally been superseded by DTMF.

### **Jitter**

Jitter refers to packet delay variations in voice transmissions. An excessive delay between the sending of packets and their arrival at the receiving end results in irregular voice communications and they are difficult to understand.

### **ISD (Individual Speed Dialing)**

Individual Speed Dialing (ISD) enables 10 external individual speed-dial numbers to be saved at every authorized phone in addition to the system speed dialing (SSD).

### **SSD - System Speed Dialing**

Frequently required external phone numbers can be stored in the system memory of the communication system. Every number is represented by a speed-dial number, which can be used instead of the full phone number by all stations.

### **Latency**

Latency is the time required to transport a data packet from one application to another, including the time for transmission over the network and for preparing and processing the data at the transmitting and receiving devices.

### **LCR (Least Cost Routing)**

You can use the Least Cost Routing (LCR) function to specify the provider you want to use, e.g., for trunk calls, mobile phone calls or international calls. You use the communication system to define the least-cost provider and conduct all calls via this specific path.

### **LIN (Location Identification Number)**

LIN is a unique, max. 16-digit number that corresponds to the 10-digit NANP (North American Numbering Plan).

### **LWCA (Lightweight CA)**

LWCA is a restricted certification function.

### **Media Stream Channel**

A media gateway can terminate circuit-switched ISDN B channels and use the voice data carried to generate media stream channels for an IP-based packet-switched network. Media stream channels feature a combination of audio, video, and T.120 media.

### **DTMF (Dual Tone Multifrequency)**

Dual Tone Multifrequency (DTMF) is the dialing method in analog telephony that is predominantly used in switching technology today for transmitting the phone number to the telephone network.

### **MIM (Mobile Instant Messaging)**

MIM is a Presence and Instant Messaging Service for mobile phones.

### **Mobility**

The term mobility designates the use of Pocket PCs and mobile phones and their integration in the communication system of a company.

### **MOH (Music on Hold)**

Music on Hold (MOH) can be played to callers who cannot be switched through immediately.

### **MSN (Multiple Subscriber Number)**

When connecting ISDN phones via an S0 bus (point-to-multipoint connections), every single ISDN phone (ISDN station) is assigned a unique Multiple Subscriber Number (MSN). The ISDN stations can be reached via their MSNs.

### **MULAP (Multiple Line Appearance)**

MULAPs are special groups in which multiple telephones are combined. A group member may be assigned multiple phones under a single call number (Basic MULAP) here. In addition, such a group can be used to implement special features required for communication between an Executive and Secretary, for example, or within teams (Executive MULAP, Team MULAP).

### **Multi-Gateway**

In the case of a multi-gateway network, calls are routed via several different gateways.

### **myAttendant**

myAttendant is the Attendant Console of OpenScape Office.

### **myPortal**

myPortal is the Java-based user portal that enables subscribers to access the Unified Communications functions. Apart from information on the presence status, convenient dialing aid via favorites and directories, subscribers can also access voicemail messages and faxes.

### **myPortal for Outlook**

myPortal for Outlook is the user portal integrated in Microsoft Outlook that enables subscribers to access unified communications functions. It is analogous to myPortal. myPortal for Outlook also provides a convenient Desktop Dialer.

### **NAC (Network Admission Control)**

NAC is a technology that supports defenses against viruses and worms from within the network. With NAC, terminal devices are checked for conformity with guidelines during the authentication. If the virus scanner is not up-to-date, for example, or if the client operating system does not have the latest security patch installed, the device involved is quarantined and provided with the current updates until it meets the applicable security guidelines.

### **NAT (Network Address Translation)**

NAT is a procedure for replacing one IP address in a data packet with another. It is used to map private IP addresses to public IP addresses. Masking or PAT (Port Address Translation) is when the port numbers are also rewritten.

### **NTBA (Network Termination for ISDN Basic Access )**

An NTBA (Network Termination for ISDN Basic Access), also known as NT (Network Termination), is the network termination device for the ISDN basic rate interface. It is the link between the network operator's digital network and the ISDN configurations on the subscriber side.

### **NTPM (Network Termination for Primary Rate Multiplex Access)**

An NTPM (Network Termination for Primary Rate Multiplex Access) is the network termination device for the ISDN primary rate interface. It is the link between the network operator's digital network and the ISDN configurations on the subscriber side.

### **OLSR - Optimized Link State Routing Protocol**

OLSR is special ad-hoc protocol that enables the missing routing capability on the OSI Layer 2 to be optimized on the OSI Layer 3.

### **ONS (One Number Service)**

Call number directly assigned to a user One or more resources (telephones) may be assigned to a user. When a user is called via his or her ONS number, the call is forwarded to the phone that is currently being used by that user (e.g., a mobile phone).

### **PAP (Password Authentication Protocol)**

PAP is an authentication procedure based on the point-to-point protocol. It is used for dialing into an ISP. PAP transmits the password for authentication as clear text together with a user ID.

### **PBX (Public Branch Exchange)**

A PBX is a switching system that interconnects multiple terminals such as phones, fax and answering machines between themselves and also to the public phone network.

### **Peer**

A peer is the terminal device for communication in a peer-to-peer network. During communication, every peer makes its services available and uses the services of the other peer.

### **Peer-to-peer**

In a peer-to-peer network, all PCs have equal rights and may use and also provide services on the network.

### **Peer-entity authentication**

The corroboration that the peer entity in an association is the one claimed.

### **PKI (Public Key Infrastructure)**

In cryptology, a PKI (public key infrastructure) is a system for generating, distributing, and verifying digital certificates. The certificates issued within a PKI are used to protect computer-driven communication.

### **PPP (Point-to-Point Protocol)**

PPP is an IETF standard for transmitting IP packets over serial lines. PPP is mainly used for dialing into the Internet.

### **PPPoE (Point-to-Point Protocol over Ethernet)**

The PPPoE Protocol (PPP over Ethernet) enables the use of the Point-to-Point network protocol over an Ethernet connection.

### **Pre-shared Key**

The pre-shared key is a key that is defined for the tunnel configuration (for VPNs). In order for VPN peers communicating via the tunnel to authenticate themselves, the same password must be used for both of the tunnel endpoints.

### **PPTP (Point-to-Point Tunneling Protocol)**

PPTP is a technology used for configuring a virtual private network (VPN). Because the Internet is essentially an open network, PPTP is used to ensure that messages transmitted from one VPN node to another are secure. PPTP lets users dial into their corporate network via the Internet.

### **Presence**

The term Presence refers to the capability of a Unified Communications system to determine the location and status of a user at any time. This makes it easier to respond to the specific communication needs of a user by phone, e-mail, Instant Messaging or fax.



### **Proxy Server**

The proxy server is the connecting link between a client application and a Web server. It performs the task of filtering client application requests and thus relieves the load on the Web server.

### **PSTN (Public Switched Telephone Network)**

As the name implies, PSTN refers to a public switched telephone network. Public networks may be owned by private or public entities.

### **QoS (Quality of Service )**

You must guarantee a minimum bandwidth for Voice over IP for the entire transmission duration. If multiple applications with equal rights are operating via IP, then the available bandwidth for a transmission path is split. In this case, a voice connection may experience packet losses which can reduce voice quality. There are different ways to guarantee the highest possible quality for transmission; these methods are collectively referred to as Quality of Service (QoS).

### **RAS (Remote Access Service)**

A RAS (Remote Access Service) user is an IP subscriber (e.g., a teleworker) who logs into the system remotely and behaves like an internal IP station. This subscriber can therefore use the complete functional scope of the communication system.

### **RJ45 (Registered Jack 45)**

RJ45 is an eight-pin connector that is used for connecting a 10BaseT cable in network technology, for example.

### **Roaming**

Roaming is the capability of a mobile network subscriber to automatically make calls or access other mobile network services in a foreign network, i.e., one that differs from the home network of the subscriber.

### **RTCP (Real-Time Control Protocol)**

The real time control protocol (RTCP) is used for the negotiation and compliance of Quality of Service (QoS) parameters through the periodic exchange of control messages between senders and receivers.

### **RTP (Real-Time Transport Protocol)**

RTP is an IETF Standard for streaming real-time multimedia data using the Internet Protocol. Typically, RTP runs on top of the UDP protocol, and uses dynamic UDP ports negotiated between the sender and receiver of specific media streams.

### **RTT (Round Trip Time)**

RTT is the time interval required by a data packet to move from the source to the target and back.

### **SA (Security Association)**

SA is a security association between two communicating units in computer networks. It describes how the two parties will use security services to communicate securely with each other.

### **SDSL (Symmetric Digital Subscriber Line)**

SDSL is particularly suited to Internet telephony, intranet applications in companies with local networks, for video conferencing and is, for example, designed for teleworkers who can use it to send and receive data with the same bandwidth. In contrast to ADSL, SDSL uses identical bandwidths from and to the Internet.

### **Secure CLI**

Secure CLI is a security feature that provides secure command line and data transfer interfaces with the help of the Secure File Transfer Protocol (SFTP).

### **SFTP (Secure File Transfer Protocol)**

SFTP is a security protocol for transporting connection data records.

### **ShrewSoft VPN Client**

The ShrewSoft VPN client is an open source and free VPN client with a graphical user interface. It includes, among other things, ISAKMP, Xauth and RSA support, and AES, Blowfish and 3DES encryption protocols.

### **Single Gateway**

In the case of a single-gateway network, calls are routed via a single gateway. OpenScape Office MX or HiPath 3000 can act as a gateway.

### **SIP (Session Initiation Protocol)**

SIP is a standard Internet protocol defined in RFC 3261 for setting up and managing voice connections and video conferences over an IP network.

### **SNMP (Simple Network Management Protocol)**

SNMP is a procedure for obtaining information on the status of network components and PCs.

### **SPE (Signaling and Payload Encryption)**

Signaling & Payload Encryption (SPE) serves to enhance security when transmitting voice data. The VoIP payload and signaling data streams from and to the gateway and between IP phones are encrypted.

### **SRTP (Secure Real-Time Transport Protocol)**

SRTP is an encrypted RTP protocol. It is particularly suitable for transmitting communication data over the Internet and is used in IP telephony.

### **SSH (Secure Shell)**

SSH is a protocol that provides support for secure remote login, secure file transfer, and secure TCP/IP forwarding. It can automatically encrypt, authenticate, and compress transmitted data.

### **SSL (Secure Socket Layer)**

SSL is a protocol for transporting documents over the Internet. With SSL, data is provided with a private key before it is transmitted. By convention, URLs that require an SSL connection start with https: instead of http:.

### **Status**

The status, together with the "Presence" concept, indicates whether a subscriber is available, busy, offline, etc., so that other subscribers in the communication system know if this subscriber can be reached.

### **STUN (Simple Traversal of UDP through NAT)**

STUN is a network protocol for detecting, identifying, and bypassing firewalls and NAT routers.

### **Survivability**

Survivability is the capability of an internetwork to maintain service continuity in the presence of faults within the network.

### **TAE (Telekommunikations-Anschluss-Einheit) - German standard for telephone plugs and sockets**

A TAE is a type of connector for analog phone connections with the a/b interface and for ISDN connections to plug the NTBA into the main line. It is used to connect analog telephones, fax machines and ISDN phone systems.

### **TCP (Transmission Control Protocol)**

TCP is a protocol that governs how data should be exchanged by PCs. All operating systems in modern PCs support TCP and use it for data exchange with other computers.

### **TFTP (Trivial File Transfer Protocol)**

TFTP is a trivial file transfer protocol that supports only the reading and writing of files. Many of the functions supported by the superordinate protocol are unavailable, for example, functions allocating rights, displaying existing files or user authentication.

### **Telnet**

A protocol that links two PCs in order to provide a terminal connection to the remote PC. Instead of dialing into the PC, the user connects over the Internet via Telnet. The user initiates a Telnet session, connects to the Telnet host and logs in. The connection enables the user to work with the remote PC as though it were a terminal connected to it.

### **TOS (Type of Service)**

TOS is a field in the header of IP data packets. It is used for the prioritization of these packets and evaluated for Quality of Service, for example.

### **UCD (Uniform Call Distribution)**

UCD enables incoming calls in the communication system to be uniformly distributed to a group of stations (UCD-group).

### **UDP (User Datagram Protocol)**

UDP is a network protocol that belongs to the Transport layer of the Internet protocol family. UDP is responsible for routing data transmitted over the Internet to the correct application.

### **UMTS (Universal Mobile Telecommunications System)**

UMTS is a third-generation mobile network standard with which significantly higher data transmission rates (384 kbps to 7.2 Mbit/sec.) can be achieved as compared to the mobile network standards of the second generation or the GSM standard.

### **Unified Communications**

Unified Communications is the integration of various communication systems, media, devices and applications within an environment (e.g., IP telephony, site-based and mobile telephony, e-mail, instant messaging, desktop applications, voicemail, fax, conferencing and unified messaging).

### **Unified Messaging**

Unified Messaging is the integration of different communication data such as e-mail, SMS, fax, telephony, etc., in a uniform message store. This message store can be accessed by several different devices.

### **VAD (Voice Activity Detection)**

VAD (Voice Activity Detection) is an algorithm in speech processing to detect the presence or absence of speech in the digital transmission of audio data.

### **VCAPI Interface**

VCAPI is a virtual CAPI interface that emulates the presence of a local ISDN card. If an ISDN card has been installed on a PC in the internal network, then this ISDN card can be made available to all stations on the network via the VCAPi interface.

### **VDSL (Very High Speed Digital Subscriber Line)**

VDSL is used to transfer symmetrical or asymmetrical data streams at high speed over short distances. VDSL is an alternative to ADSL and SDSL that additionally offers higher transmission speeds.

### **VoIP (Voice over IP)**

VoIP is the transmission of voice data over IP-based networks.

**VPN (Virtual Private Network)**

A VPN uses the public infrastructure of the Internet to connect sites and provide teleworkers with access to internal networks. External partners are provided with secure access to the internal data network by using encryption and authentication mechanisms.

**WAN (Wide Area Network)**

WAN is the designation for wide area data networks such as the Internet, for example.

**WBM (Web-Based Management)**

WBM is a web-based user interface that is displayed in an Internet browser using HTML or JAVA pages (web pages) and a web protocol (HTTP or HTTPS).

**X.509 standard (VPN certificate)**

X.509 is an ITU-T standard for a public key infrastructure and currently the most important standard for digital certificates.

**XMPP (Extensible Messaging and Presence Protocol)**

Internet standard that is primarily used for Instant Messaging. XMPP supports the interaction with users of other networks such as AIM, ICQ or Windows Live Messenger (WLM), for example. Among other things, XMPP and its extensions support conferencing with multiple users (e.g., multi-user chats) and the display of the online status.

**Second Degree**

Second degree means that a station is calling and already has a second call waiting for that station.

# Index

## A

- accidents, reporting 26
- accounting 43
- Actions (Menu) 81
- activate licenses 143
- activation, software (see software activation)
- Address Resolution Protocol 99
- ad-hoc conference 182
- Admin log (also called admin protocol) 375
- Admin Log (Menu) 80
- advisory messages 232
- AF/EF code points 117
- AF/EF Codepoints (Menu) 82
- Allowed Lists (Menu) 85
- alternative workplace 161
- analog telephone 121
- Analog telephones 41
- Announcement (Menu) 86
- announcements for call distribution 267
- announcements for voicemail 188
- answering machine 121
- AP 1120 S 41
- Application Launcher 40, 429
  - profile for configuration data 430
- application-controlled conference 179
- applications
  - recommended and certified 43
- attenuation values for trunk connections (OpenScape Office MX) 537
- audio codec 116
- AutoAttendant 200
  - personal 203
- Autom. Night Service (Menu) 86
- automatic action 476
  - DLS notification 477
  - garbage collection 477
- automatic callback 230
- automatic recall 221
- automatic suffix-dialing 209
- automatic updates 157
- Auxiliary Equipment (Menu) 86

## B

- back up 453
- backup
  - immediate 455
  - scheduled 456

- backup directory 453
- backup medium 453, 454
- backup set 453, 454
- backup set for diagnostic purposes 491
- bandwidths in the LAN 392
- bandwidths in WAN 394
- Basic MULAP 253
  - ring type 254
  - SIP phones 254
- Basic Settings (Menu) 81
- Battery buffering 37
- broadband connection 93, 100

## C

- cable port 94
- cabling for LAN, WAN and DMZ connections of OpenScape Office MX 28
- call
  - missed 174
  - scheduled 174
- Call charges (Menu) 82
- call deflection after timeout 226
- call detail recording with 12 kHz and 16 kHz pulses 62
- call distribution 260, 261
  - accept UCD calls automatically 265
  - AICC (Automatic Incoming Call Connection) 265
  - announcements 267
  - configuration 261
  - night service 266
  - overflow 266
  - priority of external calls 264
  - priority of internal calls 264
  - queue 265
  - release UCD calls from analog lines 268
  - subscriber state 262
  - transfer to UCD group 268
  - UCD agent 262
  - UCD group 261
  - wrapup time 263
- call forwarding 225
  - rule-based 163
  - status-based 162
- Call Forwarding (Menu) 85
- call forwarding on busy 223
- call forwarding-no answer after timeout 224
- call monitoring 484
- call number format 176

- Call Pickup (Menu) 85
- call pickup from voicemail 188
- call pickup group 236
  - call pickup for recalls 237
  - call pickup outside of a call pickup group 237
  - display of a caller's name 236
  - display of a caller's phone number 236
  - SIP phones 237
  - warning tone 236
- call signaling 214
- call waiting tone/call waiting 230
- call waiting/call waiting tone 230
- callback 229
  - journal 174
  - Phone menu 192
- callback on busy 230
- CallBridge 43
- Calling Line Identification Presentation - CLIP 214
- Calling Line Identification Restriction - CLIR 215
- CallMe 161
- CallMe service 161
- canonical call number format 176
- capacities 502
- capacity limits 502
- CAR table update 410
- CAR tables, update 398
- Carrier Select Override 277
- CDP (Certificate Distribution Point) 374
- CE mark, OpenScape Office MX 29
- central box, OpenScape Office MX 47
- Central License Server (see license server)
- Class of Service Groups (Menu) 85
- Classes of Service (Menu) 85
- client logs 493
- clients, hardware and software prerequisites 153
- CLIP 58, 62, 64
- CLIP - Calling Line Identification Presentation 214
- CLIP no screening 217
- CLIR - Calling Line Identification Restriction 215
- Codec Parameters (Menu) 84
- codes for features 518
- COLP - Connected Line Identification Presentation 216
- COLR - Connected Line Identification Restriction 216
- communication system, remote access 494
- CON Group Assignment (Menu) 86
- CON groups 271
  - allocation of SSD numbers 272
- CON Matrix (Menu) 86
- condition
  - rule-based call forwarding 163
- conference 178
  - ad-hoc 182
  - application-controlled 178
  - authentication 178
  - automatic invitation by e-mail 178
  - automatic invitation via Outlook appointment 178
  - conference controller 178
  - conference participants 178
  - conference tone 178
  - dial-in number 178
  - extend 178
  - Mobility Entry stations 178, 182, 183, 185, 186
  - open 186
  - permanent 185
  - phone-controlled 178
  - record 178
  - scheduled 183
  - types 178
  - virtual conference room 178
- conference management 179
- conference, phone-controlled 179
- Conferencing (Menu) 88
- Configuration (Menu) 78
- configuration data 453
- configuration data for diagnostics 491
- configure external providers (Menu) 87
- conformity of OpenScape Office MX
  - Canadian standards 31
  - CE 30
  - international standards 31
  - U.S. standards 31
- Connected Line Identification Presentation - COLP 216
- Connected Line Identification Restriction - COLR 216
- contact 173
- Contact Center
  - agent 299
  - agent callback 311
  - break 301
  - CCV objects 304
  - class of service (authorization level) of an agent 299
  - clients 291
  - communication system with IP trunks and outside line 327
  - conditions for operation 327
  - configuration 315
  - display queue details 310
  - example of a Contact Center configuration with OpenScape Office HX 317
  - example of a Contact Center configuration with OpenScape Office MX 315
  - fallback solution 312
  - Grade of Service 310
  - holiday schedule 303

## Index

- myAgent 291
- myReports 294
- myReports user roles 295
- predefined report templates 332
- preferred agents 301
- procedure for configuration 326
- queue 302
- Report Designer 332
- reports 331
- restrictions on system features 328
- Rule editor 304
- schedule 303
- use of DECT telephones (HiPath Cordless Office) 330
- VIP call list 311
- VIP caller priority 311
- wallboard display 310
- wrapup 309
- wrapup reasons 309
- contact center 19, 290
- Contact Center (Menu) 88
- Cordless 41
- CorNet-IP 115
- CorNet-IP security 118
- corporate network 282
- cover page editor 194
- CRL (Certificate Revocation List) 362, 374
- CSV file 111
- Current draw 37
- customer trace log 484

## D

- Data
  - UC clients 38
- data
  - communications clients 38
  - technical 35, 37
- data backup (see backup)
- Data Protection 331
- data protection 29
- data security 29
- Date and Time (Menu) 82
- DECT phones 41
- default router 99
- defer a call 228
- Denied Lists (Menu) 85
- Departments (Menu) 87
- departments, OpenScape Office 170
- depth
  - dimensions 37
- Desk Sharing 348
- desktop dialer 150, 176

- DHCP 114
  - server 114
- DHCP Mode (Menu) 83
- DHCP relay agent 114
- diagnosis log 491
- diagnosis logs 480
- diagnosis protocol 480
- dial pause 210
- dial plan 109, 278, 475
- dialable call number format 176
- Dial-In Control Server 282
- dial-up network status 474
- digit dialing 206
- digit transmission 277
- digital loopback 483
- digital signature 360
- dimensions 37
- direct answering 212
- Direct Station Select (DSS) key 211
- directories 164
- Directory Service 156, 429
- DISA (Menu) 81
- Display (Menu) 81
- Display Conventions 20
- disposal 26
- DMZ (Menu) 83
- DNS (Domain Name Service) 97
  - client 97
  - first/second server 98
  - gateway functionality 97
- DNS name 98
- DNS zones 98
- Do Not Disturb 228
- download (see update)
- DSL (Digital Subscriber Line) 93
- DSS key 211
- Dual mode 41
- dual-mode telephony 345
- dynamic announcement 203
- DynDNS (Dynamic Domain Name Service) 98
- DynDNS (Menu) 82
- DynDNS service 98

## E

- E911 emergency call service 285
- edit a phone number 207
- electrical environment
  - OpenScape Office LX MX 28
  - OpenScape Office MX 27
- electromagnetic interference, OpenScape Office MX 29
- e-mail



- notification 195
- e-mail to SMS 197
- e-mail, send 196
- e-mails 205
- emergency 135
- emergency calls
  - prerequisites 283
- emergency, what to do 25
- en-bloc dialing 206
- Enterasys 42
- Entrance telephone 42
- Entrance Telephone (Menu) 86
- entrance telephone/door opener 432
- Environmental Conditions 37
- ESP header 354
- ET-S adapter 42
- Euro-ISDN features 515
- event 490
  - e-mail settings 491
  - log entries 490
  - log file 490
  - reaction table 491
- event viewer 483
- Events (Menu) 80
- exception
  - rule-based call forwarding 163
- Executive function (see Executive/Secretary configuration)
- Executive MULAP 255
  - ring type 256
  - SIP phones 257
- Executive/Secretary (see Executive/Secretary configuration)
- Executive/Secretary configuration 248
  - fax box 251
  - ring type 250
  - SIP phones 251
- expansion box, OpenScape Office MX 47
- expression filter 372
- external call forwarding - no answer 227
- external directory 167
- external directory (LDAP) 168
- External Directory (Menu) 87

**F**

- factory default image 464
- factory reset, OpenScape Office MX 464
- FastViewer 187
- favorites list 173
- fax 188
  - analog 431
  - T.38 198

- fax box group 258
- fax group (see fax box group)
- Fax Group 3 121
- Fax Group 4 120
- fax messages 189, 205
- Fax Printer 152, 194
- feature
  - disable via codes 518
  - enable via codes 518
- feature codes for Mobility Entry 339
- features
  - voice, network-wide 388
- file share 453
- File Upload (Menu) 88
- firewall 156, 369, 429
- fixed call forwarding 224
- Flex Call 349
- Flexible Menu (Menu) 82
- forward master zones 98
- forwarding 158
- FTP Server (Menu) 83
- full update (see update, full)
- function keys 119
- functions
  - myPortal 150
  - myPortal for Mobile 151, 335
  - myPortal for OpenStage 151
  - myPortal for Outlook 150

**G**

- gatekeeper 118
- Gateway (Menu) 82
- Gateway Modules 36
- gateway modules (OpenScape Office MX) 55
- Gigaset 41
- GMAA 62
- GMAL 64
- GME 60
- GMS 57
- GMSA 58
- GMT 61
- golden image 464
- grace period 135
- group call 238
  - DND for group member 238
  - ring type 240
  - SIP phones 240
  - voicemail box 239
- groups 236
- Groups (Menu) 87
- Groups/Hunt Groups (Menu) 85

## Index

### H

- H.323 115
- H.323 stack trace 485
- hardware configuration of OpenScape Office MX 476
- hardware installation of OpenScape Office MX
  - grounding 68
  - installation methods 68
  - installation site 67
  - power supply (for U.S. and Canada only) 67
  - preparatory steps 68
  - prerequisites 66
  - procedure 65
  - set up trunk connection 69
- hardware of OpenScape Office MX 47
- hardware, replace 144
- height
  - dimensions 37
- HiPath Cordless IP 41
- hold 218
- Holiday Schedules (Menu) 89
- Hot Desking 348
- hotline 284
- hotline after timeout 284
- humidity 37
- hunt group 241
  - ring type 243
  - SIP phones 243
  - voicemail 241

### I

- ICMP (Internet Control Message Protocol) 477
- IDS (Intrusion Detection System) 372
- IKE SA 359
- image file 457
- Incoming Calls (Menu) 84
- Individual Speed Dialing (ISD) 210
- Info text 158
- initiating a restart of OpenScape Office 462
- installation methods for the OpenScape Office MX communication system 68
- installing the OpenScape Office MX hardware
  - closing activities 70
- instant message 199
- instant messages 204
- instant messaging 204
- integration of OpenScape Office MX in LAN infrastructure 69
- Intercept/Attendant/Hotline (Menu) 81
- Interfaces 36, 42
- internal directory 166
- internal paging 259
  - transfer call 260

- Internet access 93, 100
  - configuration 94
  - via an external Internet modem 95
  - via an external Internet router 94
- Internet connection 35, 36
- Internet modem 95
- Internet router 94
- Internet telephony 100
- Internet Telephony Service Provider (ITSP) 100, 101
- Internet Telephony Service Provider (Menu) 84
- inventory management 469
- inventory of OpenScape Office LX 475
- inventory of OpenScape Office MX 475
- IP Address Filtering (Menu) 82
- IP addresses 475
- IP Client (Menu) 84
- IP client (see IP stations)
- IP Clients (Menu) 84
- IP Mapping (Menu) 83
- IP Mobility 348
- IP phones 40
- IP protocol 115
- IP protocols 528
- IP Routing (Menu) 83
- IP stations 112
- IPSec tunnel 359
- ISDN card 120
- ISDN devices 41
- ISDN message decoder 485
- ISDN modem 120
- ISDN phone 120
- ISDN stations 120
- ISDN trunk
  - selective seizure 269
- ITSP (Internet Telephony Service Provider) 100
- ITSP status 474

### J

- Java 156, 429
- journal 174
  - group entries 174
  - retention period 174
  - sort 174

### K

- key combination for the Desktop Dialer 176
- Key modules 40
- key programming 119
- Key Programming (Menu) 84

### L

- LAN (Menu) 83

- LAN ports 113
- LAN requirements 391
- languages 499
- LCR (Least Cost Routing) 275
  - class of service 280
  - dial plan 278
  - functionality 275
  - outdial rules 280
  - routing table 279
- LCR (routing) 83
- LDAP (Menu) 82
- LDAP connection 156, 429
- lease time 114
- LEDs of OpenScape Office MX
  - gateway modules 56
  - motherboard 52
- license 136
- License Authorization Code (LAC) 143
- license file 143
- license server (CLS) 134
- Lightweight CA 361
- line length for subscriber lines (OpenScape Office MX) 535
- locking the phone 375
- loudspeaker 121

## M

- MAC address filtering 373
- MAC Address Filtering (Menu) 82
- Mail Exchange entry 98
- Mail Exchanger 98, 99
- manual action 480
- manual suffix-dialing 209
- mapping (presence status) 158
- MCL Single Stage 282
- MCL Two-Stage 282
- Mediatrix 4102S 41
- medium, backup (see backup medium)
- message overview 204
- message texts 232
- messages
  - manage 204
- min network supplier 282
- mobile logon 349
- mobile phone 39, 337
- mobile PIN 349
- mobile stations 123
- mobile user logon 349
- Mobility Clients (Menu) 89
- Mobility Entry 338
  - feature codes 339
- Mobility Entry Groups (Menu) 85

- Mobility Entry stations
  - conferencing 178, 182, 183, 185, 186
  - modem 121
  - module release latch of OpenScape Office MX
    - motherboard 53
  - motherboard of OpenScape Office MX 48
    - connectors 49
    - LEDs 52
    - module release latch 53
    - remove 53
    - Reset switch 51
    - system behavior after unlocking module release latch 466
- MSN Assign (Menu) 85
- multibox system 70
  - convert a three-box system to a two-box system 71
  - updates 71
- Multibox System (Menu) 78
- multi-location 380
- multi-user chat 428
- Music on Hold (Menu) 78
- Music On Hold (MOH) 267
- Music On Hold (MOH) for call distribution 267
- MX record 98
- myAgent 39
  - prerequisites 292
- myAttendant 38
- myPortal 38
  - functions 150
  - presence status 150
- myPortal for Mobile 334
  - functions 151, 335
  - presence status 335
- myPortal for OpenStage
  - functions 151
  - presence status 151
- myPortal for Outlook
  - functions 150
- myReports 39
  - prerequisites 296
  - user roles 295

## N

- name announcement 203
- NAT (Menu) 83
- NAT (Network Address Translation) 97
- NAT rules 97
- NCP client 363
- network
  - heterogeneous, hybrid 380
  - homogeneous, native 380
  - license 390

## Index

- network carriers 282
- network connection, check 477
- Network Interfaces (Menu) 83
- network parameters (LAN, WAN) 391
- network plan 379
- network status 469
- networking
  - remove nodes from internetwork 381
- Night Service (Menu) 86
- notes on using myAgent and UC clients simultaneously 298
- notification
  - fax message 195
  - voicemail 195
- notification by phone 195
- notification service 195
- numbering
  - closed 395
  - open 395

## O

- On/Off switch of OpenScape Office MX 48
  - system behavior on pressing the switch 464
- Online User 497
- open conference 186
- Open Directory Service 170
- OpenScape Office
  - configure departments 170
- OpenScape Office Assistant, hardware and software prerequisites 72
- OpenScape Office MX system box 47
  - slot and access designations 54
- OpenScape Office MX, reset 464
- OpenScape Office MX, shut down 464
- OpenScape Office HX 37
- OpenScape Personal Edition 40
- OpenScape Office LX 35
- OpenScape Office MX 35
- OpenStage 40, 41
- OpenStage Gate View 43, 432
- operating conditions (environmental, mechanical)
  - OpenScape Office LX 32
  - OpenScape Office MX 31
- Operating System 35, 36, 37
- optiPoint 40, 41
- outdial rules 280
- override 231

## P

- padding 355
- parking 219
- password

- Phone menu 192
- path optimization 396
- path replacement 396
- payload SA 359
- PBX (Menu) 84
- PC clients 40
- permanent conference 185
- personal announcement 203
- personal AutoAttendant 203
- phone lock, individual 375
- Phone menu 192
- port 156, 429
- Port Management (Menu) 82
- port numbers 528
- ports 370
  - port administration 371
- Power consumption 37
- Power supply 37
- power supply 37
- power supply circuit and connection
  - OpenScape Office LX/HX 27
  - OpenScape Office MX 27
- prerequisites for Application Launcher 156, 429
- prerequisites for myAgent 292
- prerequisites for myPortal for Mobile 336
- prerequisites for myPortal for OpenStage 156
- prerequisites for myReports 296
- presence status 150, 151, 158, 203
  - automatic reset 158
  - call forwarding 162
  - Outlook 158
  - phone menu 192
  - visibility 158
- pre-shared keys 360
- prevention of voice calling for stations 212
- Primary Rate Interface 282
- prioritization of outside lines (trunks) 107
- priority 195
- priority classes 117
- private trunk 213
- profile for personal AutoAttendant 203
- profile with configuration data for Application Launcher 430
- profiles
  - subscribers 131
- proper use of the communication system 26
- protective grounding for OpenScape Office MX 68
- protocol 115
- proxy mode 372
- PSTN (Menu) 83
- Public Instant Messaging 428

**Q**

QSIG Feature (Menu) 85  
 Quality of Service (Menu) 82  
 Quality of Service (QoS) 117

**R**

radio frequency interference, OpenScape Office MX 29  
 RAS user 112  
 rebooting the UC Suite (integrated applications) 463  
 record 178  
 Recorder (Menu) 88  
 recycling 26  
 redialing 207  
 rejecting calls 228  
 reloading OpenScape Office 462  
 remote access 494  
 remote service via VPN 497  
   PIN for activation/deactivation 497  
 remote services 494  
 Reset switch for OpenScape Office MX 51  
 Reset switch of OpenScape Office MX  
   system behavior after initiating a reload 468  
 reset switch of OpenScape Office MX  
   system behavior after initiating a reset (restart) 466  
 resources required to install OpenScape Office MX 66  
 restart Web Services 463  
 restarting OpenScape Office 462  
 restarting the UC Suite (integrated applications) 463  
 restore 453, 456  
 restore (see restore)  
 reverse master zones 98  
 ringing assignment 227  
 routes 104, 105  
   add direction prefix incoming 106  
 routing 99  
 Routing (Menu) 83, 85  
 routing table 279  
 RPCAP daemon 489  
 RTP (Realtime Transport Protocol) 115  
 rule 163

**S**

safety information 21  
 Samba Share 377  
 scheduled conference 183  
 Schedules (Menu) 88  
 scope of the voicemail box 188  
 Secretary function (see Executive/Secretary  
   configuration)  
 Security (Menu) 82  
 Security Associations SA 359  
 security checklist 352

Server (Menu) 88  
 shutting down OpenScape Office MX 464  
 Signaling and Payload Encryption (SPE) 376  
 single location 380  
 SIP (Session Initiation Protocol) 115  
 SIP client 112  
 SIP features 517  
 SIP Parameters (Menu) 84  
 SIP Phones 41  
 SIP telephone  
   features of UC clients 516  
 slave zones 98  
 Slot Modules (Menu) 78  
 smartphone 39, 337  
 SMS 205  
   notification 195  
 SMS notification 197  
 SMS template 197  
 SNMP (Menu) 80  
 SNMP (Simple Network Management Protocol) 478  
   communities 478  
   Management Information Database (MIB) 478  
   traps 479  
 software activation 456  
 Software Image (Menu) 79  
 software transfer 456  
 software update (see update)  
 software updates 456  
 speaker call 212  
 speaker call for groups 259  
 Special Days (Menu) 86  
 speed dialing system 208  
 Speed Dials (Menu) 82  
 SSDP (Smart Services Delivery Platform) 495  
   PIN for activating/deactivating the service plugin  
   497  
 SSL (Menu) 82  
 SSL (Secure Socket Layer) 374  
 standards 500  
 standards for trunk connections (OpenScape Office  
   MX) 538  
 static routes 99  
 station flags 546  
 station status 474  
 stations 109  
   analog 121  
   configure in Expert Mode 126  
   configure with wizards 124  
   IP 112  
   ISDN 120  
   mobile 123  
 stations (Classes of Service Menu) 85

## Index

- Stations (Menu) 84
  - status of interfaces 469
  - status of the communication system 469
  - status-based voicemail announcements 188
  - STUN (Simple Traversal of UDP through NAT) 102
  - subscriber line ranges (OpenScape Office MX) 535
  - subscribers
    - configuring users of OpenScape Office clients 128
  - survivability 426
  - System (Menu) 81
  - system behavior of OpenScape Office MX
    - after initiating a reload via the Reset switch 468
    - after initiating a reset (restart) via the Reset switch 466
    - after pressing the On/Off switch 464
    - after unlocking module release latch of motherboard 466
  - system client 112
  - system connection 156, 429
  - system directory 169
  - system flags 540
  - System Flags (Menu) 81
  - system language for voicemail 188
  - System Speed Dialing (SSD) 208
  - system-wide flags 540
- ## T
- T.38 Fax 198
  - tablet PC 39, 337
  - TAPI 43
  - TCP (Transmission Control Protocol) 115
  - TCP dump 489
  - TDM telephones 41
  - team (see team configuration)
  - team configuration 245
    - fax box 247
    - ring type 247
    - SIP phones 247
  - team function (see team configuration)
  - team group 245
    - fax box 247
    - ring type 247
    - SIP phones 247
  - Team/Top (Menu) 85
  - Telephones 40
  - teleworking 161, 348
  - Templates (Menu) 87
  - Terminal server and Citrix server environments 150
  - Texts (Menu) 82
  - TIFF file
    - notification 195
  - Time Parameters (Menu) 81
  - toggle/connect 220
  - toll restriction 269
  - tools required to install OpenScape Office MX 66
  - top group 248
    - fax box 251
    - ring type 250
    - SIP phones 251
  - trace 482
    - format configuration 482
    - log 483
    - output interfaces 483
  - trace component 489
  - trace profile 486
  - Traces (Menu) 79
  - transfer calls 220
  - transfer to group from announcement 260
  - transfer, software (see software transfer)
  - translation of station numbers to names 218
  - transmission of customer-specific call number information 217
  - transparent and proxy mode 372
  - trunk connection, OpenScape Office MX 69
    - attenuation values 538
    - standards 538
  - trunk queuing 213
  - trunk release for emergency call 285
  - trunks 104
    - type of seizure 105
  - Trunks (Menu) 85
  - Trunks/Routing (Menu) 85
- ## U
- UC Suite
    - client logs 493
    - e-mail notification 493
  - UC Suite (Menu) 87
  - UC Suite
    - maintenance 492
    - monitoring 492
    - notification 493
    - system logs 492
  - UCD (Menu) 85
  - UCD (Uniform Call Distribution) (see call distribution)
  - UDP (User Datagram Protocol) 115
  - update 456
    - custom 458
    - full 458
  - update licenses 144
  - update, software (see software updates)
  - upgrade 456
    - from V2 to V3 379
  - URL blocker 371

- log file 372
- user (station) profiles 131
- user buttons 204
  - layout 204
  - multiple 204
  - sort 204
- User Directory (Menu) 87
- user-defined profile, custom profile 203
- users of OpenScape Office clients 122
  - configure 128

**V**

- Voice Gateway (Menu) 84
- voicemail 188
  - call pickup 188
  - save 188
  - status-based announcements 188
- Voicemail (Menu) 82
- voicemail box 158, 188, 203
  - Phone menu 192
- voicemail box, see voicemail 188
- voicemail group 258
- voicemail messages 189, 204
- voltage 37
- VPN
  - authentication 360
  - bandwidths 354
  - clients 362
  - security mechanisms 359
- VPN (Menu) 82
- VPN (Virtual Private Network) 352
  - end-to-site 353
  - site-to-site 353
- VPN certificates 361
- VPN client 42
- VPN status 474

**W**

- WAN 96
- WAN (Menu) 83
- WAN requirements 393
- warnings 21
  - caution 24
  - danger 23
  - note 24
  - warning 23
- WAV file
  - notification 195
- Web Collaboration 187
- Web Collaboration (Menu) 89
- web filter 372
- Web Services 156, 429

- restart 463
- Web Services (Menu) 89
- width
  - dimensions 37
- Wiki 42
- Windows XP client 363
- WLAN Phones 41
- write protection for the Samba Share 377

**X**

- XMPP 158, 428
- XMPP (Menu) 89