



A MITEL
PRODUCT
GUIDE

Unify OpenScape Desk Phone CP Family

OpenScape Desk Phone CP Family

Administrator Documentation SIP

10/2025

Notices

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

Trademarks

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

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Contents

1 Overview.....	10
1.1 Important Notes.....	10
1.2 Maintenance Notes.....	11
1.3 Product-oriented environmental protection.....	11
1.4 Labeling.....	12
1.5 License Information.....	12
1.6 About the Manual.....	12
1.7 Conventions for this Document.....	12
1.8 The OpenScape Desk Phone CP Family.....	12
1.8.1 OpenScape Desk Phone CP700/700X.....	13
1.8.2 OpenScape Desk Phone CP600/600E.....	14
1.8.3 OpenScape Desk Phone CP400.....	15
1.8.4 OpenScape Desk Phone CP200/CP205.....	17
1.8.5 OpenScape Desk Phone CP100.....	18
1.9 Administration Interfaces.....	19
1.9.1 Web-based Management (WBM).....	19
1.9.2 DLS/DMS (OpenScape Deployment Service / Device Management Service).....	19
1.9.3 Local Phone Menu.....	20
2 Startup.....	21
2.1 Prerequisites.....	21
2.2 Assembling and Installing the Phone.....	21
2.2.1 Shipment.....	21
2.2.2 Connectors at the bottom side.....	22
2.2.3 Assembly.....	24
2.2.4 How to Connect the Phone.....	24
2.2.5 How to Better Use LAN Network Connections.....	25
2.2.6 Key Module.....	26
2.2.6.1 Key module settings for CP600/600E Broadsoft.....	26
2.3 Quick Start.....	27
2.3.1 How to Access the Web Interface (WBM).....	27
2.3.1.1 Licenses.....	28
2.3.2 How to Set the Terminal Number.....	29
2.3.3 Basic Network Configuration.....	29
2.3.4 DHCP Resilience.....	30
2.3.5 Date and Time / SNTP.....	30
2.3.6 SIP Server Address.....	30
2.3.7 Extended Network Configuration.....	31
2.3.8 Vendor Specific: VLAN Discovery and DLS Address.....	31
2.3.8.1 How to Use a Vendor Class.....	31
2.3.8.2 How to Use Option #43 "Vendor Specific".....	37
2.3.9 DLS Server Address.....	38
2.3.9.1 Using Vendor Class.....	39
2.3.9.2 Using Option #43 "Vendor Specific".....	44
2.3.10 Using the Web Interface (WBM).....	45
2.3.11 Using the Local Menu.....	46
2.3.12 Set DMS Address via DHCP.....	47
2.3.12.1 Using Option 43.....	47
2.3.12.2 Using Option 66.....	48
2.4 Cloud Deployment.....	48
2.4.1 Process of cloud deployment.....	48

2.4.2 Aborting cloud deployment process by User.....	51
2.4.3 Re-trigger cloud deployment.....	52
2.4.4 Deployment errors.....	52
3 Administration.....	53
3.1 Access via Local Phone.....	53
3.1.1 OpenScape Desk Phone CP100.....	53
3.1.2 OpenScape Desk Phone CP20X.....	54
3.1.3 OpenScape Desk Phone CP400/600/600E/700/700X.....	54
3.2 Bluetooth Interface.....	55
3.3 LAN Settings.....	55
3.3.1 LAN Port Settings.....	55
3.3.2 VLAN.....	58
3.3.2.1 Automatic VLAN discovery using LLDP-MED.....	59
3.3.2.2 Automatic VLAN discovery using DHCP.....	60
3.3.2.3 Manual configuration of a VLAN ID.....	61
3.4 IP Network Parameters.....	63
3.4.1 Quality of Service (QoS).....	63
3.4.1.1 Layer 2 / 802.1p.....	63
3.4.1.2 Layer 3 / Diffserv.....	64
3.4.2 Protocol Mode IPv4/IPv6.....	66
3.4.3 Gratuitous ARP control.....	67
3.4.4 Parse DHCPv4 option 43 and DHCPv6 option 17.....	67
3.4.5 Parse DHCP option 66.....	68
3.4.6 Use DHCP.....	69
3.4.7 IP Address - Manual Configuration.....	71
3.4.8 Default Route/Gateway.....	73
3.4.9 Specific IP Routing.....	74
3.4.10 DNS.....	79
3.4.10.1 DNS Domain Name.....	79
3.4.10.2 DNS Servers.....	79
3.4.10.3 Terminal Hostname.....	80
3.4.10.4 IP TTL.....	81
3.4.11 Configuration & Update Service.....	82
3.4.12 SNMP.....	84
3.5 Wi-Fi Settings.....	88
3.5.1 Setting up a CP700X for the first time with WLAN connection.....	89
3.5.2 Disabling LAN port (for CP700X).....	90
3.5.3 Advanced Wi-Fi settings.....	91
3.6 Security.....	93
3.6.1 System.....	93
3.6.2 SRTP Configuration.....	94
3.6.3 Access control.....	96
3.6.4 Security Log.....	97
3.6.5 Security-Related Faults.....	98
3.6.6 Microsoft® Exchange.....	99
3.6.6.1 Configuring Oath2 authentication.....	99
3.6.6.2 Accessing Microsoft® Exchange.....	101
3.6.7 Password Policy.....	101
3.6.7.1 General Policy.....	101
3.6.7.2 Display password change prompt.....	102
3.6.7.3 Admin Policy.....	102
3.6.7.4 Character Set.....	103
3.6.7.5 Change Admin and User password.....	104
3.6.8 Certificate Policy.....	105
3.6.8.1 Online Certificate Check.....	105

3.6.8.2 Server Authentication Policy.....	105
3.6.8.3 SCEP.....	107
3.7 System Settings.....	111
3.7.1 Terminal and User Identity.....	111
3.7.1.1 Terminal Identity.....	111
3.7.1.2 Display Identity.....	112
3.7.2 Emergency and Voice Mail.....	112
3.7.3 Energy Saving.....	113
3.7.3.1 Backlight Time Setting (OpenScape Desk Phone CP600/600E/700/700X only).....	113
3.7.3.2 Energy Efficient Ethernet (OpenScape Desk Phone CP205/400/600/600E/700/700X only).....	114
3.7.4 Call logging.....	114
3.7.4.1 Logging of Missed Calls (via User menu).....	115
3.7.4.2 Translation set change.....	116
3.7.5 Date and Time.....	117
3.7.5.1 SNTP is Available, but no Automatic Configuration by DHCP Server.....	117
3.7.5.2 No SNTP Server Available.....	118
3.7.6 SIP Addresses and Ports.....	118
3.7.6.1 SIP Addresses.....	118
3.7.6.2 SIP Ports.....	120
3.7.7 SIP Registration.....	120
3.7.7.1 Re-registration timer.....	122
3.7.8 SIP Communication.....	123
3.7.8.1 Outbound Proxy.....	123
3.7.8.2 SIP Transport Protocol.....	124
3.7.8.3 SIP connection.....	125
3.7.8.4 Failover on SIP 5XX server response.....	126
3.7.8.5 Media/SDP.....	127
3.7.8.6 Early 183 response.....	129
3.7.8.7 Keep resolved DNS records.....	129
3.7.8.8 Prefer FROM header.....	130
3.7.8.9 DNS-SRV fallback on re-registration.....	131
3.7.8.10 Support provisional response (PRACK).....	132
3.7.8.11 Send all codecs in SDP answer.....	133
3.7.9 SIP Session Timer.....	134
3.7.10 Resilience and Survivability.....	136
3.7.10.1 TLS Connectivity Check.....	137
3.7.10.2 TCP Connectivity Check.....	138
3.7.10.3 Response Timer.....	139
3.7.10.4 Non-INVITE Transaction Timer.....	140
3.7.10.5 Maximum Registration Backoff Timer.....	141
3.7.10.6 Backup SIP Server.....	142
3.7.11 Interactive Connectivity Establishment (ICE).....	144
3.7.11.1 General.....	144
3.7.11.2 Addressing.....	145
3.7.11.3 Candidates.....	146
3.7.11.4 Technical.....	147
3.8 Feature access.....	148
3.9 Feature Configuration.....	150
3.9.1 Allow Refuse.....	150
3.9.2 Hot/Warm Phone.....	151
3.9.3 Initial Digit Timer.....	152
3.9.4 Show Forwarding icon.....	153
3.9.5 Allow user downloads.....	154
3.9.6 Redial original forwarded.....	155
3.9.7 Group Pickup.....	156
3.9.7.1 Feature Code.....	156

3.9.7.2 Pickup alert.....	157
3.9.8 Call Transfer.....	159
3.9.8.1 Transfer on Ring.....	159
3.9.8.2 Transfer on Hangup.....	160
3.9.9 Callback URIs.....	160
3.9.9.1 Call Completion.....	161
3.9.10 Message Waiting Address.....	162
3.9.11 Indicate Messages.....	163
3.9.12 System Based Conference.....	164
3.9.13 RTCP-XR server.....	165
3.9.14 Call-Center Agent.....	173
3.9.14.1 Broadsoft Agent Logon/Logoff.....	176
3.9.15 Server Based Features.....	177
3.9.16 uaCSTA Interface.....	179
3.9.16.1 External CSTA server configuration.....	179
3.9.17 Local Menu Timeout.....	180
3.9.18 Call Recording.....	181
3.9.19 Rollover Visual Alert.....	182
3.9.20 Landing screen.....	183
3.9.21 DSS monitoring.....	184
3.9.22 Bridged Call Appearance.....	185
3.10 Free Programmable Keys.....	185
3.10.1 How to Configure Free Programmable Keys (FPKs).....	186
3.10.2 Key module settings for CP600/600E/700/700X.....	186
3.10.2.1 Feature Key for CP700/700X.....	187
3.10.3 How to Enable "Long Press" for Free Programmable Keys.....	188
3.10.4 Selected Dial Action on Calls.....	189
3.10.5 Clear (no feature assigned).....	190
3.10.6 Selected Dialing.....	191
3.10.7 Repeat Dialing.....	192
3.10.8 Call Forwarding (Standard).....	192
3.10.9 Call Forwarding by Call Type.....	193
3.10.9.1 Call Forwarding Indication.....	195
3.10.10 Ringer off.....	196
3.10.11 Hold.....	197
3.10.12 Alternate.....	197
3.10.13 Blind Call Transfer.....	197
3.10.14 Transfer Call.....	198
3.10.15 Deflect a Call.....	198
3.10.16 Shift Level.....	199
3.10.17 Phone-Based Conference.....	199
3.10.18 Accept Call via Headset.....	200
3.10.19 Do Not Disturb.....	200
3.10.20 Group Pickup.....	201
3.10.21 Repertory Dial.....	201
3.10.22 Feature Toggle.....	202
3.10.23 Mobility / Mobile User Logon.....	203
3.10.23.1 Bluetooth mobility.....	203
3.10.23.2 Disable HFU.....	204
3.10.24 Directed Pickup.....	204
3.10.25 Callback.....	204
3.10.25.1 Cancel Callbacks.....	205
3.10.26 Pause Callbacks.....	205
3.10.27 Resume Callbacks.....	206
3.10.28 Consultation.....	206
3.10.29 Call Waiting.....	207

3.10.30 Call Recording.....	207
3.10.30.1 Auto Answer With Zip Tone.....	208
3.10.31 Server Feature.....	208
3.10.32 BLF Key.....	209
3.10.33 Send Request via HTTP/HTTPS.....	211
3.10.34 Built-in Forwarding.....	213
3.10.35 2nd Alert.....	214
3.10.36 Start Phonebooks.....	214
3.10.36.1 Network directories for Broadsoft.....	215
3.10.37 Show phone screen (OpenScope Desk Phone CP100/CP200/CP205 only).....	215
3.10.38 Release.....	215
3.10.39 Stimulus Idle screen menu options.....	216
3.11 Door opener on OpenScope Desk Phone CP600/600E/700/700X.....	218
3.12 Action URLs.....	219
3.13 Fixed Function Keys on OpenScope Desk Phone CP100/CP200/CP205.....	220
3.14 Main menu screen options on OpenScope Desk Phones CP400/600/600E/CP700.....	221
3.14.1 Main Menu Option Configuration.....	221
3.15 Multiline Appearance/Keyset.....	224
3.15.1 Line Key Configuration.....	224
3.15.2 How to Configure Line Keys for Keyset Operation.....	227
3.15.3 Configure Keyset Operation.....	228
3.15.4 Immediate Ring.....	231
3.15.5 Direct Station Select (DSS).....	232
3.15.5.1 General DSS Settings.....	232
3.15.5.2 Settings for a DSS key.....	233
3.15.6 Distinctive Ringers per Keyset Lines.....	235
3.15.7 Multiple Call Arrangement.....	237
3.15.8 E/A Cockpit settings.....	239
3.16 Key Modules.....	239
3.17 Dialing.....	241
3.17.1 Canonical Dialing Configuration.....	241
3.17.2 Canonical Dial Lookup.....	245
3.17.3 Phone location.....	246
3.17.4 Dial Plan.....	247
3.18 Ringer Setting.....	248
3.18.1 Distinctive.....	249
3.18.2 Map to Specials.....	250
3.18.3 Ringer Mode.....	251
3.18.4 Ringer Volume.....	252
3.18.5 Special Ringers.....	252
3.19 Mobility.....	254
3.20 Transferring Phone Software, Application, and Media Files.....	255
3.20.1 File name.....	255
3.20.2 FTP/HTTPS Server.....	256
3.20.3 Common FTP/HTTPS Settings (Defaults).....	256
3.20.4 Phone Application.....	258
3.20.4.1 Upgrade using File.....	259
3.20.4.2 Upgrade using FTP/HTTPS.....	259
3.20.4.3 Download/Update Phone Application.....	260
3.20.5 Picture Clips.....	261
3.20.5.1 FTP/HTTPS Access Data.....	262
3.20.5.2 Download Picture Clip.....	263
3.20.5.3 Picture Clips via LDAP.....	264
3.20.6 LDAP Template.....	265
3.20.6.1 FTP/HTTPS Access Data.....	266
3.20.6.2 Download LDAP Template.....	267

Contents

3.20.7 Screensaver.....	268
3.20.7.1 FTP/HTTPS Access Data.....	268
3.20.7.2 Download Screensaver.....	269
3.20.8 Ringer File.....	270
3.20.8.1 FTP/HTTPS Access Data.....	271
3.20.8.2 Download Ringer File.....	272
3.20.9 Company logo.....	273
3.21 Corporate Phonebook: Directory Settings.....	275
3.21.1 LDAP.....	275
3.21.2 Contact details update.....	277
3.21.2.1 Source of the contact details.....	278
3.22 XSI access.....	279
3.23 RingCentral API connection.....	279
3.23.1 Syncing call log data.....	280
3.23.2 Syncing the phonebook.....	281
3.23.3 Syncing the DND settings.....	281
3.24 Network directories.....	282
3.25 Call log.....	283
3.26 Speech.....	283
3.26.1 RTP Base Port.....	283
3.26.2 Codec Preferences.....	284
3.26.3 Audio Settings.....	287
3.27 Password.....	287
3.27.1 Troubleshooting: Lost Password.....	288
3.28 Restart Phone.....	288
3.29 Factory Reset.....	289
3.30 SSH — Secure Shell Access.....	289
3.31 Diagnostics.....	290
3.31.1 Display General Phone Information.....	290
3.31.2 View Diagnostic Information.....	291
3.31.3 User Access to Diagnostic Information.....	292
3.31.4 Diagnostic Call.....	292
3.31.5 LAN Monitoring.....	294
3.31.6 LLDP-MED.....	294
3.31.7 IP Tests.....	296
3.31.8 Process and Memory Information.....	296
3.31.9 Fault Trace Configuration.....	298
3.31.10 EasyTrace Profiles.....	304
3.31.10.1 Phone administration problems.....	304
3.31.10.2 Audio related problems.....	305
3.31.10.3 Bluetooth problems.....	306
3.31.10.4 Call proceeding problems.....	306
3.31.10.5 Conversations / LDAP problems.....	307
3.31.10.6 Keyset problems.....	307
3.31.10.7 Mobility / DLS problems.....	308
3.31.10.8 Network problems.....	308
3.31.10.9 Security problems.....	308
3.31.11 Bluetooth Advanced Traces.....	309
3.31.12 Advanced Audio Traces.....	309
3.31.13 M5T Advanced Traces.....	310
3.31.14 QoS Reports.....	311
3.31.14.1 Conditions and Thresholds for Report Generation.....	311
3.31.14.2 View Report.....	313
3.31.15 Core dump.....	315
3.31.16 Remote Tracing — Syslog.....	316
3.31.17 HPT Interface (For Service Staff).....	317

3.32 MWI LED.....	317
3.33 Missed Call LED.....	318
3.34 AlertBar LED hint.....	319
3.35 Impact Level Notification.....	320
4 Technical Reference.....	323
4.1 Default Port List.....	323
4.2 Troubleshooting: Error Codes.....	324
5 Examples and HowTos.....	326
5.1 Canonical Dialing.....	326
5.1.1 Canonical Dialing Settings.....	326
5.1.2 Canonical Dial Lookup.....	326
5.1.2.1 Conversion examples.....	327
5.2 How to Set Up the Corporate Phonebook (LDAP).....	328
5.2.1 Prerequisites.....	328
5.2.2 Create an LDAP Template.....	329
5.2.3 Load the LDAP Template onto the Phone.....	333
5.2.4 Configure LDAP Access.....	333
5.3 An LLDP-Med Example.....	334
5.4 Example Dial Plan.....	336
5.4.1 Introduction.....	336
5.4.2 Dial Plan Syntax.....	336
5.4.3 How To Set Up And Deploy A Dial Plan.....	337
6 Glossary.....	340
 Index.....	 346

1 Overview

1.1 Important Notes



WARNING: Do not operate the equipment in environments where there is a danger of explosions.



WARNING: If Power over Ethernet (PoE) is not available: For safety reasons the phone should only be operating using the supplied plug-in power unit.



WARNING: Use only original accessories. Using other accessories may be dangerous and will invalidate the warranty, extended manufacturer's liability and the CE mark.



WARNING: Never open the telephone or add-on equipment. If you encounter any problems, contact System Support.



WARNING: Installation requirement for USA, Canada, Norway, Finland, and Sweden: Connection to networks which use outside cables is prohibited. Only in-house networks are permitted.



WARNING: For USA and Canada only:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This product is a UL Listed Accessory, I.T.E., in U.S.A. and Canada.

This equipment also complies with the Part 68 of the FCC Rules and the Industrie Canada CS-03.

1.2 Maintenance Notes



WARNING: Do not perform maintenance work or servicing of the telephone in environments where there is a danger of explosions.



WARNING: Use only original accessories. Using other accessories may be dangerous and will invalidate the warranty and the CE mark.



WARNING: Never open the telephone or a key module. If you encounter any problems, contact System Support.

1.3 Product-oriented environmental protection

Unify is committed in terms of its product strategy to bringing environmentally friendly products to market, taking account of the entire product life cycle. Unify strives to acquire the relevant environmental labels for its products in the event that the environmental label programs permit qualification for individual Unify products.



ENERGY STAR is a U.S. Environmental Protection Agency voluntary program that helps businesses and individuals save money and protect our climate through superior energy efficiency.

Products that earn the ENERGY STAR prevent greenhouse gas emissions by meeting strict energy efficiency criteria or requirements set by the U.S. Environmental Protection Agency.

Learn more at www.energystar.gov.

Unify is an ENERGY STAR partner participating in the ENERGY STAR program for Enterprise Servers and Telephony.

The Unify product OpenScape DeskPhone CP100, OpenScape DeskPhone CP200, OpenScape DeskPhone CP400 and OpenScape DeskPhone CP600/600E and OpenScape DeskPhone CP700/700X have earned the ENERGY STAR.

Special setting instructions for energy-efficient use of telephones can be found on [Energy Saving](#) on page 113.

1.4 Labeling



The compliance of the equipment according to EU directives is confirmed by the CE mark. This Declaration of Conformity and, where applicable, other existing declarations of conformity as well as further information on regulations that restrict the usage of substances or affect the declaration of substances used in products can be found in the Unify Expert WIKI at <http://wiki.unify.com> under the section *Declarations of Conformity*.

1.5 License Information

For more information about the EULA and Open Source licenses, see [Licenses](#) on page 28.

1.6 About the Manual

The instructions within this manual will help you in administering and maintaining OpenScape Desk Phone CP telephones. The instructions contain important information for safe and proper operation of the phones. Follow them carefully to avoid improper operation and get the most out of your multi-function telephone in a network environment.

This guide is intended for service providers and network administrators who administer VoIP services using the OpenScape Desk Phone CP and who have a fundamental understanding of VoIP, SIP, IP networking, and telephony. The tasks described in this guide are not intended for end users.

These instructions are laid out in a user-oriented manner, which means that you are led through the functions of the OpenScape Desk Phone CP step by step, wherever expedient. For the users, a separate manual is provided.

You can find further information on the official Unify website (<http://www.unify.com/>) and on the Unify Wiki (<http://wiki.unify.com/>).

1.7 Conventions for this Document

The terms for parameters and functions used in this document are derived from the web interface (WBM). In some cases, the phone's local menu uses shorter, less specific terms and abbreviations. In a few cases the terminologies differ in wording. If so, the local menu term is added with a preceding "/".

For the parameters described in this document, a WBM screenshot and the path in the local phone menu is provided.

This document describes the software version V1.

1.8 The OpenScape Desk Phone CP Family

The OpenScape Desk Phone CP phone family comprises the following devices.

- [OpenScape Desk Phone CP700/700X](#) on page 13
- [OpenScape Desk Phone CP600/600E](#) on page 14

- [OpenScape Desk Phone CP400](#) on page 15
- [OpenScape Desk Phone CP200/CP205](#) on page 17
- [OpenScape Desk Phone CP100](#) on page 18

1.8.1 OpenScape Desk Phone CP700/700X



1	Handset - use it for handset calls.
2	Graphic display - allows the intuitive operation of the phone.
3	Menu Key - switches to the main menu.
4	Navigator - allows you to navigate through the various applications on your phone.
5	Softkeys - select a function or open a menu.
6	Audio keys - allow you to optimally configure the audio features and screen brightness on your phone.
7	Notification-LED - incoming calls, new voice messages or missed calls indicator.
8	Dialpad - allows you to enter phone numbers or text.
9	Out-of-Office/Call Forwarding key - opens a menu to set up immediate call forwarding or to activate Do not disturb.
10	NFC transmitter (logo: ) - allows simple Bluetooth pairing.

11	MWI key - Message waiting indicator; it also provides access to the voicemail system.
12	Hold key - puts current call on hold.
13	Transfer key - puts a call on hold and gives you dial tone to call another party.
14	Conference key - establishes a conference call.
15	Redial key - activates a function configured by the administrator.
16	Programmable keys - keys to which you can assign functions or phone numbers.

1.8.2 OpenScape Desk Phone CP600/600E



1	With the Handset , the user can pick up and conduct calls in the usual manner.
2	The Microphone is used in the speakerphone mode.
3	The Display provides intuitive support for telephone operation.
4	With the Menu Key , the user/administrator can return to the Main Menu Screen.

5	With the Navigation Keys , the user/administrator can navigate through the various phone functions.
6	With the Soft Keys , the user/administrator can operate the phone's functions.
7	Audio Keys: + and -: Increases/decreases the speaker/headset, handset volume and screen brightness. Mute : Turns off/on the microphone during conversations. Speaker : Turns on/off the hands-free mode (speakerphone). Headset : Switches the audio between handset/speakerphone and headset
8	The Notification LED visually signals incoming calls and new voice messages.
9	The Keypad is used for entering phone numbers and text.
10	The Out-of-Office Key provides an easy way to set up Call Deflection and DND.

1.8.3 OpenScape Desk Phone CP400



1	With the Handset , the user can pick up and conduct calls in the usual manner.
2	The Microphone is used in the speakerphone mode.

3	The Display provides intuitive support for telephone operation.
4	With the Menu Key , the user/administrator can return to the Main Menu Screen.
5	With the Navigation Keys , the user/administrator can navigate through the various phone functions.
6	With the Soft Keys , the user/administrator can operate the phone's functions.
7	Audio Keys: + and -: Increases/decreases the speaker/headset and handset volume. Mute : Turns off/on the microphone during conversations. Speaker : Turns on/off the hands-free mode (speakerphone). Headset : Switches the audio between handset/speakerphone and headset
8	The Notification LED visually signals incoming calls and new voice messages.
9	The Keypad is used for entering phone numbers and text.
10	The Out-of-Office Key provides an easy way to set up Call Deflection and DND.
11	The Free programmable Keys can be set up with various functions defined by user.

1.8.4 OpenScape Desk Phone CP200/CP205



1	With the Handset , the user can pick up and conduct calls in the usual manner.
2	The Microphone is used in the speakerphone mode.
3	The Display provides intuitive support for telephone operation.
4	Conversation Keys: Hold : Places a call in hold. Transfer : Transfers a current call to another party. Conference : Initiates a conference call.
5	With the Menu Key , the user has access to the user menu.
6	With the Messages Key , the user has access to the voicemail.
7	With the Navigation Keys , the user/administrator can navigate through the various phone functions.
8	With the Function Keys , the user can comfortably operate the phone's functions like Conversations, Phonebook, Call Deflection and Redial.
9	The Keypad is used for entering phone numbers and text.

10	Audio Keys: + and -: Increases/decreases the speaker/headset and handset volume. Mute: Turns off/on the microphone during conversations. Speaker: Turns on/off the hands-free mode (speakerphone). Headset: Switches the audio between handset/speakerphone and headset
11	The Notification LED visually signals incoming calls and new voice messages.

1.8.5 OpenScape Desk Phone CP100



1	With the handset, the user can pick up and conduct calls in the usual manner.
2	The display permits intuitive operation of the phone, it is realized as a three line display.
3	Incoming calls, voice mails and others are visually signaled via the Notification LED.

4	You can customize your telephone by assigning phone numbers and functions to the programmable keys. Preset default values: • Call log (Directory is the default for this key when at its shifted level) • Built-in forwarding (Transfer is the default for this key when at its shifted level) • Repeat dialing (Hold is the default for this key when at its shifted level)
5	The dialpad can be used to enter phone numbers and write text.
6	You can use the navigation keys to navigate conveniently through the various phone functions, applications and configuration menus.
7	Use the function keys to launch the following functions: Â: the mailbox key retrieves voicemail. @: the service key opens the Program/Service menu.
8	:: the speaker key activates/deactivates speakerphone mode. ": the WIP key adjusts the volume or contrast. ;: the mute key switches the microphone on/off. This function is useful to prevent the other party from listening in under certain circumstances, for example when consulting with someone else in the room or in case of annoying background noise.

1.9 Administration Interfaces

You can configure the OpenScape Desk Phone CP by using any of the methods described in this chapter.

1.9.1 Web-based Management (WBM)

This method employs a web browser for communication with the phone via HTTPS. It is applicable for remote configuration of individual IP phones in your network. Direct access to the phone is not required.

NOTICE: To use this method, the phone must first obtain IP connectivity.

1.9.2 DLS/DMS (OpenScape Deployment Service / Device Management Service)

The OpenScape Deployment Service (DLS) and Broadsoft Device Management Service (DMS) are Management applications for administering phones in both OpenScape and non-OpenScape networks. For further information, please refer to the DLS or DMS Administration Guide.

NOTICE: To use this method, the phone must first obtain IP connectivity.

1.9.3 Local Phone Menu

This method provides direct configuration of the OpenScape Desk Phone CP via the local phone menu. Direct access to the phone is required.

NOTICE: As long as the IP connection is not properly configured, you have to use this method to set up the phone.

2 Startup

2.1 Prerequisites

The OpenScape Desk Phone CP acts as an endpoint client on an IP telephony network, and has the following network requirements:

- An Ethernet connection to a network with SIP clients and servers.

NOTICE: Only use switches in the LAN to which the OpenScape Desk Phone CP phone is connected. An operation at hubs can cause serious malfunctions in the hub and in the whole network.

- OpenScape Voice server.
- An FTP Server for file transfer, e. g. firmware, configuration data, application software
- A DHCP (Dynamic Host Configuration Protocol) server (recommended).
- DLS (OpenScape Deployment Service) for advanced configuration and software deployment (recommended).

For additional information see: http://wiki.unify.com/wiki/IEEE_802.1x

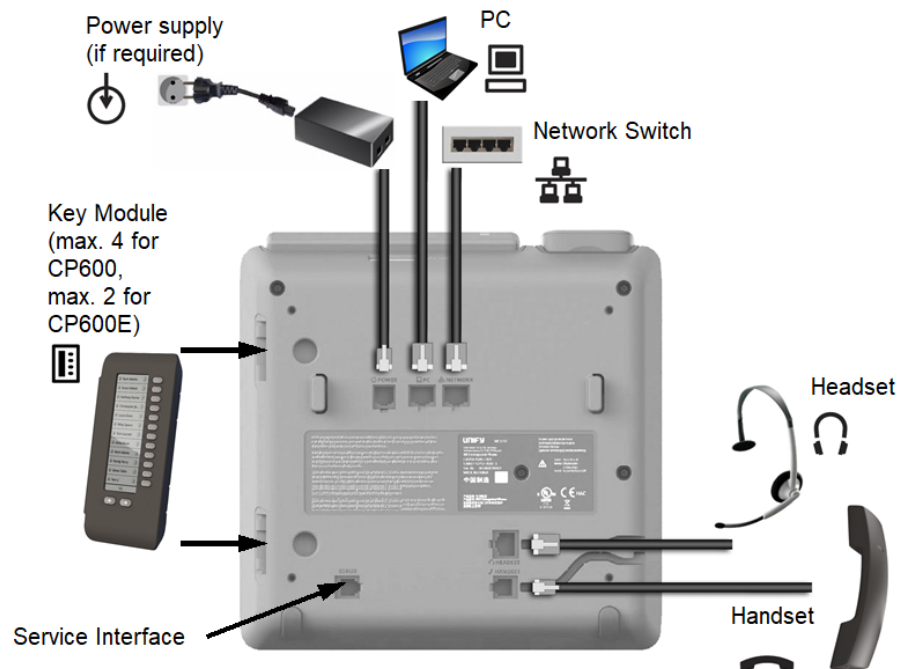
2.2 Assembling and Installing the Phone

2.2.1 Shipment

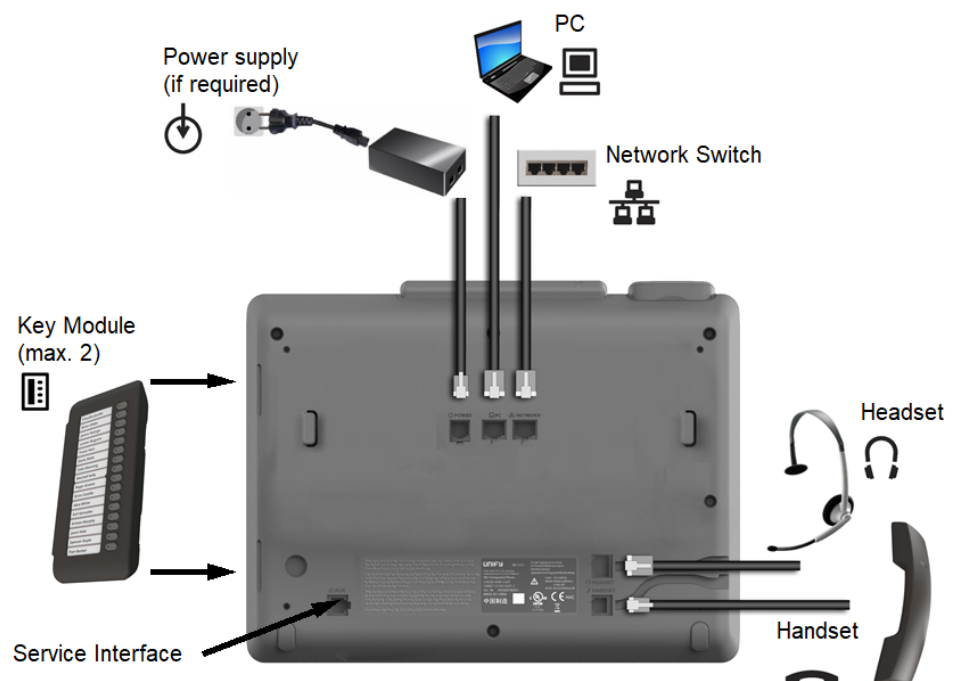
- Phone
- Handset
- Handset cable
- **Subpackage:**
 - Document "Information and Important Operating Procedures"

2.2.2 Connectors at the bottom side

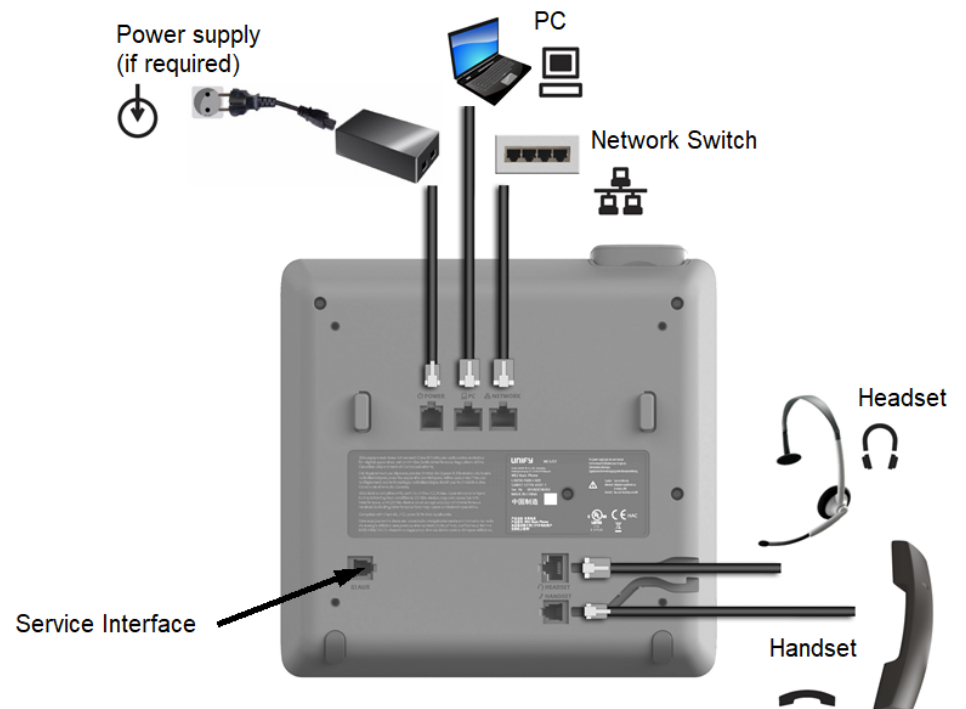
OpenScape Desk Phone CP600



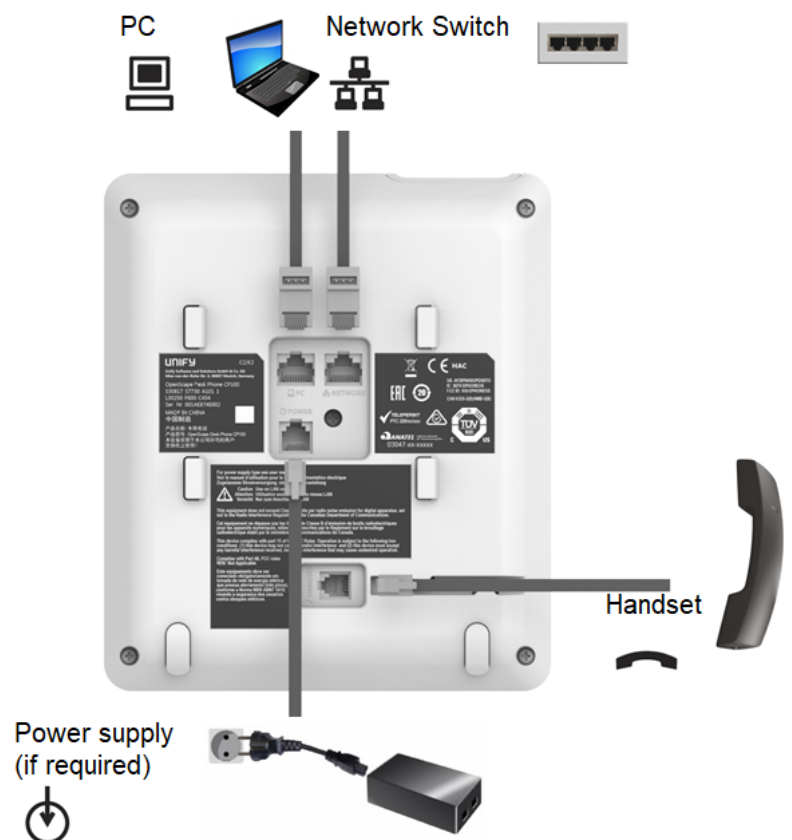
OpenScape Desk Phone CP400



OpenScope Desk Phone CP200/CP205



OpenScope Desk Phone CP100



2.2.3 Assembly

Insert the plug on the long end of the handset cable into the jack  on the base of the telephone and press the cable into the groove provided for it. Next, insert the plug on the short end of the handset cable into the jack on the handset.

2.2.4 How to Connect the Phone

- 1) Plug the LAN cable into the connector  at the bottom of the telephone and connect the cable to the LAN resp. switch. If PoE (Power over Ethernet) is to be used, the PSE (Power Sourcing Equipment) must meet the IEEE 802.3af specification.

For details about the required power supply, see the following table:

Model	Power Consumption
OpenScape Desk Phone CP100	PoE (Power Class 1)
OpenScape Desk Phone CP200/CP205	PoE (Power Class 1)
OpenScape Desk Phone CP400	PoE (Power Class 2)
OpenScape Desk Phone CP600 ¹	PoE (Power Class 2)
OpenScape Desk Phone CP600E ¹	PoE (Power Class 2)
OpenScape Desk Phone CP700 ¹	PoE (Power Class 2)
OpenScape Desk Phone CP700X ²	PoE (Power Class 3)

- 2) If Power over Ethernet (PoE) is NOT supported or an OpenScape Desk Phone CP600 phone has more than one Key Module connected:

Plug the power supply unit into the mains. Connect the plug-in power supply unit to the  jack at the bottom of the phone.

Plug-in Power Supply	Order No.
Power Supply, power cable and plug (Type E+F) for EU	L30250-F600-C141
Power Supply, power cable and plug for Great Britain	L30250-F600-C142

¹ If more than one Key Module is connected, a Plug-in Power Supply is required (see below).

² Up to 4 Key Modules can be connected using PoE.

Plug-in Power Supply	Order No.
Power Supply, power cable and plug for USA	L30250-F600-C143
Power Supply, power cable and plug for Switzerland	L30250-F600-C182
Power Supply, power cable and plug for Italy	L30250-F600-C183
Power Supply, power cable and plug for Australia	L30250-F600-C184
Power Supply, power cable and plug for South Africa	L30250-F600-C185
Power Supply without power cable	L30250-F600-C148

3) If applicable, connect the following optional jacks:

-  LAN connection to PC
-  Headset (accessory)

2.2.5 How to Better Use LAN Network Connections

The OpenScape Desk Phone CP100 and OpenScape Desk Phone CP200 provide a 100 Mbps Ethernet-Switch. The OpenScape Desk Phone CP205, OpenScape Desk Phone CP400, OpenScape Desk Phone CP600 and OpenScape Desk Phone CP700/700X phones provide a 1000 Mbps Ethernet-Switch. This allows you to connect one additional network device (e. g. a PC) directly via the telephone to the LAN. The direct connection functionality from phone to PC needs to be activated by administrator first. This type of connection allows you to save one network connection per switch, with the advantage of less network cables and shorter connection distances.



WARNING: Do not use this connection for further OpenScape Desk Phone CP, OpenScape Desk Phone IP or OpenStage phones!

OpenScape Desk Phone CP100/200/205/400/600/600E/700



2.2.6 Key Module

A key module provides additional program keys. The following table shows which key modules can be connected to the particular phone types.

Phone Type	Key Modules	additional keys per module
OpenScape Desk Phone CP100	-	-
OpenScape Desk Phone CP200/CP205	-	-
OpenScape Desk Phone CP400	2	16
OpenScape Desk Phone CP600	4	12
OpenScape Desk Phone CP600E	2	12
OpenScape Desk Phone CP700	2	12
OpenScape Desk Phone CP700X	4	12

The configuration of a key on the key module is just the same as the configuration of a phone key.

2.2.6.1 Key module settings for CP600/600E Broadsoft

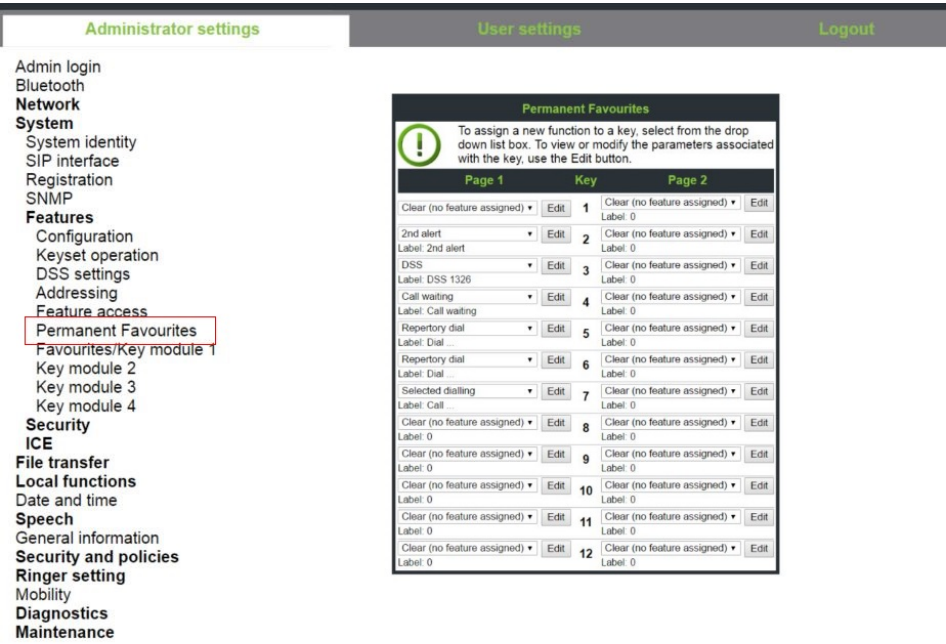
Based on a configuration item, the Favourites screen is able to be presented permanently, even when Key Modules are attached, with an independent set of 12 programmable keys on a Broadsoft phone. These keys are not associated with any of the keys on any Key Modules. When Favourites is configured to function this way, it is referred to as **Permanent Favourites**.

Permanent Favourites is available when the phone is in Broadsoft mode. If **Server Type** is set to **Broadsoft**, then Permanent Favourites is functional on a CP600/600E. Note that this condition will not check if phone is indeed connected to a Broadsoft server.

Program keys via WBM

When server type is set to Broadsoft, WBM will present a "Permanent Favourites" page at below path:

Admin Settings > System > Features > Permanent Favourites



To assign a new function to a key, select from the drop down list box the action. To save the function to the key and view or modify the parameters associated with the key, use the Edit button.

2.3 Quick Start

This section describes a typical case: the setup of an OpenScape Desk Phone CP endpoint in an environment using a DHCP server and the web interface. For different scenarios, cross-references to the corresponding section of the administration chapter are given.

NOTICE: Alternatively, the DLS (Deployment Service) administration tool can be used. Its Plug & Play functionality allows to provide the phone with configuration data by assigning an existing data profile to the phone's MAC address or E.164 number. For further information, see the Deployment Service Administration Manual.

NOTICE: Any settings made by a DHCP server are not configurable by other configuration tools.

2.3.1 How to Access the Web Interface (WBM)

Prerequisites

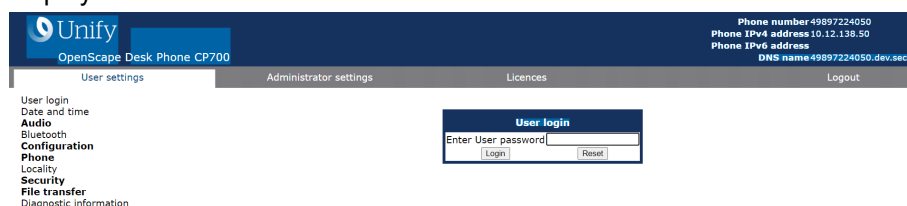
- The phone's IP address or URL is required for accessing the phone's web interface via a web browser. By default, the phone will automatically search for a DHCP server on startup and try to obtain IP data and further configuration parameters from that central server.

- If no DHCP server is available in the IP network or if the DHCP parameter is disabled, the IP address, subnet mask and default gateway/route must be defined manually.
- **To obtain the phone's IP address, proceed as follows:**

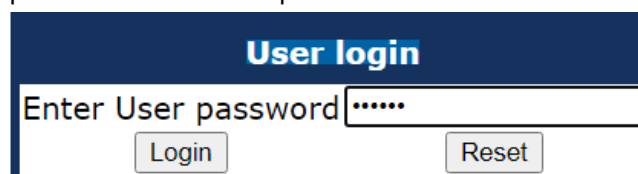
- 1) Access the local phone's Admin menu as described in Access via Local Phone.
 - **If DHCP is enabled (default):** In the Admin menu, navigate to Network > IPv4 configuration > IP address. The IP address is displayed.
 - If DHCP is disabled or if no DHCP server is available in the IP network, the IP address, Subnet Mask and Default Route/Gateway must be defined manually as described in How to Manually Configure the Phone's IP address.
- 2) **Open your web browser (MS Internet Explorer or Mozilla Firefox) and enter the appropriate URL. Example:** https://192.168.1.15 or https://myphone.phones.

For configuring the phone's DNS name, please refer to [Terminal Hostname](#) on page 80.

If the browser displays a certificate notification, accept it. The start page of the web interface appears. In the upper right corner, the phone number, the phone's IP address, as well as the DNS name assigned to the phone are displayed. The left corner contains the user menu tree.



- 3) Click on the tab "Administrator Pages". In the dialog box, enter the admin password. The default password is 123456.



- 4) The administration main page opens. The left column contains the menu tree. If you click on an item which is printed in normal style, the corresponding dialog opens in the center of the page. If you click on an item printed in bold letters, a sub-menu opens to the right of the main menu.

2.3.1.1 Licenses

This area provides the user with the information about EULA (End User License Agreement) and Open Source licenses. This section is on the main area within WBM, which is not password protected to allow access for the user.

UNIFY		Phone number 7107 Phone IPv4 address 10.202.23.47 Phone IPv6 address DNS name 7107.uk.unify.com
Licenses	User Pages	Administrator Pages
EULA User opensource licences Openstage Software Licence	Additional license terms for the use of software by end users (EULA) (c) Copyright Unify Software and Solutions GmbH & Co. KG 2017 All rights reserved. The software is the property of Unify Software and Solutions GmbH & Co. KG and protected by national and international copyrights. For: Name of product: OpenStage 60 / OpenScape Desk Phone IP 55G (HFA) V3R0.39.240 Activation period: 30 days after first installation Test version available: no Important - please read carefully: Please read these license terms and conditions for the use of software by end users (EULA) carefully. You (hereinafter also referred to as "Customer") should review the terms of this EULA and either agree or disagree with these terms. The software will only be installed if you agree with the terms of this EULA. 1. Definitions 1.1 "Affiliate" means companies affiliated with Unify or Customer as per sec. 15 et seq. of the German Stock Corporation Act (Aktien-gesetz, AktG). In the event the AktG does not apply, "Affiliate" shall mean any entity which directly or indirectly controls, is controlled by or is under common control with Unify or Customer, respectively; „control" as used herein shall mean the possession of the power to direct, or cause the direction of, the management and the policies of an entity, whether through ownership of a majority of the voting rights or by contract or otherwise. 1.2 "Agreement" means the separate agreement (e.g. software license agreement), under which the Customer obtained the Software from Unify or a Unify Partner. 1.3 "Base Software" means - as opposed to Single User Software - Software installed on a server computer, the so-called "host", which is accessed by Clients in order to make use of the functionalities of the Base Software. 1.4 "Client" means a clearly identifiable entity which can access a server computer and one or more of the Product Instance(s). Clients can be, for example and depending on the specific product, users, agents, devices, identities or communication channels. The number and type of Clients authorized to use the Product Instance(s) on a particular server computer is defined in the Agreement. 1.5 "Client Access License" or "CAL" means a License that allows a specific number of Client(s) to access and use the Base Software. Depending on the product, a CAL covers at least one (1) Client but may also cover a defined number of Clients (by example and without limitation, 20, 25, 100 Clients) or permit an unlimited number of Clients to access the Base Software. 1.6 "Customer" means the party acquiring a copy of the Software, who is neither an Unify Partner nor an Affiliate of Unify. 1.7 "Documentation" means the technical and/or functional descriptions provided along with the Software. Documentation may be provided in electronic form or online, e.g. via the Internet. Documentation may also include, by example and without limitation, a description of performance characteristics, special features, hardware and software requirements, installation requirements, conditions of use and end user manuals. To the extent required by the respective Freeware vendor or OSS Licensor, the Documentation also comprises of the applicable license terms for Freeware and the relevant OSS Licenses. 1.8 "Firmware" means Single User Software which is embedded into the microcontroller of an electronic device (e.g. a telephone-handset). 1.9 "Freeware" means a computer program which may be used without payment or other compensation (for example, by advertising). Freeware may be subject to proprietary license terms imposed by the Freeware vendor, which, by example and without limitation, may limit the right to distribute or redistribute the Freeware. Freeware may have functional limitations which a commercial version does not have. In general, the Freeware vendor does not deliver source code with the Freeware. 1.10 "License" means the right to use a particular computer program. A license may be perpetual (i.e. it is granted permanently) and is usually granted in exchange for a one-time license fee, or it may be time-limited i.e. it is granted only for the term of a subscription arrangement, and usually in exchange for a recurring license fee. The exact kind and scope of the License acquired by the Customer is further defined in the Agreement. 1.11 "License Terms" or "EULA" means this document. 1.12 "Open Source License" or "OSS License" means license terms for a computer program that, beyond the right to use the computer program without license-fee or royalty, grant the user rights that are usually reserved for the lowner of the copyright.	Logout

2.3.2 How to Set the Terminal Number

Prerequisites

If the user and administrator menus are needed in the course of setup, the terminal number, which by default is identical with the phone number, must be configured first. When the phone is in delivery status, the terminal number input form is presented to the user/administrator right after booting, unless the Plug&Play facility of the DLS is used. For further information about this setting, please refer to Terminal Identity. With the WBM, the terminal number is configured as follows:

- 1) Log on as administrator to the WBM by entering the access data for your phone.
- 2) In the Administrator menu (left column), select System > System Identity to open the "System Identity" dialog. Enter the terminal number, i. e. the SIP name / phone number. For further information, please refer to Terminal Identity.

2.3.3 Basic Network Configuration

For basic functionality, DHCP must provide the following parameters:

- IP Address: IP Address for the phone.
- Subnet Mask (option #1): Subnet mask of the phone.
- **Default Route (option #3 "Router")**: IP Address of the default gateway which is used for connections beyond the subnet.
- **DNS IP Addresses (option #6 "Domain Server")**: IP Addresses of the primary and secondary DNS servers.

If no DHCP server is present, see [IP Address - Manual Configuration](#) on page 71 for IP address and subnet mask, and [Default Route/Gateway](#) on page 73 for the default route.

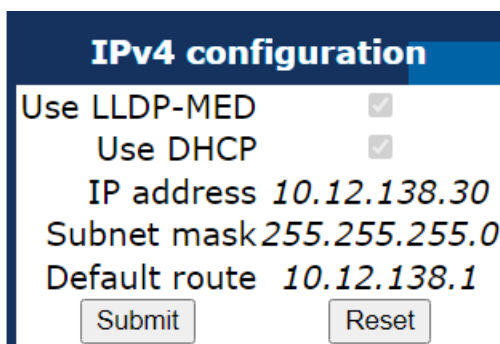
2.3.4 DHCP Resilience

Prerequisites

It is possible to sustain network connectivity in case of DHCP server failure. If DHCP lease reuse is activated, the phone will keep its DHCP-based IP address even if the lease expires. To prevent address conflicts, the phone will send ARP requests in 5 second intervals. Additionally, it will send discovery messages periodically to obtain a new DHCP lease.

Step by Step

In the left column, select **Network > IPv4 configuration**. Select the check box to enable DHCP lease reuse.



The screenshot shows the 'IPv4 configuration' window. It has a title bar 'IPv4 configuration' in a blue header. Below the header, there are two checked checkboxes: 'Use LLDP-MED' and 'Use DHCP'. Below these, the 'IP address' is set to '10.12.138.30', the 'Subnet mask' is '255.255.255.0', and the 'Default route' is '10.12.138.1'. At the bottom, there are two buttons: 'Submit' and 'Reset'.

2.3.5 Date and Time / SNTP

An SNTP (Simple Network Time Protocol) server provides the current date and time for network clients. The IP address of an SNTP server can be given by DHCP.

In order to provide the correct time, it is required to give the time zone offset, i.e. the shift in hours to be added to the UTC time provided by the SNTP server.

The following DHCP options are required:

- **SNTP IP Address (option #42 "NTP Servers")**: IP Address or hostname of the SNTP server to be used by the phone.
- **Time zone offset (option #2 "Time Offset")**: Offset in seconds in relationship to the UTC time provided by the SNTP server. For manual configuration of date and time see [Date and Time](#) on page 117.

2.3.6 SIP Server Address

The IP Address or hostname of the SIP server can be provided by DHCP.

The option's name and code are as follows:

- option #120 "SIP Servers DHCP Option". For manual configuration of the SIP server address see [SIP Addresses](#).

2.3.7 Extended Network Configuration

To have constant access to other subnets, you can enter a total of two more network destinations. For each further domain/subnet you wish to use, first the IP address for the destination, and then that of the router must be given. The option's name and code are as follows:

- **option #33 "Static Routing Table"**

For manual configuration of specific/static routing see [Specific IP Routing](#) on page 74.

Also the DNS domain wherein the phone is located can be specified by DHCP. The option's name and code are as follows:

- **option #15 "Domain Name"**

For manual configuration of the DNS domain name see [DNS Domain Name](#) on page 79.

2.3.8 Vendor Specific: VLAN Discovery and DLS Address

NOTICE: The VLAN ID can also be configured by LLDP-MED (see Automatic VLAN discovery using LLDP-MED).

If the phone is to be located in a VLAN (Virtual LAN), a VLAN ID must be assigned. If the VLAN shall be provided by DHCP, VLAN Discovery must be set to "DHCP" (see [Automatic VLAN discovery using LLDP-MED](#) on page 59). The corresponding DHCP option is vendor-specific, thus a specific procedure is necessary.

If a DLS (Deployment Service) server is in use, its IP address must be provided. It is recommended to configure the DLS server address by DHCP, as this method enables full Plug & Play: having received the DLS address from DHCP, the phone will contact the DLS during start-up. Provided that the DLS is configured appropriately, it will send all necessary configuration data to the phone. Additionally, this method is relevant to security, as it ensures the authenticity of the DLS server.

For manual configuration of the DLS server address see Configuration & Update Service.

For the configuration of vendor-specific settings by DHCP, there are two alternative methods:

- the use of a vendor class - see How to Use a Vendor Class,
- or
- the use of DHCP option 43 - see How to Use Option #43 "Vendor Specific".

For DMS follow the instructions in [Set DMS Address via DHCP](#) on page 47.

2.3.8.1 How to Use a Vendor Class

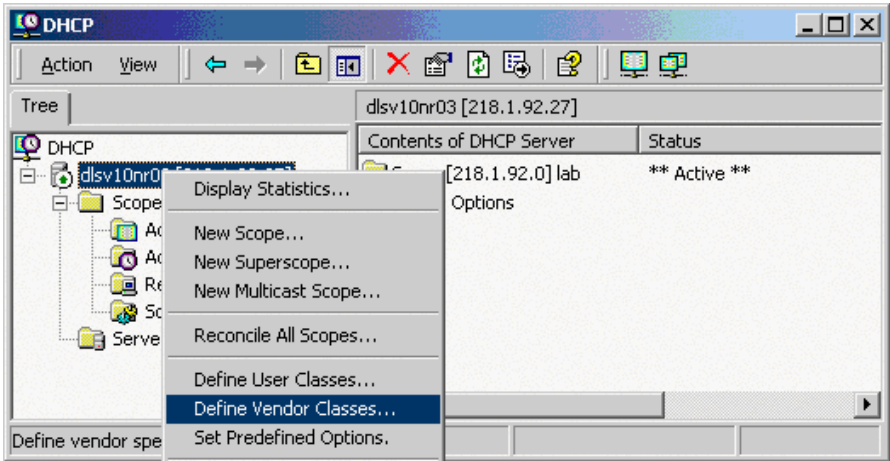
It is recommended to define a vendor class on the DHCP server, thus enabling server and phone to exchange vendor-specific data exclusively. The data

is disclosed from other clients. The following steps are required for the configuration of the Windows DHCP server and for Unix/Linux.

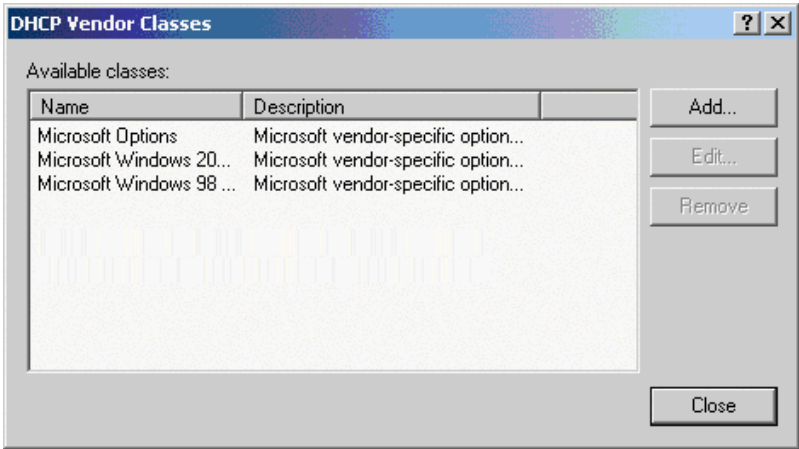
Example: Configuration of the Window DHCP Server

Setting up a new vendor class using the Windows DHCP Server

- 1) In the Windows Start menu, select **Start > Programs > Administrative Tools > DHCP**.
- 2) In the DHCP console menu, right-click the DHCP server in question and select **Define Vendor Classes...** in the context menu.



- 3) A dialog window opens with a list of the classes that are already available.



- 4) Define a new *vendor class* with the name **OptipPhone** and enter a description of this class.

ID:	Binary:	ASCII:
0000	4F 70 74 69 49 70 50 68	OptiIpPh
0008	6F 6E 65	one

Click **OK** to apply the changes. The new vendor class now appears in the list.

- 5) Exit the window with **Close**.

Add Options to the New Vendor Class

Next, two options resp. tags will be added to the vendor class. Two passes are needed for this: in the first pass, tag #1 with the required value "Siemens" is entered, and in the second pass, the VLAN ID is entered as tag #2.

NOTICE: For DHCP servers on a Windows 2003 Server (pre-SP2):

Windows 2003 Server contains a bug that prevents you from using the DHCP console to create an option with the ID 1 for a user-defined vendor class. Instead, this entry must be created with the netsh tool in the command line (DOS shell).

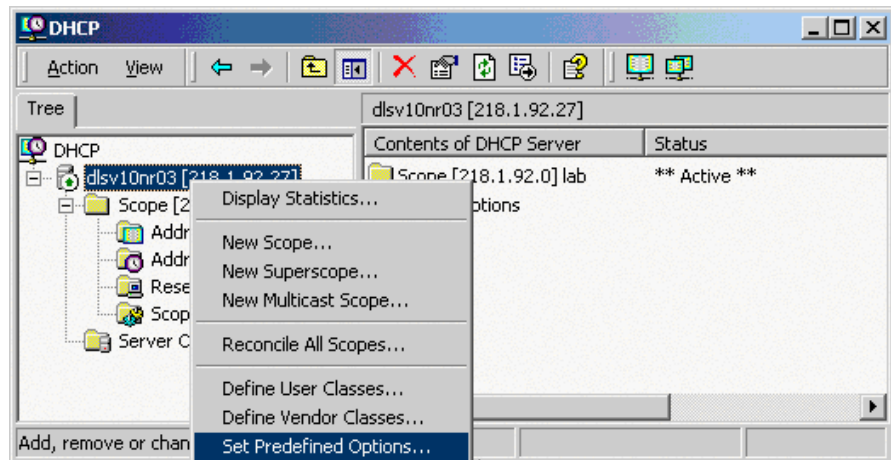
You can use the following command to configure the required option (without error message) so that it is also appears later in the DHCP console:

```
netsh dhcp server add optiondef 1 "Optipoint
element 001" STRING 0 vendor=OptiIpPhone
comment="Tag 001 for Optipoint"
```

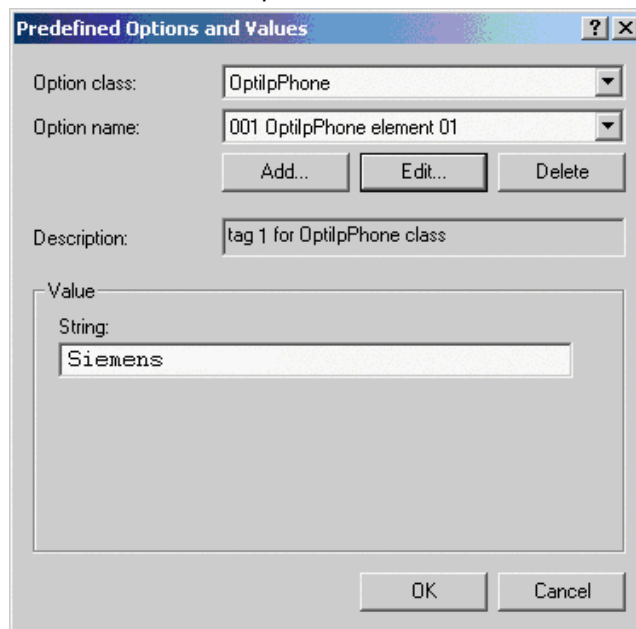
The value **SIEMENS** for optiPoint Element 1 can then be re-assigned over the DHCP console.

This error was corrected in Windows 2003 Server SP2.

- 1) In the DHCP console menu, right-click the DHCP server in question and select Set Predefined Options from the context menu.



- 2) In the dialog, select the previously defined OptilpPhone class and click on Add... to add a new option.



3) Enter the following data for the new option:

a) First Pass: Option 1

- **Name:** Free text, e. g. "OptilpPhone element 01"
- **Data type:** "String"
- **Code:** "1"
- **Description:** Free text.

b) Second Pass: Option 2

- **Name:** Free text, e. g. "OptilpPhone element 02"
- **Data type:** "Long"
- **Code:** "2"
- **Description:** Free text.

4) Enter the value for this option.

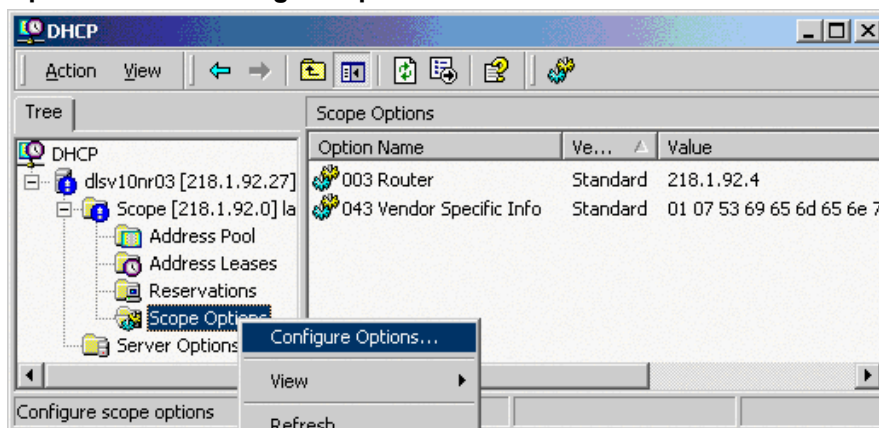
a) First Pass: "Siemens"

b) Second Pass: VLAN ID

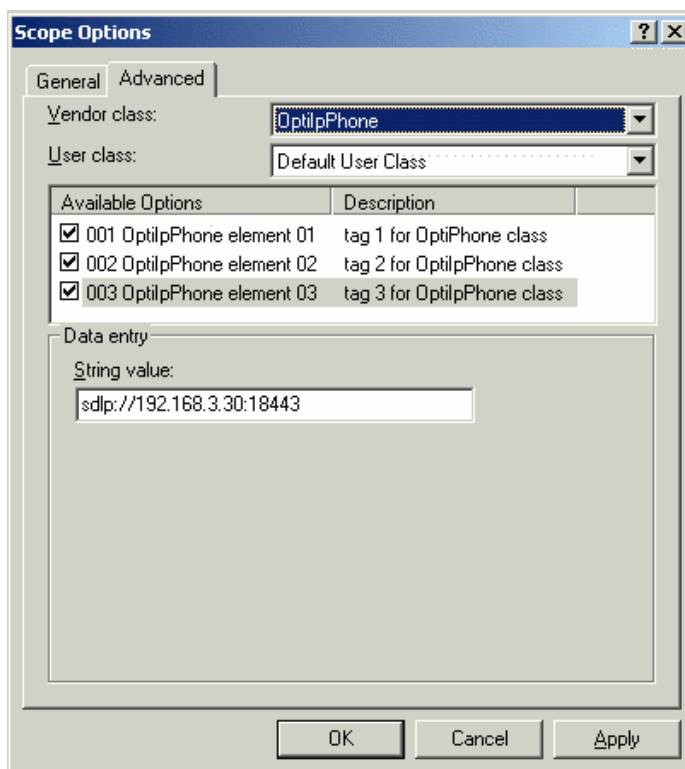
5) Press OK, repeat steps 2 to 4 for the second pass, and press OK again.

Defining the scope for the new vendor class

- 1) Select the DHCP server in question and the **Scope** and right-click **Scope Options**. Select **Configure Options...** in the context menu.



- 2) Select the **Advanced** tab. Under **Vendor class**, select the class that you previously defined (**OptilpPhone**) and, under **User class**, select **Default User Class**.



Activate the check boxes for the options that you want to assign to the scope (in the example, **001**, **002**, and **003**). Click **OK**.

- 3) The DHCP console now shows the information that will be transmitted for the corresponding workpoints. Information from the **Standard** vendor is transmitted to all clients, whereas information from the **OptilpPhone** vendor is transmitted only to the clients (workpoints) in this vendor class.

Setup using a DHCP server on Unix/Linux

The following snippet from a DHCP configuration file (usually `dhcpd.conf`) shows how to set up a configuration using a vendor class and the "vendor-encapsulated-options" option.

```
class "OptiIpPhone" {
    option vendor-encapsulated-options
    # The vendor encapsulated options consist of hexadecimal values for
    the option number (for instance, 01), the length of the value (for in
    stance, 07), and the value (for instance, 53:69:65:6D:65:6E:73). The
    options can be written in separate lines; the last option must be fol
    lowed by a ';' instead of a ':'.
    # Tag/Option #1: Vendor "Siemens"
    #1 7 S i e m e n s
    01:07:53:69:65:6D:65:6E:73:
    # Tag/Option #2: VLAN ID
    #2 4 0 0 1 0
    02:04:00:00:00:0A;
    match if substring (option vendor-class-identifier, 0, 11) =
    "OptiIpPhone";
}
```

2.3.8.2 How to Use Option #43 "Vendor Specific"

Alternatively, option #43 can be used for setting up the VLAN ID. Two tags are required:

- **Tag 001:** Vendor name
- **Tag 002:** VLAN ID
- **Tag 003:** DLS address

Optionally, the DLS address can be given in an alternative way:

- **Tag 4:** DLS hostname

The Vendor name tag is coded as follows (the first line indicates the ASCII values, the second line contains the hexadecimal values):

Code	Length	Vendor name						
1	7	S	i	e	m	e	n	s
01	07	53	69	65	6D	65	6E	73

The following example shows a VLAN ID with the decimal value "10":

Code	Length	VLAN ID			
2	4	0	0	1	0
02	04	00	00	00	0A

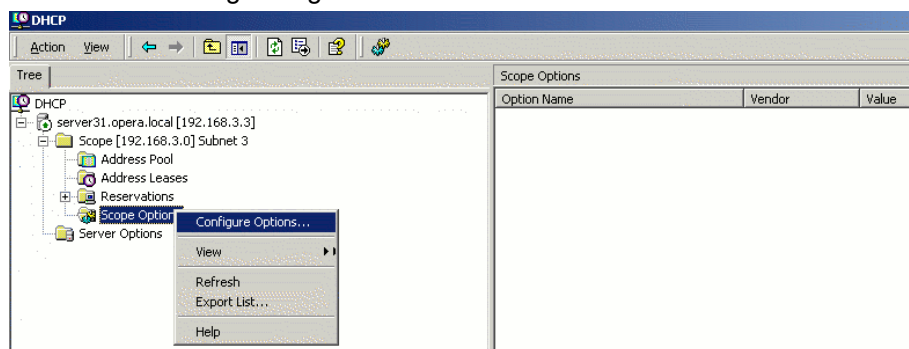
For manual configuration of the VLAN ID see [Manual configuration of a VLAN ID](#) on page 61.

The DLS IP address tag consists of the protocol prefix "sdlp://", the IP address of the DLS server, and the DLS port number, which is "18443" by default. The following example illustrates the syntax:

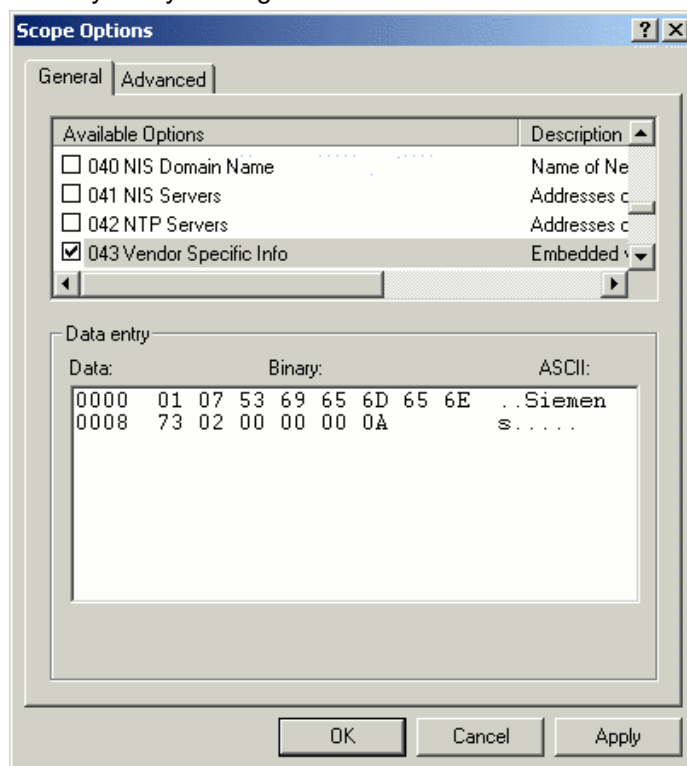
[illegible]

Setup Using the Windows DHCP Server

- 1) In the Windows Start menu, select **Start > Programs > Administrative Tools > DHCP**.
- 2) Select the DHCP server and the scope. Choose "Configure Options" in the context menu using the right mouse button.



- 3) Enter the VLAN ID. Providing the length is not required here, as the VLAN ID is always 4 Bytes long.



2.3.9 DLS Server Address

This setting only applies if a DLS (Deployment Service)/DMS server is in use.

It is recommended to configure the DLS/DMS server address by DHCP, as this method enables full Plug & Play and ensures the authenticity of the DLS server.

For manual configuration of the DLS server address see [Configuration & Update Service](#) on page 82.

For configuration of the DMS see [Set DMS Address via DHCP](#) on page 47.

For the configuration of vendor-specific settings by DHCP, there are two alternative methods: 1) the use of a vendor class, or 2) the use of DHCP option 43.

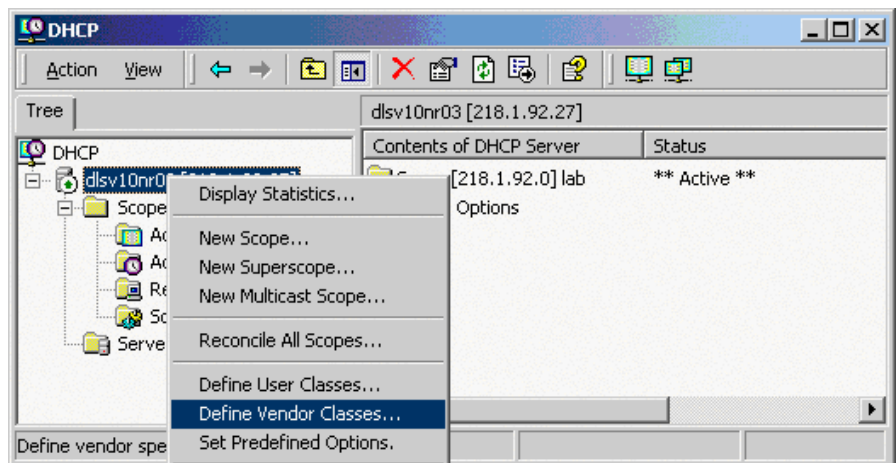
2.3.9.1 Using Vendor Class

It is recommended to define a vendor class on the DHCP server, thus enabling server and phone to exchange vendor-specific data exclusively. The data is disclosed from other clients. If not done already, create a vendor class by the name of "OptilpPhone".

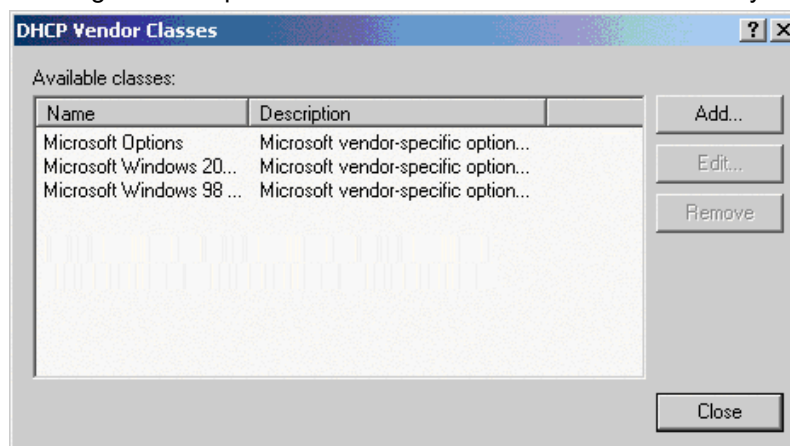
The following steps are required for the configuration of the Windows DHCP server.

Setting up a new vendor class using the Windows DHCP Server

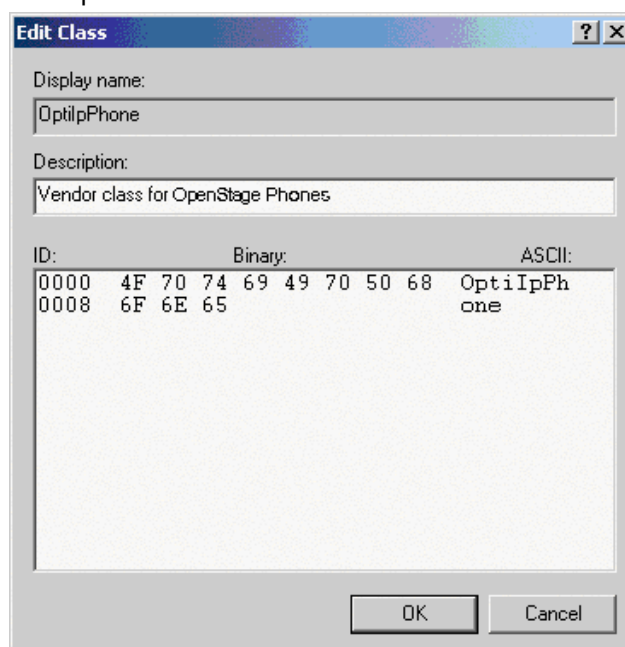
- 1) In the Windows Start menu, select **Start > Programs > Administrative Tools > DHCP**.
- 2) In the DHCP console menu, right-click the DHCP server in question and select **Define Vendor Classes...** in the context menu.



- 3) A dialog window opens with a list of the classes that are already available.



- 4) Define a new *vendor class* with the name **OptilpPhone** and enter a description of this class.



Click **OK** to apply the changes. The new vendor class now appears in the list.

- 5) Exit the window with **Close**.

Add Options to the New Vendor Class

Next, two options resp. tags will be added to the vendor class. Two passes are needed for this: in the first pass, tag #1 with the required value "Siemens" is entered, and in the second pass, the DLS address is entered as tag #3.

NOTICE: For DHCP servers on a Windows 2003 Server (pre-SP2):

Windows 2003 Server contains a bug that prevents you from using the DHCP console to create an option with the ID 1 for a user-defined vendor class. Instead, this entry must be created with the net sh tool in the command line (DOS shell).

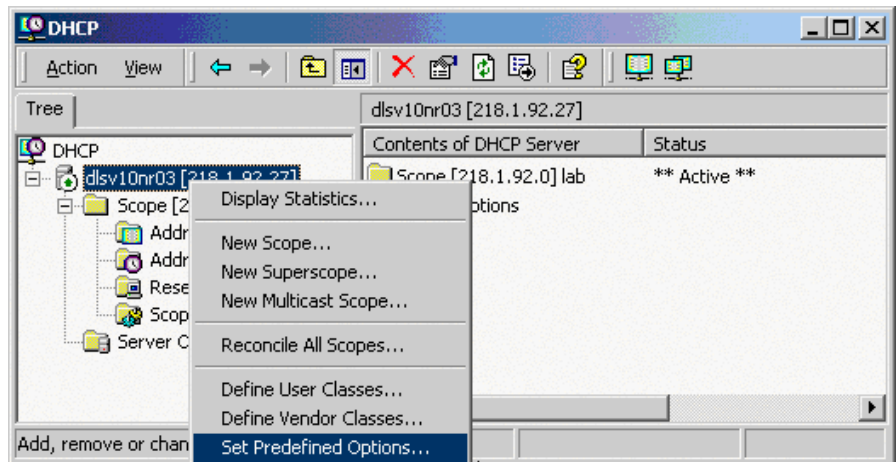
You can use the following command to configure the required option (without error message) so that it is also appears later in the DHCP console:

```
netsh dhcp server add optiondef 1 "Optipoint
element 001" STRING 0 vendor=OptiIpPhone
comment="Tag 001 for Optipoint"
```

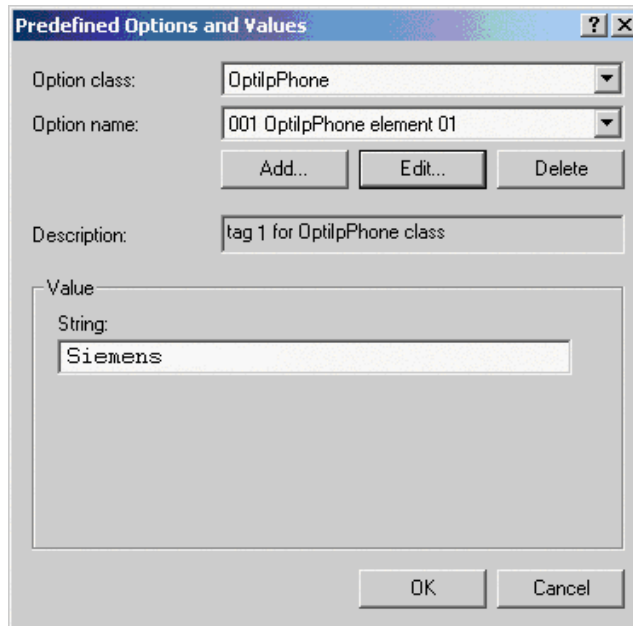
The value **SIEMENS** for optiPoint Element 1 can then be re-assigned over the DHCP console.

This error was corrected in Windows 2003 Server SP2.

- 1) In the DHCP console menu, right-click the DHCP server in question and select Set Predefined Options from the context menu.



- 2) In the dialog, select the previously defined OptilpPhone class and click on Add... to add a new option.



3) Enter the following data for the new option:

a) **First Pass:** Option 1

- **Name:** Free text, e. g. "OptilpPhone element 01"
- **Data type:** "String"
- **Code:** "1"
- **Description:** Free text.

b) **Second Pass:** Option 3

- **Name:** Free text, e. g. "OptilpPhone element 03"
- **Data type:** "String"
- **Code:** "3"
- **Description:** Free text.

4) Enter the value for this option.

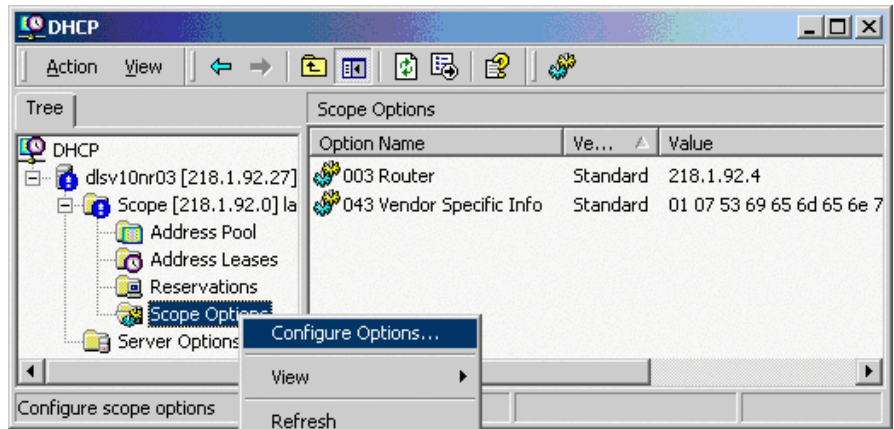
a) **First Pass:** "Siemens"

- b) **Second Pass:** DLS address The DLS address has the following format:
 <PROTOCOL>:://<IP ADDRESS OF DLS SERVER>:<PORT NUMBER>
 Example: sdip://192.168.3.30:18443

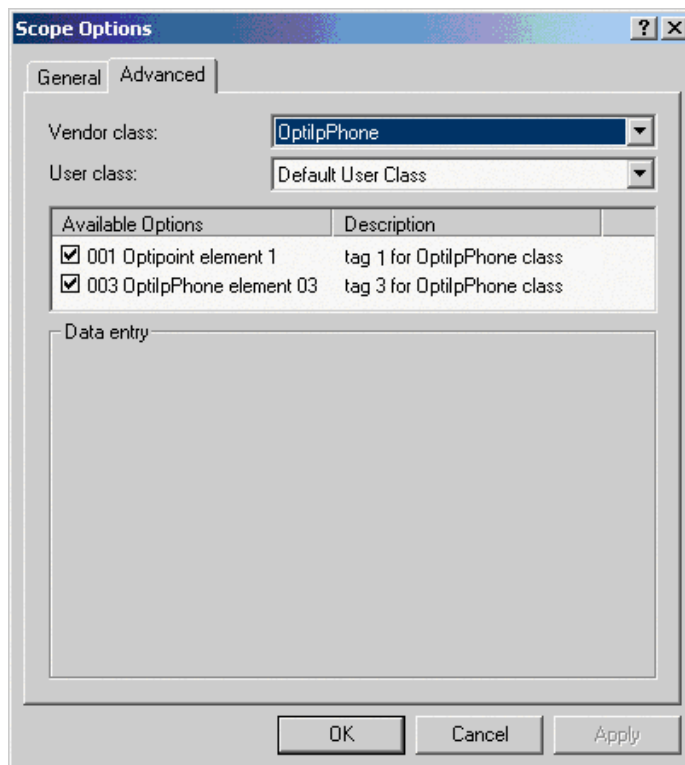
5) Press OK, repeat steps 2 to 4 for the second pass, and press OK again.

Defining the scope for the new vendor class

- 1) Select the DHCP server in question and the Scope and right-click Scope Options. Select Configure Options... in the context menu.



- 2) Select the Advanced tab. Under Vendor class, select the class that you previously defined (OptilpPhone) and, under User class, select Default User Class.



Activate the check boxes for the options that you want to assign to the scope (in the example, 001 and 003)

- 3) The DHCP console now shows the information that will be transmitted for the corresponding workpoints. Information from the Standard vendor is transmitted to all clients, whereas information from the OptilpPhone vendor is transmitted only to the clients (workpoints) in this vendor class.

Setup using a DHCP server on Unix/Linux

The following snippet from a DHCP configuration file (usually dhcpd.conf) shows how to set up a configuration using a vendor class and the "vendor-encapsulated-options" option.

```
class "OptiIpPhone" {
    option vendor-encapsulated-options
    # The vendor encapsulated options consist of hexadecimal values for
    the option number (for instance, 01), the length of the value (for in
    stance, 07), and the value (for instance, 53:69:65:6D:65:6E:73). The
    options can be written in separate lines; the last option must be fol
    lowed by a ';' instead of a ':'.
    # Tag/Option #1: Vendor "Siemens"
    #1 7 S i e m e n s
    01:07:53:69:65:6D:65:6E:73:
    # Tag/Option #3: DLS IP Address (here: sdip://192.168.3.30:18443)
    #3 25 s d l p : / / 1 9 2 . 1 6 8 . 3 . ...etc.
    03:19:73:64:6C:70:3A:2F:2F:31:39:32:2E:31:36:38:2E:33:2E:33:30:
3A:31:38:34:34:33;
    match if substring (option vendor-class-identifier, 0, 11) =
    "OptiIpPhone";
}
```

2.3.9.2 Using Option #43 "Vendor Specific"

Alternatively, option #43 can be used for setting up the DLS address. Two tags are required:

- **Tag 001:** Vendor name
- **Tag 003:** DLS IP address

Additionally, you can enter a host name for the DLS server:

- **Tag 004:** DLS hostname

The data is entered in hexadecimal values. Note that the length of the information contained in a tag must be given.

The Vendor name tag is coded as follows (the first line indicates the ASCII values, the second line contains the hexadecimal values):

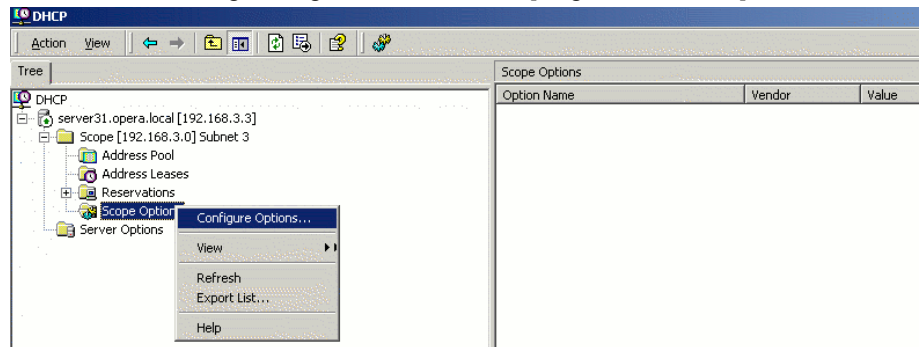
Code	Length	Vendor name						
1	7	S	i	e	m	e	n	s
01	07	53	69	65	6D	65	6E	73

The DLS IP address tag consists of the protocol prefix "sdip://", the IP address of the DLS server, and the DLS port number, which is "18443" by default. The following example illustrates the syntax:

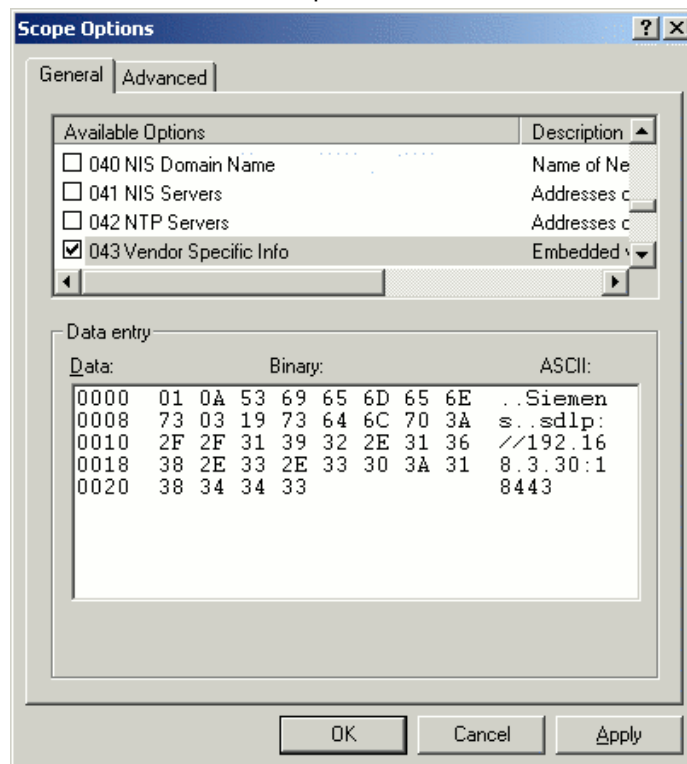
Code	Length	DLS IP address																								
3	25	s	d	i	p	:	/	/	1	9	2	.	1	6	8	.	2	.	1	9	:	1	8	4	4	3
03	19	73	64	6C	70	3A	2F	2F	31	39	32	2E	31	36	38	2E	32	2E	31	39	3A	31	38	34	34	33

Setup using the Windows DHCP Server

- 1) In the Windows Start menu, select **Start > Programs > Administrative Tools > DHCP**.
- 2) Select the DHCP server and the scope. Choose "Configure Options" in the context menu using the right mouse button. [Engl. Screenshot]



- 3) Enter the IP address and port number of the DLS server.



2.3.10 Using the Web Interface (WBM)

- 1) Log in to the Administrator Pages of the WBM. For details about accessing the WBM, see [How to Access the Web Interface \(WBM\)](#) on page 27.
- 2) In the menu at the lefthand side, go to System > Registration.

- 3) Enter the IP addresses of the OpenScape Voice Communication System in the SIP address fields. There are three address fields that need to be completed:

- SIP server
- SIP registration
- SIP gateway

Registration	
SIP addresses	
SIP server address	10.12.70.16
SIP registrar address	10.12.70.16
SIP gateway address	0.0.0.0

- 4) In the **User ID** number field, enter the internal extension number of the phone. It can be 1 to 24 characters

Registration	
SIP addresses	
SIP server address	10.12.70.16
SIP registrar address	10.12.70.16
SIP gateway address	0.0.0.0
SIP session	
Session timer enabled	☒
Session duration (seconds)	3600
Registration timer (seconds)	3600
Subscription timer (seconds)	3600
Refresh minimum (seconds)	0
Server type	OS Voice
Realm	realm3
User ID	49897224030
Password	
MLPP base	Local
MLPP domain	dsn+uc
Other domain	

long.

- 5) Enter the subscriber password in the Password field.

2.3.11 Using the Local Menu

Take the following steps to configure Bluetooth (for further information see [Access via Local Phone](#) on page 53):

- 1) Join the Main menu screen **@** to activate the Settings menu and then select the Administration menu with help of the Up Arrow, Down Arrow and OK keys.
- 2) When the Admin menu is active, you will be prompted to enter the administrator password. The default admin password is "123456". It is recommended to change the password (see [Password](#) on page 287) after your first login.
- 3) In the administration menu, go to **Bluetooth > Feature access**. For further instructions on entering data using the Local menu see [OpenScape Desk Phone CP400/600/600E/700/700X](#) on page 54. The path is as follows:


```

|--- Administration
    |--- Bluetooth
        |--- Feature access
            |--- Enable
      
```
- 4) To enable the Bluetooth access press the Soft key "Enable" and confirm.
- 5) The changes have been saved.

2.3.12 Set DMS Address via DHCP

When an IP phone is booting, it first obtains an IP address via DHCP. The DHCP server can provide the DMS address to the phone via Option 43 or Option 66. The DMS address is mutually exclusive with a possibly provided DLS address. A phone can either connect to a DLS or DMS server.

2.3.12.1 Using Option 43

DHCP vendor specific option 43 can specify a voice VLAN ID and URL of a BroadSoft DMS server. IP phones will recognize vendor specific options only, if vendor string (here: "Siemens") matches correctly. All values are given in hexadecimal numbering format. Here is a detailed description of all DHCP option 43 bytes:

Tag	Length	Content (Example)
01	07	5369656d656e73
02	04	00000065
03	1d	68747470733a2f2f393332E3132322E3131342E39363a3434332f646d73
ff		

There are three Tags, each with an explicit length value. List if tags is delimited by a ending ff.

- **Tag 01 specifies the vendor (here: Siemens)**
 - Tag: 01; Length: 07; Value: Siemens
- **Tag 02 specifies VLAN ID of Voice VLAN (here: 101)**
 - Tag: 02; Length: 04; Value: 65 (Hex)
- **Tag 03 specifies IP address of Broadsoft DMS (here: 93.122.114.96:443/dms)**
 - Tag: 03; Length: 1d; Value: https://93.122.114.96:443/dms (Hex)

- End of record
 - **End:** ff (Hex)

Providing a VLAN ID is optional and only mentioned for completeness. You can find details for configuration of a VLAN ID here: http://wiki.unify.com/wiki/VLAN_ID_Discovery_over_DHCP.

2.3.12.2 Using Option 66

The DHCP server needs to be configured to provide the DMS server URL via Option 66. Here is a detailed description of the Option 66 bytes

Option	Length	Content (Example)
42	1d	68747470733a2f2f393332e3132322e3131342e39363a3434332f646d73

Compared to Option 43, Option 66 does not have specific tags. It only has a length and content field. The above example provides the following URL in the content field:

- **DHCP option field:** 42(Hex); Length: 1d; Content: <https://93.122.114.96:443/dms> (Hex)

2.4 Cloud Deployment

This chapter describes how a phone progresses through the cloud deployment process from factory start-up until the cloud service provider considers it to be ready for use by its User.

The phone determines that a cloud deployment process is to be used based on the IP settings it receives from the DHCP at the customer site. The Unify Redirect server redirects the phone to a DLS-WPI based management system operated by the cloud service provider. This management system completes the configuration of the phone with all the information required for it to be usable and may also customize the phone for the cloud service provider's 'house' style. If zero touch deployment is available then the phone will be automatically connected to the management system. However, if zero touch deployment is not possible, then a cloud deployment pin must be entered at the phone. This PIN is a code that determines which cloud service provider is responsible for the phone. The code is provided as part of a pin supplied from the cloud organization to the user.

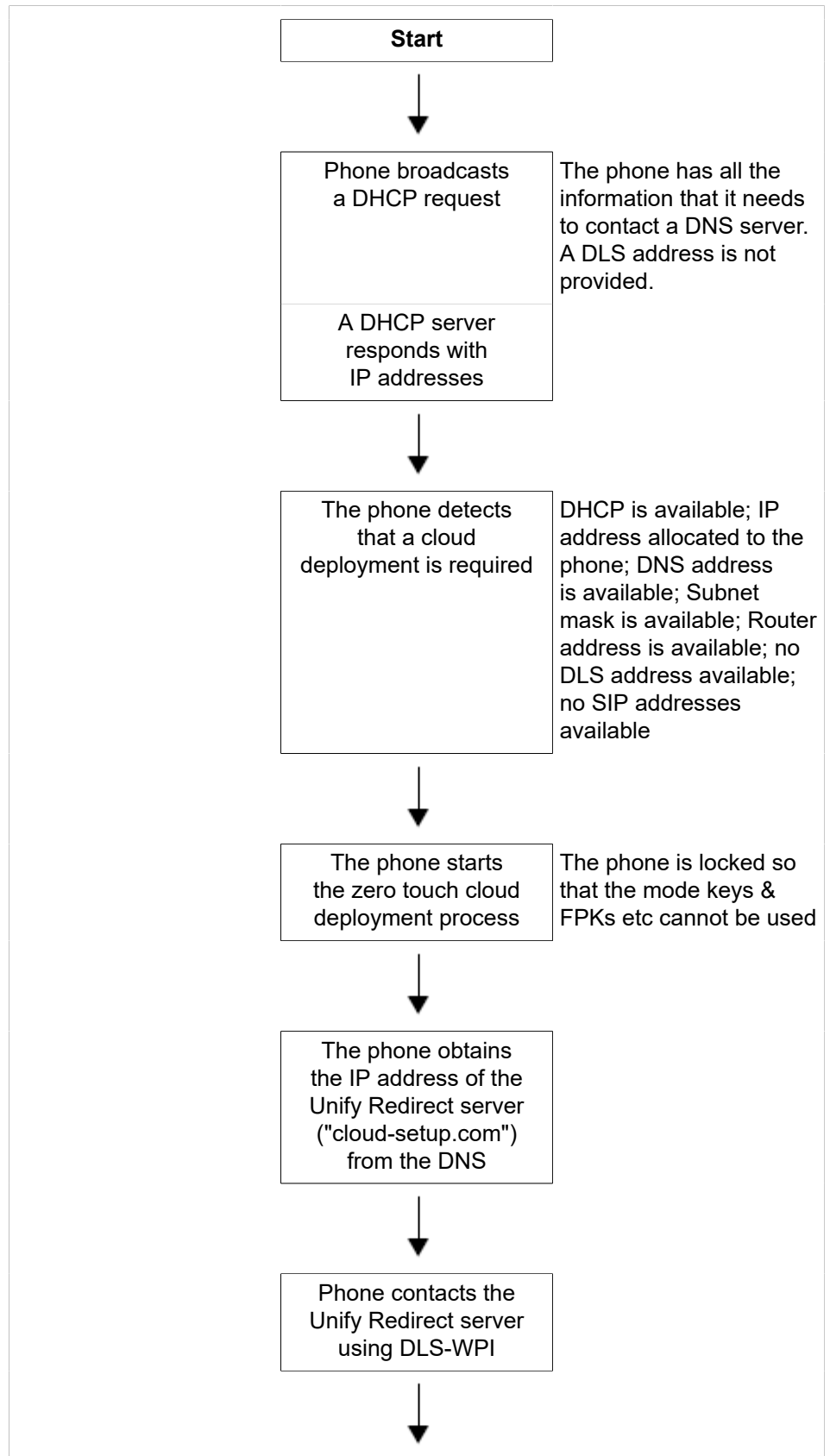
2.4.1 Process of cloud deployment

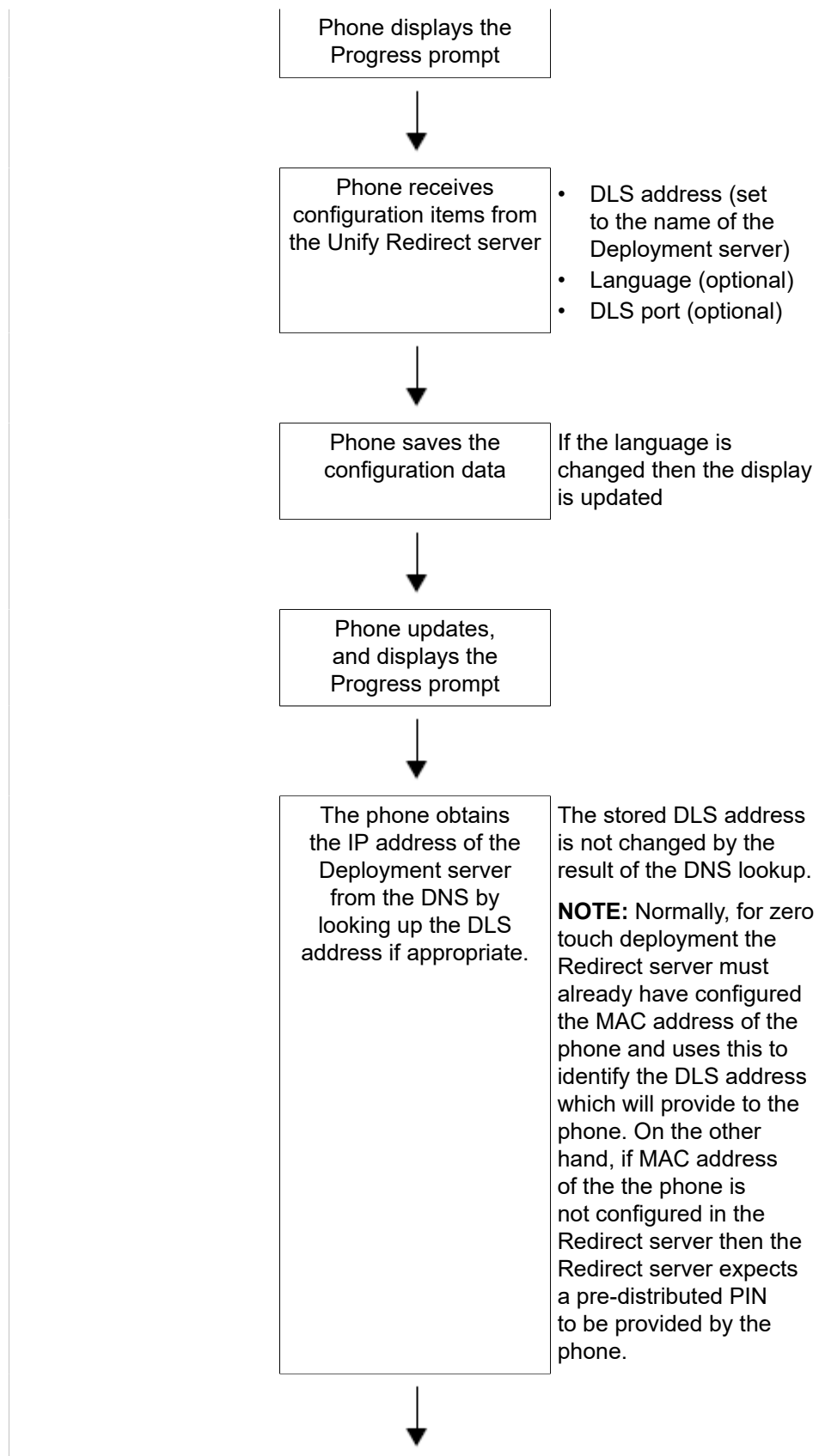
The following flow chart shows the way from a factory start-up until a user prepared OpenStage phone, deployed by a relevant DLS-WPI based management system.

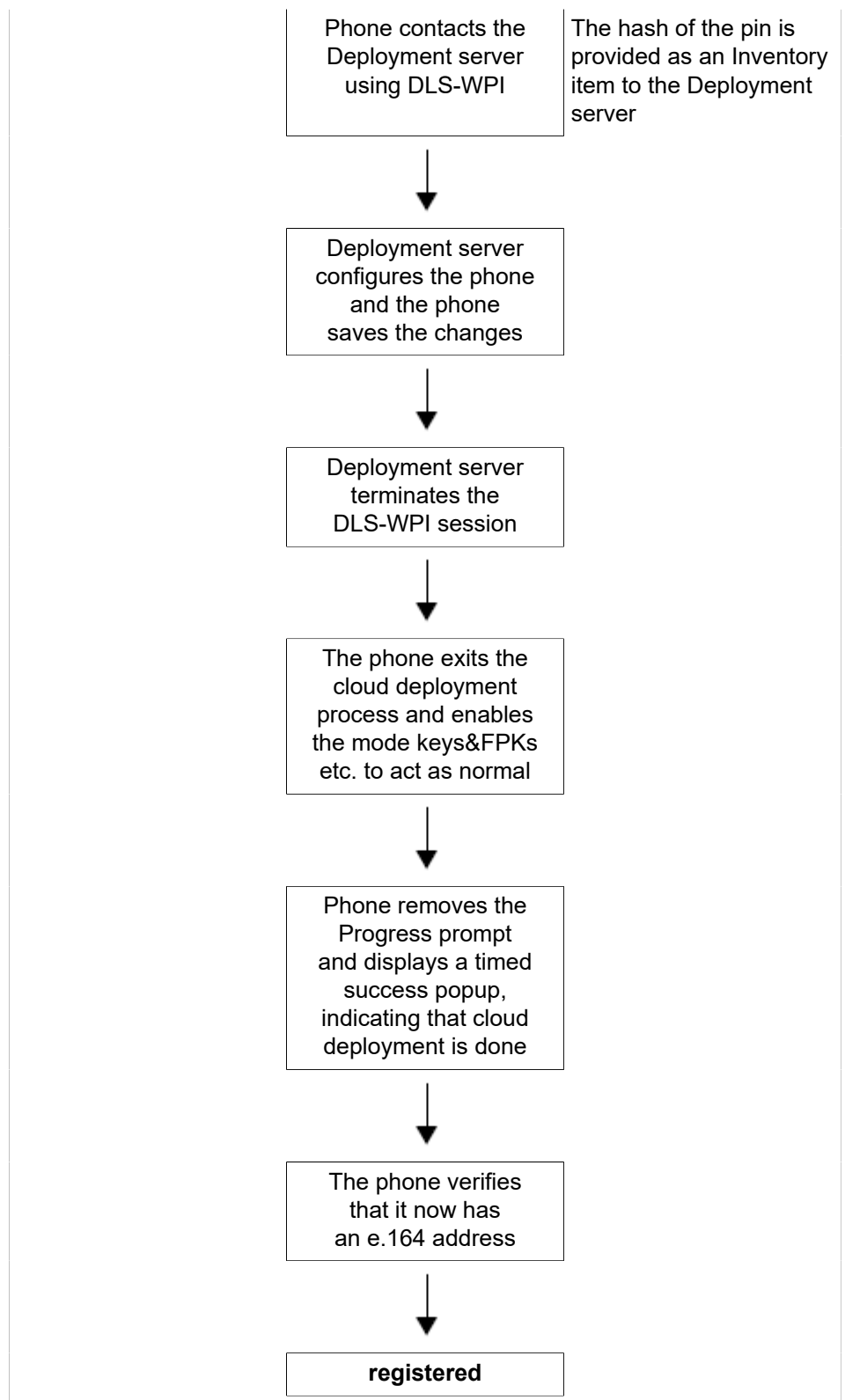
Preconditions:

- Phone is not running
- Phone is set to factory default values
- The phone has a LAN connection

- The LAN connection provides access to the public internet







2.4.2 Aborting cloud deployment process by User

The phone detects that a cloud deployment is required and starts the cloud deployment process. The Phone expects the input of the PIN by the User. At

this point the User has the option to cancel the process with **Cancel**. If the User confirms his decision, the deployment process is aborted.

2.4.3 Re-trigger cloud deployment

Cloud deployment may be restarted by triggering a Factory reset:

The DLS-WPI requests a restart to factory defaults of the phone. The phone restart should then trigger the cloud deployment process.

2.4.4 Deployment errors

During deployment the display will always show deployment specific information. A persistent warning popup displays the information that will be shown in an idle screen error after deployment failed.

- It is shown to notify the phone User that deployment failed to complete as expected.
- It is a non-timed warning popup
- It is non-dismissible by user action
- It is shown over the idle screen only
- It is shown/re-shown whenever the idle screen is displayed or redisplayed to the user
- It is formatted as the warning icon followed by a warning text which ends in a code displayed in round brackets.
- The warning text is = "Deployment incomplete"
- It displays only the highest priority error condition should more than one error condition apply (note that priority 1 is the highest)

Code	Priority	Cause
AU	1	Abandoned by user Occurs when the pin prompt is dismissed
RS	1	Unable to get the address for the Unify Redirect server DNS lookup failed
RN	3	Unable to establish contact with Unify Redirect server — no reply
RR	2	Unable to establish contact with Unify Redirect server — refused
DS	1	Unable to get the address for the Deployment server DNS lookup failed
DN	3	Unable to establish contact with Deployment server — no reply
DR	2	Unable to establish contact with Deployment server — refused

3 Administration

This chapter describes the configuration of every parameter available on the OpenScape Desk Phone CP phones. For access via the local phone menu, see the following; for access using the web interface (WBM), please refer to [How to Access the Web Interface \(WBM\)](#) on page 27.

3.1 Access via Local Phone

NOTICE: The data entered in input fields is parsed and controlled by the phone. Thus, data is accepted only if it complies to the value range.

For entering passwords with non-numeric characters, please consider the following:

By default, password entry is in numeric mode and a minimum length of 6 characters. For changing the mode, press the # key once or repeatedly, depending on the desired character. The # key cycles around the input modes as follows:

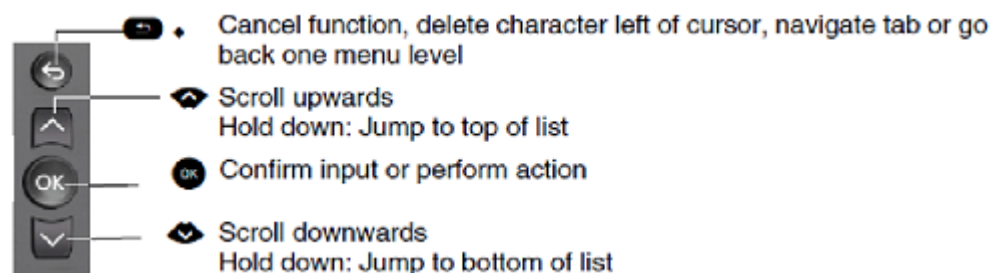
(Abc) -> (abc) -> (123) -> (ABC) -> back to start.

Usable characters are 0-9 A-Z a-z . * # , ? ! " ' + - () @ / : _

3.1.1 OpenScape Desk Phone CP100

1) Access the Administration Menu

- Press the Settings key @ and select **Administration settings**. You will be prompted to enter the administrator password.
- Or press the **otherprops="frog">@** key and use the Up Arrow, Down Arrow and OK keys consecutively to select the Admin menu.

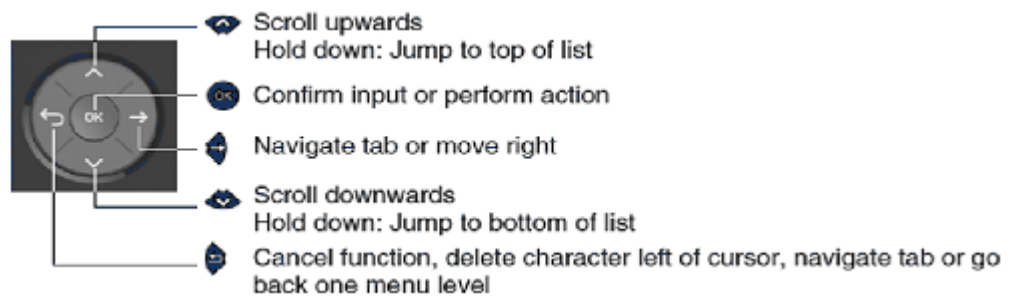


- 2) Enter the administrator password (default password is 123456). It is highly recommended to change the password (see [Password](#) on page 287) after your first login.
- 3) Confirm with OK key.

3.1.2 OpenScape Desk Phone CP20X

1) Access the Administration Menu

- Press the Settings key @ and select Administration settings. You will be prompted to enter the administrator password.
- Or press the @ or ^ key and use the Up Arrow, Down Arrow and OK keys consecutively to select the Admin menu.

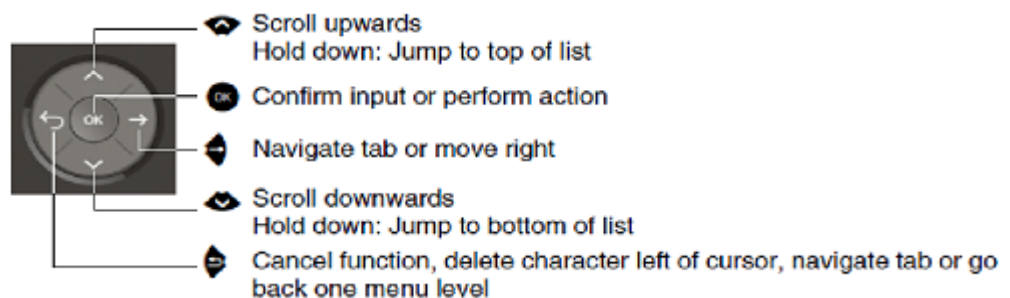


- 2) Enter the administrator password (default password is 123456). It is highly recommended to change the password (see [Password](#) on page 287) after your first login.
- 3) Confirm with OK key.

3.1.3 OpenScape Desk Phone CP400/600/600E/700/700X

1) Access the Administration Menu

- Press the Settings key @ and select Administration settings. You will be prompted to enter the administrator password.
- Or join the Main menu screen @ to activate the Settings menu and then select the Administration menu with the Up Arrow, Down Arrow and OK keys.



- 2) When the Admin menu is active, you will be prompted to enter the administrator password. The default admin password is "123456". It is highly recommended to change the password (see [Password](#) on page 287) after your first login.
- 3) Navigate within the Administration Menu.
- 4) Select a parameter

If a parameter is set by choosing a value from a selective list, an arrow symbol appears in the parameter field that has the focus. Press the OK key to enter the selective list. Use the Up Arrow and Down Arrow keys to scroll up and down in the selection list. To select a list entry, press the OK key.

5) Enter the parameter value

For selecting numbers and characters, you can use special keys. See the following table:

Key	Key Function during text input	Key function when held down
*	Enter special characters.	Ringer on/off when pressed short, ringer set to alerting with longpress.
#	Toggle between lowercase characters, uppercase characters, and digits in the following order: (Abc) -> (abc) -> (123) -> (ABC) -> back to start.	Phonelock on/off.

With the OpenScape Desk Phone CP100/200/205/400/600/600E use the keypad for entering parameter values. Use the Navigation Keys or Navigation Block to navigate and execute administrative actions in the Administration Menu.

6) Save and exit

When you are done, select Save & exit and press OK key.

3.2 Bluetooth Interface

You can activate and deactivate the Bluetooth interface. If the Bluetooth interface is deactivated no Bluetooth services are available.

Administration via WBM

Bluetooth

Bluetooth

Enable Bluetooth interface
☒

Administration via Local Phone

|--- Bluetooth

NOTICE: This feature is for OpenScape Desk Phones CP600, CP700 and CP700X only.

3.3 LAN Settings

3.3.1 LAN Port Settings

The OpenScape Desk Phone CP100/200/205/400/600/600E phone provides an integrated switch which connects the LAN, the phone itself and a PC port. By default, the switch will auto negotiate transfer rate

(10/100/1000 Mb/s autosensing, configurable, Gigabit not available on OpenScape Desk Phone CP200 or CP100) and duplex method (full or half duplex) with whatever equipment is connected. Optionally, the required transfer rate and duplex mode can be specified manually using the LAN Port Speed parameter.

NOTICE: In the default configuration, the LAN port supports automatic detection of cable configuration (pass through or crossover cable) and will reconfigure itself as needed to connect to the network. If the phone is set up to manually configure the switch port settings, the cable detection mechanism is disabled. In this case care must be taken to use the correct cable type.

The PC Ethernet port (default setting: Disabled) is controlled by the PC port mode parameter. If set to "Disabled", the PC port is inactive; if set to "Enabled", it is active. If set to "Mirror", the data traffic at the LAN port is mirrored at the PC port. This setting is for diagnostic purposes. If, for instance, a PC running Ethereal/Wireshark is connected to the PC port, all network activities at the phone's LAN port can be captured.

NOTICE: Do not use this connection for further phones!

NOTICE: Removing the power from the phone or a phone reset/reboot will result in the temporary loss of the network connection to the PC port.

When PC port autoMDIX is enabled, the switch determines automatically whether a regular MDI connector or a MDI-X (crossover) connector is needed, and configures the connector accordingly.

Data required

- **LAN port status:** Represents the connected (i.e. negotiated) speed (or "Link down" if not connected). This is read-only item.
- **LAN port speed:** Settings for the ethernet port connected to a LAN switch. Value range: "Any," "10 Mbps half duplex", "10 Mbps full duplex", "100 Mbps half duplex", "100 Mbps full duplex", "Gigabit/s full duplex" (OpenScape Desk Phone CP205/400/600 only) . Default: "Any"
- **PC port status:** Represents the connected (i.e. negotiated) speed (or "Link down" if not connected). This is read-only item.
- **PC port speed:** Settings for the ethernet port connected to a PC. Value range: "Any," "10 Mbps half duplex", "10 Mbps full duplex", "100 Mbps half duplex", "100 Mbps full duplex", "Gigabit/s full duplex" (OpenScape Desk Phone CP205/400/600/700/700X only). Default: "Any"
- **PC port mode:** Controls the PC port. Value range: "disabled", "enabled", "mirror". Default: "disabled"
- **PC port autoMDIX:** Switches between MDI and MDI-X automatically. Value range: "On", "Off" Default: "Off"

Administration via WBM

Network > Wired settings

Wired settings

LAN connection

Use LLDP-MED ☐

Use DHCP ☒

DHCPv6 enabled ☐

Use DHCP reuse ☐

VLAN discovery

VLAN ID

LLDP-MED operation

Time to live (seconds)

LAN port

LAN port status

LAN port speed

IPv4 routing

Route 1 IP address

Route 1 gateway

Route 1 mask

Route 2 IP address

Route 2 gateway

Route 2 mask

IPv6 routing

Route 1 dest.

Route 1 prefix len

Route 1 gateway

Route 2 dest.

Route 2 prefix len

Route 2 gateway

Administration via Local Phone

```
|--- Admin
    |--- Network
        |--- Wired settings
            |--- LAN port status
            |--- LAN port speed
```

Administration via WBM

Network > PC port configuration

PC port configuration

PC port status

PC port speed

PC port mode

PC port autoMDIX ☐

Administration via Local Phone

```
|--- Admin
    |--- Network
        |--- PC port Configuration
            |--- PC port status
            |--- PC port speed
            |--- PC port mode
            |--- PC port autoMDIX
```

3.3.2 VLAN

VLAN (Virtual Local Area Network) is a technology that allows network administrators to partition one physical network into a set of virtual networks (or broadcast domains).

Partitioning a physical network into separate VLANs allows a network administrator to build a more robust network infrastructure. A good example is a separation of the data and voice networks into data and voice VLANs. This isolates the two networks and helps shield the endpoints within the voice network from disturbances in the data network and vice versa.

NOTICE: The implementation of a voice network based on VLANs requires the network infrastructure (the switch fabric) to support VLANs.

In a layer 1 VLAN, the ports of a VLAN-aware switch are assigned to a VLAN statically. The switch only forwards traffic to a particular port if that port is a member of the VLAN that the traffic is allocated to. Any device connected to a VLAN-assigned port is automatically a member of this VLAN, without being a VLAN aware device itself. If two or more network clients are connected to one port, they cannot be assigned to different VLANs. When a network client is moving from one switch to another, the switches' ports have to be updated accordingly by hand.

With a layer 2 VLAN, the assignment of VLANs to network clients is realized by the MAC addresses of the network devices. In some environments, the mapping of VLANs and MAC addresses can be stored and managed by a central database. Alternatively, the VLAN ID, which defines the VLAN whereof the device is a member, can be assigned directly to the device, e. g. by DHCP. The task of determining the VLAN for which an Ethernet packet is destined is carried out by VLAN tags within each Ethernet frame. As the MAC addresses are (more or less) wired to the devices, mobility does not require any administrator action, as opposed to layer 1 VLAN.

The phone must be configured as a VLAN aware endpoint if the phone itself is a member of the voice VLAN, and the PC connected to the phone's PC port is a member of the data VLAN.

When a Voice VLAN ID is configured:

- The CPU port already rejects all packets that do not have the Voice VLAN ID. If the packets are received at the LAN port and have the Voice VLAN ID, they reach the CPU port.
- Untagged LAN port packets are tagged with Management VLAN tag 1.
- CPU port does not receive untagged packets with Management VLAN tag 1 unless port mirroring is active.

When a Voice VLAN ID is NOT configured:

- PC port's untagged packets receive an internal Data VLAN ID from the phone. PC port accepts VLAN tagged frames that have the internal Data VLAN ID. All other tagged frames are dropped.
- CPU port does not receive packets tagged with the Data VLAN ID, as it's not part of that VLAN.
- Packets tagged with the internal Data VLAN ID, become untagged when exiting the LAN port.

There are 3 ways for configuring the VLAN ID:

- By LLDP-MED
- By DHCP
- Manually

3.3.2.1 Automatic VLAN discovery using LLDP-MED

This is the default setting. The VLAN ID is configured by the network switch using LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery). If the switch provides an appropriate TLV (Type-Length-Value) element containing the VLAN ID, this VLAN ID will be used. If no appropriate TLV is received, DHCP will be used for VLAN discovery.

Administration via WBM

Network > Wired settings

Wired settings

LAN connection

Use LLDP-MED

☐

Use DHCP

☒

DHCPv6 enabled

☐

Use DHCP reuse

☐

VLAN discovery

DHCP

VLAN ID

1

LLDP-MED operation

Time to live (seconds)

120

LAN port

LAN port status

100 Mbps half duplex

LAN port speed

Any

IPv4 routing

Route 1 IP address

Route 1 gateway

Route 1 mask

Route 2 IP address

Route 2 gateway

Route 2 mask

IPv6 routing

Route 1 dest.

Route 1 prefix len

Route 1 gateway

Route 2 dest.

Route 2 prefix len

Route 2 gateway

Submit

Reset

Administration via Local Phone

To enable VLAN discovery via LLDP-MED, set the Use LLDP-MED option to Yes and select LLDP-MED in the VLAN discovery option.

```
|--- Administration
    |--- Network
        |--- Wired settings
            |--- Use LLDP-MED
            |--- Use DHCP
            |--- Use DHCPv6
            |--- VLAN discovery
            |--- VLAN ID
```

3.3.2.2 Automatic VLAN discovery using DHCP

To automatically discover a VLAN ID using DHCP, the phone must be configured as DHCP enabled, and VLAN discovery mode must be set to "DHCP". LLDP-MED should be disabled. The DHCP server must be configured to supply the Vendor Unique Option in the correct VLAN over DHCP format. If a phone configured for VLAN discovery by DHCP fails to discover its VLAN, it will proceed to configure itself from the DHCP within the non-tagged LAN. Under these circumstances, network routing may probably not be correct.

Administration via WBM

Network > Wired settings

To enable VLAN discovery via LLDP-MED, activate the LLDP-MED Enabled checkbox and select LLDP-MED in the VLAN discovery option. Afterwards, click Submit.

Wired settings	
LAN connection	
Use LLDP-MED	☐
Use DHCP	☒
DHCPv6 enabled	☐
Use DHCP reuse	☐
VLAN discovery	DHCP
VLAN ID	1
LLDP-MED operation	
Time to live (seconds)	120
LAN port	
LAN port status	100 Mbps half duplex
LAN port speed	Any
IPv4 routing	
Route 1 IP address	
Route 1 gateway	
Route 1 mask	
Route 2 IP address	
Route 2 gateway	
Route 2 mask	
IPv6 routing	
Route 1 dest.	
Route 1 prefix len	
Route 1 gateway	
Route 2 dest.	
Route 2 prefix len	
Route 2 gateway	
Submit Reset	

Administration via Local Phone

To enable VLAN discovery via DHCP, activate the DHCPv6 Enabled checkbox and select DHCP in the VLAN discovery option.

```
|--- Administration
|--- Network
|--- Wired settings
|--- Use LLDP-MED
|--- Use DHCP
|--- Use DHCPv6
|--- VLAN discovery
|--- VLAN ID
```

3.3.2.3 Manual configuration of a VLAN ID

To configure layer 2 VLAN manually, first make sure that VLAN discovery is set to "Manual" (see [Automatic VLAN discovery using LLDP-MED](#) on page 59). Then, the phone must be provided with a VLAN ID between 1 and 4095. If you misconfigure a phone to an incorrect VLAN, the phone will possibly not connect

to the network. In DHCP mode it will behave as though the DHCP server cannot be found, in fixed IP mode no server connections will be possible.

Administration via WBM

The phone must be provided with a VLAN Id between 1 and 4095. Set the VLAN discovery to Manual. Afterwards, click Submit.

Network > Wired settings

Wired settings

LAN connection

Use LLDP-MED

Use DHCP

DHCPv6 enabled

Use DHCP reuse

VLAN discovery

VLAN ID

DHCP

1

LLDP-MED operation

Time to live (seconds)

LAN port

LAN port status

LAN port speed

100 Mbps half duplex

Any

IPv4 routing

Route 1 IP address

Route 1 gateway

Route 1 mask

Route 2 IP address

Route 2 gateway

Route 2 mask

IPv6 routing

Route 1 dest.

Route 1 prefix len

Route 1 gateway

Route 2 dest.

Route 2 prefix len

Route 2 gateway

Submit

Reset

Administration via Local Phone

```
|--- Administration
  |--- Network
    |--- Wired settings
      |--- Use LLDP-MED
      |--- Use DHCP
      |--- Use DHCPv6
      |--- VLAN discovery
      |--- VLAN ID
```

3.4 IP Network Parameters

3.4.1 Quality of Service (QoS)

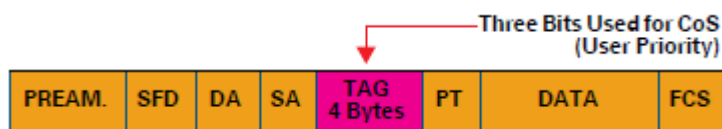
The QoS technology based on layer 2 and the two QoS technologies Diffserv and TOS/IP Precedence based on layer 3 are allowing the VoIP application to request and receive predictable service levels in terms of data throughput capacity (bandwidth), latency variations (jitter), and delay.

NOTICE: Layer 2 and 3 QoS for voice and call signalling transmission can be set via LLDP-MED (see [LLDP-MED](#) on page 294). If so, the value can not be changed by any other interface.

3.4.1.1 Layer 2 / 802.1p

QoS on layer 2 is using 3 Bits in the 802.1q/p 4-Byte VLAN tag which has to be added in the Ethernet header.

The CoS (class of service) value can be set from 0 to 7. 7 is describing the highest priority and is reserved for network management. 5 is used for voice (RTP-streams) by default. 3 is used for signaling by default.



Data required

- **Layer 2:** Activates or deactivates QoS on layer 2. Value range: "Yes", "No" Default: "Yes"
- **Layer 2 voice:** Sets the CoS (Class of Service) value for voice data (RTP streams). Value range: 0-7 Default: 5
- **Layer 2 signalling:** Sets the CoS (Class of Service) value for signaling. Value range: 0-7 Default: 3
- **Layer 2 default:** Sets the default CoS (Class of Service) value. Value range: 0-7 Default: 0

Administration via WBM

Network > QoS > Service

QoS	
Service	
Layer 2	☒
Layer 2 voice	5
Layer 2 signalling	3
Layer 2 default	0
Layer 3	☒
Layer 3 voice	EF
Layer 3 signalling	AF31
MLPP	
Priority	EF
Immediate	EF
Flash	EF
Flash override	EF
Submit Reset	

Administration via Local Phone

```

|--- Admin
    |--- Network
        |--- QoS
            |--- Service
                |--- Layer 2
                |--- Layer 2 voice
                |--- Layer 2 signalling
                |--- Layer 2 default
  
```

3.4.1.2 Layer 3 / Diffserv

Diffserv assigns a class of service to an IP packet by adding an entry in the IP header.

Traffic flows are classified into 3 per-hop behavior groups:

1) Default

Any traffic that does not meet the requirements of any of the other defined classes is placed in the default per-hop behaviour group. Typically, the forwarding has best-effort forwarding characteristics. The DSCP (Diffserv Codepoint) value for Default is "0 0 0 0 0 0".

2) Expedited Forwarding (EF referred to RFC 3246)

Expedited Forwarding is used for voice (RTP streams) by default. It effectively creates a special low-latency path in the network. The DSCP (Diffserv Codepoint) value for EF is "1 0 1 1 1 0".

3) Assured Forwarding (AF referred to RFC 2597)

Assured forwarding is used for signaling messages by default (AF31). It is less stringent than EF in a multiple dropping system. The AF values are containing two digits X and Y (AFX Y), where X is describing the priority class and Y the drop level.

Four classes X are reserved for AFX Y: AF1 Y (low priority), AF2 Y, AF3 Y and AF4 Y (high priority).

Three drop levels Y are reserved for AFX Y: AFX1 (low drop probability), AFX2 and AFX3 (High drop probability). In the case of low drop level, packets are buffered over an extended period in the case of high drop level, packets are promptly rejected if they cannot be forwarded.

Data required

- **Layer 3:** Activates or deactivates QoS on layer 3. Value range: "Yes", "No" Default: "Yes"
- **Layer 3 voice:** Sets the CoS (Class of Service) value for voice data (RTP streams). Value range: "BE", "AF11", "AF12", "AF13", "AF21", "AF22", "AF23", "AF31", "AF32", "AF33", "AF41", "AF42", "AF43", "EF", "CS7", "CS3", "CS4", "CS5", 0, 1, 2 ... through 63. Default: "EF"
- **Layer 3 signalling:** Sets the CoS (Class of Service) value for signaling. Value range: "BE", "AF11", "AF12", "AF13", "AF21", "AF22", "AF23", "AF31", "AF32", "AF33", "AF41", "AF42", "AF43", "EF", "CS7", "CS3", "CS4", "CS5", 0, 1, 2 ... through 63. Default: "AF31"

Administration via WBM

Network > QoS > Service

QoS

Service

Layer 2 ☒

Layer 2 voice 5

Layer 2 signalling 3

Layer 2 default 0

Layer 3 ☒

Layer 3 voice EF

Layer 3 signalling AF31

MLPP

Priority EF

Immediate EF

Flash EF

Flash override EF

Submit Reset

Administration via Local Phone

| --- Admin

```

|--- Network
    |--- QoS
        |--- Service
            |--- Layer 3
            |--- Layer 3 voice
            |--- Layer 3 signalling

```

3.4.2 Protocol Mode IPv4/IPv6

An IPv4 address consists of 4 number blocks, each between 0 and 255, separated by ".".

Example:

1.222.44.123

An IPv6 address consists of 8 hexadecimal number blocks, separated by ":".

Example:

2001:0db8:85a3:08d3:1319:8a2e:0370:7347 or, if not all blocks are used:

2000:1::3

Administration via WBM

Network > Common settings

Set the Protocol Mode to IPv4 or IPv6 or both (the default setting is IPv4_IPv6).

Afterwards, click Submit.

s

Administration via Local Phone

```

|--- Admin
    |--- Network
        |--- Common settings
            |--- Protocol Mode

```

3.4.3 Gratuitous ARP control

As an administrator, you can enhance security by preventing maliciously fabricated ARP frames, including Gratuitous ARP.

Blocking of gratuitous ARP frames can be configured via WBM, DLS and Local settings.

To drop gratuitous ARP frames before they can be used in an ARP attack, set option **Gratuitous ARP control** to **Block all**.

Default is **Allow all**.

IMPORTANT: Blocking of gratuitous ARP frames is available only in an IPv4 network. If protocol mode IPv6 is configured, option **Gratuitous ARP control** is set to read-only.

For information on preventing packets from the PC port being received on the CPU port when a Voice VLAN ID is configured, see [VLAN](#) on page 58.

Administration via WBM

Network > Common settings

S

Administration via Local Phone

```
|--- Admin
    |--- Network
        |--- Common settings
            |--- Gratuitous ARP control
```

3.4.4 Parse DHCPv4 option 43 and DHCPv6 option 17

The OpenScape Desk Phones provide the option to disable parsing of DLS address data via DHCPv4 option 43 and DHCPv6 option 17 to facilitate cloud migration.

If enabled, the phone parses DHCPv6 option 17 and DHCPv4 option 43 for DLS address and port configuration as usual.

If disabled, the phone does not parse DHCPv6 option 17 and DHCPv4 option 43 for DLS address and port configuration.

Default value is 'Enabled'.

If the option changes during runtime, the phone immediately triggers a DHCP renew for both IPv6 and IPv4 DHCP clients (in case they are running):

- When the value has changed from "false" to "true", the phone can possibly assign a DLS address and port as usual via DHCP, which will overwrite any manual assigned DLS address and port.
- When the value has changed from "true" to "false", the phone clears any DHCP assigned values for DLS address and port.

NOTICE: Parsing VLAN information via option 43 is not affected by the new configuration option.

NOTICE: In case a factory reset is triggered and the setting of parsing DCHP option 43 is kept as is, the phone does not get the DLS address and port from DHCP upon reboot.

Administration via WBM

Network > Common settings

Common settings

Protocol mode

IPv4_IPv6

DNS domain

dev.sec

Primary DNS

10.12.0.2

Secondary DNS

HTTP proxy

IP TTL

64

Parse DHCP option 43

☒

Parse DHCP option 66

☒

Gratuitous ARP control

Allow all

Submit

Reset

Administration via Local Phone

```
|--- Admin
  |--- Network
    |--- Common settings
      |--- Parse DCHP option 43
```

3.4.5 Parse DHCP option 66

The OpenScape Desk Phones provide the option to disable parsing of DLS address data via DHCP option 66 to facilitate cloud migration.

If enabled, the phone parses DHCPv4 option 66 configuration as usual. If disabled, the phone does not parse DHCPv4 option 66. Default value is 'Enabled'.

Enabling/Disabling the feature works similar to what is described for [Parse DHCPv4 option 43](#) and [DHCPv6 option 17](#) on page 67.

Administration via WBM

Network > Common settings

Administration via Local Phone

```
|--- Admin
    |--- Network
        |--- Common settings
            |--- Parse DCHP option 66
```

3.4.6 Use DHCP

If this parameter is set to "Yes" (default), the phone will search for a DHCP server on startup and attempt to obtain IP data and further configuration parameters from that central server. The data obtained from DHCP server will be read-only on the phone while DHCP server is enabled.

If no DHCP server is available in the IP network, please deactivate this option.

In this case, the IP address, subnet mask and default gateway/route must be defined manually.

NOTICE: The change will take effect only after restarting the phone.

NOTICE:

The phone will wait for a DHCP response from one of the DHCP servers that includes the required configuration data for a vendor class of "OptilpPhone", which includes option 43. This may delay the boot sequence by approximately 20s.

The following parameters can be obtained by DHCP:

Basic Configuration

- IP Address
- Subnet Mask

Optional Configuration

- Default Route (Routers option 3)
- IP Routing/Route 1 & 2 (Static Routes option 33), Classless static route option 121, Private/Classless Static Rout (Microsoft) option 249)
- SNTP IP Address (NTP Server option 42)
- Timezone offset (Time Server Offset option 2)
- Primary/Secondary DNS (DNS Server option 6)
- DNS Domain Name (DNS Domain option 15)
- SIP Addresses/ SIP Server & Registrar (SIP Server option 120)
- VLAN ID, DLS address (Vendor specific Information option 43)

The following parameters can be obtained by DHCPv6:

Basic Configuration

- Global Address

Global Address Prefix Length

Optional Configuration

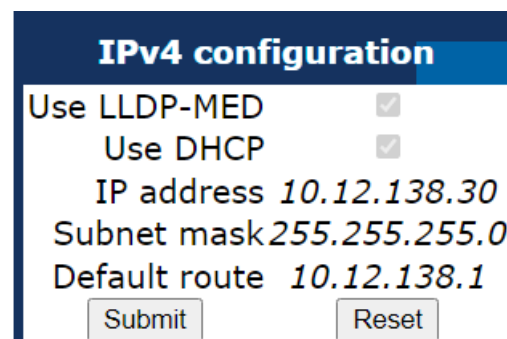
- Primary/Secondary DNS (DNS recursive name server option 23)
- SNTP IP Address (Simple Network Time Protocol Server option 31)
- SIP Addresses / SIP Server & Registrar (SIP Server Domain Name List option 21, SIP Server IPv6 Address List option 22)
- VLAN ID, DLS address (Vendor specific Information option 17)

DHCPv6 options are preferred in Dual Stack Mode if a parameter is configured both via DHCP and via DHCPv6, for instance DNS or SNTP server addresses.

Administration via WBM - IPv4

Network > IPv4 configuration

Set DHCP Enabled to "selected". Afterwards, click Submit.



IPv4 configuration

Use LLDP-MED ☒

Use DHCP ☒

IP address *10.12.138.30*

Subnet mask *255.255.255.0*

Default route *10.12.138.1*

s

Administration via Local Phone

| --- Admin

```
|--- Network
      |--- IPv4 configuration
```

or / and

Administration via WBM - IPv6

Network > IPv6 configuration

Set DHCPv6 Enabled to "selected" (default setting is Enabled). Afterwards, click Submit.

Administration via Local Phone

```
|--- Admin
      |--- Network
            |--- IPv6 configuration
```

3.4.7 IP Address - Manual Configuration

If not provided by DHCP dynamically, you must specify the phone's IP address and subnet mask manually.

NOTICE: IP addresses can be entered in the following formats:

Decimal format. Example: 11.22.33.44 or 255.255.255.0 (no leading zeroes).

Octal format. Example: 011.022.033.044 (leading zeroes must be used with every address block)

Hexadecimal format. Example: 0x11.0x22.0x33.0x44 (prefix 0x must be used with every address block)

By default, IP configuration by DHCP and LLDP-MED is enabled. For manual IP configuration, please proceed as follows:

Data required

- IP address: used for addressing the phone.
- Subnet mask: subnet mask that is needed for the subnet in use.

Administration via WBM

- 1) Navigate to Network > Wired settings. Check **Use DHCP** and **DHCPv6 Enabled** and set **Use LLDP-MED** to "not selected". Afterwards, click Submit.

Network > Wired settings

Wired settings	
LAN connection	
Use LLDP-MED	☒
Use DHCP	☒
DHCPv6 enabled	☒
Use DHCP reuse	☐
VLAN discovery	LLDP-MED v
VLAN ID	
LLDP-MED operation	
Time to live (seconds)	120 v
LAN port	
LAN port status	100 Mbps full duplex
LAN port speed	Any v
IPv4 routing	
Route 1 IP address	
Route 1 gateway	
Route 1 mask	
Route 2 IP address	
Route 2 gateway	
Route 2 mask	
IPv6 routing	
Route 1 dest.	
Route 1 prefix len	
Route 1 gateway	
Route 2 dest.	
Route 2 prefix len	
Route 2 gateway	
Submit Reset	

- 2) Navigate to Network > IPv4 configuration or IPv6 configuration, depending on the settings in Protocol Mode IPv4/IPv6. Set DHCP Enabled, resp. DHCPv6 Enabled and LLDP-MED Enabled to "not selected". Enter the IP address and the Subnet mask. If applicable, enter the Default route. Afterwards, click Submit.

Network > IPv4 configuration

IPv4 configuration

Use LLDP-MED ☒
 Use DHCP ☒
 IP address *10.12.138.30*
 Subnet mask *255.255.255.0*
 Default route *10.12.138.1*

Submit
Reset

Network > IPv6 configuration

IPv6 configuration

Use LLDP-MED ☒
 DHCPv6 enabled ☒
 Global address
 Global address prefix len
 Global gateway
 Link local address

Submit
Reset

Administration via Local Phone

```

|--- Admin
    |--- Network
        |--- Wired settings
            |--- Use LLDP-MED
            |--- Use DHCP
            |--- DHCPv6 enabled

|--- Admin
    |--- Network
        |--- IPv4 Configuration
            |--- IP address
            |--- Subnet mask

|--- Admin
    |--- Network
        |--- IPv6 Configuration
            |--- Global address
            |--- Global Prefix Len
  
```

3.4.8 Default Route/Gateway

If not provided by DHCP dynamically (see [Use DHCP](#) on page 69), enter the IP address of the router that links your IP network to other networks. If the value was assigned by DHCP, it can only be read.

NOTICE: The change will only have effect if you restart the phone.

Administration via WBM - IPv4 Configuration

Enter the Default route, i.e. the IP address of the router that links your IP network to other networks. Afterwards, click Submit.

Network > IPv4 configuration

IPv4 configuration

Use LLDP-MED ☒

Use DHCP ☒

IP address 10.12.138.30

Subnet mask 255.255.255.0

Default route 10.12.138.1

Submit Reset

Administration via Local Phone - IPv4 Configuration

```
|--- Admin
    |--- Network
        |--- IPv4 configuration
            |--- Default route
```

Administration via WBM - IPv6 Configuration

Enter the IP address of the Global Gateway that links your IP network to other networks. Afterwards, click Submit.

Network > IPv6 configuration

IPv6 configuration

Use LLDP-MED ☒

DHCPv6 enabled ☒

Global address

Global address prefix len

Global gateway

Link local address

Submit Reset

Administration via Local Phone - IPv6 Configuration

```
|--- Admin
    |--- Network
        |--- IPv6 configuration
            |--- Global Gateway
```

3.4.9 Specific IP Routing

To have constant access to network subscribers of other domains, you can enter a total of two more network destinations, in addition to the default route/

gateway. This is useful if the LAN has more than one router or if the LAN is divided into subnets.

IPv4 Route Configuration

Data required

- **Route 1/2 IP address:** IP address of the selected route.
- **Route 1/2 gateway:** IP address of the gateway for the selected route.
- **Route 1/2 mask:** Network mask for the selected route.

Administration via WBM - Wired settings

Enter the required data:

- **For Route 1:** Route 1 IP address, Route 1 Gateway, and Route 1 mask.
- **For Route 2:** Route 2 IP address, Route 2 Gateway, and Route 2 mask.

Click Submit.

Network > Wired settings > IPv4 routing

Wired settings

LAN connection

Use LLDP-MED

☒

Use DHCP

☒

DHCPv6 enabled

☒

Use DHCP reuse

☐

VLAN discovery

LLDP-MED

VLAN ID

LLDP-MED operation

Time to live (seconds)

120

LAN port

LAN port status

100 Mbps full duplex

LAN port speed

Any

IPv4 routing

Route 1 IP address

Route 1 gateway

Route 1 mask

Route 2 IP address

Route 2 gateway

Route 2 mask

IPv6 routing

Route 1 dest.

Route 1 prefix len

Route 1 gateway

Route 2 dest.

Route 2 prefix len

Route 2 gateway

Submit

Reset

Administration via Local Phone

```
|--- Admin
    |--- Network
        |--- Wired settings
            |--- IPv4 routing
                |--- Route 1 IP address
                |--- Route 1 gateway
                |--- Route 1 mask
                |--- Route 2 IP address
                |--- Route 2 gateway
                |--- Route 2 mask
```

IPv6 Route Configuration

Data required

- **Route 1/2 destination:** IPv6 address of the selected route.
- **Route 1/2 prefix len:** Prefix length for the selected route.
- **Route 1/2 gateway:** IPv6 address of the gateway for the selected route.

Administration via WBM - Wired settings

Enter the required data:

- **For Route 1:** Route 1 Dest., Route 1 Prefix Len, and Route 1 Gateway.
- **For Route 2:** Route 2 Dest., Route 2 Prefix Len, and Route 2 Gateway.

Click Submit.

Network > Wired settings > IPv6 routing

Wired settings	
LAN connection	
Use LLDP-MED	☒
Use DHCP	☒
DHCPv6 enabled	☒
Use DHCP reuse	☐
VLAN discovery	LLDP-MED v
VLAN ID	
LLDP-MED operation	
Time to live (seconds)	120 v
LAN port	
LAN port status	100 Mbps full duplex
LAN port speed	Any v
IPv4 routing	
Route 1 IP address	
Route 1 gateway	
Route 1 mask	
Route 2 IP address	
Route 2 gateway	
Route 2 mask	
IPv6 routing	
Route 1 dest.	
Route 1 prefix len	
Route 1 gateway	
Route 2 dest.	
Route 2 prefix len	
Route 2 gateway	
Submit	Reset

Administration via Local Phone

```

|--- Admin
|--- Network
|--- Wired settings
|--- IPv6 routing
|--- Route 1 dest.
|--- Route 1 prefix len
|--- Route 1 gateway
|--- Route 2 dest.
|--- Route 2 prefix len
|--- Route 2 gateway

```

3.4.10 DNS

The main task of the domain name system (DNS) is to translate domain names to IP addresses. For some features and functions of the OpenScape Desk Phone CP phone, it is necessary to configure the DNS domain the phone belongs to, as well as the name servers needed for DNS resolving.

3.4.10.1 DNS Domain Name

This is the name of the phone's local domain.

Administration via WBM

Enter the DNS domain the phone belongs to. Afterwards, click Submit.

Network > Common settings

Common settings	
Protocol mode	IPv4_IPv6
DNS domain	dev.sec
Primary DNS	10.12.0.2
Secondary DNS	
HTTP proxy	
IP TTL	64
Parse DHCP option 43	☒
Parse DHCP option 66	☒
Gratuitous ARP control	Allow all
Submit Reset	

Administration via Local Phone

```
|--- Admin
    |--- Network
        |--- Common settings
            |--- DNS domain
```

3.4.10.2 DNS Servers

If not provided by DHCP automatically, a primary and a secondary DNS server can be configured.

NOTICE: Depending on the configuration chosen for survivability, DNS SRV is required. For details, please refer to Resilience and Survivability.

Data required

- **Primary DNS:** IP address of the primary DNS server.
- **Secondary DNS:** IP address of the secondary DNS server.

Administration via WBM**Network > Common settings**

Enter the IP addresses of the Primary DNS and the Secondary DNS server. Afterwards, click Submit.

Administration via Local Phone

```
|--- Admin
    |--- Network
        |--- Common settings
            |--- Primary DNS
            |--- Secondary DNS
```

3.4.10.3 Terminal Hostname

The phone's hostname can be customised.

NOTICE: DHCP and DNS must be appropriately connected and configured at the customer site.

The corresponding DNS domain is configured in **Network > Common settings > DNS domain** (see [DNS Domain Name](#) on page 79).

The current DNS name of the phone is displayed at the right-hand side of the banner of the admin and user web pages, under DNS name. To see configuration changes, the web page must be reloaded.

NOTICE: It is recommended to inform the user about the DNS name of the phone. The complete WBM address can be found under **User menu > Network information > Web address**.

The DNS name can be constructed from pre-defined parameters and free text. Its composition is defined by the DNS name construction parameter **Administration > System Identity > DNS name construction**. The following options are available:

- **None:** No hostname is send to the DHCP server during DHCP configuration.
- **MAC based:** The DNS name is built from the prefix "OIP" followed by the phone's MAC address.
- **Web name:** The DNS name is set to the the string entered in Web name.
- **Only number:** The DNS name is set to the Terminal number, that is, the phone's call number (E.164).
- **Prefix number:** The DNS name is constructed from the the string entered in Web name, followed by the Terminal number.

Administration via WBM

System > System Identity

Administration via Local Phone

```
|--- Administration
    |--- System identity
        |--- Web name
        |--- DNS name construction
```

3.4.10.4 IP TTL

Defines the “Time-To-Live” (TTL) value within the IP header for any packet being sent by the phone. The default value is “64”.

This parameter can be set through the WMB interface, the local phone or DLS.

Administration via WBM

Administrator settings > Network > Common settings

Select the desired value for IP TTL and click Submit.

Administration via Local Phone

```
|--- Admin
      |--- Network
            |--- Common settings
                  |--- IP TTL
```

3.4.11 Configuration & Update Service

The OpenScape Deployment Service (DLS) is a OpenScape Management Application for administering workpoints in both OpenScape and non-OpenScape networks. Amongst the most important features are: security (e.g. PSS generation and distribution within an SRTP security domain), mobility for OpenScape SIP phones, software deployment, plug&play support, as well as error and activity logging.

DLS address, i.e. the IP address or hostname of the DLS server, and Default mode port, i.e. the port on which the DLS server is listening, are required to enable proper communication between phone and DLS. Set Revert to default security to disable mutual authentication and return to DEFAULT mode. SECURE mode related settings are reset and certificates are removed.

The Mode (labeled Mode in the local phone's Admin menu) determines the security level for the communication between the phone and the DLS. Mutual authentication establishes a higher security level of the connection by mutually exchanging credentials between the DLS and the phone. After this, the communication is encrypted, and a different port is used, thus ensuring that the phone is unambiguously connected to the correct DLS server.

NOTICE: The URI of the DCMP, as well as the polling interval, are configured by the DLS. For this purpose, it is necessary that the phone establishes a first contact to the DLS, e. g. by phone restart or local configuration change.

To enhance secure phone connection to DLS or DLI, admin can perform one of the following actions:

- **Lock DLS address:** Lock Contact-Me messages to exclusively use the DLS-WPI address configured on the phone. A different DLS address given by the contact-me message will be ignored by the phone.

NOTICE: If a DLS-WPI address has not be configured and this setting is enabled, then the phone will not contact a DLS/DLI until an address is configured.

- **Disable DLS-WPI:** Disable the DLS-WPI interface completely. The phone will not use the DLS-WPI at all, neither as a result of a Contact-Me request nor due to local events (e.g. local changes, security log, etc.).

NOTICE: When enabled, DMS access is not affected. Cloud deployment is affected, as redirect Service will no longer work.

NOTICE: It is possible to operate the DLS server behind a firewall or NAT (Network Address Translation), which prevents the DLS from sending Contact-Me messages directly to the phone. Only outbound connections from the phone are allowed. To overcome this restriction, a DLS Contact-Me proxy (DCMP) can be deployed. The phone periodically polls the DCMP (DLS Contact- Me Proxy), which is placed outside of the phone's network, for pending contact requests from the DLS. If there are contact requests, the phone will send a request to the DLS in order to obtain the update, just as with a regular DLS connection.

A Security PIN can be provided which is used for decrypting data provided by the DLS during bootstrap. Bootstrapping is the process by which an initial non-secure connection to the DLS is elevated to a secure connection. Once the connection has been elevated to secure mode it will stay in that mode for subsequent connections to the same DLS. For further information, please refer to the DLS documentation.

Data required

- **DLS address:** IP address or hostname of the server on which the Deployment Service is running.
- **Default mode port:** Port on which the DLS Deployment Service is listening. Default: 18443.
- **Revert to default security:** When set, security mode will be set to default. When using local phone administration, this will be set by selection option 'Default security' after pressing Save&exit.

NOTICE: The DLS will also need to be reset to default mode manually.

- **Mode:** Indicates whether the communication between the phone and the DLS is secure. Value range: "Default", "Secure", "Secure PIN". This parameter is read-only. Default: "Default".
- **Security PIN:** Used for enhanced security.

Administration via WBM
Network > Update Service

Update service

Select either DLS or DMS for use by providing an address, but only for one of them

Deployment service (DLS)

Disable DLS-WPI

DLS address

Default mode port

Lock DLS address

Revert to default security

Mode

Security PIN

☐

☐

☐

Default

Device management service (DMS)

DMS address

Username

Password

Minimum update check (seconds)

Update check during working hours

Ignore software update from config file

Check for update

☒

☐

Now

Reset

Submit

Administration via Local Phone

```
|--- Admin
  |--- Network
    |--- Deployment service
      |-- Disable DLS-WPI
      |--- DLS address
      |--- Default mode port
      |--- Revert to default security
      |--- Mode
      |--- Security PIN
```

3.4.12 SNMP

The Simple Network Management Protocol is used by network management systems for monitoring network-attached devices for conditions that warrant administrative attention. An SNMP manager surveys and, if needed, configures several SNMP elements, e.g. VoIP phones.

OpenScape Desk Phone CP phones support SNMPv1.

There are currently 4 trap categories that can be sent by the phones:

Standard SNMP traps

OpenScape Desk Phone CP phones support the following types of standard SNMP traps, as defined in RFC 1157:

- **coldStart**: sent if the phone does a full restart.
- **warmStart**: sent if only the phone software is restarted.
- **linkUp**: sent when IP connectivity is restored.
- **QoS Related traps**: These traps are designed specifically for receipt and interpretation by the QDC collection system. The traps are common to SIP phones, HFA phones, Gateways, etc.
- **Traps for important high level SIP related problems**: Currently, these traps are related to problems in registering with a SIP Server and to a failure in remotely logging off a mobile user. These traps are aimed at a nonexpert user (e.g. a standard Network Management System) to highlight important telephony related problems.
- **Traps specific to OpenScape Desk Phone CPTraps**:
Currently, the following traps are defined:
 - **TraceEventFatal**: sent if severe trace events occur; aimed at expert users.
 - **TraceEventError**: sent if severe trace events occur; aimed at expert users.

NOTICE: Starting from V1R12, OpenScape CPx00 phones support secondary SNMP server configuration, enabling redundant trap management and improved network monitoring reliability.

Data required

- **Generic traps**
 - **Trap sending enabled**: Enables or disables the sending of a TRAP message to the SNMP manager. Value range: "Yes", "No" Default: "No"
 - **Trap destination**: IP address or hostname of the SNMP manager that receives traps.
 - **Trap destination port**: Port on which the SNMP manager is receiving TRAP messages. Default: 162
 - **Trap community**: SNMP community string for the SNMP manager receiving TRAP messages. Default: "snmp"
 - **Queries allowed**: Allows or disallows queries by the SNMP manager.
 - **Query password**: Password for the execution of a query by the SNMP manager.
 - **Secondary destination enabled**: Enables or disables the sending of TRAP messages to the secondary SNMP manager.
 - **Secondary Trap destination**: IP address or host name of the secondary SNMP manager that receives traps.
 - **Secondary Trap destination port**: Port on which the secondary SNMP manager is receiving TRAP messages.
 - **Secondary Trap community**: Secondary SNMP community string for the SNMP manager receiving TRAP messages.

- **Diagnostic traps**

- **Diagnostic sending enabled:** Enables or disables the sending of diagnostic data to the SNMP manager. Value range: "Yes", "No" Default: "No"
- **Diagnostic destination:** IP address or hostname of the SNMP manager receiving diagnostic data.
- **Diagnostic destination port:** Port on which the SNMP manager is receiving diagnostic data.
- **Diagnostic community:** SNMP community string for the SNMP manager receiving diagnostic data.
- **Diagnostic to generic destination:** Enables or disables the sending of diagnostic data to a generic destination. Value range: "Yes", "No" Default: "No".
- **Secondary destination enabled:** Enables or disables the secondary destination.
- **Secondary Diagnostic destination:** IP address or host name of the secondary SNMP manager receiving diagnostic data.
- **Secondary Diagnostic port:** Port on which the secondary SNMP manager is receiving diagnostic data.
- **Secondary Diagnostic community:** Secondary SNMP community string for the SNMP manager receiving diagnostic data.

- **QoS report traps**

- **QoS traps to QCU:** Enables or disables the sending of TRAP messages to the QCU server. Value range: "Yes", "No" Default: "No"
- **QCU address:** IP address or hostname of the QCU server.
- **QCU port:** Port on which the QCU server is listening for messages. Default: 12010.
- **QCU community:** QCU community string. Default: "QOSCD".
- **QoS to generic destination:** Enables or disables the sending of QoS traps to a generic destination. Value range: "Yes", "No" Default: "No".
- **Secondary QCU enabled:** Enables or disables the secondary QCU.
- **Secondary QCU address:** IP address or host name of the secondary QCU server.
- **Secondary QCU port:** Port on which the secondary QCU server is listening for messages
- **Secondary QCU community:** Secondary QCU community string.

Administration via WBM

System > SNMP

SNMP	
Generic traps	
Trap sending enabled	☐
Trap destination	
Trap destination port	162
Trap community	*****
Queries allowed	☐
Query password	*****
Secondary destination enabled	☐
Secondary Trap destination	
Secondary Trap destination port	162
Secondary Trap community	*****
Diagnostic traps	
Diagnostic sending enabled	☐
Diagnostic destination	
Diagnostic destination port	
Diagnostic community	
Diagnostic to generic destination	☐
Secondary destination enabled	☐
Secondary Diagnostic destination	
Secondary Diagnostic port	
Secondary Diagnostic community	
QoS report traps	
QoS traps to QCU	☐
QCU address	
QCU port	12010
QCU community	*****
QoS to generic destination	☐
Secondary QCU enabled	☐
Secondary QCU address	
Secondary QCU port	12010
Secondary QCU community	*****
Submit Reset	

Administration via Local Phone

```

<codeblock>
|--- Admin
|   |--- System
|       |--- SNMP
|           |--- Generic traps
|               |--- Trap sending enabled
|               |--- Trap destination
|               |--- Trap destination port
|               |--- Trap community
|               |--- Queries allowed
|               |--- Query password
|               |--- Secondary destination enabled
|               |--- Secondary Trap destination
|               |--- Secondary Trap destination port
|               |--- Secondary Trap community
|           |--- Diagnostic traps
|               |--- Diagnostic sending enabled
|               |--- Diagnostic destination
|               |--- Diagnostic destination port
|               |--- Diagnostic community
|               |--- Diagnostic to generic destination
|               |--- Secondary destination enabled
|               |--- Secondary Diagnostic destination
|               |--- Secondary Diagnostic port

```

```
|--- Secondary Diagnostic community
|--- QoS report traps
|--- QoS traps to QCU
|--- QCU address
|--- QCU port
|--- QCU community
|--- QoS to generic destination
|--- Secondary QCU enabled
|--- Secondary QCU address
|--- Secondary QCU port
```

3.5 Wi-Fi Settings

The OpenScope Desk Phone CP700X provides the option to connect to a Wi-Fi network.

Wi-Fi parameters can be configured via WBM and local Settings. You can activate/deactivate Wi-Fi network access and set up new Wi-Fi networks that will be added to **Stored Wi-Fi networks**, to be used by the phone.

Wi-Fi connection with encryption type WPA2-PSK with pre-shared key using AES are characterized as secure network. The supported authentication protocols are the following:

- EAP-TLS
- EAP-LEAP
- FAST

NOTICE: Wi-Fi connection with no encryption type, WEP or WPA are characterized as unsecure networks.

The authorization by name and password is optional. User certificate and root certificate are also optional. The administrator can upload both certificates to phone via DLS. If more than one certificates are uploaded, the administrator can choose which certificate will be used.

Certificates are uploaded to phone only via DLS. There is the option to upload common certificates to be used for all networks or SSID specific ones. Common sets of certificates will also have common backup pair. For each SSID the administrator can use common or SSID specific certificates.

NOTICE: If WPA-EAP network is added common certificates are used as default, with no option to choose SSID specific certificates.

Administration via WBM

Network > Wi-Fi settings

Wi-Fi settings				
Enable Wi-Fi interface	☐			
Wi-Fi MAC address	00:1a:e8:db:fd:f4			
Wi-Fi link status	down			
Last connected Wi-Fi network name	""			
Wi-Fi country settings	United Kingdom			
Advanced settings				
Frequency band	All (5 GHz + 2.4 GHz)			
Allowed channels (5 GHz)	All			
Manual selection of allowed channels (5 GHz)				
Allowed channels (2.4 GHz)	All			
Manual selection of allowed channels (2.4 GHz)				
Enable 802.11r (Fast BSS Transition)	☒			
Roaming RSSI threshold	-75			
Submit	Reset			
Add new Wi-Fi network				
Wi-Fi SSID				
Hidden SSID	☐			
Wi-Fi password				
Encryption type	WPA2/WPA3-Personal			
IP settings	DHCP			
IP address				
Subnet mask				
Default route				
Authentication protocol	None			
EAP anonymous identity				
EAP identity				
EAP password				
Add Wi-Fi network	Reset			
Stored Wi-Fi networks				
Wi-Fi SSID	Signal	Encryption type	IP settings	Wi-Fi Password
123	None	WPA2/WPA3-Personal	DHCP	
				Change password Forget
Refresh signal information				

Administration via Local Phone

```
|--- Admin
    |--- Network
        |--- Wi-Fi settings
```

3.5.1 Setting up a CP700X for the first time with WLAN connection

When a CP700X phone is setup for the first time using only Wi-Fi to get a LAN connection a temporary Wi-Fi connection is used automatically.

The device is connected to a predefined WLAN with the following configuration:

- SSID: AWS-INIT
- Security key: WPA-PSK / WPA2-PSK
- WPA-PSK passphrase: AWS-INIT

All other network parameters are at their default settings:

- DHCP mode: On
- 11 protocol: 802.11b/g/n
- 11b/g/n channels: 1,6,11
- World mode regulatory domain: World mode (802.11d)

If the phone is not successfully connected to this WLAN within ten seconds, it will disable WLAN for 10s and then it will try again for 10s. If this also fails, the phone will need to be rebooted. This process can also be interrupted by configuring the phone either through the local phone menu or through the DLS using prestaging. As soon as one of the Networks A-D has a SSID filled in, probing of AWS-INIT will stop.

Wi-Fi discovery requires that the DHCP server is configured to return a valid DLS IP address as part of the DHCP response sent to the phone. The DLS IP address is sent using DHCP Option 43 (vendor specific data).

Once the phone has discovered a DLS address, it will open up a secure connection to DLS for downloading configuration parameters using the WPI protocol. Any certificates needed for Wi-Fi authentication or SIP/TLS will also be downloaded as a part of this process. If a DLS address is specified in the downloaded configuration, that DM will be used subsequently. If not, the DLS discovery procedure will be used for each time the phone is started. The downloaded configuration should also contain a new network configuration, which will cause the phone to disconnect from the AWS-INIT SSID.

3.5.2 Disabling LAN port (for CP700X)

The OpenScape Desk Phone CP700X provides the option to disable the LAN port connection when a Wi-Fi network is configured.

When LAN port is disabled, the ethernet connection is no longer supported. Wi-Fi LAN is automatically enabled (if not already enabled) and it cannot be disabled.

NOTICE: The LAN port may be disabled whether Wi-Fi LAN is enabled or disabled.

In case a Wi-Fi LAN connection cannot be established, then:

- 1) the Wi-Fi settings must be corrected, or
- 2) the LAN port must be re-enabled manually.

NOTICE: If LAN port is disabled and all Wi-Fi networks are deleted (there is no available network), "LAN port disabled" option is read-only and LAN port should be automatically enabled.

Administration via WBM

Network > Wired settings > LAN port configuration (LAN port disabled)

Administration via Local Phone

```
|--- Admin
      |--- Network
            |--- Wired settings
                  |--- LAN port configuration (LAN
port disabled)
```

3.5.3 Advanced Wi-Fi settings

The OpenScape Desk Phone CP700X provides advanced Wi-Fi options to reduce downtime during Wi-Fi roaming process.

Advanced Wi-Fi options

- **Frequency band**

Select one of the following options to set the frequency band:

- 1) All (5 GHz + 2.4 GHz)
- 2) 5 GHz
- 3) 2.4 GHz

- **Allowed channels (5GHz)**

Select one of the following options to configure only a specific subset of allowed frequencies during network scan and Wi-Fi operation:

- 1) All
- 2) Non DFS
- 3) UNII-1
- 4) UNII-3
- 5) UNII-1, UNII-2
- 6) UNII-1, UNII-2, UNII-3
- 7) UNII-1, UNII-2 Extended

Channel denomination for 5 GHz:

Channel denomination	Channels
Non DFS	36, 40, 44, 48, 149, 153, 157, 161, 165
UNII-1	36, 40, 44, 48
UNII-2	52, 56, 60, 64
UNII-2 Extended	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
UNII-3	149, 153, 157, 161, 165

- **Manual selection of allowed channels (5GHz)**

Allowed channels can be specified as a comma separated list of channel numbers, i.e. you can manually allow UNII-1 channels by a list "36, 40, 44, 48".

Invalid inputs are rejected:

- Allowed characters are numbers, comma and optional white space characters.
- Invalid channel numbers for 5 GHz. If selected list of allowed channels is in conflict with active regulatory domain, then only channels valid for active regulatory domain are used.
- If new input is invalid but previous value of *Manual selection of allowed channels (5 GHz)* was valid, then the new value is rejected and the previous value is kept (to prevent from invalid configuration).
- If new input is invalid and previous value was empty, then value of field *Allowed channels (5 GHz)* is automatically changed to *All* when user

leaves the dialog and discards the changes (to prevent from invalid configuration).

- **Allowed channels (2.4 GHz)**

Select one of the following options to configure only a specific subset of allowed frequencies during network scan and Wi-Fi operation:

- 1) All
- 2) 1, 6, 11

- **Manual selection of allowed channels (2.4 GHz)**

Allowed channels can be specified as a comma separated list of channel numbers, i.e. you can manually allow channels by a list "1, 2, 3, 4".

Invalid inputs are rejected:

- Allowed characters are numbers, comma and optional white space characters.
- Invalid channel numbers for 2.4 GHz. If selected list of allowed channels is in conflict with active regulatory domain, then only channels valid for active regulatory domain are used.
- If new input is invalid but previous value of *Manual selection of allowed channels (5 GHz)* was valid, then the new value is rejected and the previous value is kept (to prevent from invalid configuration).
- If new input is invalid and previous value was empty, then value of field *Allowed channels (5 GHz)* is automatically changed to *All* when user leaves the dialog and discards the changes (to prevent from invalid configuration).

- **Enable 802.11r (Fast BSS Transition)**

Select one of the following values:

- 1) True
- 2) False

- **Roaming RSSI threshold**

Edit the text field to configure the roaming RSSI threshold:

Value can be set as a negative integer (RSSI value in dBm).

Invalid inputs will be rejected:

- Valid input is negative integer from range -30 to -90. Any other input is considered invalid (alphabetic characters except minus sign, positive integers or integers outside of the specified range).

Administration via Local Phone

```
|--- Admin
      |--- Network
            |--- Wi-Fi settings
                  |--- Advanced settings
```

Administration via WBM

Network > Wi-Fi settings > Advanced settings

NOTICE:

Fields are the same as in LocalAdmin, except:

- 1) *Manual selection of allowed channels (5 GHz)* and *Manual selection of allowed channels (2.4 GHz)* do not dynamically change their read-only status (they are always writable).
 - 2) If field *Allowed channels (5 GHz)* is not set to *Manual selection*, then any input in field *Manual selection of allowed channels (5 GHz)* is ignored.
 - 3) If field *Allowed channels (2.4 GHz)* is not set to *Manual selection*, then any input in field *Manual selection of allowed channels (2.4 GHz)* is ignored.
-

3.6 Security

OpenScape Desk Phone CP phones support secure (i.e. encrypted) speech transmission via SRTP. For enabling secure (encrypted) calls, a TLS connection to the OpenScape Voice server is required.

If use secure calls is activated, the encryption of outgoing calls is enabled, and the phone is capable of receiving encrypted calls. When the phone is connected to an OpenScape Voice system, call security is indicated to the user as follows:

- An icon in the call view tells the user whether a call is secure (encrypted) or not.
 - If an active call changes from secure to insecure, e. g. after a transfer, a popup window and an alert tone will notify the user.
-

NOTICE:

For secure (encrypted) calls, it is required that both endpoints support SRTP. The secure call indication tells the user that the other endpoint has acknowledged the secure connection.

In order to use SRTP, the phone must be configured for NTP (for further information please see Date and Time). The reason is that the key generation uses the system time of the particular device as a basis. Thus, encryption will only work correctly if all devices have the same UTC time.

If SIP server certificate validation or backup SIP server certificate validation is activated, the phone will validate the server certificate sent by the OpenScape Voice server to establish a TLS connection. The server certificate is verified against the root certificate from a trusted certificate authority (CA), which must first be stored on the phone. A DLS (OpenScape Deployment Service) server is required to deliver the root certificate.

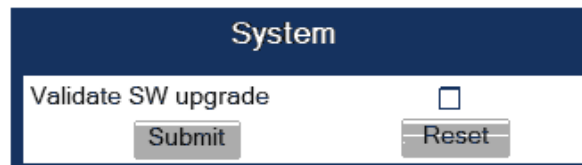
3.6.1 System

If this option is enabled and you try to load a new software bind onto the phone, there will be a check that the new software bind has a validated signature. In case the validation fails, the new software bind will be rejected and there will be an error message.

By default this feature is enabled.

Administration via WBM

Administrator settings > System > Security > System



The screenshot shows a web interface titled 'System'. Below the title is a section labeled 'Validate SW upgrade' which contains an unchecked checkbox. Below the checkbox are two buttons: 'Submit' and 'Reset'.

Administration via Local Phone

```
|--- Administration
    |--- System
        |--- Security
            |--- System
                |--- Validate SW upgrade
```

3.6.2 SRTP Configuration

The SRTP type sets the key exchange method for SRTP.

The use of secure calls activates the encryption of outgoing calls and enables the receiving of encrypted calls.

NOTICE: For secure (encrypted) calls, it is required that both endpoints support SRTP (and TLS). The secure call indication tells the user that the other endpoint has acknowledged the secure connection.

SRTP key mode

The **SRTP key mode** sets the key exchange method (negotiation method) for secure calls via SRTP. The following encryption key exchange methods are available:

- MIKEY
- SDES (see SDES Configuration)
- DTLS
- DTLS + SDES

NOTICE:

The **SRTP key mode**, **Use SRTCP** and **Crypto context update** options are only available for secure (encrypted) calls, i.e. these parameters are enabled only if **Use secure calls** is activated and **SRTP key mode** is not configured as MIKEY.

When **Use SRTCP** is activated (together with **Use secure calls**), the phone will use SRTCP (Secure RTCP) to transmit and receive RTP control packets.

NOTICE: If **SRTP** is enabled, ANAT interworking (see Media/SDP) is only possible if SDES is configured as the key exchange protocol for SRTP.

Insecure call periodic alert

When enabled, the phone user hears a periodic tone (every 15 seconds) while an insecure call is active.

When disabled (default), the phone user hears the tone only at the start of the call.

SDP mode

The SDP negotiation parameter specifies whether the use of SRTP will be forced by the phone. The following choices are available:

- **RTP + SRTP (2mline)** - Both non-encrypted (non-secure) and encrypted (secure) media connections are offered. Non-encrypted connections are preferred over encrypted connections, i.e. the phone uses the non-encrypted RTP connection if the remote party accepts it and only switches to SRTP if RTP is not accepted.
- **SRTP + RTP (2mline)**- With SRTP + RTP, the phone will try to establish an SRTP connection, but fall back to RTP if this should fail. This is the recommended option.
- **SRTP only** -With SRTP only, only an encrypted (secure) media connection is allowed; if the remote party should not support SRTP, no connection will be established.
- **SRTP or RTP (1mline)**

NOTICE:

“**2mline**” means that sdp type (RTP or SRTP) has its own line in the sdp with the ordering of these lines identifying their priority. “**1mline**” means there is a single line in the sdp and the phones makes a 'best effort' to support SRTP but will fall back to RTP if necessary.

Crypto context update

The **Crypto context update** item allows changing to a different mechanism how the cryptographic context is updated.

- **Full crypto context reset** (default) - CP phone recreates the locally stored SRTP crypto context whenever it either receives new SRTP key generated by the other party (Rx direction) or when it generates its own new SRTP master key (Tx direction). The "Full crypto context reset" particularly applies to the ROC (Roll Over Counter) that must be in this case reset back to 0.
- **Key update (RFC compliant)**- Upon refreshing the SRTP keys, CP phone only updates the respective crypto context (Rx or Tx), without recreating it. Therefore, ROC preserves its value throughout the key update.

For encryption algorithms, the ranking for each crypto-suite for negotiation can be defined, or they can be enabled or disabled:

- AES_128_SHA1_80 - Available for both SDES and DTLS.
- AES_128_SHA1_32 - Available for both SDES and DTLS.

- AES_256_SHA1_80 - Available only for SDES.
- AES_256_GCM - Available for DTLS, providing authenticated encryption with associated data (AEAD) for enhanced security.
- AES_128_GCM - Available for DTLS, providing authenticated encryption with associated data (AEAD) for enhanced security.

Administration via WBM

System > Security > SRTP config

Administration via Local Phone

```
|--- Administration
    |--- System
        |--- Security
            |--- SRTP config
                |--- Use secure calls
                |--- Use SRTCP
            |--- Insecure call periodic alert
                |--- SRTP key mode
                |--- SDP mode
                |--- Crypto context update
                |--- AES_256_SHA1_80 (SDES)
ranking
                |--- AES_256_GCM (DTLS) ranking
                |--- AES_128_GCM ranking
                |--- AES_128_SHA1_80 ranking
                |--- AES_128_SHA1_32 ranking
```

3.6.3 Access control

The CCE access parameter controls TCP and UDP access for the CCE (CommsChannel Extender). This affects the local CTI access and HPT access. When Disable is selected, both TCP and UDP are disabled. With Enable, there are no restrictions.

With **Factory reset claw**, the 'hooded claw' keypad mechanism to initiate a factory reset without requiring an authenticated access can be enabled or disabled.

The **Serial port** parameter controls access to the serial port. When set to No password, a terminal connected to the port can interact with the phone's operating system without restrictions. When Passwd reqd is selected, the serial port requires a password for access (root user is not available). When Unavailable is chosen, the serial port is not accessible.

As a prerequisite, the root user needs to create a user and to define a password via Serial Access, so that access can be granted when the Password required prompt is issued.

WBM TLS interface allows the web server to support obsolete TLS versions (TLS1.0 and TLS 1.1) as well as the latest versions (current latest versions are TLS 1.3 and TLS 1.2). By default only the latest TLS version is allowed. Other interfaces (e.g. SIP) are not affected by this setting.

Server TLS interface allows all interfaces, except the web server, to support obsolete TLS versions (TLS 1.0 and TLS 1.1) as well as the latest versions (current latest versions are TLS 1.3 and TLS 1.2). By default only the latest TLS version is allowed. The web server interface is not affected by this setting.

Administration via WBM

System > Security > Access control

Administration via Local Phone

```
|--- Administration
    |--- System
        |--- Security
            |--- Access control
                |--- CCE access
                |--- Factory reset claw
                |--- Serial port
                |--- WBM TLS interface
                |--- Server TLS interface
```

3.6.4 Security Log

A cyclic security log is used to capture important security specific events. It can be exported as CSV data to an external application for analysis.

NOTICE: The security log cannot be disabled.

- The Max. lines parameter defines the maximum number of entry lines that can be kept in the security log before old entries are overwritten by new entries.
- Automatic Archive to DLS controls whether the log is sent to the DLS. When activated, the DLS is used to automatically archive the security log so that no log entries will be lost.
- **Archive when at:** This value sets the trigger for log archiving. Automatic archiving of new security log entries will occur when the percentage of unarchived entries in the log is as specified or more. The possible values are "0%", "10%", "20%", "30%", "35%", "40%", "45%", "50%", "55%", "60%", "65%", "70%", "80%", "90%".
- The value may be set to 0% by both the phone and the DLS and this value will prevent the phone from archiving or telling the DLS that it needs archiving.

The security log upload may be accomplished in two ways:

- If "Automatic archive to DLS" is enabled, if the security log reaches the threshold % for unarchived entries, the phone will initiate an upload.
- If "Automatic archive to DLS" is NOT enabled and the security log reaches the threshold % for unarchived entries, the phone only sets the "archive-me" flag, it does not initiate the archive.

It is up to the DLS to recognize the flag and initiate an upload.

- Last archived shows the date when the security log was last archived to the DLS.

Administration via WBM

System > Security > Logging

Administration via Local Phone

```
|--- Administration
    |--- System
        |--- Security
            |--- Logging
                |--- Max. lines
                |--- Archive to DLS
                |--- Archive when at
                |--- Last archived
```

3.6.5 Security-Related Faults

Security log entry shows the date and time of a loss of security log entries.

NOTICE: The entries in this list are only displayed until they are reported to the DLS, which usually happens very fast. After that, the entries are automatically deleted from the phone. If the entries are not deleted automatically, they can be deleted manually by using the Cancel faults parameter.

- **OCSR failure:** Shows the date and time when the phone was unable to connect to any certificate checking server for revoked certificates.
- **Admin access:** Shows the date and time when the phone encountered multiple consecutive failures to enter the admin password.
- **User access:** Shows the date and time when the phone encountered multiple consecutive failures to enter the user password.

Administration via WBM

System > Security > Faults

Administration via Local Phone

```
|--- Administration
    |--- System
        |--- Security
            |--- Faults
                |--- Security log entry
                |--- OCSR failure
                |--- Admin access
                |--- User access
                |--- Cancel faults
```

3.6.6 Microsoft® Exchange

Microsoft® Exchange Server provides a suite of messaging and collaboration services, including email, calendars, contacts, and tasks. The CP400/600/700 Phone can access Microsoft® Exchange to synchronize contacts on the phone.

To ensure secure access to Microsoft® Exchange, Admin is required to configure Oath2 authentication.

3.6.6.1 Configuring Oath2 authentication

Admin can configure Oath2 authentication to enable CP400/600/CP700 phones to access Exchange services with enhanced security. When accessing Microsoft® Exchange, Oath2 authentication replaces basic and

NTLM authentication for cloud based Exchange installation. This method is configurable via WBM.

NOTICE: Local Settings and DLS can still configure the Server and Folder options, but they cannot be used to trigger the authentication process. The user is required to enter their credentials to a HTML page via their web browser (see description below).

After user activates Microsoft® Exchange access on the CP phone, WBM retrieves the Oath2 application information from the phone's database. WBM submits a HTTPS request to the authenticator server to authorize the user. A new page is displayed to the user, requiring the user to enter credentials. Upon succesful completion of the credentials, the user can access Microsoft® Exchange. For more information, see: [Accessing Microsoft® Exchange](#) on page 101.

NOTICE: The credentials required from the user are determined by the organisation when they completed the registration with the Authenticator, but may include Single Sign On (SSO) or Multi-Factor Authentication (MFA).

Administration via WBM

System > Security > Microsoft® Exchange

Microsoft® Exchange

Basic settings

Server address

Contacts folder

Authentication App settings

Authenticator server path

Tenant ID

Client Id

Client Secret

Redirect address for user login

login.microsoftonline.com

common

cloud-setup.com:18443

Submit

Reset

Administration via Local Phone

```
|--- Administration
  |--- System
    |--- Security
      |--- Microsoft Exchange
        |--- Basic Settings
          |--- Server address
          |--- Contacts folder
          |--- Authentication App settings
            |--- Application server path
            |--- Tenant ID
            |--- Client ID
            |--- Client Secret
            |--- Redirect address for user login

login
```

3.6.6.2 Accessing Microsoft® Exchange

Admin can allow the user to log in and out from Microsoft® Exchange.

Prerequisite: Admin has configured Oath2 authentication.

Admin is prompted to confirm the account to be logged in.

Upon confirmation, user WBM provides a **Login** button to allow the user to log in. The user is required to confirm and provide their credentials. User WBM confirms the action, and the user is logged in.

Microsoft® Exchange

Basic settings

Server: outlook.office365.com

Username: ixpertalab\tester

Password: •••••

Folder to sync (optional): Kontakty

Submit Reset

Authentication status

Login

✓ **Changes saved successfully**

Refresh

To allow the user to log out, Admin is required to repeat the confirmation process. User WBM now provides a **Logout** button.

Microsoft® Exchange

Basic settings

Server address: outlook.office365.com

Contacts folder: Kontakty

Authentication App settings

Authenticator server path: login.microsoftonline.com

Tenant ID:

Client Id: 5783565e-eea8-4c16-8c

Client Secret: •••••

Redirect address for user login: cloud-setup.com:18443/

Submit Reset

Authentication status

Logout

3.6.7 Password Policy

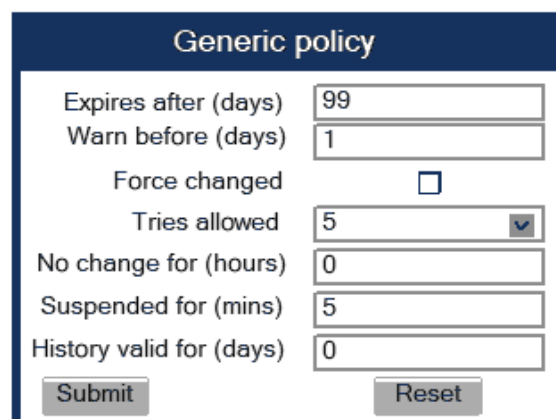
3.6.7.1 General Policy

- **Expires after (days):** Sets the maximum validity period of a password.
- **Warn before (days):** Specifies when the user/admin is notified that his password will expire.

- **Force changed:** Only affects the User password. When Force changed is activated, the user will be forced to change his/her password at next login. This only applies to users, not to administrators.
- **Tries allowed:** Specifies the maximum number of password entry trials before the password is suspended. Values: 0 (no limits), 2, 3, 4, 5
- **No change for (hours):** Specifies a period before a password is allowed to be changed again. Value range: 0 to 99
- **Suspended for (mins):** Defines how long a password will be suspended after the number of failed retries has exceeded. Value range: 0 to 99
- **History valid for (days):** Defines a period in days during which the history is valid. Passwords no longer used are kept in history lists for the user and admin passwords to prevent reuse of past passwords. This list is organised as FIFO (First In, First Out) so that it always contains the latest passwords.

Administration via WBM

Security and Policies > Password > Generic Policy



Generic policy	
Expires after (days)	99
Warn before (days)	1
Force changed	☐
Tries allowed	5
No change for (hours)	0
Suspended for (mins)	5
History valid for (days)	0
Submit Reset	

3.6.7.2 Display password change prompt

The admin can make the phone prompt the user to change the password immediately. Such a prompt may be triggered by the use of "Force changed" via Admin WBM page or by a similar request by the DLS. It is also possible the appearance of this prompt if the user's password has expired or otherwise has been invalidated. The prompt is shown when the user attempts to use their password. In case the user ignores the prompt and does not change the password, the prompt will be displayed again. Only affects the User password.

NOTICE: This feature can be configured through the administration WBM and the DLS too. For further instructions, see the *General Policy* and *DLS Administration Guide*.

3.6.7.3 Admin Policy

- **Expiry date:** Shows the date and time when the admin password will expire.
- **Minimum length:** Defines the minimum number of characters for the admin password.

- **Password history:** Specifies the number of entries to be kept in the admin password history. New passwords must not match any password in the history.
- **Current status:** Determines the status for the admin password. When set to "Active", the admin password is available for use. With "Suspended", the admin password is not available for a period or until reset. When set to "Disabled", all access via the admin password is disabled. The status of the admin password can only be set via DLS. It is changed internally to "suspended" when the password has been entered incorrectly more times than allowed.

Administration via WBM

Security and Policies > Password > Admin Policy

Admin policy

Expiry date 2038-01-19T03:14:07+00:00

Minimum length 6

Password history 0

Current status Active

Submit Reset

3.6.7.4 Character Set

The composition of the password can be configured in detail.

- **Ucase chars reqd.:** Defines the minimum number of uppercase characters. Value range: 0 to 24
- **Lcase chars reqd.:** Defines the minimum number of lowercase characters. Value range: 0 to 24
- **Digits required:** Defines the minimum number of digits. 0 to 24
- **Special chars reqd:** Defines the minimum number of special characters. The set of possible characters is ` - = [] ; ' # \ , . / ^ ~ ! " Â £ \$ % ^ & * () _ + { } : @ ~ | < > ? Value range: 0 to 24
- **Bar repeat length:** Specifies the maximum number of consecutive uses of a character. Value range: 0 to 24, but not 1 (with 1 set as value, no password would be valid, because it would be forbidden to use any character once).
- **Min char difference:** Specifies the minimum number of characters by which a new password must differ from the previous password. Value range: 0 to 24

Administration via WBM

Security and Policies > Password > Character set

Character set

Ucase chars reqd.	0
Lcase chars reqd.	0
Digits required	0
Special chars reqd	0
Bar repeat length	0
Min char difference	0

Submit

Reset

3.6.7.5 Change Admin and User password

The passwords for user and administrator can be set here. They have to be confirmed after entering. The factory setting for the Admin password is "123456"; it should be changed after the first login (Password handling in previous versions see [Password](#) on page 287).

Administration via WBM

Security and Policies > Password > Change Admin password

Change Admin password

Old password	
New password	
Confirm password	

Submit

Reset

Security and Policies > Password > Change User password

Change User password

Admin password	
New password	
Confirm password	

Submit

Reset

Administration via Local Phone

```
|--- Admin
  |--- Security & policies
    |--- Password
      |--- Change Admin password
        |--- Current password
        |--- New password
        |--- Confirm password
      |--- Change User password
        |--- Admin password
        |--- New password
        |--- Confirm password
```

3.6.8 Certificate Policy

3.6.8.1 Online Certificate Check

The Online Certificate Status Protocol (OCSP) is used to check if a certificate to be used has been revoked. This protocol is used to query an Online Certificate Status Responder (OCSR) at the point when the certificate is being validated. The address of an OCSR can be configured on the phone and can also be obtained from the certificate to be checked (which will have the priority).

- **OCSP check:** If activated, the configured OCSR is requested to check if the certificate has been revoked.
- **OCSR 1 address:** Specifies the IP address (or FQDN) of a primary OCSP responder.
- **OCSR 2 address:** Specifies the IP address (or FQDN) of a secondary OCSP responder which is used in case there is no response from OCSR 1.
- **Confirm 802.1x installation:** When activated, the phone displays a toast notification after all 802.1X certificates have been installed.

Administration via WBM

Security and Policies > Certificates > Generic

Generic	
OCSP check	☐
OCSR 1 address	
OCSR 2 address	
Confirm 802.1x installation	☐
Submit Reset	

3.6.8.2 Server Authentication Policy

For individual certificates provided by specific servers, the level of authentication can be configured. When "None" is selected, no certificate check is performed. With "Trusted", the certificate is only checked against the signature credentials provided by the remote entity for signature, and the expiry date is checked. When "Full" is selected, the certificate is fully checked against the credentials provided by the remote entity for signature, the fields must match the requested subject/usage, and the expiry date is checked.

- Secure file transfer sets the authentication level for the HTTPS server to be used (see [Common FTP/HTTPS Settings \(Defaults\)](#) on page 256).
- Secure send URL sets the authentication level for the server to which special HTTP requests are sent on key press ("Send URL" function, see [Send Request via HTTP/HTTPS](#) on page 211).
- Secure SIP server sets the authentication level for the SIP server connected to the phone (see [SIP Registration](#) on page 120).
- Secure 802.1x sets the authentication level for the 802.1x authentication server.
- LDAP via TLS sets the authentication level for LDAP access.

- Secure DMS server sets the authentication level for a Device Management Server.
- Secure XSI server sets the authentication level for a Broadsoft Extended Server.
- Secure Exchange server
- Secure Circuit server
- Secure E/A Cockpit server
- Secure OpenScape UC server
- Secure auto configuration server sets the authentication level for a TR-069 auto config Server.

Administration via WBM

Security and Policies > Certificates > Authentication policy

Authentication policy	
Secure file transfer	None ▼
Secure send URL	None ▼
Secure SIP server	None ▼
Secure 802.1x server	Trusted ▼
LDAP via TLS	None ▼
Secure DMS server	None ▼
Secure XSI server	None ▼
Secure Exchange server	None ▼
Secure Circuit server	None ▼
Secure E/A Cockpit server	None ▼
Secure OpenScape UC server	None ▼
Secure auto configuration server	None ▼
Submit Reset	

Administration via Local Phone

```

|--- Admin
    |--- Security & policies
        |--- Certificates
            |--- Authentication policy
                |--- Secure file transfer
                |--- Secure send URL
                |--- Secure SIP server
                |--- Secure file transfer
                |--- LDAP via TLS
                |--- Secure DMS server
                |--- Secure XSI server
                |--- Secure Exchange server
                |--- Secure Circuit server
                |--- Secure E/A Cockpit server
                |--- Secure OpenScape UC server
                |--- Secure auto configuration
server
  
```

3.6.8.3 SCEP

SCEP (Simple Certificate Enrollment Protocol) allows automatic provisioning and renewal of certificates on your phone. SCEP server supports only one certificate per device. If there is another request, it is rejected or previous certificate is overwritten, based on server settings. To set up SCEP, the following parameters must be configured:

SCEP

- **Address:** SIP address configured for SCEP.
- **Url:** Name of the Url, e.g.scep.
- **Port** (optional item): Port configured for SCEP, e.g. 8080.
- **Secret** (optional item): Shared Secret is a certificate hash verifying the authenticity of the certificate. CA authenticates the device with shared secret.
- **CA fingerprint (sha1)** (optional item): CA fingerprint is a certificate hash verifying the authenticity of the certificate. Device authenticates the CA with fingerprint. Sha1 encryption is used.
- **Renew before expiry:** The device sends a request for a new certificate a given number of days in advance.

Possible options are:

- 0
- 10
- 20
- 30

Certificate configuration

For certificate generation, **Common (CN)** field is mandatory. The parameters **Country (C)**, **Province (ST)**, **City (L)** and **Organization (O)** are optional and can be configured for customer specific identification.

- **Country (C)**
- **Province (ST)**
- **City (L)**
- **Organization (O)**
- **Common (CN)**
- **Signature algorithm:** Algorithm of the root CA certificate for the SCEP server.

The following options are available:

- SHA256
- SHA512

- **Key length**

The following options are available:

- 1024
- 2048
- 4096

- **Certificate type**

The following options are available:

- None
- SIP / HFA client
- Radius 802.1x

NOTICE: Since HFA V1R6.5.0 and since SIP V1R6.5.0, the following will also be available: DLS client, Https client, LDAP client, BWDMS client.

NOTICE: For the CP700X phone there is also the **WLAN client** option.

- **Action**

The following options are available:

- None
- Enroll
- Renew
- Delete
- Cancel pending
- Assign existing cert

- **Certificate status**

Phone contacts SCEP Gateway and asks for certificate on the following occasions:

- After startup (if there is SCEP configured but no certificate received yet).
- On demand (via the Admin page).
- When certificate expiration date is within configured range.

Certificate renewal

Before making requests for renewal, the phone checks for server capabilities based on the configuration. The following capabilities are mandatory:

- SHA256
- Renew

If server does not support all mandatory capabilities, phone does not attempt to request any certificates.

This is logged as ERROR to trace file and Security log. In case the certificate request was a result of immediate action (On demand), error toast with text **SCEP server does not have required capabilities** is displayed.

After the phone sends a SCEP request, the SCEP server returns CA certificate and fingerprint and the phone checks validity of received CA certificate against the fingerprint. In case validity check fails, phone rejects this certificate and creates an ERROR log in trace file and Security checklist. In case the certificate request was result of immediate action (On demand), error toast with text **Certificate error** is displayed.

NOTICE: For existing certificate, phone asks SCEP server for certificate renewal by updating the existing enrolled certificate with a new one.

NOTICE: In case SCEP returns multiple CA certificates, they all need to be stored in proper location and used in services they belong to.

Once certificate is downloaded, it needs to be copied with correct name for all certificate paths it is supposed to be used. Certificate change is then published to all observing services.

Handling pending status

When the phone sends a request to SCEP server, server can reply with status PENDING. This may mean it is waiting for manual approval from administrator or any other action which prevents it to deploy certificate immediately.

In that case, phone needs to resend enroll request to check whether status has changed. Phone will resend the request in the following intervals (the interval gets longer every time PENDING is returned) : 5min, 10 min, 30min, 1hour, 6 hours, 24hours. If certificate is not provided at the last attempt (after 24 hours), request is no longer sent and Admin must trigger the action again manually.

NOTICE: In case of SCEP server change or replacement, phone certificates deployed by the previous SCEP must be deleted before deployment from the new SCEP server. In case the pending certificate was approved by SCEP admin, phone admin should re-request the certificate enrollment to launch the deployment.

Administration via WBM

Security and Policies > Certificates > SCEP

SCEP	
Address:	
Url:	
Port:	
Secret:	
CA fingerprint (sha1):	
Renew before expiry:	0 ▼
Certificate configuration	
Country (C):	
Province (ST):	
City (L):	
Organization (O):	
Common (CN):	
Signature algorithm:	SHA256 ▼
Key length:	1024 ▼
Certificate type:	None ▼
Action:	None ▼
Certificate status:	
Submit Reset	

Administration via Local Phone

```

|--- Admin
|   |--- Security & policies
|       |--- Certificates
|           |--- SCEP
|               | --- Address
|               | --- Url
|               | --- Port
|               | --- Secret
|               | --- CA fingerprint (sha1)
|               | --- Renew before expiry
|           | --- Certificate configuration
|               | --- Country (C)
|               | --- Province (ST)
|               | --- City (L)
|               | --- Organization (O)
|               | --- Common (CN)
|               | --- Signature algorithm
|               | --- Key length
|               | --- Certificate type
|               | --- Action
|               | --- Certificate status

```

3.7 System Settings

3.7.1 Terminal and User Identity

3.7.1.1 Terminal Identity

Within a SIP environment, both Terminal Number and Terminal Name may serve as a phone identification. The values are used in the userinfo part of SIP URIs.

In order to register with a SIP registrar, the phone sends REGISTER messages to the registrar containing the contents of Terminal number.

Data required

- **Terminal number:** Number to be registered at the SIP registrar.
- **Terminal name:** Name to be registered at the SIP registrar.

Administration via WBM

System > System Identity

Administration via Local Phone

```
|--- Admin
  |--- System
    |--- System Identity
      |--- Terminal number
      |--- Terminal name
      |--- Display identity
      |--- Enable identity
      |--- Web name
      |--- DNS name construction
```

3.7.1.2 Display Identity

If an individual name or number is entered as Display identity and Enable ID is activated, it is displayed in the phone’s status bar instead of the Terminal number.

Administration via WBM

System > System Identity

System Identity

Terminal number

4711

Terminal name

openstage

Display identity

4711

Enable ID

☒

Web name

DNS name construction

Only number ☒

Submit

Reset

Administration via Local Phone

```
|--- Admin
  |--- System
    |--- Identity
      |--- Display identity
      |--- Enable ID
```

3.7.2 Emergency and Voice Mail

It is important to have an Emergency number configured. If the phone is locked, a clickable area is created, which consists of clickable buttons that will be used for making an emergency call.

NOTICE: If more than one emergency number is needed, additional numbers can be configured in the canonical dial settings ([Canonical Dialing Configuration](#) on page 241).

As far as the Voice mail is concerned, if a mailbox located at a remote server shall be used, its Voice mail number must be entered.

Administration via WBM

System > Features > Configuration

General	
Emergency number	3335
Voice mail number	
MWI LED	AlertBar LED ▼
Missed call LED	AlertBar LED ▼
Allow refuse	☒
Hot/Warm phone	No action ▼
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☒
Server features	☐
Not used timeout (minutes)	2 ▼
Transfer on hangup	☐
Bridging enabled	☒
Dial plan enabled	☐
FPK program timer	On ▼
DSS monitored	☐
Show icon for all forwarding types	☐

Administration via Local Phone

```

|--- Admin
|   |--- System
|       |--- Features
|           |--- Configuration
|               |--- General
|                   |--- Emergency number
|                   |--- Voicemail number

```

3.7.3 Energy Saving

3.7.3.1 Backlight Time Setting (OpenScape Desk Phone CP600/600E/700/700X only)

After the phone has been inactive within the timespan specified in Backlight time, the display backlight is switched off to save energy.

The possible values are: 1 minute, 5 minutes, 30 minutes, 60 minutes, 2 hours, 4 hours, or 8 hours. Moreover, this parameter can also be configured by the user. The default value is 1 minute.

Administration via WBM

Local functions > Energy saving

Energy saving	
Backlight time	2 hours ▼
Submit	Reset

Administration via Local Phone

```
|--- Admin
      |--- Local Functions
            |--- Energy saving
                  |--- Backlight time
```

3.7.3.2 Energy Efficient Ethernet (OpenScape Desk Phone CP205/400/600/600E/700/700X only)

The OpenScape Desk Phone CP205/400/600/600E/700/700X phones support the standard IEEE 802.3az (Energy Efficient Ethernet).

The energy saving benefit provided by this standard can only be received when the phone is connected to a network component which also is able to support the IEEE 802.3az standard.

3.7.4 Call logging

This configuration item allows the phone to detect if a number dialled by the User is likely to be a Feature Access Code (FAC) by comparing the start of the dialled number with the configured FAC prefixes. If the dialled number does match a FAC prefix and the SIP server has provided a different number for the called party then the number shown in the Dialed tab list of Call Log is changed from the dialled number to the server provided number. If the new configuration item is left empty then the Dialed tab list display will remain as currently populated (i.e. the dialled number is shown in the list).

A further enhancement for an entry matched to a FAC in the Dialed tab list of Call Log is that the context menu for the list entry now provides both numbers from the last call associated with the entry as Dial options in the context menu for the list entry (similar to that already provided by the context menu for the Details form of such an entry). Note that the Call Log display on OpenScape Desk Phone CP100/200/205 has been simplified so that an entry only displays a name or a number (not both) and there is no access to entry details. However, this only limits the display and the default dialling number for an OpenScape Desk Phone CP100/200/205 entry is determined as above.

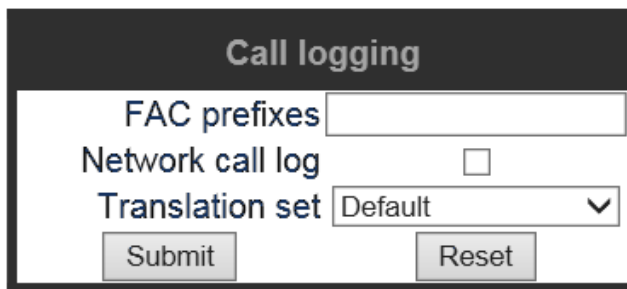
Call Log entry grouping rules for the Dialed tab list remain unchanged, if multiple FACs all map to numbers associated with one contact then they are grouped together.

Data required

- **FAC prefixes:** A comma separated list of feature prefixes considered to represent feature codes configured at the SIP server for abbreviated dialling.
- **Network call log:** BroadSoft feature. The Network directories and the XSI has to be activated.
- **Translation set:** The translation sets is customer non-specific and available for any customer to configure at admin level. More information available in the [Translation set change](#) on page 116.

Administration via WBM

Local functions > Call logging



Call logging

FAC prefixes

Network call log ☐

Translation set

3.7.4.1 Logging of Missed Calls (via User menu)

This feature allows the user to

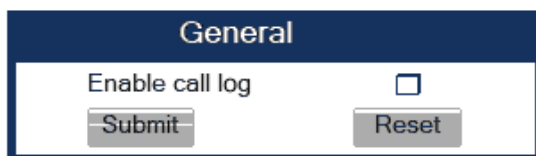
- distinguish logged calls based on the device on which the calls were completed, and
- decide whether missed calls that were answered elsewhere shall be
 - included into the call log, or
 - excluded from the call log, i.e. not logged at all
- decide whether a number which also exists in missed calls tab of call log is to be deleted from call log when this number is called
 - manually
 - when called

In the **Call Lists**, missed calls that were completed elsewhere are marked with a check mark. For details, please refer to the *User manual*.

Forwarded calls are not logged under "Missed calls", but under "Forwarded" in the call log.

Administration via WBM (User menu)

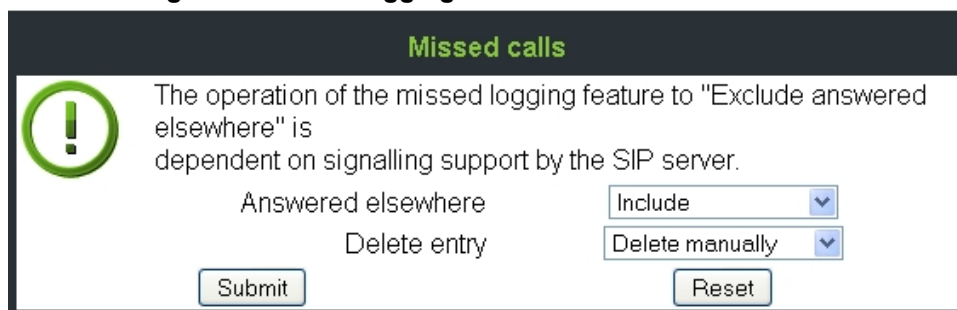
User > Configuration > Call logging > General



General

Enable call log ☐

User > Configuration > Call logging > Missed calls



Missed calls

 The operation of the missed logging feature to "Exclude answered elsewhere" is dependent on signalling support by the SIP server.

Answered elsewhere

Delete entry

Administration via Local Phone (User menu)

```
|--- User
    |--- Configuration
```

```

|--- Call logging
|   |--- General
|       |--- FAC prefixes
|   |--- Missed calls
|       |--- Answered elsewhere
|           |--- Include
|           |--- Exclude
|       |--- Delete entry
|           |--- Manually
|           |--- When called

```

Answered elsewhere > Include: Calls completed elsewhere will be logged as missed calls. In the call log these calls are marked with a check mark.

Answered elsewhere > Exclude: Calls completed elsewhere will not be visible on phone; they will not be logged at all.

Delete entry > Manually: Call numbers remain in call log until they are deleted manually.

Delete entry > When called: Call numbers existing in missed call list are deleted automatically when they are called again.

3.7.4.2 Translation set change

Customer specific translation of 'Conversation' term for CP400/600/600E (Broadsoft only). E.g. 'Call Log' can be used instead of 'Conversation' in a specific environment.

The translation sets is customer non-specific and available for any customer to configure at admin level. A customer can add specific translation to any item. The item mentioned above is an example only.

Access via Local Admin Settings tree:

The path of the configuration item:

Admin > Local functions > Call logging menu.

The label is: "Translation set".

The configuration uses a dropdown configuration screen to choose between multiple preset options (0 - "Default", 1 - "Set 1"). 'Default' means that no dialect is chosen and default translation labels will be used. 'Set 1' means to use special translations to make the chosen screen labels as required.

Access via WBM:

The path of the configuration item:

Admin > Local functions > Call logging menu.

The label is: "Translation set".

The configuration uses a dropdown configuration screen to choose between multiple preset options (0 - "Default", 1 - "Set 1"). 'Default' means that no dialect is chosen and default translation labels will be used. 'Set 1' means to use special translations to make the chosen screen labels as required by customer.

3.7.5 Date and Time

If the DHCP server in your network provides the IP address of the SNTP server, no manual configuration is necessary. If not, you have to set the SNTP IP address parameter manually.

For correct display of the current time, the Timezone offset must be set appropriately. This is the time offset from UTC (Universal Time Coordinated). If, for instance, the phone is located in Munich, Germany, the offset is +1 (or simply 1); if it is located in Los Angeles, USA, the offset is -8. For countries or areas with half-hour time zones, like South Australia or India, non-integer values can be used, for example 10.5 for South Australia (UTC +10:30).

If the phone is located in a country with DST (Daylight Saving Time), you can choose whether DST is toggled manually or automatically. For manual toggling, disable Auto time change and enable or disable Daylight saving; the change will be in effect immediately. For automatic toggling, enable Auto time change; now, daylight saving is controlled by the DST zone / Time zone parameter. This parameter determines when DST starts or ends, and must be set according to the location of the phone.

The Difference (minutes) parameter defines how many minutes the clock is put forward for DST. In Germany, for instance, the value is +60.

NOTICE: Please note that Difference (minutes) must be specified both for manual and automatic DST toggling.

3.7.5.1 SNTP is Available, but no Automatic Configuration by DHCP Server

Data required

- **SNTP IP address:** IP address or hostname of the SNTP server.
- **Timezone offset (hours):** Shift in hours corresponding to UTC.
- **Daylight saving:** Enables or disables daylight saving time in conjunction with Auto time change. Value range: "Yes", "No".
- **Difference (minutes):** Time difference when daylight saving time is in effect.
- **Auto time change / Auto DST:** Enables or disables automatic control of daylight saving time according to the DST zone. Value range: "Yes", "No". Default setting is Yes. After a factory reset, the system will be reset to this value.
- **Time zone/DST zone:** Area with common start and end date for daylight saving time. Value range: "Australia 2007 (ACT, South Australia, Tasmania, Victoria)", "Australia 2007 (New South Wales)", "Australia (Western Australia)", "Australia 2008+ (ACT, New South Wales, South Australia, Tasmania, Victoria)", "Brazil", "Canada", "Canada (Newfoundland)", "Europe (Portugal, United Kingdom)", "Europe (Finland)", "Europe (Rest)", "Mexico", "United States", "New Zealand", "New Zealand (Chatham)". Default setting for **US** is "**United States**". After a factory reset, the system will be reset to this value.

Administration via WBM

Date and Time

Date and time	
Time source	
SNTP primary	192.168.12.1
SNTP backup	172.25.14.51
Timezone offset (hours)	2
Daylight saving	
Daylight saving	☒
Difference (minutes)	60
Auto time change	☒
DST zone	Not set
Submit	Reset

Administration via Local Phone

```
|--- Administration
  |--- Date and Time
    |--- Time source
      |--- SNTP primary
      |--- SNTP backup
      |--- Timezone offset
```

3.7.5.2 No SNTP Server Available

If no SNTP server is available, date and time must be set manually.

NOTICE: The manual setting of time and date is located in the user menu, not in the administrator menu.

3.7.6 SIP Addresses and Ports

3.7.6.1 SIP Addresses

In this group of parameters, the IP addresses or host names for the SIP server, the SIP registrar, and the SIP gateway are defined.

SIP server address provides the IP address or host name of the SIP proxy server (OpenScape Voice). This is necessary for outgoing calls. SIP registrar address contains the IP address or host name of the registration server, to which the phone will send REGISTER messages. When registered, the phone is ready to receive incoming calls. SIP gateway address gives the IP address or host name of the SIP gateway. If configured, the SIP gateway is used for outgoing calls; otherwise the server specified in SIP server address is used. A SIP gateway is able to perform a conversion of SIP to TDM, which enables to send calls directly into the public network.

NOTICE: Enhanced survivability using DNS SRV is available. To make use of it, a special configuration is required. For details, please refer to [Resilience and Survivability](#) on page 136.

Data required

- **SIP server address:** IP address or host name of the SIP proxy server.
- **SIP registrar address:** IP address or host name of the registration server.
- **SIP gateway address:** IP address or host name of the SIP gateway.

Administration via WBM**System > Registration**

Registration	
SIP addresses	
SIP server address	10.12.70.16
SIP registrar address	10.12.70.16
SIP gateway address	0.0.0.0
SIP session	
Session timer enabled	☒
Session duration (seconds)	3600
Registration timer (seconds)	3600
Subscription timer (seconds)	3600
Refresh minimum (seconds)	0
Server type	OS Voice
Realm	realm3
User ID	49897224030
Password	*****
MLPP base	Local
MLPP domain	dsn+uc
Other domain	
SIP survivability	
Backup registration allowed	☒
Backup proxy address	0.0.0.0
Backup registration timer (seconds)	3600
Backup transport	UDP
Backup connection	Listening
Backup OBP flag	☐
Standard CSTA	
Server address	
Server port	5060
E/A Cockpit	
Server address	
Allow server push	☒
Mobility logoff action	None
Submit	Reset

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- Registration
            |--- SIP Addresses
                |--- SIP server
                |--- SIP registrar
                |--- SIP gateway
  
```

3.7.6.2 SIP Ports

In this group of parameters, the ports for the SIP server, the SIP registrar, and the SIP gateway are defined (for further information see [SIP Addresses](#) on page 118), as well as the SIP port used by the phone (SIP local).

Data required

- **SIP server:** Port of the SIP proxy server. Default: 5060.
- **SIP registrar:** Port of the server at which the phone registers. Default: 5060.
- **SIP gateway:** Port of the SIP gateway. Default: 5060.
- **SIP local:** Port used by the phone for sending and receiving SIP messages. Default: 5060.

NOTICE: When changing the SIP Transport protocol from UDP/TCP to TLS, the SIP port now also have to be changed correspondingly (e.g. SIP port from 5060 to 5061) and on changing vice versa.

Administration via WBM

Network > Port configuration

Port number configuration	
SIP server	5060
SIP registrar	5060
SIP gateway	5060
SIP local	5060
Backup proxy	5060
RTP base	5010
LDAP server	389
Submit Reset	

Administration via Local Phone

```
|--- Admin
  |--- Network
    |--- Port Configuration
      |--- SIP server
      |--- SIP registrar
      |--- SIP gateway
      |--- SIP local
```

3.7.7 SIP Registration

Registration is the process by which centralized SIP Server/Registrars become aware of the existence and readiness of an endpoint to make and receive calls. The phone supports a number of configuration parameters to allow this to

happen. Registration can be authenticated or un-authenticated depending on how the server and phone is configured.

For operation with an OpenScape Voice server, set Server type to "OS Voice". When HiQ8000 is to be used, set it to "HiQ8000". The expiry time of a registration can be specified by Registration timer.

Unauthenticated Registration

For unauthenticated registration, the following parameters must be set on the phone: Terminal number or Terminal name (see [Terminal Identity](#) on page 111), SIP server and SIP registrar address (see [SIP Addresses](#) on page 118).

In unauthenticated mode, the server must pre-authenticate the user. This procedure is server specific and is not described here.

Authenticated Registration

The phone supports the digest authentication scheme and requires some parameters to be configured in addition to those for unauthenticated registration. By providing a User ID and a Password that match a corresponding account on the SIP registrar, the phone authenticates itself. Optionally, a Realm can be specified, defining the protection domain where SIP authentication is valid. Each protection domain is globally unique, with its own set of usernames and passwords.

NOTICE: A challenge from the server for authentication information is not only restricted to the REGISTER message, but can also occur in response to other SIP messages, e. g. INVITE.

NOTICE:

If registration fails at startup or after a previously successful registration, the phone will attempt to re-register every 30 seconds.

If the registration request receives no response, the phone will retry every 60 seconds by default. This interval is configurable (see [Maximum Registration Backoff Timer](#) on page 141).

Data required

- **Registration timer (seconds):** Expiry time of the registration in seconds.
Default value: 3600.
- **Server type:** Type of the server the phone will register to. Value range: "Other", "OS Voice", "HiQ8000", "Genesys", "Broadsoft", "Google Voice", "Ring Central".
Default value: "OS Voice"
- **Realm:** Protection domain for authentication.
- **User ID:** Username required for an authenticated registration.
- **Password:** Password required for an authenticated registration.

- **Subscription timer (seconds):** Expiry time of subscription in seconds.

Default value: 3600.

Range: 60-7200

Server type: Available for all server types

Administration via WBM

System > Registration

Registration

SIP Addresses

SIP server address: 192.168.1.165
SIP registrar address: 192.168.1.165
SIP gateway address:

SIP Session

Session timer enabled: ☐
Session duration (seconds): 3600
Registration timer (seconds): 3600
Refresh minimum (seconds): 0
Server type: RingCentral
Realm:
User ID:
Password:
MLPP base: Local
MLPP Domain: dsn+uc
Other Domain:

SIP Survivability

Backup registration allowed: ☐
Backup proxy address:
Backup registration timer (seconds): 3600
Backup transport: UDP
Backup connection: Persistent (SB)
Backup OBP flag: ☒
Submit Reset

3.7.7.1 Re-registration timer

For REGISTER event, the “expires time” must be configurable by a “guard time”. The “expires time” is provided by the SIP server in its response to a REGISTER request by the phone. The SIP standard states that the devices can refresh from half of the expires time to the end. If the answer from SIP server is a refresh time of 600 sec. this means the devices can send the refresh after 300 sec up to 600 sec later.

“Guard time” can be configured on the phone in order to reduce the refresh time using the “Refresh minimum” setting.

In the previous case, if the answer from SBC is 600 sec. and the guard time is 15 sec. the refresh from device will sent between 585 sec (600-15) and 600 seconds after previous registration.

In case of SUBSCRIBE for every event or group of events (the same type), the Subscription refresh time is also configured by the guard time.

Administration via WBM

The new data item is Admin controlled, but also part of the User profile for mobility. It is not changeable during a call.

System > Registration > SIP session

SIP Session	
Session timer enabled	☐
Session duration (seconds)	3600
Registration timer (seconds)	3600
Refresh minimum (seconds)	0
Server type	OS Voice
Realm	
User ID	
Password	
MLPP base	Local
MLPP Domain	dsn+uc
Other Domain	

3.7.8 SIP Communication

3.7.8.1 Outbound Proxy

If this option is set to "Yes", the phone routes outbound requests to the configured proxy. The outbound proxy will fulfill the task of resolving the domain contained in the SIP request. If "No" is set, the phone will attempt to resolve the domain by itself.

If a Default OBP (Outbound Proxy checkbox) domain is set and the number or name dialed by the user does not provide a domain, this value will be appended to the name or number. Otherwise, the domain of the outbound proxy will be appended.

Data required

- **Outbound proxy:** Determines whether an outbound proxy is used or not. Value range: "Yes", "No" Default: "Yes"; when System > Registration > Server type is set to "HiQ8000" (firmware version V3 onwards): "Yes"
- **Default OBP domain:** Alternative value for the domain that is given in the outbound request.

Administration via WBM

System > SIP interface

SIP interface

Outbound proxy

☐

Default OBP domain

SIP transport

UDP

SIP connection

Persistent (SB)

TLS renegotiation

Secure (RFC5746)

Call transaction response timer (ms)

32000

NoCall transaction response timer (ms)

32000

Reg. backoff (seconds)

60

Connectivity check timer (seconds)

0

Keep alive format

Sequence

Media Negotiation

Single IP

Media IP Mode

IPv4

Early 183 response

☐

Keep resolved DNS records

☐

Prefer FROM header for display name

☐

DNS-SRV fallback on re-registration

☐

Submit

Reset

Administration via Local Phone

```
|--- Admin
  |--- System
    |--- SIP Interface
      |--- Outbound proxy
      |--- Default OBP domain
```

3.7.8.2 SIP Transport Protocol

Selects the transport protocol to be used for SIP messages. The values "UDP", "TCP", and "TLS" are available. The default is "UDP"; default when **System > Registration > Server type** is set to "HiQ8000" (firmware version V3 onwards): "TLS".

Administration via WBM

System > SIP interface

SIP interface	
Outbound proxy	☐
Default OBP domain	
SIP transport	UDP
SIP connection	Persistent (SB)
TLS renegotiation	Secure (RFC5746)
Call transaction response timer (ms)	32000
NoCall transaction response timer (ms)	32000
Reg. backoff (seconds)	60
Connectivity check timer (seconds)	0
Keep alive format	Sequence
Media Negotiation	Single IP
Media IP Mode	IPv4
Early 183 response	☐
Keep resolved DNS records	☐
Prefer FROM header for display name	☐
DNS-SRV fallback on re-registration	☐
Submit Reset	

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- SIP Interface
            |--- SIP transport
  
```

3.7.8.3 SIP connection

When using persistent connections the phone is always acting as connection client, no listening port gets opened to allow incoming connection attempts.

A Persistent connection for SIP-TCP will result in only a single client connection to the SIP server — the SIP server will reuse the available TCP connection for sending SIP requests to the phone (like at SIP-TLS).

Persistent (SB) means persistent connection with Switchback.

Value range: "Listening", "Persistent (SB)" Default: "Persistent (SB)"

Administration via WBM

System > SIP interface

SIP interface

Outbound proxy

☐

Default OBP domain

SIP transport

UDP

SIP connection

Persistent (SB)

TLS renegotiation

Secure (RFC5746)

Call transaction response timer (ms)

32000

NoCall transaction response timer (ms)

32000

Reg. backoff (seconds)

60

Connectivity check timer (seconds)

0

Keep alive format

Sequence

Media Negotiation

Single IP

Media IP Mode

IPv4

Early 183 response

☐

Keep resolved DNS records

☐

Prefer FROM header for display name

☐

DNS-SRV fallback on re-registration

☐

Submit

Reset

Administration via Local Phone

```
|--- Admin
  |--- System
    |--- SIP Interface
      |--- SIP connection
```

3.7.8.4 Failover on SIP 5XX server response

An administrator can make the phone failover to the next SRV priority IP on 500/503 server responses, so that the users can continue to use their desk phones on temporary issues. The failover will happen when there is NO! response from the current connected remote end but the DNS-SRV query has revealed at least 1 more IPs that the phone can connect to.

Administration via WBM:

Administrator can activate the functionality locally on the device, WBM or via DLS. The path is:

System > SIP interface.

Set "Failover on" to "Timeout and Error".

SIP interface

Outbound proxy	☐
Default OBP domain	
SIP transport	TCP ▼
SIP connection	Listening ▼
TLS renegotiation	Secure (RFC5746) ▼
Failover on	timeout only ▼
Event check-sync	timeout only ▼
Call transaction response timer (ms)	3000
NonCall transaction response timer (ms)	32000
Reg. backoff (seconds)	60
Connectivity check timer (seconds)	15
Keep alive format	Sequence ▼
Media negotiation	Single IP ▼
Media IP mode	IPv4 ▼
Early 183 response	☐
Keep resolved DNS records	☐
Prefer FROM header for display name	☐
DNS-SRV fallback on re-registration	☐
Submit	Reset

NOTICE: The following criteria must be fulfilled in order to failover to the next SRV priority on a 500 or 503 error response:

- Failover on" is set to "Timeout and Error"
- The Desk Phone CP device has a valid DNS-SRV configuration
- At least 1 IP discovered via DNS-SRV is not blacklisted
- The Desk Phone CP device has sent any SIP request

When receiving a 500 or 503 error response on a SIP request (with "Failover on" set to "Timeout and Error"), the phone will failover immediately without taking any timers into account (e.g. transaction timer).

NOTICE: All other functionality regarding survivability remains untouched from this enhancements, e.g.

- Blacklisting IPs if unreachable or replied with a SIP 500 or 503 error code (Penalty Box management)
- Fallback after IPs removed from blacklist
- Survivability event packages

3.7.8.5 Media/SDP

OpenScape Desk Phone CP phones support IPv4/IPv6 media address negotiation in SDP using ANAT (Alternative Network Address Types). ANAT

allows for for the expression of alternative network addresses (e. g., different IP versions) for a particular media stream.

When Media negotiation is set to "ANAT", ANAT is supported; the phone will re-register with the SIP server and advertise ANAT support in the SIP header. When set to "Single IP", ANAT support is disabled.

NOTICE: If SRTP is enabled, ANAT interworking is only possible if SDES is configured as the key exchange protocol for SRTP (see [System](#) on page 93).

Media IP mode defines which IP version is to be used for voice transmission. With "IPv4", only IPv4 is used; with "IPv6", only IPv6 is used; with "IPv4_IPv6", both IPv4 and IPv6 can be used, but IPv4 is preferred; with "IPv6_IPv4", both IPv6 and IPv4 can be used, but IPv6 is preferred.

Administration via WBM

System > SIP interface

SIP interface

Outbound proxy

☐

Default OBP domain

SIP transport

UDP

SIP connection

Persistent (SB)

TLS renegotiation

Secure (RFC5746)

Call transaction response timer (ms)

32000

NoCall transaction response timer (ms)

32000

Reg. backoff (seconds)

60

Connectivity check timer (seconds)

0

Keep alive format

Sequence

Media Negotiation

Single IP

Media IP Mode

IPv4

Early 183 response

☐

Keep resolved DNS records

☐

Prefer FROM header for display name

☐

DNS-SRV fallback on re-registration

☐

Submit

Reset

Administration via Local Phone

```
|--- Admin
  |--- System
    |--- SIP Interface
      |--- Media negotiation
      |--- Media IP mode
```

3.7.8.6 Early 183 response

If **True**, in response to an initial SDP offer in a SIP INVITE the phone will generate a SIP 183 response that includes an SDP answer with all the attributes that will be provided in a subsequent 200 OK.

If **False**, the phone will not generate a SIP 183 response, with early SDP answer, to a SIP INVITE.

Administration via WBM

System > SIP interface

SIP interface	
Outbound proxy	☐
Default OBP domain	
SIP transport	UDP
SIP connection	Persistent (SB)
TLS renegotiation	Secure (RFC5746)
Call transaction response timer (ms)	32000
NoCall transaction response timer (ms)	32000
Reg. backoff (seconds)	60
Connectivity check timer (seconds)	0
Keep alive format	Sequence
Media Negotiation	Single IP
Media IP Mode	IPv4
Early 183 response	☐
Keep resolved DNS records	☐
Prefer FROM header for display name	☐
DNS-SRV fallback on re-registration	☐
Submit Reset	

Administration via Local Phone

```
|--- Admin
    |--- System
        |--- SIP Interface
            |--- Early 183 response
```

3.7.8.7 Keep resolved DNS records

If this option is set to True, when there is a negative DNS answer while trying to establish a SIP connection, the previous successful DNS records are used until the next successful DNS lookup. This will allow the user to place calls when there is a DNS server issue.

NOTICE: There must be at least one successful DNS lookup where the phone can keep and use the DNS records for the

future work. After a device reboot, DNS records are not retained and there will be a new lookup.

Since this option is set to False (default option), the DNS records will not be retained. Every attempt to resolve an IP address has to be successful in order to establish a SIP connection.

Administrator can activate the functionality locally on the device, WBM or via DLS.

Administration via WBM

Administrator settings > System > SIP interface

SIP interface

Outbound proxy

☐

Default OBP domain

SIP transport

UDP

SIP connection

Persistent (SB)

TLS renegotiation

Secure (RFC5746)

Call transaction response timer (ms)

32000

NoCall transaction response timer (ms)

32000

Reg. backoff (seconds)

60

Connectivity check timer (seconds)

0

Keep alive format

Sequence

Media Negotiation

Single IP

Media IP Mode

IPv4

Early 183 response

☐

Keep resolved DNS records

☐

Prefer FROM header for display name

☐

DNS-SRV fallback on re-registration

☐

Submit

Reset

Administration via Local Phone

```
|--- Administrator settings
  |--- System
    |--- SIP Interface
      |--- Keep resolved DNS records
```

3.7.8.8 Prefer FROM header

If this option is set to True, the phone display will use the information provided by the "FROM Header" field. In any other case (not activated) the display information will be provided by the "P-Asserted-id Header" (PAI Header). By default, the feature is disabled.

Administration via WBM:

System > SIP interface

SIP interface	
Outbound proxy	☐
Default OBP domain	
SIP transport	UDP
SIP connection	Persistent (SB)
TLS renegotiation	Secure (RFC5746)
Call transaction response timer (ms)	32000
NoCall transaction response timer (ms)	32000
Reg. backoff (seconds)	60
Connectivity check timer (seconds)	0
Keep alive format	Sequence
Media Negotiation	Single IP
Media IP Mode	IPv4
Early 183 response	☐
Keep resolved DNS records	☐
Prefer FROM header for display name	☐
DNS-SRV fallback on re-registration	☐
Submit Reset	

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- SIP Interface
            |--- Prefer FROM header for display name
  
```

3.7.8.9 DNS-SRV fallback on re-registration

If this option is set to True and SBC server is used, the phone sends an INVITE message directly to the SBC where it is registered while doing re-registration (DNS-SRV fallback), and not to the primary SBC first.

If **False**, the phone will always try to reconnect to the primary SBC when doing re-registration. If the attempt is not successful, the call succeeds through the secondary SBC since the phone has already registered.

Blacklisted IPs will remain blacklisted, unless there is a re-registration attempt.

Administration via WBM:

Administrator can activate the functionality locally on the device, WBM or via DLS.

System > SIP interface

SIP interface

Outbound proxy

Default OBP domain

SIP transport

SIP connection

TLS renegotiation

Failover on

Event check-sync

Call transaction response timer (ms)

NoCall transaction response timer (ms)

Reg. backoff (seconds)

Connectivity check timer (seconds)

Keep alive format

Media Negotiation

Media IP Mode

Early 183 response

Keep resolved DNS records

Prefer FROM header for display name

DNS-SRV fallback on re-registration

☐

UDP

Persistent (SB)

Secure (RFC5746)

timeout only

challenge

32000

32000

60

0

Sequence

Single IP

IPv4

☐

☐

☐

☐

Submit

Reset

```
Administration via Local Phone
|--- Administrator settings
|   |--- System
|       |--- SIP Interface
|           |--- DNS-SRV fallback on re-registration
```

3.7.8.10 Support provisional response (PRACK)

If this option is set to True, the phone indicates and supports provisional responses in outgoing INVITE requests. Header contains "100rel" to indicate the support.

Default value is 'True'.

Administration via WBM:

Administrator can activate the functionality locally on the device, WBM or via DLS.

System > SIP interface

SIP interface	
Outbound proxy	☐
Default OBP domain	
SIP transport	TCP
SIP connection	Listening
TLS renegotiation	Secure (RFC5746)
Failover on	timeout only
Event check-sync	challenge
Call transaction response timer (ms)	6000
NonCall transaction response timer (ms)	6000
Ringing state termination timer (seconds)	600
Reg. backoff (seconds)	60
Connectivity check timer (seconds)	90
Subscription failure retry timer (seconds)	180
Keep alive format	Sequence
Media negotiation	Single IP
Media IP mode	IPv4_IPv6
Early 183 response	☐
Keep resolved DNS records	☐
Prefer FROM header for display name	☐
DNS-SRV fallback on re-registration	☐
Support provisional response (PRACK)	☒
Send all codecs in SDP answer	☒
Submit	Reset

Administration via Local Phone

```

|--- Administrator settings
    |--- System
        |--- SIP Interface
            |--- Support provisional response
                (PRACK)
  
```

3.7.8.11 Send all codecs in SDP answer

If this option is set to True, the phone includes all supported (enabled) audio codecs in an SDP answer.

If set to 'False', the phone includes the negotiated audio codec in an SDP answer. The audio codecs that are affected are:

- PCMU
- PCMA
- G722
- G729
- OPUS

NOTICE: DTMF events codec type (101) and video codecs are not affected.

Default value is 'True'.

Administration via WBM:

Administrator can activate the functionality locally on the device, WBM or via DLS.

System > SIP interface

SIP interface

☐

Outbound proxy

Default OBP domain

SIP transport

TCP

SIP connection

Listening

TLS renegotiation

Secure (RFC5746)

Failover on

timeout only

Event check-sync

challenge

Call transaction response timer (ms)

6000

NonCall transaction response timer (ms)

6000

Ringing state termination timer (seconds)

600

Reg. backoff (seconds)

60

Connectivity check timer (seconds)

90

Subscription failure retry timer (seconds)

180

Keep alive format

Sequence

Media negotiation

Single IP

Media IP mode

IPv4_IPv6

Early 183 response

☐

Keep resolved DNS records

☐

Prefer FROM header for display name

☐

DNS-SRV fallback on re-registration

☐

Support provisional response (PRACK)

☒

Send all codecs in SDP answer

☒

Submit

Reset

```
Administration via Local Phone
|--- Administrator settings
|   |--- System
|       |--- SIP Interface
|           |--- Send all codecs in SDP answer
```

3.7.9 SIP Session Timer

Session timers provide a basic keep-alive mechanism between 2 user agents or phones. This mechanism can be useful to the endpoints concerned or for stateful proxies to determine that a session is still alive. This is achieved by the phone sending periodic re-INVITES to keep the session alive. If no re-INVITE is received before the interval passes, the session is considered terminated. Both phones are supposed to terminate the call, and stateful proxies can remove any state for the call.

This feature is sufficiently backward compatible such that only one end of a call needs to implement the SIP extension for it to work.

The parameter Session timer enabled determines whether the mechanism shall be used, and Session duration (seconds) sets the expiration time, and thus the interval between refresh re-INVITES.

NOTICE: Some server environments support their own mechanism for auditing the health of a session. In these cases, the Session timer must be deactivated. For OpenScape Voice, the Session timer should be deactivated.

Data required

- **Session timer enabled:** Activates or deactivates the session timer mechanism. Value range: "Yes", "No" Default value: "No"
- **Session duration (seconds):** Sets the expiration time for a SIP session. Default: 3600

Administration via WBM**System > Registration**

Registration	
SIP Addresses	
SIP server address	192.168.1.165
SIP registrar address	192.168.1.165
SIP gateway address	
SIP Session	
Session timer enabled	☐
Session duration (seconds)	3600
Registration timer (seconds)	3600
Server type	OS Voice
Realm	
User ID	
Password	
MLPP base	Local
MLPP Domain	dsn+uc
Other Domain	
SIP Survivability	
Backup registration allowed	☐
Backup proxy address	
Backup registration timer (seconds)	3600
Backup transport	UDP
Backup connection	Persistent (SB)
Backup OBP flag	☒
Submit	Reset

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- Registration
            |--- SIP session
                |--- Session timer
                |--- Session duration
  
```

3.7.10 Resilience and Survivability

To allow for stable operation even in case of network or server failure, OpenScape Desk Phone CP100/200/205/400/600/600E phones have the capability of switching to a fallback system. The switchover is controlled by various configurable check and timeout intervals.

Survivability is achieved in two different ways:

- 1) DNS SRV can be used for enhanced survivability, either in a scenario with a survivability proxy, or in a scenario with multiple primary SIP servers. The DNS server provides the phone with a prioritized list of SIP servers via DNS SRV. The phone fetches this list periodically from the server, depending on the TTL (time to live) specified for the DNS SRV records.
- 2) To enable DNS SRV requests from the phone, please make the following settings:
 - For a scenario with multiple "primary" SIP servers enter the corresponding DNS SRV domain name under SIP server and SIP registrar and set the SIP server and SIP registrar ports to 0. The web interface paths are specified in "System > Registration > SIP server address/SIP registrar address" and "Network > Port configuration > SIP server/SIP registrar". For details, see [SIP Addresses](#) on page 118 and [SIP Ports](#) on page 120.
 - For a scenario with a survivability proxy enable the use of an outbound proxy for routing outbound requests. The web interface path is System > SIP interface > Outbound proxy. For details, see [Outbound Proxy](#) on page 123.

Enter the DNS SRV domain name as SIP gateway address and set the SIP gateway port to 0. The web interface paths are "System > Registration > SIP gateway address" and "Network > Port configuration > SIP gateway". For details, see [SIP Addresses](#) on page 118 and [SIP Ports](#) on page 120.

NOTICE: Depending on the solution design the values for the SIP server and SIP registrar settings for a scenario with a survivability proxy "enabled" could be a standard DNS name, a DNS SRV name or an IP and should reflect the corresponding SIP domain from the primary SIP Server(s).

A survivability proxy acts as a relay between the phone and the primary SIP server. Thus, the address of the survivability proxy is specified as gateway or SIP server at the phone (see [SIP Registration](#) on page 120). When the TCP/TLS connection between the survivability proxy and the SIP server breaks down, e. g. because of server failure, the survivable proxy itself acts as a replacement for the primary SIP server. Vice versa, in case the phone can not reach the survivability proxy itself, it will register directly with the primary SIP server, provided that it is specified in the DNS SRV server list.

The survivability proxy notifies the phone whenever the survivability changes, so it can indicate possible feature limitations to the user. Furthermore, to enhance survivability, the phone will be kept up-to-date about the current survivability state even after a restart.

Another way to realize survivability is the use of multiple, geographically separated SIP servers. Normally, the phone is registered with that server that has the highest priority in the DNS SRV server list. If the highest priority

server fails to respond to the TCP/TLS connectivity check or SIP messages (see [TLS Connectivity Check](#) on page 137), the phone will register with the server that has the second highest priority. The availability will be verified continuously in the background when using TLS or TCP as SIP transport protocol via an ongoing connectivity-check. See [TLS Connectivity Check](#) on page 137 for TLS connectivity check and [TCP Connectivity Check](#) on page 138 for TCP connectivity check.

- 3) Use of a Backup SIP Server. Along with the registration at the primary SIP server, the phone is registered with a backup SIP server. In normal operation, the phone uses the primary server for outgoing calls. If the phone detects that the connection to the primary SIP server is lost, it uses the backup server for outgoing calls. This connection check is realized by 2 timers; for details, see [Response Timer](#) on page 139 and [Non-INVITE Transaction Timer](#) on page 140. For configuring the backup server, please refer to [Backup SIP Server](#) on page 142.

NOTICE: In survivability mode, some features will presumably not be available. The user will be informed by a message in the Call View display.

3.7.10.1 TLS Connectivity Check

A regular check ensures that the TLS link to the main SIP server is active. When the Connectivity check timer is set to a non-zero value, test messages will be sent at the defined interval. If the link is found to be dead, the phone uses DNS SRV to find another SIP server. Certainly, the DNS SRV records must be properly configured in the DNS server. Value range: 0 (off), and 10 to 3600 sec.

If no other primary SIP server is found via DNS SRV, the phone will switch over to a backup server for making receiving calls. For configuring the backup server, please refer to [Backup SIP Server](#) on page 142.

There are three different mechanisms for the phone to do the continuous connectivity check in the background. Sequence (a proprietary mechanism), CRLF and TCP keep-alive.

For Sequence or CRLF mechanism, the SIP server needs to add “connectivity-check” to the Server header in the response to a registration request. Both mechanisms will send payload via the established connection to verify the connectivity.

If the SIP server does not add “connectivity-check” to the Server header, the phone will use standard TCP keep-alive messages. Those messages do not contain payload and are done on TCP socket level.

Administration via WBM

System > SIP interface

SIP interface	
Outbound proxy	☐
Default OBP domain	
SIP transport	UDP v
SIP connection	Persistent (SB)
TLS renegotiation	Secure (RFC5746)
Call transaction response timer (ms)	32000
NoCall transaction response timer (ms)	32000
Reg. backoff (seconds)	60
Connectivity check timer (seconds)	0
Keep alive format	Sequence v
Media Negotiation	Single IP v
Media IP Mode	IPv4 v
Early 183 response	☐
Keep resolved DNS records	☐
Prefer FROM header for display name	☐
DNS-SRV fallback on re-registration	☐
Submit Reset	

3.7.10.2 TCP Connectivity Check

A regular check ensures that the TCP link to the main SIP server is active. When the Connectivity check timer is set to a non-zero value, TCP keep live messages will be sent at the defined interval. If the link is found to be dead, the phone uses DNS SRV to find another SIP server. Certainly, the DNS SRV records must be properly configured in the DNS server. Value range: 0 (off), and 10 to 3600 sec.

The same mechanisms as described in [TLS Connectivity Check](#) on page 137, also apply for "TCP connectivity check".

If no other primary SIP server is found via DNS SRV, the phone will switch over to a backup server for making receiving calls. For configuring the backup server, please refer to [Backup SIP Server](#) on page 142.

Administration via WBM

System > SIP interface

SIP interface	
Outbound proxy	☐
Default OBP domain	
SIP transport	UDP v
SIP connection	Persistent (SB) v
TLS renegotiation	Secure (RFC5746) v
Call transaction response timer (ms)	32000 v
NoCall transaction response timer (ms)	32000 v
Reg. backoff (seconds)	60 v
Connectivity check timer (seconds)	0 v
Keep alive format	Sequence v
Media Negotiation	Single IP v
Media IP Mode	IPv4 v
Early 183 response	☐
Keep resolved DNS records	☐
Prefer FROM header for display name	☐
DNS-SRV fallback on re-registration	☐
Submit Reset	

3.7.10.3 Response Timer

The Call transaction response timer is started whenever the phone sends a new INVITE message to the SIP server.

If the call transaction timer expires before the phone gets a response from the SIP server, the phone assumes that the server had died and then attempts to contact the backup server, if configured. If there is no backup server configured, the phone just tidies up internally.

The data is given in milliseconds. The default value is 32 000; for OpenScape Voice, the recommended setting is 3.7 seconds (3700 ms).

Administration via WBM

System > SIP interface

SIP interface

Outbound proxy

☐

Default OBP domain

SIP transport

UDP

SIP connection

Persistent (SB)

TLS renegotiation

Secure (RFC5746)

Call transaction response timer (ms)

32000

NoCall transaction response timer (ms)

32000

Reg. backoff (seconds)

60

Connectivity check timer (seconds)

0

Keep alive format

Sequence

Media Negotiation

Single IP

Media IP Mode

IPv4

Early 183 response

☐

Keep resolved DNS records

☐

Prefer FROM header for display name

☐

DNS-SRV fallback on re-registration

☐

Submit

Reset

Administration via Local Phone

```
|--- Admin
  |--- System
    |--- SIP Interface
      |--- Call trans. (ms)
```

3.7.10.4 Non-INVITE Transaction Timer

The NonCall transaction response timer is started whenever the phone sends a non-INVITE message to the SIP server. If the timer expires before the phone gets a response from the SIP server, the phone assumes that the server had died and then attempts to contact the backup server, if configured. If no backup server is configured, the phone will just tidy up internally.

The data is given in milliseconds. The default value is 32 000; for OpenScape Voice, the recommended setting is 6 seconds (6000 ms).

Administration via WBM

System > SIP interface

SIP interface	
Outbound proxy	☐
Default OBP domain	
SIP transport	UDP
SIP connection	Persistent (SB)
TLS renegotiation	Secure (RFC5746)
Call transaction response timer (ms)	32000
NoCall transaction response timer (ms)	32000
Reg. backoff (seconds)	60
Connectivity check timer (seconds)	0
Keep alive format	Sequence
Media Negotiation	Single IP
Media IP Mode	IPv4
Early 183 response	☐
Keep resolved DNS records	☐
Prefer FROM header for display name	☐
DNS-SRV fallback on re-registration	☐
Submit Reset	

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- SIP Interface
            |--- NonCall transactions (ms)
  
```

3.7.10.5 Maximum Registration Backoff Timer

If a registration attempt should result in a timeout, the phone waits a random time before sending another REGISTER message. The Reg. backoff (seconds) parameter determines the maximum waiting time.

Administration via WBM

System > SIP interface

SIP interface

Outbound proxy

☐

Default OBP domain

SIP transport

UDP

SIP connection

Persistent (SB)

TLS renegotiation

Secure (RFC5746)

Call transaction response timer (ms)

32000

NoCall transaction response timer (ms)

32000

Reg. backoff (seconds)

60

Connectivity check timer (seconds)

0

Keep alive format

Sequence

Media Negotiation

Single IP

Media IP Mode

IPv4

Early 183 response

☐

Keep resolved DNS records

☐

Prefer FROM header for display name

☐

DNS-SRV fallback on re-registration

☐

Submit

Reset

Administration via Local Phone

```
|--- Admin
  |--- System
    |--- SIP Interface
      |--- Reg. backoff
```

3.7.10.6 Backup SIP Server

The Backup registration allowed flag indicates whether or not the phone treats the backup proxy server as a SIP registrar. If set to "Yes", the phone tries to register its SIP address with the server whose IP address or hostname is specified by Backup proxy address. Once an IP address has been entered, the SIP-UDP Port is opened, even if SIP-TLS is used for the OS Voice connection.

The Backup registration timer determines the duration of a registration with the backup SIP server.

The Backup transport option displays the current transport protocol used to carry SIP messages to the Backup proxy server.

The Backup OBP flag indicates whether or not the Backup proxy server is used as an outbound proxy.

Data required

- **Backup registration allowed / Backup registration flag:** Determines whether or not the backup proxy is used as a SIP Registrar. Value Range: "Yes", "No" Default: "Yes"
- **Backup proxy address:** IP address or hostname of the backup proxy server.

- **Backup registration timer:** Expiry time of the registration in seconds. Default: 3600
- **Backup transport:** Transport protocol to be used for messages to the backup proxy. Value range: "TCP", "UDP" Default: "UDP"
- **Backup Connection:** SIP connection type of the Backup Connection (Listening or Persistent with Switchback). More information see [SIP connection](#) on page 125. Value range: "Listening", "Persistent (SB)" Default: "Persistent (SB)"
- **Backup OBP flag:** Determines whether or not the backup proxy is used as an outbound proxy. Value range: "Yes", "No" Default: "No"
- **Network > Port Configuration > Backup proxy:** Port of the backup proxy server. Default: 5060

Administration via WBM

System > Registration

Registration	
SIP Addresses	
SIP server address	192.168.1.165
SIP registrar address	192.168.1.165
SIP gateway address	
SIP Session	
Session timer enabled	☐
Session duration (seconds)	3600
Registration timer (seconds)	3600
Server type	OS Voice
Realm	
User ID	
Password	
MLPP base	Local
MLPP Domain	dsn+uc
Other Domain	
SIP Survivability	
Backup registration allowed	☐
Backup proxy address	
Backup registration timer (seconds)	3600
Backup transport	UDP
Backup connection	Persistent (SB)
Backup OBP flag	☒
Submit Reset	

Network > Port configuration

Port configuration	
SIP server	5060
SIP registrar	5060
SIP gateway	5060
SIP local	5060
Backup proxy	5060
RTP base	5010
Download server (default)	21
LDAP server	389
HTTP proxy	0
LAN port status	100 Mbps half duplex
LAN port speed	Any
PC port status	Link down
PC port speed	Any
PC port mode	disabled
PC port autoMDIX	☐
Submit Reset	

3.7.11 Interactive Connectivity Establishment (ICE)

ICE arguments in the SDP are sent to negotiate media with the purpose of improving the availability of the phone to establish a media connection (audio and video) from a peer device. For ICE to provide this improvement both peers must support ICE.

ICE works by adding to the SDP several candidate addresses by which the peer device may contact the phone.

ICE is used to provide a direct media connection between Circuit clients and the phone.

NOTICE: ICE Lite is also supported, according to [Section 8.2 of RFC 5245](#). The phone continues to use its Full ICE implementation to work with the ICE Lite implementation on Google Voice server.

3.7.11.1 General

- **Enabled:** Lets the phone include ICE attributes in an SDP offer and provide ICE attributes in an SDP answer to an SDP offer that included ICE attributes for subsequent calls.
- **Update SDP allowed:** Indicates that the phone will generate an updated SDP offer/answer as required by the ICE standard.

- **TURN IP mapping:** The TURN server will provide an address mapping between IPv4 and IPv6 peer endpoints. In other case (not activated) only endpoints supporting the required IP family may be addressed.

Administration via WBM

System > ICE > General

Administration via Local Phone

```
|--- Administration
    |--- System
        |--- ICE
            |--- General
                |--- Enabled
                |--- Update SDP allowed
                |--- TURN IP mapping
```

3.7.11.2 Addressing

- **Main server:** Select **None**, if no ICE server is used, **STUN** if the ICE servers are both STUN servers and will only return Server reflexive candidates, or **TURN** if the ICE servers are both TURN servers and will return Relayed and Server reflexive candidates.
- **Main address:** Address of the ICE server.
- **Main port:** Port of the ICE server.
- **Main username:** Username for authentication with the ICE server.
- **Main password:** Password for authentication with the ICE server.
- **Backup server:** Select **None**, if no Backup ICE server is used, **STUN** if the ICE servers are both STUN servers and will only return Server reflexive candidates, or **TURN** if the ICE servers are both TURN servers and will return Relayed and Server reflexive candidates..
- **Backup address:** Address of the Backup ICE server.
- **Backup port:** Port of the Backup ICE server.
- **Backup username:** Username for authentication with the Backup ICE server.
- **Backup password:** Password for authentication with the Backup ICE server.

The Main server is tried first but if this is unavailable then the Backup server is tried.

Administration via WBM

System > ICE > Addressing

Addressing

Main server	none
Main address	
Main port	3478
Main username	
Main password	*****
Backup server	none
Backup address	
Backup port	3478
Backup username	
Backup password	*****
Submit Reset	

Administration via Local Phone

```

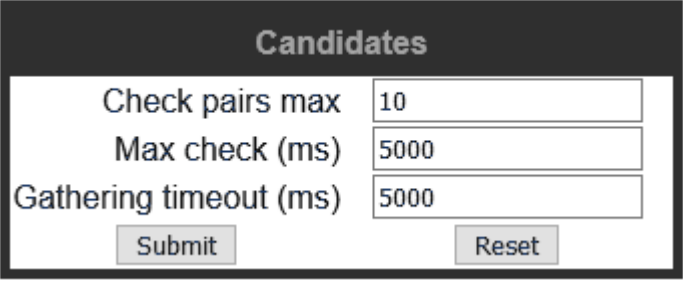
|--- Administration
    |--- System
        |--- ICE
            |--- Addressing
                |--- Main server
                |--- Main address
                |--- Main port
                |--- Main username
                |--- Main password
                |--- Backup server
                |--- Backup address
                |--- Backup port
                |--- Backup username
                |--- Backup password
  
```

3.7.11.3 Candidates

- **Check pairs max:** Maximum number of candidate pairs for connectivity checking.
- **Max Check (ms):** Sets the amount of time in milliseconds allowed to perform the connectivity checks.
- **Gathering timeout (ms):** Sets the amount of time in milliseconds allowed to gather all local candidates.

Administration via WBM

System > ICE > Candidates



Candidates

Check pairs max	10
Max check (ms)	5000
Gathering timeout (ms)	5000

Administration via Local Phone

```

|--- Administration
    |--- System
        |--- ICE
            |--- Candidates
                |--- Check pairs max
                |--- Max Check (ms)
                |--- Gathering timeout (ms)
  
```

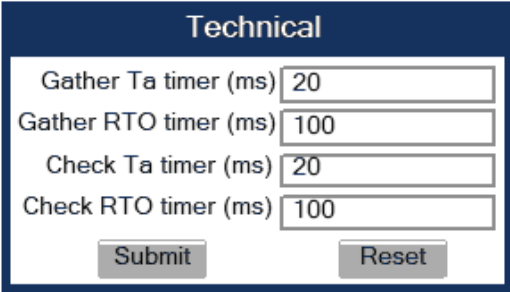
3.7.11.4 Technical

This node contains configuration that only experts should change!

- **Gather Ta timer (ms):** Sets the Ta timer value in milliseconds which controls the pacing of the candidates gathering.
- **Gather RTO timer (ms):** Sets the RTO timer value in milliseconds which controls the pacing of the ICE Gathering retransmissions sent on a candidate pair.
- **Check Ta timer (ms):** Sets the Ta timer value in milliseconds which controls the pacing of the ICE Connectivity Checks sent on a candidate pairs.
- **Check RTO timer (ms):** Sets the RTO timer value in milliseconds which controls the pacing of the ICE Connectivity Check retransmissions sent on a candidate pair.

Administration via WBM

System > ICE > Technical



Technical

Gather Ta timer (ms)	20
Gather RTO timer (ms)	100
Check Ta timer (ms)	20
Check RTO timer (ms)	100

Administration via Local Phone

```

|--- Administration
    |--- System
        |--- ICE
            |--- Technical
  
```

```
|--- Gather Ta timer (ms)
|--- Gather RTO timer (ms)
|--- Check Ta timer (ms)
|--- Check RTO timer (ms)
```

3.8 Feature access

Certain OpenScape Desk Phone CP features and interfaces can be enabled or disabled:

- Blind transfer (see [Blind Call Transfer](#) on page 197)
- 3rd call leg (consultation from a second call; see user manual)
- Callback (see [Callback](#) on page 204 and [Callback URIs](#) on page 160)
- Call pickup (see [Directed Pickup](#) on page 204)
- Group pickup (see [Group Pickup](#) on page 201)
- Call deflection (see [Deflect a Call](#) on page 198)
- Call forwarding (see [Call Forwarding \(Standard\)](#) on page 192)
- Do not disturb (see [Do Not Disturb](#) on page 200)
- Refuse call (see [Allow Refuse](#) on page 150)
- Repertory dial key (see [Repertory Dial](#) on page 201)
- Ext/int forwarding (see [Call Forwarding by Call Type](#) on page 193)
- DSS feature (see [Direct Station Select \(DSS\)](#) on page 232)
- BLF feature (see [BLF Key](#) on page 209)
- Agent feature (see [Call-Center Agent](#) on page 173)
- CTI control (see [uaCSTA Interface](#) on page 179)
- Web based manag. (see [Web-based Management \(WBM\)](#) on page 19)
- Feature toggle (see [Feature Toggle](#) on page 202)
- Phone lock (see user manual)
- Limited FPK set (see [Free Programmable Keys](#) on page 185)

Administration via WBM

System > Features > Feature access

Feature access	
Call control	
Blind transfer	☒
3rd call leg	☒
Call establish	
Callback	☒
Call pickup	☒
Group pickup	☒
Call deflection	☒
Call forwarding	☒
Do not disturb	☒
Refuse call	☒
Repertory dial key	☒
Ext/Int forwarding	☐
Call associated	
DSS feature	☒
BLF feature	☒
Agent feature	☐
CTI	
CTI control	☒
Services	
Web based manag.	☒
Feature toggle	☒
Phone lock	☒
Limited FPK set	No limitation
Submit	Reset

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- Features
            |--- Feature access
  
```

```

|--- Call control
|--- Blind transfer
|--- 3rd call leg

```

Administration via Local Phone

```

|--- Admin
|--- System
|--- Features
|--- Feature access
|--- Call establish
|--- Callback
|--- Call pickup
|--- Group pickup
|--- Call deflection
|--- Call forwarding
|--- Do not disturb
|--- Refuse call
|--- Repertory dial key
|--- Ext/int forwarding

|--- Admin
|--- System
|--- Features
|--- Feature access
|--- Call associated
|--- DSS feature
|--- BLF feature
|--- Agent feature

|--- Admin
|--- System
|--- Features
|--- Feature access
|--- CTI
|--- CTI control

|--- Admin
|--- System
|--- Features
|--- Feature access
|--- Services
|--- Web based manag.
|--- Feature toggle
|--- Limited FPK set

```

3.9 Feature Configuration

3.9.1 Allow Refuse

This parameter defines whether the Refuse Call feature is available on the phone. The possible values are "Yes" or "No". The default is **"NO"**.

NOTICE: This parameter can also be configured under System > Features > Feature access (see [Feature access](#) on page 148).

Administration via WBM

System > Features > Configuration

Configuration	
General	
Emergency number	
Voice mail number	123456
MWI LED	AlertBar only ▼
Missed call LED	AlertBar LED ▼
AlertBar LED hint	☐
Allow refuse	☐
Hot/Warm phone	No action ▼
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☐
Server features	☐
Not used timeout (minutes)	2 ▼
Transfer on hangup	☐
Bridging enabled	☐
Dial plan enabled	☐
FPK program timer	On ▼
Selected Dial Action on calls	No action ▼
DSS monitored	☐
Show icon for all forwarding types	☐
Automatic key module switchback	☒
Simultaneous key module switching	☒
Use simple CallLog	☐
Allow user downloads	☒

Administration via Local Phone

```
|--- Admin
    |--- System
        |--- Features
            |--- Configuration
                |--- General
                    |--- Allow refuse
```

3.9.2 Hot/Warm Phone

If the phone is configured as hot phone, the number specified in Hot warm destination is dialed immediately when the user goes off-hook. For this purpose, Hot warm phone must be set to "Hot phone". If set to "Warm phone", the specified destination number is dialed after a delay which is defined in Initial digit timer (seconds) (for details, see [Initial Digit Timer](#) on page 152). During the delay period, the user can dial a number which will be used instead of the hot/warm destination. In addition, the user will be provided with a dial tone

during the delay period. With the setting "No action", hot phone or warm phone functionality is disabled.

Administration via WBM

System > Features > Configuration

Configuration

General

Emergency number

Voice mail number

MWI LED

Missed call LED

AlertBar LED hint

Allow refuse

Hot/Warm phone

Hot/Warm destination

Initial digit timer (seconds)

Allow uaCSTA

Server features

Not used timeout (minutes)

Transfer on hangup

Bridging enabled

Dial plan enabled

FPK program timer

Selected Dial Action on calls

DSS monitored

Show icon for all forwarding types

Automatic key module switchback

Simultaneous key module switching

Use simple CallLog

Allow user downloads

123456

AlertBar only

AlertBar LED

No action

30

2

On

No action

Administration via Local Phone

```
|--- Admin
  |--- System
    |--- Features
      |--- Configuration
        |--- General
          |--- Hot / warm phone
          |--- Hot / warm destination
          |--- Initial digit timer
```

3.9.3 Initial Digit Timer

This timer is started when the user goes off-hook, and the dial tone sounds. When the user has not entered a digit until timer expiry, the dial tone is turned off, and the phone changes to idle mode. The Initial digit timer (seconds) parameter defines the duration of this timespan.

Administration via WBM

System > Features > Configuration

Configuration	
General	
Emergency number	
Voice mail number	123456
MWI LED	AlertBar only ▼
Missed call LED	AlertBar LED ▼
AlertBar LED hint	☐
Allow refuse	☐
Hot/Warm phone	No action ▼
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☐
Server features	☐
Not used timeout (minutes)	2 ▼
Transfer on hangup	☐
Bridging enabled	☐
Dial plan enabled	☐
FPK program timer	On ▼
Selected Dial Action on calls	No action ▼
DSS monitored	☐
Show icon for all forwarding types	☐
Automatic key module switchback	☒
Simultaneous key module switching	☒
Use simple CallLog	☐
Allow user downloads	☒

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- Features
            |--- Configuration
                |--- General
                    |--- Initial digit timer
  
```

3.9.4 Show Forwarding icon

The **Show icon for all forwarding types** parameter controls whether a call forwarding icon is displayed for any type of call forwarding. If this option is disabled, only "Forwarding conditional" is indicated by the icon.

The default value is **Disabled**.

Administration via WBM

System > Features > Configuration

Configuration

General

Emergency number	
Voice mail number	123456
MWI LED	AlertBar only
Missed call LED	AlertBar LED
AlertBar LED hint	☐
Allow refuse	☐
Hot/Warm phone	No action
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☐
Server features	☐
Not used timeout (minutes)	2
Transfer on hangup	☐
Bridging enabled	☐
Dial plan enabled	☐
FPK program timer	On
Selected Dial Action on calls	No action
DSS monitored	☐
Show icon for all forwarding types	☐
Automatic key module switchback	☒
Simultaneous key module switching	☒
Use simple CallLog	☐
Allow user downloads	☒

Administration via Local Phone

```
|--- Admin
  |--- System
    |--- Features
      |--- Configuration
        |--- General
          |--- Show icon for all
            forwarding types
```

3.9.5 Allow user downloads

The **Allow user downloads** parameter controls whether users can download files.

If this option is disabled, the three File Transfer options—**Slideshow images**, **Avatar images**, **Ringtones**, and **Contacts transfer**—are not available in the **User Settings** area of the phone's Web-Based Management (WBM). In this case, the user cannot transfer files from their PC to the phone.

The default value is **Enabled**.

Administration via WBM

System > Features > Configuration

Configuration	
General	
Emergency number	
Voice mail number	123456
MWI LED	AlertBar only ▼
Missed call LED	AlertBar LED ▼
AlertBar LED hint	☐
Allow refuse	☐
Hot/Warm phone	No action ▼
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☐
Server features	☐
Not used timeout (minutes)	2 ▼
Transfer on hangup	☐
Bridging enabled	☐
Dial plan enabled	☐
FPK program timer	On ▼
Selected Dial Action on calls	No action ▼
DSS monitored	☐
Show icon for all forwarding types	☐
Automatic key module switchback	☒
Simultaneous key module switching	☒
Use simple CallLog	☐
Allow user downloads	☒

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- Features
            |--- Configuration
                |--- General
                    |--- Allow user downloads

```

3.9.6 Redial original forwarded

The **Redial original forwarded** parameter controls the display order and redial behavior for forwarded outgoing calls.

If enabled, it moves the originally called entry above the connected party entry in the Conversations list and ensures the Redial function calls the originally dialed number instead of the forwarded destination. However, users can download files.

The default value is **Disabled**.

Administration via WBM

System > Features > Configuration

Configuration

General

Emergency number	
Voice mail number	123456
MWI LED	AlertBar only
Missed call LED	AlertBar LED
AlertBar LED hint	☐
Allow refuse	☐
Hot/Warm phone	No action
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☐
Server features	☐
Not used timeout (minutes)	2
Transfer on hangup	☐
Bridging enabled	☐
Dial plan enabled	☐
FPK program timer	On
Selected Dial Action on calls	No action
DSS monitored	☐
Show icon for all forwarding types	☐
Automatic key module switchback	☒
Simultaneous key module switching	☒
Redial original forwarded	☐

Administration via Local Phone

```
|--- Admin
  |--- System
    |--- Features
      |--- Configuration
        |--- General
          |--- Redial original
            forwarded
```

3.9.7 Group Pickup

NOTICE: This feature is only available when allowed under System > Features > Feature access (see [Feature access](#) on page 148).

3.9.7.1 Feature Code

This feature allows a user to answer a call from any alerting phone that is in the same pickup group. Prerequisites: The phone has to be assigned to a pickup group on OpenScape Voice and the corresponding URI of the Call Pickup group service provided by the server is configured on the phone. Also, the phone must display a Group pickup alert on screen in order to pick up the call and even if this alert does not appear on screen then by the 1st key press it should be showed up. An example pickup URI is "***3". See [Pickup alert](#) on page 157 for options on visual and audible indication.

Administration via WBM

NOTICE: The BLF pickup code parameter is only relevant when the phone is connected to an Asterisk or RingCentral server.

NOTICE: RingCentral Group Pickup enables to be a part of more than one group, and each of them can be configured per specific key. For more information, see [BLF Key](#) on page 209.

System > Features > Addressing

Addressing	
General	
MW server URI	
Conference	1234567890
Group pickup URI	
Directed pickup URI	
Callback: FAC	*66
Callback cancel all	#66
BLF pickup code	
BLF resource list URI	
LIS server	
LIS server URL	
LIS retry timeout	10
RTCP-XR server	
RTCP-XR server URI	
RTCP-XR server port	0
Submit Reset	

3.9.7.2 Pickup alert

If desired, an incoming call for the pickup group can be indicated acoustically and visually if Group pickup visual alert is configured.

The Group pickup tone allowed parameter activates or deactivates the generation of an acoustic signal for incoming pickup group calls. The default is "Yes". If this is activated, Group pickup as ringer determines whether the current ring tone or an alert beep is used. If set to "Yes", a pickup group call will

be signaled by a short ring tone; the currently selected ringtone is used. If set to "No", a pickup group call will be signaled by an alert tone. The default is "Yes".

Depending on the phone state and the setting for Group pickup as ringer, the group pickup tone comes from the loudspeaker, the handset, or the headset. The volumes can be set in the local user menu, under **Audio > Volumes**.

The following table shows the group pickup alert behaviour for each possible scenario:

Phone State			Group pickup as ringer=yes	Group pickup as ringer=no
Ringer on	Idle		Ring tone Speaker	Beep Speaker
	In call	Handset	Ring tone Speaker	Beep Handset
		Handset Open listening	Beep Handset and Speaker	Beep Handset and Speaker
		Headset	Ring tone Speaker	Beep Headset
		Headset Open listening	Beep Headset and Speaker	Beep Headset and Speaker
		Hands-free	Beep Speaker	Beep Speaker
Ringer off	Idle		Nothing	Nothing
	In call	Handset	Nothing	Beep Handset
		Handset Open listening	Beep Handset and Speaker	Beep Handset and Speaker
		Headset	Nothing	Beep Headset
		Headset Open listening	Beep Headset and Speaker	Beep Headset and Speaker
		Hands-free	Beep Speaker	Beep Speaker

Group pickup visual alert defines the user action required to accept a pickup call.

- If Prompt is selected, an incoming pickup call is signaled by a prompt on the display and the flashing Pick up key. As soon as the user goes off-hook or presses the speaker key, the pickup call is accepted. Alternatively, the user can press the corresponding function key, if configured.
- If Notify is selected, an incoming pickup call is signaled by the Pickup call? prompt on the display and by the flashing Pick up key. To accept the call, the user must confirm the alert by pressing the OK key or by pressing the flashing Pick up key. The user can then either lift the handset or press the Speaker key or the Headset key to accept the call.
- If FPK only (default setting) is selected, an incoming call is signaled only by the flashing Pick up key. To accept the call, the user must press the flashing

Pick up key. The Pickup call? prompt is then shown on the display, and the user can either lift the handset or press the Speaker key or the Headset key or press the Pickup key again to accept the call.

Administration via WBM

System > Features > Configuration

Alerting	
BLF alert	Beep ▼
Group pickup alert	Off ▼
Group pickup tone interval	15
Group pickup visual alert	Prompt ▼
MLPP ringer	▼
Callback ringer	▼
Impact level ringer	▼

Administration via Local Phone

```
|--- Admin
    |--- System
        |--- Features
            |--- Alerting
                |--- Group pickup tone
                |--- Group pickup as ringer
                |--- Group pickup visual
```

3.9.8 Call Transfer

3.9.8.1 Transfer on Ring

If this function is active, a call can be transferred after the user has dialed the third participant's number, but before the third party has answered the call. This feature is enabled or disabled in the User menu. The default is "Yes".

Administration via WBM (User menu)

User > Configuration > Outgoing calls

Outgoing calls	
Autodial delay (seconds)	6 ▼
Allow callback	☒
Allow busy when dialing	☐
Allow transfer on ring	☒
Allow immediate dialing	☐
Submit Reset	

Administration via Local Phone (User menu)

```
|--- User
    |--- Configuration
```

```
|--- Outgoing calls
|--- Transfer on ring
```

3.9.8.2 Transfer on Hangup

This feature applies to the following scenario: While A is talking to B, C calls A. A accepts the call, so B is on hold and the call between A and C is active. If Transfer on hangup is enabled, and A goes on-hook, B gets connected to C. If disabled, C will be released when A hangs up, and A has the possibility to reconnect to B. By default, the feature is disabled.

Administration via WBM

System > Features > Configuration

General

Emergency number	3335
Voice mail number	
MWI LED	AlertBar LED ▼
Missed call LED	AlertBar LED ▼
Allow refuse	☒
Hot/Warm phone	No action ▼
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☒
Server features	☐
Not used timeout (minutes)	2 ▼
Transfer on hangup	☐
Bridging enabled	☒
Dial plan enabled	☐
FPK program timer	On ▼
DSS monitored	☐
Show icon for all forwarding types	☐

Administration via Local Phone

```
|--- Admin
|--- System
|--- Features
|--- Configuration
|--- General
|--- Transfer on hangup
```

3.9.9 Callback URIs

The Callback option allows the user to request a callback on certain conditions. The callback request is sent to the SIP server. The Code for callback busy requests a callback if the line is busy, i. e. if there is a conversation on the remote phone. Code for callback no reply applies when the call is not answered,

i. e. if nobody lifts the handset or accepts the call in another way. The Code for callback cancel all deletes all the callback requests stored previously on the telephone system/SIP server.

NOTICE: The callback feature can be enabled or disabled under System > Features > Feature access (see [Feature access](#) on page 148).

Data required

- **Callback: FAC:** Access code that is sent to the server for all kind of Callback.
- **Code for callback cancel all / Callback: Cancel all:** Access code for canceling all callback requests on the server.

Administration via WBM

System > Features > Addressing

Administration via Local Phone

```
|--- Admin
    |--- System
        |--- Features
            |--- Addressing
                |--- Callback: FAC
                |--- Callback: Cancel all
```

3.9.9.1 Call Completion

Used with Asterisk only

Administration via WBM

System > Features > Call Completion

Call completion	
Functional CCSS	☒
Callback ringer	alert-internal
Allow after call (s)	30
Max. callbacks	5
Submit Reset	

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- Features
            |--- Call completion
                |--- Functional CCSS
                |--- Callback ringer
                |--- Allow after call (s)
                |--- Max. callbacks
  
```

3.9.10 Message Waiting Address

The MWI (Message Waiting Indicator) is an optical signal which indicates that voicemail messages are on the server. Depending on the SIP server / gateway in use, the Message waiting server address, that is the address or host name of the server that sends message waiting notifications to the phone, must be configured.

With OpenScape Voice, this setting is not typically necessary for enabling MWI functionality.

Administration via WBM

System > Features > Addressing

Addressing	
General	
MW server URI	
Conference	1234567890
Group pickup URI	
Directed pickup URI	
Callback: FAC	*66
Callback cancel all	#66
BLF pickup code	
BLF resource list URI	
LIS server	
LIS server URL	
LIS retry timeout	10
RTCP-XR server	
RTCP-XR server URI	
RTCP-XR server port	0
Submit Reset	

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- Features
            |--- Addressing
                |--- MWI server URI

```

3.9.11 Indicate Messages

The indication of old and new messages on the display can be configured. There are 4 categories of voicemail messages: new, new urgent, old, and old urgent. For each category, the administrator can define whether the message count is shown or hidden, and set a header for the category. If all four settings on the form are set to "Hide", the VoiceMail summary screen is not shown to the user. Any other permutation of "Show/Hide" settings must result in a VoiceMail summary.

Data required

- **New items:** Determines whether new items are indicated. Value range: "Show", "Hide"

- **Alternative label:** Label for new items.
- **New urgent items:** Determines whether new urgent items are indicated. Value range: "Show", "Hide"
- **Alternative label:** Label for new urgent items.
- **Old items:** Determines whether new urgent items are indicated. Value range: "Show", "Hide"
- **Alternative label:** Label for old items.
- **Old urgent items:** Determines whether old urgent items are indicated. Value range: "Show", "Hide"
- **Alternative label:** Label for old urgent items.

Administration via WBM

Local functions > Messages settings

Administration via Local Phone

```
|--- Admin
    |--- Local functions
        |--- Messages settings
            |--- New items
            |--- Alternative label
            |--- New urgent items
            |--- Alternative label
            |--- Old items
            |--- Alternative label
            |--- Old urgent items
            |--- Alternative label
```

3.9.12 System Based Conference

The Conference URI provides the number/URI used for system based conferences, which can involve 3 to 16 members. This feature is not available with every system.

NOTICE: It is recommended not to enter the full URI, but only the user part. For instance, enter "123", not "123@<SIP SERVER ADDRESS>". A full address in this place might cause

a conflict when OpenScape Desk Phone CP uses multiple nodes.

Administration via WBM

System > Features > Addressing

Addressing	
General	
MW server URI	
Conference	1234567890
Group pickup URI	
Directed pickup URI	
Callback: FAC	*66
Callback cancel all	#66
BLF pickup code	
BLF resource list URI	
LIS server	
LIS server URL	
LIS retry timeout	10
RTCP-XR server	
RTCP-XR server URI	
RTCP-XR server port	0
Submit Reset	

3.9.13 RTCP-XR server

The RTCP-XR (Real Time Control Protocol Extended Reports) transmits voice quality reports after the conclusion of a call.

RTCP-XR URI:

URI to be used for transmitting voice quality reports after the conclusion of a call.

RTCP-XR port:

Port value of RTCP-XR server.

If RTCP-XR port value is not configured or is empty, the RTCP-XR port value will be taken from the SIP server port value.

Table 1: RTCP-XR parameters

Parameter	Sub-param	Meaning	Value	
CallID		Call id from the SIP dialog	CallID = "CallID" HCOLON Call-ID-Param	"7f93c777b71d424d8505d526231000ef"
LocalID		reporting endpoint for the media session	LocalID = "LocalID" HCOLON (name-addr/addr-spec)	
RemoteID		remote endpoint of the media session	RemoteID = "RemoteID" HCOLON (name-addr/addr-spec)	
OrigID		endpoint which originated the session	OrigID = "OrigID" HCOLON (name-addr/addr-spec)	
LocalGroup		identification for the purposes of aggregation for the local endpoint	LocalGroupID = "LocalGroup" HCOLON word-plus	
LocalAddr	IP	IP address of the endpoint/UA, which is the receiving end of the stream being measured	LocalAddr = "LocalAddr" HCOLON IPAddress WSP Port WSP Ssrc	
	PORT	port of the endpoint/UA	LocalAddr = "LocalAddr" HCOLON IPAddress WSP Port WSP Ssrc	
	SSRC	SSRC of the endpoint/UA	LocalAddr = "LocalAddr" HCOLON IPAddress WSP Port WSP Ssrc	
LocalMAC		Media Access Control (MAC) address of the local SIP device	LocalMACAddr = "LocalMAC" HCOLON hex2 *(":" hex2)	
RemoteAddr	IP	IP address of the source of the stream being measured	RemoteAddr = "RemoteAddr" HCOLON IPAddress WSP Port WSP Ssrc	
	PORT	port of the source of the stream	RemoteAddr = "RemoteAddr" HCOLON IPAddress WSP Port WSP Ssrc	
	SSRC	SSRC of the source of the stream	RemoteAddr = "RemoteAddr" HCOLON IPAddress WSP Port WSP Ssrc	
Timestamps		provided in Coordinated Universal Time (UTC) using the ABNF format provided in RFC 3339	TimeStamps = "Timestamps" HCOLON StartTime WSP StopTime	
	START	provided in Coordinated Universal Time (UTC) using the ABNF format provided in RFC 3339	StartTime = "START" EQUAL date-time	

Parameter	Sub-param	Meaning	Value	
	STOP	provided in Coordinated Universal Time (UTC) using the ABNF format provided in RFC 3339	StopTime = "STOP" EQUAL date-time	
SessionDesc		shortened version of the session SDP but contains only the relevant parameters for session quality reporting purposes		
SessionDesc		shortened version of the session SDP but contains only the relevant parameters for session quality reporting purposes	SessionDescription = "SessionDesc" HCOLON [PayloadType WSP] [PayloadDesc WSP] [SampleRate WSP] [PacketsPerSecond WSP] [FrameDuration WSP] [FrameOctets WSP] [FramesPerPacket WSP] [FmtpOptions WSP] [PacketLossConcealment WSP] [SilenceSuppressionState]	
	PT	PT parameter used in the RTP packets	PayloadType = "PT" EQUAL (1*3DIGIT)	
	PD	text description of the codec, should use the IANA registry for media-type names defined by RFC 4855	PayloadDesc = "PD" EQUAL (word / DQUOTE word-plus DQUOTE)	
	SR	Rate at which a voice was sampled in the case of narrowband codecs, this value will typically be 8000. For codecs that are able to change sample rates, the lowest and highest sample rates MUST be reported (e.g., 8000;16000).	SampleRate = "SR" EQUAL (1*6DIGIT) *(SEMI (1*66DIGIT))	

Parameter	Sub-param	Meaning	Value	
	FD	FrameDuration can be combined with the FramesPerPacket to determine the packetization rate; the units for FrameDuration are milliseconds. NOTE: for frame-based codecs, each frame constitutes a single frame; for sample-based codecs, a "frame" refers to the set of samples carried in an RTP packet.	FrameDuration = "FD" EQUAL (1*4DIGIT)	
	F0	Number of octets in each frame at the time the report is generated (i.e., last value). This may be used where FrameDuration is not available.	FrameOctets = "FO" EQUAL (1*5DIGIT)	
	FPP	Number of frames in each RTP packet at the time the report is generated.	FramesPerPacket = "FPP" EQUAL (1*2DIGIT)	
	PPS	average number of packets that are transmitted per second	PacketsPerSecond = "PPS" EQUAL (1*5DIGIT)	
	PLC	Indicates whether a PLC algorithm was or is being used for the session. The values follow the same numbering convention as RFC 3611 (0 - unspecified ; 1 - disabled ; 2 - enhanced ; 3 - standard)	PacketLossConcealment = "PLC" EQUAL ("0" / "1" / "2" / "3")	
	SSUP	Indicates whether silence suppression, also known as Voice Activity Detection (VAD) is enabled.	SilenceSuppressionState = "SSUP" EQUAL ("on" / "off")	
JitterBuffer	SSUP		JitterBuffer = "JitterBuffer" HCOLON [JitterBufferAdaptive WSP] [JitterBufferRate WSP] [JitterBufferNominal WSP] [JitterBufferMax WSP] [JitterBufferAbsMax]	

Parameter	Sub-param	Meaning	Value
	JBA	JitterBufferAdaptive indicates whether the jitter buffer in the endpoint is adaptive, static, or unknown.	JitterBufferAdaptive = "JBA" EQUAL ("0" / "1" / "2" / "3")
	JBR	JitterBufferRate	JitterBufferRate = "JBR" EQUAL (1*2DIGIT) ;0-15
	JBN	JitterBufferNominal	JitterBufferNominal = "JBN" EQUAL (1*5DIGIT) ;0-65535
	JBM	JitterBufferMax	JitterBufferMax = "JBM" EQUAL (1*5DIGIT) ;0-65535
	JBX	JitterBufferAbsMax	JitterBufferAbsMax = "JBX" EQUAL (1*5DIGIT) ;0-65535
PacketLoss			PacketLoss = "PacketLoss" HCOLON [NetworkPacketLossRate WSP] [JitterBufferDiscardRate]
	NLR	NetworkPacketLossRate	NetworkPacketLossRate = "NLR" EQUAL (1*3DIGIT ["."1*2DIGIT]) ;percentage
	JDR	JitterBufferDiscardRate	JitterBufferDiscardRate = "JDR" EQUAL (1*3DIGIT ["."1*2DIGIT]) ;percentage
BurstGapLoss			BurstGapLoss = "BurstGapLoss" HCOLON [BurstLossDensity WSP] [BurstDuration WSP] [GapLossDensity WSP] [GapDuration WSP] [MinimumGapThreshold]
	BLD	BurstLossDensity	"BLD" EQUAL (1*3DIGIT ["." 1*2DIGIT]) ;percentage
	BD	BurstDuration	BurstDuration = "BD" EQUAL (1*7DIGIT) ;0-3,600,000 -- milliseconds
	GLD	GapLossDensity	GapLossDensity = "GLD" EQUAL (1*3DIGIT ["."1*2DIGIT]) ;percentage
	GMIN	MinimumGapThreshold	MinimumGapThreshold = "GMIN" EQUAL (1*3DIGIT) ;1-255

Administration

Parameter	Sub-param	Meaning	Value
Delay			Delay = "Delay" HCOLON [RoundTripDelay WSP] [EndSystemDelay WSP] [OneWayDelay WSP] [SymmOneWayDelay WSP] [InterarrivalJitter WSP] [MeanAbsoluteJitter]
	RTD		RoundTripDelay = "RTD" EQUAL (1*5DIGIT) ;0-65535
	ESD		EndSystemDelay = "ESD" EQUAL (1*5DIGIT) ;0-65535
	SOWD	SymmOneWayDelay is defined as half the sum of RoundTripDelay and the EndSystemDelay values for both endpoints.	SymmOneWayDelay = "SOWD" EQUAL (1*5DIGIT); 0-65535
Signal	SL	SignalLevel will normally be a negative value. This metric applies to the speech signal decoded from the received packet stream.	SignalLevel = "SL" EQUAL (["-"] 1*2DIGIT)
QualityEst		Voice Quality estimation metrics. Each quality estimate has an optional associated algorithm. These fields permit the implementation to use a variety of different calculation methods for each type of metric.	QualityEstimates = "QualityEst" HCOLON [ListeningQualityR WSP] [RLQEstAlg WSP] [ConversationalQualityR WSP] [RCQEstAlg WSP] [ExternalR-In WSP] [ExtRInEstAlg WSP] [ExternalR-Out WSP] [ExtROutEstAlg WSP] [MOS-LQ WSP] [MOSLQEstAlg WSP] [MOS-CQ WSP] [MOSCQEstAlg WSP] [QoEEstAlg]

Parameter	Sub-param	Meaning	Value
	RLQ	ListeningQualityR This field reports the listening quality expressed as an R factor (per G.107). This does not include the effects of echo or delay. The range of R is 0-95 for narrowband calls and 0-120 for wideband calls. Algorithms for computing this value SHOULD be compliant with ITU-T Recommendations P.564 and G.107.	ListeningQualityR = "RLQ" EQUAL (1*3DIGIT) ; 0 - 120
	RCQ	ConversationalQualityR This field corresponds to "R factor" in RFC 3611 in the VoIP Metrics Report Block. This parameter provides a cumulative measurement of voice quality from the start of the session to the reporting time. The range of R is 0-95 for narrowband calls and 0-120 for wideband calls. Algorithms for computing this value SHOULD be compliant with ITU-T Recommendations P.564 and G.107. Within RFC 3611, a reported R factor of 127 indicates that this parameter is unavailable; in this case, the ConversationalQualityR parameter MUST be omitted from the vq-rtcpxr event.	ConversationalQualityR = "RCQ" EQUAL (1*3DIGIT) ; 0 - 120

Parameter	Sub-param	Meaning	Value	
	MOSLQ	Mean opinion score for listening voice quality. This field corresponds to "MOSLQ" in RFC 3611 in the VoIP Metrics Report Block. This parameter is the estimated mean opinion score for listening voice quality on a scale from 1 to 5, in which 5 represents "Excellent" and 1 represents "Unacceptable". Algorithms for RFC 6035 SIP Package for Voice Quality Reporting November 2010 computing this value SHOULD be compliant with ITU-T Recommendation P.564 [10]. This field provides a text name for the algorithm used to estimate MOS-LQ.	MOS-LQ = "MOSLQ" EQUAL (DIGIT ["." 1*3DIGIT]) ; 0.0 - 4.9	
	MOSQ	Mean opinion score for conversation voice quality. This field corresponds to "MOSQ" in RFC 3611 in the VoIP Metrics Report Block. This parameter is the estimated mean opinion score for conversation voice quality on a scale from 1 to 5, in which 5 represents excellent and 1 represents unacceptable. Algorithms for computing this value SHOULD be compliant with ITU-T Recommendation P.564 with regard to the listening quality element of the computed MOS score.	MOS-CQ = "MOSQ" EQUAL (DIGIT ["." 1*3DIGIT]) ; 0.0 - 4.9	

Parameter	Sub-param	Meaning	Value
	QoEEstAlg	QoEEstAlg provides text description of the algorithm used to estimate all voice quality metrics. It is an alternative to the separate estimation algorithms for use when the same algorithm is used for all measurements.	QoEEstAlg = "QoEEstAlg" EQUAL word ; "P.564" or other

Administration via WBM

System > Features > Addressing

Addressing

General

MW server URI	
Conference	
Group pickup URI	
Directed pickup URI	
Callback: FAC	
Callback cancel all	
BLF pickup code	
BLF resource list URI	

LIS server

LIS server URL	
LIS retry timeout	10

RTCP-XR server

RTCP-XR server URI	
RTCP-XR server port	0

3.9.14 Call-Center Agent

Administration via WBM

System > Features > Feature access

Feature access	
Call control	
Blind transfer	☒
3rd call leg	☒
Call establish	
Callback	☒
Call pickup	☒
Group pickup	☒
Call deflection	☒
Call forwarding	☒
Do not disturb	☒
Refuse call	☒
Repertory dial key	☒
Ext/Int forwarding	☐
Call associated	
DSS feature	☒
BLF feature	☒
Agent feature	☐
Video calls	☒
CTI	
CTI control	☒
Services	
Bluetooth	☒
Web based manag.	☒
Feature toggle	☒
Phone lock	☒
Limited FPK set	No limitation ▼
Submit	Reset

If you want to enable the Agent feature click on the **Agent feature** check-box.
After the enablement the feature will be visible to the user.

Administration via WBM

System > Features > Configuration

Configuration	
General	
Emergency number	
Voice mail number	
MWI LED	AlertBar only ▾
Missed call LED	AlertBar LED ▾
AlertBar LED hint	☐
Allow refuse	☒
Hot/Warm phone	No action ▾
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☒
Server features	☐
Not used timeout (minutes)	2 ▾
Transfer on hangup	☐
Bridging enabled	☐
Dial plan enabled	☐
FPK program timer	On ▾
Selected Dial Action on calls	No action ▾
DSS monitored	☐
Show icon for all forwarding types	☒
Automatic key module switchback	☒
Simultaneous key module switching	☒
Alerting	
BLF alert	Beep ▾
Group pickup alert	Off ▾
Group pickup tone interval	15
Group pickup visual alert	Prompt ▾
MLPP ringer	▾
Callback ringer	▾
Impact level ringer	▾
Bluetooth	
Enable bluetooth interface	☒
Call recording	
Recorder address	
Recording mode	Disabled ▾
Audible notification	Single-shot ▾
Submit	Reset

In order to enable the Agent feature you should also click on the **Server features** check-box to enable it.

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- Features
            |--- Configuration
                |--- General
                    |--- Server features
  
```

Administration via WBM

System > Registration

Registration	
SIP addresses	
SIP server address	10.12.70.16
SIP registrar address	10.12.70.16
SIP gateway address	0.0.0.0
SIP session	
Session timer enabled	☒
Session duration (seconds)	3600
Registration timer (seconds)	3600
Subscription timer (seconds)	3600
Refresh minimum (seconds)	0
Server type	Broadsoft ▼
Realm	realm3
User ID	49897224052
Password	
MLPP base	Local ▼
MLPP domain	dsn+uc ▼
Other domain	
SIP survivability	
Backup registration allowed	☐
Backup proxy address	0.0.0.0
Backup registration timer (seconds)	3600
Backup transport	UDP ▼
Backup connection	Listening ▼
Backup OBP flag	☐
Standard CSTA	
Server address	
Server port	5060
E/A Cockpit	
Server address	
Allow server push	☒
Mobility logoff action	None ▼
Submit	Reset

In order to enable the Agent feature you should also set the **Server type** to **Broadsoft**.

3.9.14.1 Broadsoft Agent Logon/Logoff

A new feature key called "Broadsoft Call Center" can be configured by admin. A label name can be provided and the "name" of the call center that we want to control must be given. Also the "Call Center Related Line" must be provided

based on the index of the configured line key referring to the specific call center. For example, the first key on the Key Module has the index "1" and so on.

Administration via WBM

System > Features > Favourites/Key module

Broadsoft Call Center	
Key label 8	AgentLogon
Call Center Name	Call Center 1
Call Center Related Line	1
Submit Reset	

3.9.15 Server Based Features

NOTICE: Please note that the Server features parameter, despite the name similarity, is not related to the Server feature functionality as described in [Server Feature](#) on page 208.

The use of server based call forwarding and server based DND is enabled or disabled here. When phone based DND and phone based call forwarding are to be used, Server features must be deactivated. This is the default setting. For using server based Call Forwarding or server based DND, it must be activated.

NOTICE: Server features is deactivated automatically if System > Registration > Server type (see [SIP Registration](#) on page 120) is set to "HiQ8000".

NOTICE: It is recommended to set Server features when setting up the phone, and avoid further changes, as possible.

Administration via WBM

System > Features > Configuration

Configuration	
General	
Emergency number	
Voice mail number	
MWI LED	AlertBar only ▼
Missed call LED	AlertBar LED ▼
AlertBar LED hint	☐
Allow refuse	☒
Hot/Warm phone	No action ▼
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☒
Server features	☐
Not used timeout (minutes)	2 ▼
Transfer on hangup	☐
Bridging enabled	☐
Dial plan enabled	☐
FPK program timer	On ▼
Selected Dial Action on calls	No action ▼
DSS monitored	☐
Show icon for all forwarding types	☒
Automatic key module switchback	☒
Simultaneous key module switching	☒
Alerting	
BLF alert	Beep ▼
Group pickup alert	Off ▼
Group pickup tone interval	15
Group pickup visual alert	Prompt ▼
MLPP ringer	▼
Callback ringer	▼
Impact level ringer	▼
Bluetooth	
Enable bluetooth interface	☒
Call recording	
Recorder address	
Recording mode	Disabled ▼
Audible notification	Single-shot ▼
Submit	Reset

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- Features
            |--- Configuration
                |--- General
                    |--- Server features
  
```

3.9.16 uaCSTA Interface

User Agent CSTA (uaCSTA) is a limited subset of the CSTA protocol, which allows external CTI applications to interact with the phone via the SIP server.

NOTICE: Access to the users “CTI calls” menu in User > Configuration > Incoming Calls can be allowed or disallowed (see [Feature access](#) on page 148).

If Allow uaCSTA is enabled, applications which support the uaCSTA standard will have access to the OpenScape Desk Phone CP phone. The default is "Yes".

Administration via WBM

System > Features > Configuration

General	
Emergency number	3335
Voice mail number	
MWI LED	AlertBar LED ▼
Missed call LED	AlertBar LED ▼
Allow refuse	☒
Hot/Warm phone	No action ▼
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☒
Server features	☐
Not used timeout (minutes)	2 ▼
Transfer on hangup	☐
Bridging enabled	☒
Dial plan enabled	☐
FPK program timer	On ▼
DSS monitored	☐
Show icon for all forwarding types	☐

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- Features
            |--- Configuration
                |--- General
                    |--- Allow uaCSTA
  
```

3.9.16.1 External CSTA server configuration

CSTA is a standardised interface that can be used to monitor and control calls and call related features on the phone. If a different CSTA server needs to be configured, there is a possibility to do it via WBM.

Administration via WBM

System > Registration

Registration	
SIP addresses	
SIP server address	10.12.70.16
SIP registrar address	10.12.70.16
SIP gateway address	0.0.0.0
SIP session	
Session timer enabled	☒
Session duration (seconds)	3600
Registration timer (seconds)	3600
Subscription timer (seconds)	3600
Refresh minimum (seconds)	0
Server type	OS Voice
Realm	realm3
User ID	49897224030
Password	*****
MLPP base	Local
MLPP domain	dsn+uc
Other domain	
SIP survivability	
Backup registration allowed	☒
Backup proxy address	0.0.0.0
Backup registration timer (seconds)	3600
Backup transport	UDP
Backup connection	Listening
Backup OBP flag	☐
Standard CSTA	
Server address	
Server port	5060
E/A Cockpit	
Server address	
Allow server push	☒
Mobility logoff action	None
Submit	Reset

3.9.17 Local Menu Timeout

The timeout for the local user and admin menu is configurable. When the time interval is over, the menu is closed and the administrator/user is logged out. The timeout may be helpful in case a user does a long press on a line key unintentionally, and thereby invokes the key configuration menu. The menu will close after the timeout, and the key will return to normal line key operation. The timeout ranges from 1 to 5 minutes. The default value is 2.

NOTICE: The current position in the user or admin menu is kept in case the user/admin has exited the menu, e.g. for receiving a call. Thus, if the user/admin re-enters the menu, he is directed to exactly that submenu, or parameter, which he had been editing before.

Administration via WBM

System > Features > Configuration

General	
Emergency number	3335
Voice mail number	
MWI LED	AlertBar LED ▼
Missed call LED	AlertBar LED ▼
Allow refuse	☒
Hot/Warm phone	No action ▼
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☒
Server features	☐
Not used timeout (minutes)	2 ▼
Transfer on hangup	☐
Bridging enabled	☒
Dial plan enabled	☐
FPK program timer	On ▼
DSS monitored	☐
Show icon for all forwarding types	☐

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- Features
            |--- Configuration
                |--- General
                    |--- Not used timeout

```

3.9.18 Call Recording

Call recording is possible for OpenScape Desk Phone CP using an "ASC Voice Recorder". The implementation is similar to a local conference, with the recording device acting as the third conference member. To start recording, the phone calls the recording device and provides it with the mixed audio data. The recording device saves the audio as a file but the recording is not accessible by the phone.

With the Call recording mode/Recording Mode parameter, the behaviour of the feature is determined:

- **"Disabled"**: The user cannot turn recording on.
- **"Manual"**: The user starts and stops recording manually using the menu or a free programmable key. The user does not have to turn off the recording manually as it will stop when the call ends, regardless of the way it started.
- **"Auto-start"**: The recording starts automatically for each call. The user can stop it manually only during a call. When the call ends, call recording will be automatically be enabled again.

- **"All Calls"**: The recording starts automatically for all recordable calls; the user can not stop the recording manually.
- **"One call"**: The user starts and stops recording manually during a call using the menu or a free programmable key. When the call finishes, call recording will be automatically turned off again.

The Audible indication/Audible Notification parameter determines if and how the parties in a call are informed when a call is being recorded:

- **"Off"**: No audible indication is given.
- **"Single-shot"**: A single audible indication is given when recording commences or resumes.
- **"Repeated"**: An audible indication is given when recording commences or resumes, and repeated periodically during the recording.

With the Recorder address/Recorder number parameter, the SIP address of the call recorder is specified.

Administration via WBM

System > Features > Configuration

Call recording	
Recorder address	
Recording mode	Disabled ▼
Audible notification	Single-shot ▼
Submit	Reset

Administration via Local Phone

```
|--- Admin
    |--- System
        |--- Features
            |--- Configuration
                |--- Call Recording
                    |--- Recorder number
                    |--- Recorder mode
                    |--- Audible notification
```

3.9.19 Rollover Visual Alert

This feature allows user to have a visual indication of rollover calls (i.e. calls received when busy on a Keyset line that are forwarded as alerting to another line on the phone) so that he/she can directly see the call related information.

NOTICE: The configuration item Rollover Visual Alert is available on the CP600/600E/700/700X only.

Administration via WBM

System > Features > Keyset operation

Keyset operation

Rollover ring	alert beep
Rollover visual alert	no indication
LED on registration	no indication
Originating line preference	visual alert
Terminating line preference	ringing line
Line action mode	hold
Reservation timer (seconds)	60
Forwarding indicated	☐
Submit	Reset

Possible configuration parameters

The default setting for this configuration item is "no indication".

- No indication - when "Rollover visual alert" is set to "no indication", the phone does not provide any visual indication of an incoming rollover call on the phone's main display.
- Visual alert - when "Rollover visual alert" is set to "visual alert", the phone will provide a visual indication in form of a sausage on the bottom of the current screen for an incoming rollover call.

The information provided to the user on a single incoming rollover call:

- Line key label on the left side
- Remote party information on the right side

The information provided on multiple incoming rollover calls:

- The amount of incoming calls

3.9.20 Landing screen

Based on defined trigger conditions the phone may automatically show one of the following screens as the landing screen (i.e. top of the UI stack):

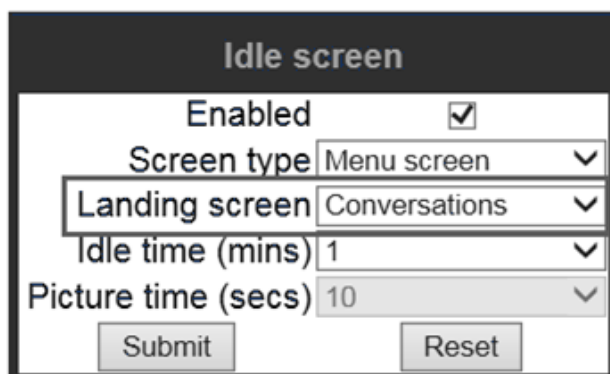
- Conversation list
- Favourites (CP600/600E/700/700X) or Team (CP400)
- Main menu

NOTICE: The default landing screen is always the Conversation list.

Administration via WBM

User > Phone > Idle screen

Allow users to configure their landing screen.



Idle screen

Enabled ☒

Screen type Menu screen ▼

Landing screen Conversations ▼

Idle time (mins) 1 ▼

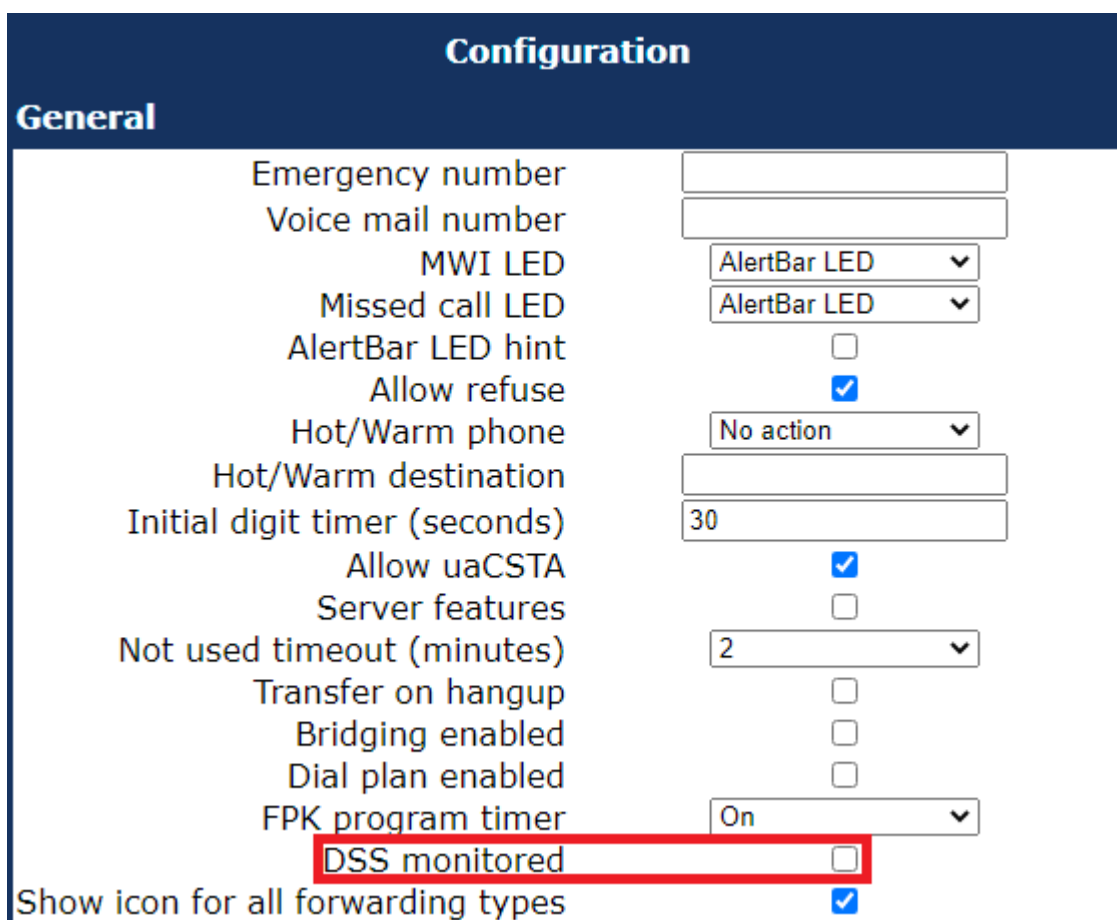
Picture time (secs) 10 ▼

3.9.21 DSS monitoring

If 'DSS monitored' is enabled on a single line phone, the single line phone can be monitored by other phones using a DSS key, so the monitored phone does not behave as a multiline phone.

Administration via WBM

Admin > System > Features > Configuration > General: "DSS monitored"



Configuration

General

Emergency number	
Voice mail number	
MWI LED	AlertBar LED ▼
Missed call LED	AlertBar LED ▼
AlertBar LED hint	☐
Allow refuse	☒
Hot/Warm phone	No action ▼
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☒
Server features	☐
Not used timeout (minutes)	2 ▼
Transfer on hangup	☐
Bridging enabled	☐
Dial plan enabled	☐
FPK program timer	On ▼
DSS monitored	☐
Show icon for all forwarding types	☒

3.9.22 Bridged Call Appearance

Bridged Call Appearance feature allows you to use multiple appearances of your line and handle multiple calls on the same line.

A CP phone can be configured with the use of Multiple Call Arrangement (MCA), can have multiple line keys (up to 6, depending on hardware), whereby all of these line keys (MCA keys) have the same E164 number configured. The BCA is an enhancement of the existing MCA that allows the use of shared lines and several BCA keys can have the same URI.

SUBSCRIBE

- SUBSCRIBE must be sent as a subscription for each shared line
- sip: SUBSCRIBE for BCA will include header Event: shared-appearance

Administration via WBM

Local Admin > System > Registration > SIP Session

SIP session	
Session timer enabled	☐
Session duration (seconds)	3600
Registration timer (seconds)	3600
Subscription timer (seconds)	3600

Set the **Server Type** to **RingCentral**.

Set **Subscription timer** to 3600

3.10 Free Programmable Keys

Free Programmable Keys (FPKs) are keys that may be programmed by the phone user or the administrator. Each FPK may have 2 functions programmed:

- Normal (under page 1 column of the relevant tab)
- Shifted (under page 2 column of the relevant tab)

NOTICE: Some functions that may be programmed to an FPK allow additional parameters to be configured too.

Some FPKs may be provided as physical keys on the most phone models and are also available via Key modules for phone models that support KMs.

The OpenScape Desk Phone CP400 phone provides 16 physical free programmable keys (FPKs), which can be associated with special phone functions. This is called „Phone keys“. On the OpenScape Desk Phone CP600 12 soft free programmable keys are provided for each KM, when the KM is not plugged in and so that can be associated with special phone functions. Also the OpenScape Desk Phone CP700/700X phone provides 6 physical free programmable keys (FPKs) and 6 soft free programmable keys (FPKs) via its Favourites screen, which can be associated with special phone functions.

The OpenScape Desk Phone CP400/700/700X can be extended with up to two key modules KM400 providing 16 FPKs each. The OpenScape Desk Phone

CP600 can be extended with up to four key modules KM600 providing 12 FPKs each. The OpenScape Desk Phone CP600E can be extended with up to two key modules KM600 providing 12 FPKs each.

The OpenScape Desk Phone CP200/CP205 and CP100 phones provide four and three pre-programmed physical free programmable keys (FPKs), respectively. This is called „Phone keys“.

The key programming can be accessed via the WBM, via the Local Phone and via DMS.

3.10.1 How to Configure Free Programmable Keys (FPKs)

Free Programmable Keys (FPKs) can be configured via the WBM.

System > Features > Program keys.

NOTICE:

The **Program Keys** configuration is valid only for the CP100/200/400 Phones.

Program keys



To assign a new function to a key, select from the drop down list box. To view or modify the parameters associated with the key, use the Edit button.

Normal	Key	Shifted
Unallocated Label: Call log	1	Unallocated
Unallocated Label: Directory	2	Unallocated
Unallocated Label: Call forward	3	Unallocated
Unallocated Label: Redial	4	Unallocated

[Download paper label](#)

To assign a new function to a key, select a function from the drop down list. To view or modify the parameters associated with the key, use the **Edit** button. Click **Submit** to save your changes.

3.10.2 Key module settings for CP600/600E/700/700X

The Favourites screen is able to be presented permanently, even when Key Modules are attached, with an independent set of 12 programmable keys. These keys are not associated with any of the keys on any Key Modules. When

Favourites is configured to function this way, it is referred to as **Permanent Favourites**.

Permanent Favourites is always available on a CP700/700X but also becomes available on a CP600/600E when it is in Broadsoft mode (Server Type should be set to Broadsoft). Note that this condition will not check if phone is indeed connected to a Broadsoft server.

Program keys via WBM

When server type is set to Broadsoft for a CP600/600E and regardless the server type for a CP700/700X, WBM will present a "Permanent Favourites" page as additional keys at below path:

Admin Settings > System > Features > Permanent Favourites

To assign a new function to a key, select from the drop down list box. To view or modify the parameters associated with the key, use the **Edit** button.

3.10.2.1 Feature Key for CP700/700X

The OpenScape Desk Phone CP700/700X has a Feature Key at the right lower corner. Feature Key is configurable in WBM and DLS.

Program key via WBM

WBM presents a **Feature Key** page as an additional key at below path:

Admin Settings > System > Features > Feature Key

To assign a new function to the Feature Key, select from the drop down list box.
To view or modify the parameters associated with the key, use the **Edit** button.

3.10.3 How to Enable "Long Press" for Free Programmable Keys

The long press feature is always available for the CP20X and for for the permanent Free Programmable Keys on CP700/700X.

Prerequisites

At the phone, the configuration menu for a specific programmable key is called by a long press on the related key.

NOTICE: The "long press" feature is disabled by default. When this parameter is disabled, it is not possible to enter the programming mode by long key press. However, the other methods for key programming remain enabled. For keyset and DSS functionality, please refer to Multiline Appearance/Keyset.

- The "long press" feature can be enabled or disabled by setting the FPK program timer parameter to On (enabled) or Off (disabled). This can be done either via the WBM Administrator pages as described below.
- – **Parameter to On:** means, that long press will access the setting menu to program the pressed key.
- – **Parameter to Off:** CP20X and CP100 - Feature on 2nd level of the FPK is accessed with long press. CP400/600/600E - Long press is disabled. Remark: 2nd level has not access to the LED.

Step by Step

In the WBM Administrator pages, navigate to System > Features > Configuration and set the FPK program timer to On or Off. Click Submit to save your changes.

System > Features > Configuration

Configuration	
General	
Emergency number	
Voice mail number	
MWI LED	AlertBar LED ▼
Missed call LED	AlertBar LED ▼
AlertBar LED hint	☐
Allow refuse	☒
Hot/Warm phone	No action ▼
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☒
Server features	☐
Not used timeout (minutes)	2 ▼
Transfer on hangup	☐
Bridging enabled	☐
Dial plan enabled	☐
FPK program timer	On ▼
DSS monitored	☐
Show icon for all forwarding types	☒

3.10.4 Selected Dial Action on Calls

This feature allows the user to perform a certain action, while the Selected Dialing FPK is pressed during an active or held call. The available options are:

- **Consult:** the action performed will be a Consultation transfer to the destination configured in the **Selected Dialing Key** menu which has been pressed.
- **Transfer:** the action performed will be a Blind transfer to the destination configured in the **Selected Dialing Key** menu which has been pressed.
- **No Action:** no action will take place. The call will continue to be active or held based on what the user has selected.

Default value: **No Action**.

Administration via WBM

System > Features > Configuration

Administrator settings

User settings

Licences

Logout

Admin login

Bluetooth

Network

System

System identity

SIP interface

Registration

SNMP

Features

Configuration

Keyset operation

DSS settings

Addressing

Feature access

Feature Key

Permanent Favourites

Key module 1

Key module 2

Door opener

Security

ICE

File transfer

Local functions

Date and time

Speech

General information

Security and policies

Ringer setting

Mobility

Diagnostics

Configuration

General

Emergency number

Voice mail number

MWI LED

Missed call LED

AlertBar LED hint

Allow refuse

Hot/Warm phone

Hot/Warm destination

Initial digit timer (seconds)

Allow uaCSTA

Server features

Not used timeout (minutes)

Transfer on hangup

Bridging enabled

Dial plan enabled

FPK program timer

Selected Dial Action on calls

DSS monitored

Show icon for all forwarding types

Automatic key module switchback

498974110602

AlertBar LED

AlertBar LED

☐

☒

No action

30

☒

☒

2

☐

☐

☐

On

No action

☐

☐

☒

Administration via Local Phone

```
|--- Admin
  |--- System
    |--- Features
      |--- Configuration
        |--- General
          |--- Selected Dial Action on Calls
```

3.10.5 Clear (no feature assigned)

The Clear (no feature assigned) function is used as the default placeholder for unallocated program keys.

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to How to Configure Free Programmable Keys (FPKs).The label displayed to the left of the key is defined in Key label <key number>.

Administration via WBM

System > Features > Program keys

Program keys

 To assign a new function to a key, select from the drop down list box. To view or modify the parameters associated with the key, use the Edit button.

Normal	Key	Shifted
Unallocated ▼	Edit	1 Unallocated ▼ Edit
Unallocated ▼	Edit	2 Unallocated ▼ Edit
Unallocated ▼	Edit	3 Unallocated ▼ Edit
Unallocated ▼	Edit	4 Unallocated ▼ Edit
Unallocated ▼	Edit	5 Unallocated ▼ Edit
Unallocated ▼	Edit	6 Unallocated ▼ Edit
Unallocated ▼	Edit	7 Unallocated ▼ Edit
Unallocated ▼	Edit	8 Unallocated ▼ Edit
Unallocated ▼	Edit	9 Unallocated ▼ Edit
Unallocated ▼	Edit	10 Unallocated ▼ Edit
Unallocated ▼	Edit	11 Unallocated ▼ Edit
Unallocated ▼	Edit	12 Unallocated ▼ Edit
Unallocated ▼	Edit	13 Unallocated ▼ Edit
Unallocated ▼	Edit	14 Unallocated ▼ Edit
Unallocated ▼	Edit	15 Unallocated ▼ Edit
Unallocated ▼	Edit	16 Unallocated ▼ Edit

[Download paper label](#)

3.10.6 Selected Dialing

On key press, a pre-defined call number is called.

The call number defined in the Dial number parameter is dialed on key press.

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to How to Configure Free Programmable Keys (FPKs).

Administration via WBM

System > Features > Program keys > Selected dialling

3.10.7 Repeat Dialing

On key press, the call number that has been dialed lastly is dialed again.
The label displayed to the left of the key is defined in Key label <key number>.

Administration via WBM

System > Features > Program keys > Repeat dialling

3.10.8 Call Forwarding (Standard)

This key function controls phone based call forwarding. If forwarding is enabled, the phone will forward incoming calls to the predefined call number, depending on the current situation.

NOTICE: To use phone based call forwarding, Server features must be switched off (see [Call-Center Agent](#) on page 173).

NOTICE: This feature can be enabled or disabled under System > Features > Feature access (see [Feature access](#) on page 148).

The Forwarding type parameter determines the forwarding behaviour.

- If "Unconditional" is selected, any incoming call will be forwarded.
- If "On no reply" is set, the call will be forwarded when the user has not answered within a specified timespan.

NOTICE: The timespan is configured in the WBM user pages under User > Configuration > Incoming calls > Forwarding > No reply delay (seconds). If "On busy" is selected, incoming calls will be forwarded when the phone is busy.

- If "On busy" is selected, incoming calls will be forwarded when the phone is busy.

Use the Key label <key number> field to define or change the name (label) of the key.

Administration via WBM

System > Features > Program keys > Forwarding

3.10.9 Call Forwarding by Call Type

This feature enhances the Call Forwarding (Standard) operation (see [Call Forwarding \(Standard\)](#) on page 192) by adding support for additional Call Forwarding settings explicitly for External and Internal calls, as well as the existing capability to forward any call, using functional menus that extend the existing Call Forwarding UI.

NOTICE: To use extended call forwarding, Server features and Allow uaCSTA must be switched on (see [Call-Center Agent](#) on page 173).

NOTICE: This feature can be enabled or disabled under System > Features > Feature access > Ext/int forwarding (see [Feature access](#) on page 148).

The label displayed to the left of the key is defined in Key label <key number>. It is possible to have an extra key defined for each Call Forwarding Call Type.

Data required

- **Forwarding type:** Determines forwarding behaviour. Value range: „CF Unconditional any“, f „CF no reply - any“, „CF busy - any“, „CF unconditional - ext.“, „CF unconditional - int.“, „CF no reply - ext.“, „CF no reply - int.“, „CF busy - ext.“, „CF busy - int“ Default: „CF Unconditional any“
- **Destination:** Destination number of call forwarding.

Administration via WBM

System > Features > Program keys > Forwarding

Administration via WBM (User menu)

User > Configuration > Incoming calls > Forwarding

Forwarding	
Forwarding- Unconditional	
Forward any call	☐
to	2153
Destination	
Forward external calls	☐
to	2102
Destination	
Forward internal calls	☐
to	not set
Destination	
Forwarding- Busy	
Forward any call	☐
to	2152
Destination	
Forward external calls	☐
to	2102
Destination	
Forward internal calls	☐
to	2102
Destination	
Forwarding- No reply	
Forward any call	☐
to	2102
Destination	
Forward external calls	☐
to	2102
Destination	
Forward internal calls	☐
to	2102
Destination	
Forwarding Favourites	
Forwarding Favorites	
Submit	Reset

3.10.9.1 Call Forwarding Indication

The forwarding icon can be now shown in the main menu of the phone, in case „unconditional“ forwarding, forward „on busy“ or forward on „no reply“ is active. The user will get a visual indication in the main menu of the phone.

The presence key LED (on OpenScape CP400/CP600/600E) and the built in forwarding key (on OpenScape CP20X) reflects the status for forwarding types „no reply“ or „busy“. If call forwarding „no reply“ or „busy“ is active (or more than one type of forwarding, including unconditional), the LED/built in key will be ON. On OpenScape CP400 / CP600 / CP600E/700/700X, the LED will be solid green. On OpenScape CP20X, the built in forwarding key will be solid green.

The forwarding icon used for unconditional forwarding can now be used for forwarding types „busy“ or „no reply“ and will be displayed in the main menu screen. (Only 1 icon can be displayed, no matter if more than one forwarding type is active.). On OpenScape CP20X, the forwarding icon (incl. forwarding destination) is toggling on the main screen. On OpenScape CP100, there is no LED displaying the forwarding functionality but a static forwarding icon is displayed on the idle screen whilst forwarding is activated.

NOTICE: Forwarding unconditional is not affected by this item. No matter what the setting is, the phone always displays a forwarding icon and make keys LED turn on if call forwarding unconditional is activated.

NOTICE: The current toast notifications remain unchanged.

Administration via WBM:

If the item is configured, the phone will show the visual indication as described above for all forwarding types. The item can be configured via path:

Admin -> System -> Features -> Configuration -> General -> Show notification on all forwarding types

Configuration	
General	
Emergency number	
Voice mail number	2404986220
MWI LED	Key & AlertBar
Missed call LED	Key & AlertBar
Allow refuse	☐
Hot/Warm phone	No action
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☒
Server features	☒
Not used timeout (minutes)	2
Transfer on hangup	☐
Bridging enabled	☐
Dial plan enabled	☐
FPK program timer	On
DSS monitored	☐
Show icon for all forwarding types	☐

3.10.10 Ringer off

This function turns off the ring tone. Incoming calls are indicated via LEDs and display only.

Click **Edit** to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys

Program keys			
	To assign a new function to a key, select from the drop down list box. To view or modify the parameters associated with the key, use the Edit button.		
	Normal	Key	Shifted
	Ringer off	Edit	1 Unallocated
			Edit

3.10.11 Hold

The call currently selected or active is put on hold.

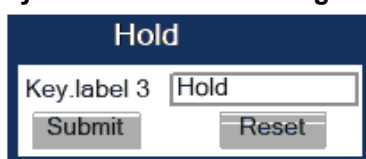
A held call can be retrieved by pressing the key a second time.

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Hold



3.10.12 Alternate

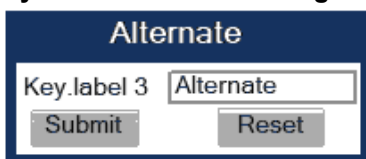
Toggles between two calls; the currently active call is put on hold.

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Alternate



3.10.13 Blind Call Transfer

A call is transferred without consultation, as soon as the phone goes on-hook or the target phone goes off-hook.

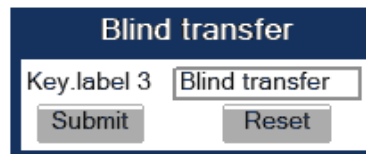
NOTICE: This feature can be enabled or disabled under System > Features > Feature access (see [Feature access](#) on page 148).

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Blind transfer



The screenshot shows a web-based management interface titled "Blind transfer". It contains a text input field labeled "Key.label 3" with the value "Blind transfer" entered. Below the input field are two buttons: "Submit" and "Reset".

3.10.14 Transfer Call

Call transfer, applicable when there is one active call and one call on hold. The active call and the held call are connected to each other, while the phone that has initiated the transfer is disconnected.

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Transfer Call



The screenshot shows a web-based management interface titled "Join". It contains a text input field labeled "Key.label 3" with the value "Transfer Call" entered. Below the input field are two buttons: "Submit" and "Reset".

3.10.15 Deflect a Call

On key press, an incoming call is deflected to the specified destination.

NOTICE: This feature can be enabled or disabled under System > Features > Feature access (see [Feature access](#) on page 148).

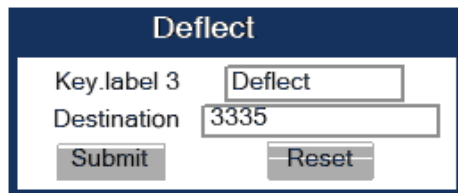
The target destination is defined in the Destination parameter.

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Deflect



3.10.16 Shift Level

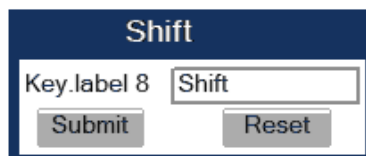
Shift the level for the programmable keys. When activated, the functions assigned to the shifted level are available on the keys.

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Shift



3.10.17 Phone-Based Conference

Establishes a three-party conference from an active call and held call.

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Conference



3.10.18 Accept Call via Headset

On key press, an incoming call is accepted via headset.

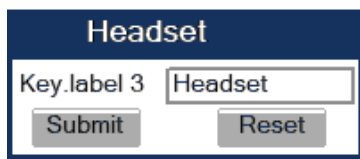
NOTICE: Headset is not available for OpenScope Desk Phone CP100.

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Headset



3.10.19 Do Not Disturb

If this feature is activated, incoming calls will not be indicated to the user.

NOTICE: This feature can be enabled or disabled under System > Features > Feature access (see [Feature access](#) on page 148).

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Do Not Disturb

3.10.20 Group Pickup

On key press, a call for a different destination within the same pickup group is answered.

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

NOTICE:

For RingCentral the Group pickup function is configured as a type of BLF. RingCentral Group Pickup enables to be a part of more than one group, and each of them can be configured per specific key. For more information, see [BLF Key](#) on page 209.

Administration via WBM

System > Features > Program keys > Group pickup

3.10.21 Repertory Dial

This feature is similar to the selected dialing function, but additionally, special calling functions are possible. The desired number and/or function is selected via the Dial string parameter.

NOTICE: This feature can be enabled or disabled under System > Features > Feature access (see [Feature access](#) on page 148).

The following call functions are available:

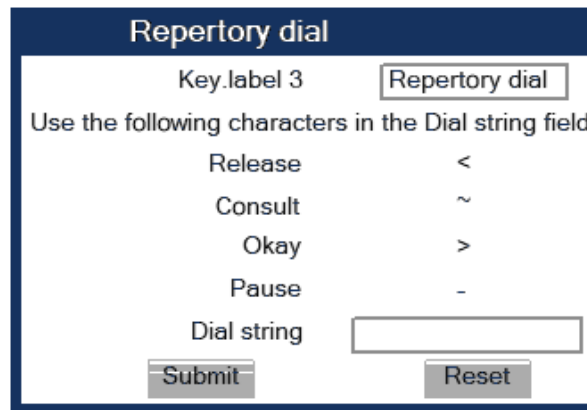
- "<" disconnect a call.
- "~" start a consultation call. Example "~3333>"
- ">" (preceded by a call number) start a call. Example "3333>"
- "-" enter a pause, e. g. for exit-code or international dialing. Example "0-011511234567>"

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Repertory dial



Repertory dial	
Key.label 3	Repertory dial
Use the following characters in the Dial string field	
Release	<
Consult	~
Okay	>
Pause	-
Dial string	
Submit	Reset

3.10.22 Feature Toggle

This feature may be used for different purposes, e.g. hunt groups or whispering. If the user is a member of a hunt group and wants another member of the hunt group to pick up an incoming call, he can signal "Busy status" using the Feature toggle function.

NOTICE: This feature can be enabled or disabled under System > Features > Feature access (see [Feature access](#) on page 148).

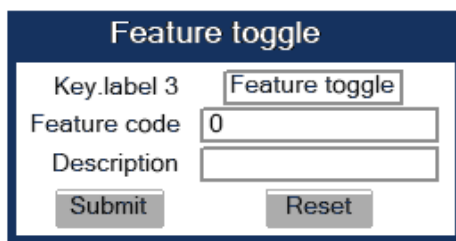
Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

The Feature code to be entered is defined in OpenScape Voice / SIP Server. For Hunt Group, e.g. the code Busy status is used.

Administration via WBM

System > Features > Program keys > Feature toggle



A screenshot of a web form titled "Feature toggle". It contains three input fields: "Key.label 3" with the value "Feature toggle", "Feature code" with the value "0", and "Description" which is empty. Below the fields are two buttons: "Submit" and "Reset".

3.10.23 Mobility / Mobile User Logon

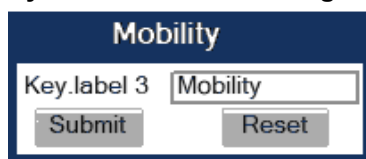
The mobility feature enables users to transfer their personal settings, such as their key layout, or personal phonebook, from one phone to another. The data is stored and managed by the DLS (Deployment Service).

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Mobility



A screenshot of a web form titled "Mobility". It contains one input field: "Key.label 3" with the value "Mobility". Below the field are two buttons: "Submit" and "Reset".

3.10.23.1 Bluetooth mobility

Bluetooth specification requires pairing of devices before connecting. Pairing is a security mechanism during which several parameters unique to both devices (among others Bluetooth hardware addresses of both devices) are combined in a number called a link key. The link key is then used to establish a session over secure channel. Bluetooth hardware address is the only datum that needs to be transferred together with the link-key set in order for the link-keys to work on different hardware.

Because of that the Bluetooth hardware address is part of the mobile user data profile and is assign to device on logon. When the user logs off, Bluetooth address is again unassigned. This way the Bluetooth hardware address and the link-keys travel with the mobile user and the user can seamlessly use his/her paired Bluetooth devices.

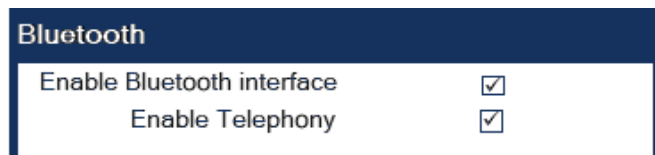
The pool of mobile Bluetooth addresses, which can be assigned to device, have to be setup on DLS server. In case of large installations, DLS admin must ensure that any chance of address collision in possible mobile scenarios will be avoid.

NOTICE: This feature is for OpenScape Desk Phone CP600/700/700X only.

3.10.23.2 Disable HFU

With this feature, Administrator can disable HFA (carkit) functionality.

Admin > Bluetooth > Feature access



Bluetooth	
Enable Bluetooth interface	☒
Enable Telephony	☒

3.10.24 Directed Pickup

This feature enables the user to pick up a call which is ringing at another phone. On pressing the key, a menu opens which requests the call number of the target phone.

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Directed pickup



Directed pickup

Key.label 3

3.10.25 Callback

When the remote phone called is busy does not reply, the user can send a callback request to the server by pressing this key.

NOTICE: This feature can be enabled or disabled under System > Features > Feature access (see [Feature access](#) on page 148).

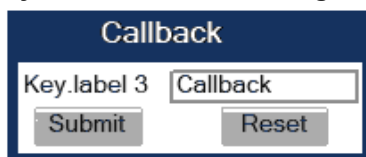
Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys,

please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Callback



3.10.25.1 Cancel Callbacks

With this this function, the user can cancel all callback requests on the server.

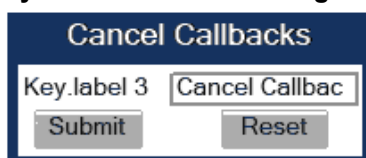
NOTICE: This feature can be enabled or disabled under System > Features > Feature access (see [Feature access](#) on page 148).

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Cancel callbacks



3.10.26 Pause Callbacks

With this this function, the user can pause the execution of all pending callback requests.

NOTICE: This feature can be enabled or disabled under System > Features > Feature access (see [Feature access](#) on page 148).

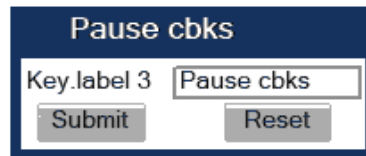
Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys,

please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Pause callbacks



The screenshot shows a web form titled "Pause cbks". It contains a text input field labeled "Key.label 3" with the value "Pause cbks" entered. Below the input field are two buttons: "Submit" and "Reset".

3.10.27 Resume Callbacks

With this this function, the user can resume the execution of pending callback requests.

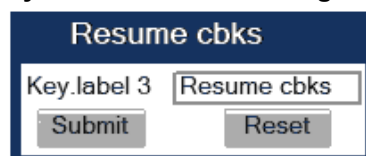
NOTICE: This feature can be enabled or disabled under System > Features > Feature access (see [Feature access](#) on page 148).

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Resume callbacks



The screenshot shows a web form titled "Resume cbks". It contains a text input field labeled "Key.label 3" with the value "Resume cbks" entered. Below the input field are two buttons: "Submit" and "Reset".

3.10.28 Consultation

When the phone is engaged in an active call, this function opens a dialing menu to make a consultation call.

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Consultation

3.10.29 Call Waiting

Enables or disables the call waiting feature. If enabled, calls from a third party are allowed during an active call.

NOTICE: The Call Waiting feature cannot be disabled if System > Registration > Server type (see [SIP Registration](#) on page 120") is set to "HiQ8000".

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Call waiting

3.10.30 Call Recording

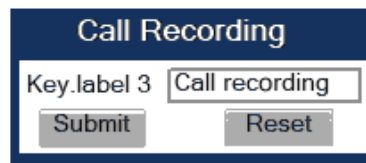
Starts or stops call recording (for configuring call recording, see [Call Recording](#) on page 181).

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys > Call recording



Call Recording

Key.label 3

3.10.30.1 Auto Answer With Zip Tone

This feature is primarily designed for call centers. If activated and a headset is used, the phone will automatically accept incoming calls without ringing and without the necessity to press a key. Moreover, additional signaling information from OpenScape Voice is not required.

To indicate a new call to the user, a zip tone is played through the headset when the call is accepted.

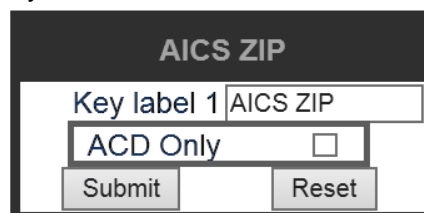
Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

NOTICE: The feature is available for OpenScape Desk Phone CP, which provide a headset jack; it only operates if the headset is plugged in. In case the key for feature activation has been pressed before the headset is connected, the feature will be automatically activated when the headset is plugged in.

Administration via WBM

System > Features > Favourites/Key module > Program keys > AICS Zip tone



AICS ZIP

Key label 1

☐

If ACD Only option selected only calls from ACD systems will be auto-answered.

3.10.31 Server Feature

Invokes a feature on the SIP server. The status of the feature can be monitored via the LED associated to the key.

NOTICE: This function is intended primarily for operation with an Asterisk SIP server. For details, please refer to the

Administration Manual for OpenScape Desk Phone CP on Asterisk.

3.10.32 BLF Key

This function offers the possibility to monitor another extension, and to pick up calls for the monitored extension.

NOTICE: This feature can be enabled or disabled under System > Features > Feature access.

NOTICE: This function is intended primarily for operation with an Asterisk SIP server. For details, please refer to the Administration Manual for OpenScape Desk Phone CP on Asterisk.

Broadsoft and RingCentral are supported too.

Data required

Key label <n>: Label for the key.

Monitored phone: Internal phone number to be monitored for status changes.

Auditable alert: Determines whether an audible alert is played to indicate an incoming call for the monitored phone.

Popup on alert: Determines whether an alert pop-up to indicate an incoming call for the monitored phone.

Action on calls: RingCentral feature. The BLF key can be configured to perform a certain action when it is pressed during a call. The available options are:

- **Transfer:**

Configuration with **Transfer** allows the user to pass a call directly to another phone configured in the **BLF** menu.

For more information see [Blind Call Transfer](#) on page 197.

- **Consult:**

Configuration with **Consult** allows the user to make a consultation call by pressing the BLF key during the call.

For more information see [Consultation](#) on page 206.

• **Group Pickup:**

When **Group Call Pickup** is used, group members receive an alert when a call is ringing on any other group member's device. Configuration with **Group Pickup** allows a group member to pickup a group call.

For more information see [Group Pickup](#) on page 201.

Group pickup ID is configured as BLF Monitored phone (Group pickup ID - string used by Ring Central to address the appropriate pickup group, used in SIP Header).

Group name is configured as BLF Key label.

NOTICE: User/extension can be a member of more than one group and each of them can be configured per specific key.

NOTICE:
RingCentral supports also Call park keys independent of BLF.

BLF

Key label 1

BLF

Monitored phone

Audible alert

☐

Popup on alert

☐

Action on calls

Transfer

Submit

Reset

BLF alerting

Administration via WBM

System > Features > Configuration > BLF alerting

RingCentral feature. The BLF key can be configured to enable audio notification when any of the monitored phones is ringing. The available options are:

- **Beep:** phone plays a beep sound.
- **Ring burst:** phone plays ringer tone for a few seconds.
- **Ring continuous:** phone plays ringer tone whilst any of the monitored phones is ringing.

Alerting

BLF alert	Beep
Group pickup alert	Off
Group pickup tone interval	15
Group pickup visual alert	Prompt
MLPP ringer	
Callback ringer	
Impact level ringer	

Administration via WBM

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

System > Features > Addressing

Addressing	
MW server URI	
Conference	
Group pickup URI	
Callback: FAC	
Callback cancel all	
BLF pickup code	
BLF resource list URI	
Submit Reset	

If a resource list URI is given, the phone subscribes to the given URI.

3.10.33 Send Request via HTTP/HTTPS

With this function, the phone can send a specific HTTP or HTTPS request to a server. The function is available at any time, irrespective of registration and call state. Possible uses are HTTP-controlled features on the system, or functions on a web server that can only be triggered by HTTP/HTTPS request, e. g. login/logout for flexible working hours.

The Protocol parameter defines whether HTTP or HTTPS is to be used for sending the URL to the server.

The Web server address is the IP address or DNS name of the remote server to which the URL is to be sent.

The Port is the target port at the server to which the URL is to be sent.

The Path is the server-side path to the desired function, i. e. the part of the URL that follows the IP address or DNS name. Example: webpage/checkin.html

In the Parameters field, one or more key/value pairs in the format "<key>=<value>" can be added to the request, separated by an ampersand (&). Example: phonenummer=3338&action=huntGroupLogon

NOTICE: The question mark will be automatically added between the path and the parameters. If a question mark has been entered at the start of the parameters, it will be stripped off automatically.

The Method parameter determines the HTTP method to be used, which can either be GET or POST. If GET is selected, the additional parameters (Parameters) and the user id/password (Web server user ID/Web server

password) are part of the URL. If POST is selected, these data form the body of the message.

In case the web server requires user authentication, the parameters Web server user ID and Web server password can be used. If not null, the values are appended between the server-side path (Path) and the additional parameters (Parameter).

If the LED controller URI is given, the LED associated with this key indicates the state of the call number or SIP URI specified, provided the SIP server sends a notification:

- **Busy notification:** LED is glowing.
- **Ringing notification:** LED is blinking.
- **Idle notification (state=terminated):** LED is dark.

NOTICE: When assigning the function described here to the release key S, please consider that this key has no LED.

If the Push support parameter is activated, the LED is controllable by a combination of an HTTP push request and an XML document. For further information, see the XML Applications Developer's Guide.

NOTICE: If you want to use the HTTP push solution, please ensure that the LED controller URI field is empty. Otherwise, the phone will only use the SIP mechanism for LED control, and ignore the push request.

The Symbolic name is used to assign a push request from the application server to the appropriate free programmable key resp. fixed function key. This value must be unique for all keys involved.

Data required

- **Key label <n>:** Label for the key.
- **Protocol:** Transfer protocol to be used. Value range: "HTTP", "HTTPS"
- **Web server address:** IP address or DNS name of the remote server.
- **Port:** Target port at the server.
- **Path:** Server-side path to the function.
- **Parameters:** Optional parameters to be sent to the server.
- **Method:** HTTP method used for transfer. Value range: "GET", "POST"
- **Web server user ID:** User id for user authentication at the server.
- **Web server password:** Password for user authentication at the server.
- **LED controller URI:** Indicates the state of the call number specified.
- **Push support :** Enables or disables LED control by push requests from the server.
- **Symbolic name :** Assigns a push request to the appropriate free programmable key resp. fixed function key.

Administration via WBM

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

System > Features > Program keys > Send URL

Send URL

Key label 2

Message details

Protocol

Web server address

Port

Path

Parameters

Method

Authenticate phone

Web server user ID

Web server password

SIP response handling

LED controller URI

Push support

Push support ☐

Symbolic name

3.10.34 Built-in Forwarding

As a programmable key function, this is relevant for OpenScape Desk Phone CP100/CP200/CP205 and OpenScape Desk Phone CP400 phones, which have no fixed forwarding key.

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

System > Features > Program keys > Built-in forwarding

Built in fwd

Key.label 3

On OpenScape Desk Phone CP100/CP200/CP205 also available on 2nd level.
For more information, see [Enable "Long Press" for Free Programmable Keys on second level for CP20X Broadsoft](#).

3.10.35 2nd Alert

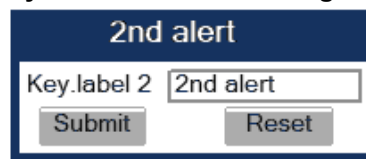
This function allows for monitoring and accepting a second incoming call. When a call is ringing while the user is dialing, the LED will light up. As soon as the user presses the key, information about the incoming call is presented, and the user can accept the call. If a call is ringing, and another call starts ringing shortly after, the LED will light up, and the user has the possibility to toggle between these calls via key press.

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

Administration via WBM

System > Features > Program keys



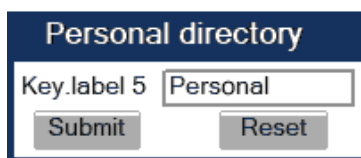
The screenshot shows a web form titled "2nd alert" with a dark blue header. Below the header, there is a text input field labeled "Key.label 2" containing the text "2nd alert". Below the input field are two buttons: "Submit" and "Reset".

3.10.36 Start Phonebooks

These key functions opens a menu which enables the user to start the personal or the corporate phonebook. For further information about the personal and corporate phonebook, please refer to the user guide for OpenScape Desk Phone CP100/CP200/CP205 phones. For more information about the corporate phonebook, please see [Corporate Phonebook: Directory Settings](#) on page 275.

Administration via WBM

System > Features > Program keys > Personal directory



The screenshot shows a web form titled "Personal directory" with a dark blue header. Below the header, there is a text input field labeled "Key.label 5" containing the text "Personal". Below the input field are two buttons: "Submit" and "Reset".

System > Features > Program keys > Corporate directory



The screenshot shows a web form titled "Corporate directory" with a dark blue header. Below the header, there is a text input field labeled "Key.label 5" containing the text "Corporate". Below the input field are two buttons: "Submit" and "Reset".

3.10.36.1 Network directories for Broadsoft

Available network directories (accessible by BroadSoft Xtended Services Interface) can be activated/deactivated and supplied with customized names.

To synchronize Network directories, the XSI has to be activated.

Administration via WBM

Local functions > Network directories

Label	Checkbox	Value
Group	☒	Gruppe
Enterprise	☒	Firma
Group common	☒	Gruppe allgemein
Enterprise common	☒	Firma allgemein
Personal	☒	Persönlich

Submit Reset

On OpenScape Desk Phone CP100/CP200/CP205 also available on 2nd level.
For more information see [Enable "Long Press" for Free Programmable Keys on second level for CP20X Broadsoft](#).

3.10.37 Show phone screen (OpenScape Desk Phone CP100/CP200/CP205 only)

On pressing this key, the phone display switches to call view mode.

Administration via WBM

System > Features > Program keys > Show phone screen

Key.label3 Show phone screen

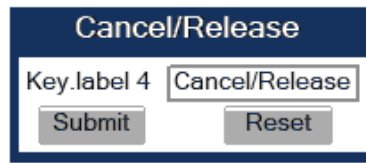
Submit Reset

3.10.38 Release

On pressing this key, the current call is disconnected. This programmable key function is available on all phone models, which have no fixed release key.

Administration via WBM

System > Features > Program keys > Release



3.10.39 Stimulus Idle screen menu options

You can have a preconfigured DTMF code incorporated as an active call screen option so that when you press that option the preconfigured code will be called automatically.

The RingCentral server supports features corresponding to Idle screen options. These features are ONLY available on idle screen and include the following:

- **Redial**

Only available in Main menu screen (CP-HI) or Idle screen (CP-LO).

NOTICE: Since there is already an existing Redial option on the phones, it should be removed as soon as the RC server side decides to configure a new Redial option.

- **Two types of Intercom**

(one is activated with *84 and the other with *85)

- **Login** (*90)
- **Logout** (*91)
- **Switch** (*80)
- **Messages** (*86)

Administration via WBM

You can configure Idle menu options via **Administrator Settings > Local functions > Soft menu options info**

Soft menu options	
Soft menu option 1	
Name/Label	<i>Call park</i>
To be shown in	<i>Call</i>
Menu position	<i>Top</i>
Action type	<i>DTMF</i>
DTMF sequence	<i>#7275</i>
Soft menu option 2	
Name/Label	<i>Record call</i>
To be shown in	<i>Call</i>
Menu position	<i>Higher</i>
Action type	<i>DTMF</i>
DTMF sequence	<i>*9</i>
Soft menu option 3	
Name/Label	<i>""</i>
To be shown in	<i>Call</i>
Menu position	<i>Undefined</i>
Action type	<i>Not configured</i>

Example of Idle Menu options:

- Example of Idle menu options display on CP-HI:
 - 1. Favourites
 - 2. Conversations
 - 3. Settings
 - 4. Redial
 - 5. Intercom
 - 6. Login
 - 7. Logout
 - 8. Switch
 - 9. Messages
- Example of Idle menu options display on CP-LO:
 - 1. Redial
 - 2. Ringer off
 - 3. Do not Disturb on
 - 4. Cancel Callbacks
 - 5. Pickup
 - 6. Intercom
 - 7. Login
 - 8. Logout
 - 9. Switch
 - 10. Messages

3.11 Door opener on OpenScape Desk Phone CP600/600E/700/700X

Door opener enables you to monitor your entrance area and control your doors remotely using your OpenScape Desk Phone CP600/600E/700/700X.

There are two different ways to control door opener:

- Via a phone call to door opener
- Via HTTP/S request to door opener

The telephone can support up to four different door openers. Each door is considered as an independent door and can be controlled using a different control method.

Door opener can be configured via the WBM or on the local phone.

Administration via WBM

System > Features > Local features

Administration via Local Phone

The configuration of door opener via Local

```
|--- Admin
    |--- System
        |--- Features
            |--- Local features
                |--- Phone call
                    |--- Name
                    |--- Door opener
number
                    |--- Door opener PIN
                    |--- Associated door
phone opener
                    |--- FPK
                    |--- HTTP/S request
                        |--- Name
                        |--- Protocol (HTTP/
HTTPS)
                        |--- Door opener
address
                        |--- Door opener port
                        |--- URL path
```

When someone rings at the door, the phone rings.

If the call is from door opener with associated camera and the **Automatic Door Video** option is enabled, the user can see the camera stream before answering the call by pressing "Show video" SRK or related Camera FPK button. Otherwise, video image is shown automatically only after answering the call.

If the call is from door opener with associated camera and the **Automatic Door Video** option is disabled, the user can see the camera stream either before or after answering the call by pressing "Show video" SRK or related Camera FPK button.

NOTICE:

Phones fully support RTSP video stream up to 640x480 pixels resolution. In case a higher resolution video feed is received, then due to hardware limitations it is displayed in smaller video window in order to maintain high-quality performance.

3.12 Action URLs

On specific phone events the phone automatically transmits an HTTP request to report something that happened on the phone.

The OpenScape Desk Phones support the following Action URLs event types:

- Phone startup
- Primary Line registered (triggered when primary line status changes from **not registered** to **registered**)
- Primary Line unregistered (triggered when primary line status changes from **registered** to **not registered**)
- Phone idle (triggered when phone becomes idle after using speaker, headset or handset)
- Phone busy (triggered when phone becomes busy when using speaker, headset or handset)
- Incoming call on primary line
- Outgoing call on primary line
- Connected call on primary line
- Disconnected call on primary line
- Call forwarding primary line
- DND primary line

If the event occurs and a URL is configured for the specific event, the phone sends a request to the configured URL. The type of request (GET, POST, PUT) can be configured. Both, http and https URLs are supported.

Certificates and security policy for validating the server is being used from Send URL.

NOTICE: In order to support mTLS, the HttpClient certificate is being used. In case no HttpClient certificate is installed, the phone fallbacks to the devices specific and the device default certificate.

Parameters can be added as part of the URL configuration.

The phone supports different placeholders as part of the URL, that are replaced by the actual value

- **\$E164** (the E164 number of the phone)
 - supported for all event types.
- **\$MAC** (The MAC address of the phone)
 - supported for all event types.
- **\$REMOTE** (the user part of the URI provided in SIP requests/responses of the remote party)
 - supported for the following event types: Incoming call, Outgoing call, Connected call, Disconnected call.

Administration

Fixed Function Keys on OpenScape Desk Phone CP100/CP200/CP205

- **\$STATUS**(the status of the feature, true=activated, false=deactivated)
 - supported for the following event types: Call forwarding, DND.

Administration via WBM

System > Features > Action URLs



Set Method, URL and placeholders for every defined event type.
Example: `https://server.local:10443/path/event?e164=$E164`
Placeholder all events: `$E164`, `$MAC`
Placeholder call events: `$REMOTE`
Placeholder forwarding, dnd events: `$STATUS`

Event	Method	URL
Phone Started	GET	<code>http://1.2.3.4/startup?e164=\$E164&mac=\$MAC</code>
Primary Line Registered	GET	
Primary Line Unregistered	GET	
Phone Idle	POST	<code>https://server.de/idle?e164=\$E164</code>
Phone Busy	POST	<code>https://server.de/busy?e164=\$E164</code>
Incoming Call Primary Line	GET	
Outgoing Call Primary Line	GET	
Connected Call Primary Line	GET	<code>https://8.8.8.8/call/\$E164/\$REMOTE</code>
Disconnected Call Primary Line	GET	
Call forwarding Primary Line	PUT	<code>https://9.9.9.9:45678/forwarding?status=\$STATUS</code>
DND Primary Line	GET	

To avoid overload on the phone, all events are queued and being processed one after the other. Under normal circumstances, this is not an issue as everything is nearly processed immediately. However, when remote servers become unavailable, this should help avoid handling too many requests simultaneously.

NOTICE: When this feature is enabled, the user is required to send a confirmation.

3.13 Fixed Function Keys on OpenScape Desk Phone CP100/CP200/CP205

The OpenScape Desk Phone CP100 comes with three programmable keys, which can be reprogrammed with specific functions. The preset (label) is:

- Call log
- Directory
- FwdMenu

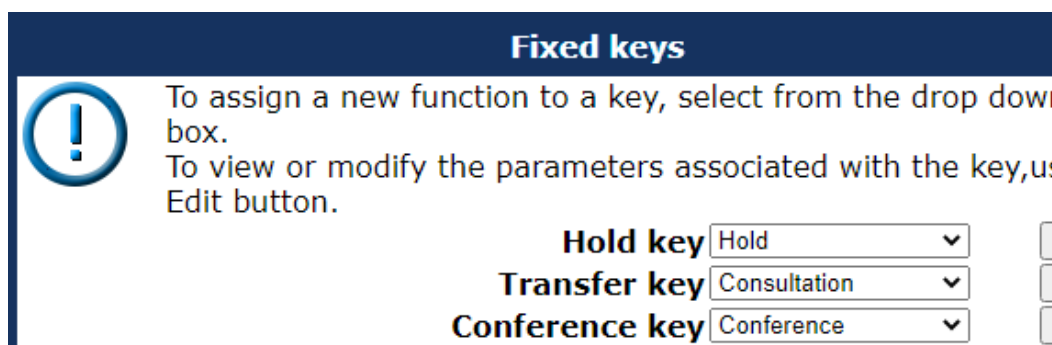
The OpenScape Desk Phone CP200/CP205 comes with three fixed keys, which can be reprogrammed with specific functions. The preset is:

- Hold
- Transfer
- Conference

If you reset the phone, these keys will be reset to the default factory settings.

Administration via WBM

System > Features > Fixed keys



Fixed keys

! To assign a new function to a key, select from the drop down box. To view or modify the parameters associated with the key, use the Edit button.

Hold key Hold ▼

Transfer key Consultation ▼

Conference key Conference ▼

On CP100/CP200/CP205 the three keys are FPKs programmed via **Program keys**.

For CP20X, to assign a new function to a key, select a function from the drop down list. To view or modify the parameters associated with the key, use the Edit button. Click Submit to save your changes.

To assign a new function to a key, select a function from the drop down list. To view or modify the parameters associated with the key, use the Edit button. Click Submit to save your changes.

3.14 Main menu screen options on OpenScape Desk Phones CP400/600/600E/CP700

Main menu screen options in the OpenScape CP 400/600/600E/CP700 Desk Phones can be extended with new menu options, given that the corresponding function is configured. When the phone is idle, the user can use the navigation keys to scroll down to additional menu options, i.e. the "Settings" and "Conversation" keys, ensuring accessibility to all the fixed main menu options of the phone.

NOTICE: The configuration is available only if server type is Broadsoft or Ring Central.

3.14.1 Main Menu Option Configuration

If the phone is configured by the administrator to be connected to a server of type "Broadsoft" or "Ring Central", the extended menu can be displayed instead of the standard menu with additional menu options.

The options are displayed after the phone's **Server type** field is set to **Broadsoft** or **RingCentral** via the WBM **System>Registration** settings or via the WBM **System>SIP session: Server Type**.

Example (Broadsoft Server Type)

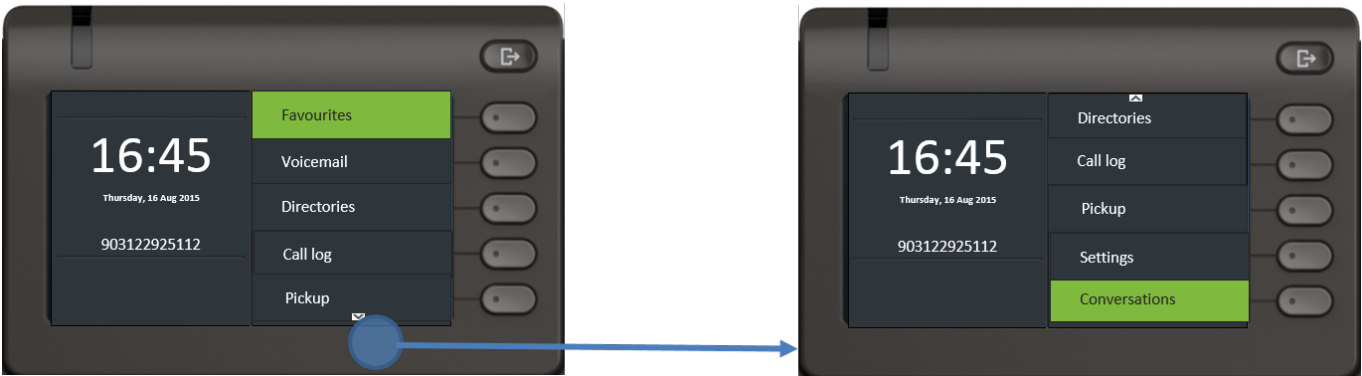
NOTICE: The four fixed function keys displayed in the idle main menu (i.e. Directories, Call log, Voicemail, Pickup for "Broadsoft" server type) are not configurable by the user.

1. Standard Menu	2. Extended Menu
Favourites (or Teams on CP400)	Favourites Voicemail (or Teams on CP400)
Voicemail (if configured)	Voicemail (if configured)
Directories	Directories
Call Log	Call Log
	Pickup
	Settings
	Conversations

NOTICE:

Favourites is available on CP600/600E only if a KM is not plugged in.

On CP400, **Favourites** is replaced by the permanent **Team** menu which only shows Keyset/DSS lines.



Main Menu options (Extended)

- **Favourites**
- **Voicemail:** Voicemail needs a valid voicemail configuration.
- **Directories:** Directory needs a valid XSI server and at least one enabled directory category. The option points to network directories.
- **Call log:** Call log needs an XSI server configuration and enabled network call logs. The option points to network call log.
- **Pickup** (only in the Main Menu of CP600): Pickup needs a configured group pickup code (Subscription not done in this case). The option calls the pickup code.

By using the down arrow to scroll down the menu options, the following hidden options can be displayed:

- Pickup (only for CP400)
- Settings
- Conversations

Example (RingCentral Server Type)

The RingCentral server allows the phone to display up to ten stimulus idle menu options. The RC server can determine where in the Main menu or idle screen menu each stimulus option is placed.

NOTICE: The RingCentral additional menu items can be displayed in all CP Phones (CP100/200/400/600/600E/700/700X). The standard menu options shown in the example below are valid only for the CP400/600/600E/700/700X Phones.

1. Standard Menu	2. Extended Menu
Favourites (or Teams on CP400)	Favourites
Conversations	Conversations
Voicemail (if configured)	Voicemail (if configured)
Settings	Settings
	Stimulus 1
	Stimulus 2
	Stimulus 3



Main Menu options (Extended)

- **Favourites**
- **Conversations**
- **Voicemail (if configured)**
- **Settings**
- By using the down arrow to scroll down the menu options, the following hidden options can be displayed:
 - Stimulus 1
 - Stimulus 2
 - Stimulus 3

3.15 Multiline Appearance/Keyset

A phone that has more than one line associated to it, and therefore works as a multiline phone, is referred to as "keyset". The lines are assigned to the phone by setting up a separate line key for each line.

The multiline appearance feature allows for multiple lines to be assigned to a keyset and for a line to be assigned to multiple keysets. This feature requires configuration in OpenScape Voice and in the telephone, and is particularly useful for executive-assistant arrangements.

NOTICE: In order to configure the phone as a keyset, it is required to

- 1) use an outbound proxy (System > SIP interface > Outbound proxy, see [Outbound Proxy](#) on page 123), and
 - 2) set the server type to "OS Voice" (System > Registration > Server type, see [SIP Registration](#) on page 120).
-

For each keyset, a Primary Line/Main DN is required. The primary line is the dialing number for that keyset.

There are two types of line:

- **Private line:** A line with restricted line status signaling towards OSV.
- **Shared line:** A line that is shared between keysets.

3.15.1 Line Key Configuration

WBM Path: **System > Features > Favourites/Key module**

NOTICE: It is recommended to configure primary lines only on keys 1 to 6, or 1 to 5, if a shift key is needed. This ensures that the lines are still accessible when the user migrates to a different phone with fewer keys via the mobility feature.

A line corresponds to a SIP address of record (AoR), which can be a phone number. It is defined by the Address parameter. For registration of the line, a corresponding entry must exist on the SIP server resp. the SIP registrar server.

A label can be assigned to the line key by setting its Key label.

Every keyset must necessarily have a line key for the primary line. To configure the key of the primary line, set Primary line to "true".

If Ring on/off is checked, the line will ring when an incoming call occurs, and a popup will appear on the display. If the option is not checked, the incoming call will be indicated only by the blinking of the key's LED. If it is desired that the line ring with a delay, the time interval in seconds can be configured by Ring delay.

When the user lifts the handset in order to initiate a call, the line to be used is determined by selection rules. To each line, a priority is assigned by the Selection order parameter. A line with the rank 1 is the first line to be considered for use. If more than one line have the same rank, the selection is made

according to the key number. Note that Selection order is a mandatory setting; it is also relevant to the Terminating line preference, as well as to other functions.

The Address (Address of Record) parameter is the phone number resp. SIP name corresponding to the entry in the SIP registrar at which the line is to be registered.

NOTICE: For the configuration of line keys, the use of the DLS (Deployment Service)/DMS is recommended. For operating the DLS, please refer to the DLS user's guide. For operating DMS, please refer to Wiki page http://wiki.unify.com/wiki/Broadsoft_DMS. Alternatively, the web interface or the local menu can be used. Note that the creation of a new line key and the configuration of some parameters can not be accomplished by the phone's local menu.

Generally, it is advisable to restrict the user's possibilities to modify line keys. This can be achieved solely by the DLS. For further instructions, see the DLS Administration Guide.

The Realm, a protection domain used for authenticated access to the SIP server, works as a name space. Any combination of user id and password is meaningful only within the realm it is assigned to. The other parameters necessary for authenticated access are User Identifier and Password. For all three parameters, there must be corresponding entries on the SIP server.

The Shared type parameter determines whether the line is a shared line, i. e. shared with other endpoints, or a private line, i. e. available exclusively for this endpoint. A line that is configured as primary line on one phone can be configured as secondary line on other phones.

NOTICE: Shared lines are not available if **System > Registration > Server type** (see [SIP Registration](#) on page 120) is set to "HiQ8000".

If a line is configured as hot line, the number indicated in Hot warm destination is dialed immediately when the user goes off-hook. This number is configured in the user menu under **Configuration > Keyset > Lines > Hot/warm destination**. To create a hot line, Hot warm action must be set to "hot line". If set to "Warm phone", the specified destination number is dialed after a delay which is defined in Initial digit timer (seconds) (for details, see [Initial Digit Timer](#) on page 152). During the delay period, it is possible for the user to dial a different number which will be used instead of the hot/warm line destination. In addition, the user will be provided with a dial tone during the delay period. With the setting "No action", the line key will not have hot line or warm line functionality.

Broadsoft feature. Different XSI users can be used per line. The XSI Username refers to a user on the XSI server and can be used to provide access to various user features like caller lists and directories.

Data required

- **Key label <n>:** Set the label of the line key with the key number <n>. Default: "Line"

- **Primary line:** Determines whether the line is the primary line. Value range: "Yes", "No" Default: "No"
- **Ring on/off:** Determines whether the line rings on an incoming call. Value range: "On", "Off" Default: "On"
- **Ring delay (seconds):** Time interval in seconds after which the line starts ringing on an incoming call. Default: 0
- **Selection order:** Priority assigned to the line for the selection of an outgoing line. Default: 0
- **Address:** Address/phone number which has a corresponding entry on the SIP server/registrar.
- **Realm:** Domain wherein user id and password are valid.
- **User Identifier:** User name for authentication with the SIP server.
- **Password:** Password for authentication with the SIP server.
- **Shared type:** Determines whether the line is a shared line (shared by multiple endpoints) or a private line (only available for this endpoint). Value range: "shared", "private". Default: "shared"
- **Hot warm action :** Determines if the line is a regular line, a hot line, or a warm line. Value range: "No action", "hot line", "warm line"
- **Hot warm destination :** The destination to be dialed from the hot/warm line when the user goes off-hook.
- **XSI Username:** The XSI user name that is related to the configured line key on the telephone.

BroadSoft DMS Parameter

```
<Item name="function-key-def" index="1">31</Item>
<Item name="key-label-unicode" index="1">Bob Smith</Item>
<Item name="line-primary" index="1">>false</Item>
<Item name="line-shared-type" index="1">1</Item>
<Item name="line-sip-uri" index="1">2405551111_1</Item>
<Item name="line-sip-user-id" index="1">bobsmith</Item>
```

Shared Call Appearance

For Shared Call Appearance please refer to:

- **Wiki page** http://wiki.unify.com/wiki/Broadsoft_DMS#Shared_call_appearance
- BroadSoft Partner Configuration Guide, Section 4.4.1 Shared Call Appearance Configuration

NOTICE: A new line key can only be added by use of the WBM or the DLS/DMS. Once a line key exists, it can also be configured by the local menu.

3.15.2 How to Configure Line Keys for Keyset Operation

Administration via WBM

- 1) Invoke the Phone keys dialog and select "line" in the pulldown menu of the key you want to configure. Next, click the **edit** button.

System > Features > Program keys

Program keys

 To assign a new function to a key, select from the drop down list box. To view or modify the parameters associated with the key, use the Edit button.

Normal	Key	Shifted
Line Label: 2101	1	Unallocated
Line Label: 2102	2	Unallocated
Line Label: 2103	3	Unallocated
Line Label: 756-6686	4	Unallocated
Line Label: 756-6687	5	Unallocated
Line Label: 756-6688	6	Unallocated
Line Label: 756-6689	7	Unallocated
Line Label: 756-0631	8	Unallocated
Line Label: 756-0633	9	Unallocated
Line Label: 756-0625	10	Unallocated
Unallocated	11	Unallocated
Unallocated	12	Unallocated
Unallocated	13	Unallocated
Unallocated	14	Unallocated
Unallocated	15	Unallocated
Unallocated	16	Unallocated

[Download paper label](#)

- 2) In the Line dialog, set the specific parameters for the line key.

Line

 It is recommended a primary line is only configured on keys 1 to 12 to maintain mobility compatibility with other phone models.

Key label 4: 756-6686

Primary line: ☐

Ring on/off: ☒

Ring delay (seconds): 0

Selection order: 1

Address: 15737566686

Realm: psap

User Identifier: 15737566686

Password:

Shared type: shared

Hot warm action: No action

Hot warm destination:

XSI Username:

- 3) (Only relevant if hot line / warm line is to be configured) The destination for hot line or warm line is set in **User menu > Configuration > Keyset > Lines**:

In the local menu, the menu path is the same.

Administration via Local Phone

The configuration of a line via Local phone is only possible when the line key has been created via Web interface or DLS before.

```

|--- Admin
    |--- System
        |--- Features
            |--- Configuration
                |--- Keyset lines
                    |--- Details For Keyset Line

<xx>

|--- Address
|--- Ring on/off
|--- Selection order
|--- Hot/warm action

```

3.15.3 Configure Keyset Operation

The following parameters provide general settings which are common for all keyset lines.

The Rollover ring setting will be used when, during an active call, an incoming call arrives on a different line. If "no ring" is selected, the incoming call will not initiate a ring. If "alert ring" is selected, a 3 seconds burst of the configured ring tone is activated on an incoming call; "alert beep" selects a beep instead of a ring tone. "Standard ring tone" selects the default ringer.

LED on registration determines whether the line LEDs will be lit for a few seconds if they have been registered successfully with the SIP server on phone startup.

The Originating line preference parameter determines which line will be used when the user goes off-hook or starts on-hook dialing.

NOTICE: When an alerting call exists, the terminating line preference decides which call to answer by just going off-hook.

The following preferences can be configured:

- **"idle line"**: An idle line is selected. The selection is based on the Hunt ranking parameter assigned to each line (see [Line Key Configuration](#) on page 224).
- **"primary"**: The designated Primary Line/Main DN is always selected for originating calls.
- **"last"**: The line selected for originating calls is the line that has been used for the last call (originating or terminating).
- **"none"**: The user manually selects a line by pressing its line key before going off-hook or by pressing the speaker key, to originate a call.

Manual line selection overrides automatic line preferences.

Line action mode determines the consequence for an established connection when the line key is pressed. If "hold" is selected, the call currently active is set to hold as soon as the line key is activated. The user has two options: 1) to reconnect to the remote phone by pressing the line key that corresponds to that call, or 2) to initiate another call from the newly selected line. If "release" is selected, the previously established call is ended.

The Reservation timer sets the period after which the reservation of a line is canceled. A line is automatically reserved for the keyset whenever the user has selected a line for an outgoing call and hears a dial tone. The reservation of a line is accomplished by the OpenScape Desk Phone CP100/200/205/400/600/600E server, which notifies all the endpoints sharing this line. If set to 0, the reservation timer is deactivated.

Forward indication activates or deactivates the indication of station forwarding, i. e. the forwarding function of OpenScape Desk Phone CP100/200/205/400/600/600E. If Forward indication is activated and station forwarding is active for the corresponding line, the LED of the line key blinks.

When Bridging enabled (**Admin > Features > Configuration**) is activated, the user may join into an existing call on a shared line by pressing the corresponding line key. On key press, the OpenScape Voice builds a server based conference from the existing call parties and the user. If the call has already been in a server based conference, the user is added to this conference.

NOTICE: When bridging shall be used, it is highly recommended to configure the phone for a system based conference (see [System Based Conference](#) on page 164). This enables adding more users to a system based conference that has been initiated by bridging.

Data required

- **Rollover ring**: Determines if a ring tone will signal an incoming call while a call is active. Value range: "Standard ring", "No ring", "Alert beep", "Alert ring" Default: "Alert beep"
- **LED on registration**: Determines if line LEDs will signal SIP registration. Value range: "Yes", "No" Default: "Yes"

- **Originating line preference:** Selects the line to be used for outgoing calls. Value range: "Idle line", "Primary", "Last", "None" Default: "Idle line"
- **Terminating line preference:** Determines which line with an incoming call shall be selected for answering. Value range: "Ringing line", "Incoming", "Incoming PLP", "Ringing PLP", "None" Default: "Idle line"
- **Line action mode:** Determines the consequence for an established connection when the line key is pressed. Value range: "Hold", "Release" Default: "Hold"
- **Reservation timer:** Sets the period in seconds after which a line reservation is cancelled. If set to 0, the reservation timer is deactivated. Default: 60
- **Forward indication:** Activates or deactivates the indication of station forwarding. Value range: "Yes", "No" Default: "No"

Administration via WBM

System > Features > Keypad Operation

Keypad operation	
Rollover ring	alert beep
Rollover visual alert	no indication
LED on registration	☒
Originating line preference	idle line
Terminating line preference	ringing line
Line action mode	hold
Reservation timer (seconds)	60
Forwarding indicated	☐
Submit Reset	

System > Features > Configuration

Configuration	
General	
Emergency number	
Voice mail number	
MWI LED	AlertBar only
Missed call LED	AlertBar LED
AlertBar LED hint	☐
Allow refuse	☒
Hot/Warm phone	No action
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uacSTA	☒
Server features	☐
Not used timeout (minutes)	2
Transfer on hanqup	☐
Bridging enabled	☒
Dial plan enabled	☐
FPK program timer	On
Selected Dial Action on calls	No action
DSS monitored	☐
Show icon for all forwarding types	☒
Automatic key module switchback	☒
Simultaneous key module switching	☒

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- Features
            |--- Keypad operation
                |--- Rollover ring
                |--- LED on registration
                |--- Orig line pref
                |--- Term line pref
                |--- Line action mode
                |--- Reservation timer
                |--- Forward indicated

```

Administration via Local Phone

```

|--- Admin
    |--- System
        |--- Features
            Configuration
                |--- General
                    |--- Bridging enabled

```

3.15.4 Immediate Ring

Enables or disables the preset delay for all line keys. This feature only applies to keyset lines.

Administration via WBM**System > Features > Program keys > Immediate ring**

Normal	Key	Shifted
Immediate ring Label: Call log	1	Unallocated

The label displayed is defined in Key label <key number>.

Use the Key label <key number> field to define or change the name (label) of the key.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, please refer to [How to Configure Free Programmable Keys \(FPKs\)](#) on page 186.

NOTICE: It is not allowed to configure more than one Immediate ring on an Assistant-device.

3.15.5 Direct Station Select (DSS)

NOTICE: This feature requires OpenScape Voice.

NOTICE: This feature can be enabled or disabled under System > Features > Feature access (see [Feature access](#) on page 148).

A DSS key is a special variant of a line key. It enables a direct connection to a target phone, allowing the user to pick up or forward a call alerting the DSS target and make/complete a call to the DSS target.

3.15.5.1 General DSS Settings

These parameters define the behaviour of all DSS keys.

NOTICE: Generally, it is advisable to restrict the user's possibilities to modify line keys, including DSS keys. This can be achieved solely via the DLS. For further instructions, see the DLS Administration Guide.

If the user picks up an incoming call for the DSS target by pressing the associated DSS key, the call is forwarded to the user's primary line. Thereafter, the user's phone rings and the user can accept the call.

NOTICE: To enable the immediate answering of a call via the DSS key, **Allow auto-answer** in the user's menu must be activated. The complete path on the WBM is: User Pages > Configuration > Incoming calls > CTI calls > Allow auto-answer.

Administration via WBM

System > Features > DSS Settings

DSS settings	
Call pickup detect timer (seconds)	3
Deflect alerting call enabled	☐
Allow pickup to be refused	☐
Forwarding shown	☐
Caller ID when alerting	☒
Submit Reset	

Call pickup detect timer (seconds)- The value of Call pickup detect timer (seconds) determines the time interval in which the deflected call is expected at the primary line. When the call arrives within this interval, it is given special priority and handling. If a second call arrives on the primary line during this interval, it will be rejected. If a second call arrives outside the interval, it will be treated just like any other incoming call. Default is 3.

Deflect alerting call enabled- If enabled,, the user can forward an alerting call at his phone to the DSS target by pressing the DSS key. Default is "No".

NOTICE: This parameter is configured under System > Features > Feature access (see [Feature access](#) on page 148).

Allow pickup to be refused - If enabled, the user is enabled to reject a call alerting on the line associated with the DSS key. Default is "No".

NOTICE: This parameter is configured under System > Features > Feature access (see [Feature access](#) on page 148).

Forwarding shown - When enabled, The DSS key can be configured to indicate the call forwarding state of the number represented by the DSS key.

Caller ID when alerting- When enabled, the caller party ID in DSS alert notifications is not shown. Default is "True".

Administration via Local Phone

```
|--- Admin
    |--- System
        |--- Features
            |--- DSS operation
                |--- Deflect to DSS
                |--- Refuse DSS pickup
                |--- Forwarding shown
                |--- Caller ID when alerting
|--- Admin
    |--- System
        |--- Features
            |--- Configuration
                |--- General
                    |--- DSS Pickup timer
```

3.15.5.2 Settings for a DSS key

The **Key label <n>** parameter provides the DSS key with a label that is displayed on the graphic display on an OpenScape Desk Phone CP phones. The label is also user configurable.

The **Monitor only** allows the users to use their DSS keys to only monitor other phones.

If desired, an alerting DSS call can be indicated acoustically and visually if **Visual alert** and **Audible alert** are configured.

The **Ring delay** gives a time interval in seconds for the DSS call to start alerting.

Address contains the call number of the line associated with the DSS key.

The **Realm** parameter stores the SIP Realm of the line associated with the DSS key.

User Identifier gives the SIP user ID of the line associated with the DSS key.

Password provides the password corresponding to the SIP user ID.

The **Outgoing calls** parameter determines the behaviour of a call over the DSS line at the target phone. An outgoing call can be attempted to the target phone by pressing its DSS key when the target phone is not alerting. So, if the **Outgoing calls** is set to "Direct", any forwarding and Do not Disturb settings on the target phone will be overridden, so that a call will always alert. If set to Line type is set to "Normal", this is not the case, and the call will be treated like a regular call.

Action on calls defines the handling of an active call at the phone when pressing the DSS key. If set to "Consult", the user has an option to start a consultation with the DSS target. If set to "Transfer", the user can only transfer the call to the DSS target. If "No action" is selected, pressing the DSS key will have no effect.

Data required

- **Key label <key number>**: Label to be displayed on the display. Default: "DSS"
- **Monitor Only**: Handling of an incoming call when pressing the DSS key. "No": the user will be able to answer the call; "Yes": the user will be able to monitor the call without answering it.
Value range: "No", "Yes"
Default: "No"
- **Visual alert**: An alerting DSS call can be indicated visually. "FPK and inline": a notification sausage is displayed independent of any attached Key Module providing the caller information; "FPK only": caller information is only displayed on a CP600 Key Module, Favorites screen or Team screen.
Value range: "FPK only", "FPK and inline".
Default: "FPK and inline"
- **Audible alert**: An alerting DSS call can be indicated acoustically. "Ringer": a DSS key will be set to play the configured ringer file or pattern; "Beep": a DSS key will be configured to only play a single beep tone (only played once, not repeated); "Off": no audible alert.
Value range: "Off", "Ringer", "Beep"
Default: "Off"
- **Ring delay (seconds)**: Time interval in seconds after which the line starts ringing on an incoming call.
Default: "0"
- **Address**: SIP Address of Record of the destination that is assigned to the DSS key.
- **Realm**: SIP Realm of the DSS destination.
- **User ID**: SIP user ID of the DSS destination.
- **Password**: Password corresponding to the SIP user ID.
- **Outgoing calls**: Determines whether forwarding and DND at the target phone will be overridden on a DSS call. Value range: "Normal", "Direct"
Default: "Normal"
- **Action on calls**: Handling of an active call when pressing the DSS key. "Consult": the user can start a consultation with the DSS target; "Transfer": the user can transfer the call to the DSS target. Value range: "Consult", "Transfer", "No action" Default: "Consult"

- **Allow in Overview:** Determines whether the line appears in the phone's line overview. Value range: "Yes", "No" Default: "Yes"

Administration via WBM

System > Features > Program keys > DSS

3.15.6 Distinctive Ringers per Keypad Lines

For implicit mapping of line ringer names the following format is to be used:

"Line-<DN of line>-Reserved"

Each line can be provided with its own distinctive ringer which will be played when a call arrives on the line. Thus for a line with DN=1234 the mapped distinctive ringer name is "Line-1234-Reserved" (The name is case-sensitive, mind the uppercase L and R in name.)

The Admin defines which lines have this ability of the initial ringer. So, the name needs to be manually constructed and configured by Admin as a new ringer name and each such name should be manually checked as being unique in the table.

The User is able to change the initial ringer only if Admin has allowed the line to have its own distinctive ringer.

NOTICE: When using "Distinctive Ringers per Keypad Lines", it is not allowed to define "bellcore_dr1", "bellcore_dr2", and "bellcore_dr3" in the same distinctive ringer table. Otherwise these settings will be used because of higher priority in SIP-

INVITE header. MLPP and Lowel Impact Level calls are also with higher priority.

The "User>Configuration>Keyset>Lines" form has the 'Destination Number' of the line being configured and this can be used to map directly to distinctive ringer names in the "Admin>Ringer setting" form. If a distinctive ringer with a matching name has not been configured into the table then the Ringer related items Ringer, Ringer tone melody, and Ringer sequence in the "User>Configuration>Keyset>Lines" form will be absent. If a matching distinctive ringer name is found then the "Ringer" items are editable with the initially shown value being the same as the value in the "Admin>Ringer setting" form. Changes made to the "Ringer" values by the User will also change the matching distinctive ringer values in "Admin>Ringer setting".

Distinctive Ringers are not applicable for DSS Keys.

Data required

- **Name:** Distinctive ringer name. Value Range: "Line-<Destination Number of line>-Reserved"
- **Ringer sound:** Specifies whether pattern, i. e. melody, or a specific sound file is used as ringer. Default: 'Pattern'
- **Pattern melody:** Determines the melody pattern if Ringer sound is set to 'Pattern'. Value Range: 1,...,8
- **Pattern sequence:** Determines the length and repetitions of pattern. Value Range: "1": 1 sec ON, 4 sec OFF, "2": 1 sec ON, 2 sec OFF "3": 0.7 sec ON, 0.7 sec OFF, 0.7 sec ON, 3 sec OFF Default: "1"

Administration via WBM

Admin > Ringer setting > Distinctive

Distinctive					
 This page allows you to set up interworking with other IP phone systems that support distinctive ringing					
Name	Ringer sound	Pattern melody	Pattern sequence	Duration (sec)	Audible
Belcore-dr1	Pattern	2	2	60	Ring
Belcore-dr2	Pattern	2	2	60	Ring
Belcore-dr3	Pattern	2	2	60	Ring
alert-emergency	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring

Administration via Local Phone

```

|--- Admin
    |--- Ringer setting
        |--- Distinctive
            |--- <1 .... 15>
                |--- Name
  
```

```

|--- Ringer sound (= Ringer in
UserMenu)
|--- Pattern melody (= Ringer
melody in UserMenu)
|--- Pattern sequence (= Ringer
tone sequence in User Menu)
|--- Duration
|--- Audible

```

User menu > Configuration > Keypad > Lines

Administration via Local Phone

The configuration of a line via Local phone is only possible when the line key has been created via WBM or DLS before by administrator.

```

|--- User Menu
|--- Configuration
|--- Keypad
|--- Lines <xx>
|--- Ringer file(= Ringer sound in
Admin Menu)
|--- Ringer melody (= Pattern
melody in Admin Menu)
|--- Ringer sequence (= Pattern
sequence in Admin Menu)

```

3.15.7 Multiple Call Arrangement

Multiple Call Arrangement (MCA) is a BroadWorks feature that allows for multiple calls to be originated concurrently from the same shared line. Practically speaking, this means that a second endpoint may place an outgoing call on the same shared line already in use by another endpoint. To achieve a non-blocking configuration for a group of endpoints sharing a line (meaning that all endpoints in that group can always place an outgoing call) every endpoint in that group must have as many shared line keys provisioned as there are endpoints in the group.

Administration via WBM

System > Features > Favourites/Key module

Example: Three lines need to be configured for a user. For the first line, use the Key 1 and choose Edit.

Favourites/Key module			
Page 1		Key	Page 2
Clear (no feature assigned) ▼	edit	1	Clear (no feature assigned) ▼ edit
Clear (no feature assigned) ▼	edit	2	Clear (no feature assigned) ▼ edit
Clear (no feature assigned) ▼	edit	3	Clear (no feature assigned) ▼ edit
Clear (no feature assigned) ▼	edit	4	Clear (no feature assigned) ▼ edit

Set up the line as following:

Line

Key label 1

Line

Primary line

☒

Ring on/off

☒

Ring delay (seconds)

0

Selection order

1

Address

202045

Realm

User Identifier

Password

Shared type

shared ▼

Hot warm action

No action ▼

Hot warm destination

Submit

Reset

The rest of the lines should be set up in the following way:

Line

Key label 2

Line

Primary line

☐

Ring on/off

☒

Ring delay (seconds)

0

Selection order

2

Address

202045

Realm

User Identifier

Password

Shared type

shared ▼

Hot warm action

No action ▼

Hot warm destination

Submit

Reset

NOTICE: Primary line should be checked out only for the first line.

The selection order has to be growing.

For all lines, the address has to have the same phone number.

3.15.8 E/A Cockpit settings

In order to allow access to the integrated E/A cockpit application, the administrator needs to configure the server address and port.

- **myserver.com** : 8443

The phone will only allow secure connections to the server provided. The default port to access the server is 8443, if no port is configured in the server address field.

Administration via WBM

System > Registration > E/A Cockpit

The phone will try to verify the given data and will allow the access to the integrated E/A cockpit application via the main menu screen if a valid host address (IP or FQDN) is given.

If Allow server push is checked, it allows the E/A Cockpit application to startup on server push requests.

Supported formats:

Format for HTTP: http://<Server-IP/DN>:<Server port>

— IP address or FQDN: e.g. http://172.25.8.67 or fqdn.tld

— IP address/FQDN + port: e.g. http://172.25.8.67:8443 or fqdn.tld:8443

- Format for HTTPS: <Server-IP/DN>:<Server port>

— IP address or FQDN: e.g. https://172.25.8.67 or fqdn.tld

— IP address/FQDN + port: e.g. https://172.25.8.67:8443 or fqdn.tld:8443

NOTICE: A single E/A cockpit group can consist of a maximum number of four executives and four assistants.

3.16 Key Modules

On an OpenScape Desk Phone CP600/ CP700/700X a key module provides 12 additional free programmable keys. On an OpenScape Desk Phone CP400 phone a key module provides 16 additional free programmable keys.

A maximum of two key modules can be connected to the OpenScape Desk Phone CP400 or CP600 and up to four key modules can be connected to the OpenScape Desk Phone CP700/700X.

On an OpenScape Desk Phone CP100/CP200/CP205 phone no key modules can be connected.

The configuration of a key on the key module is exactly the same as the configuration of a phone key.

Administration via WBM

System > Features > Key module 1

Key module 1



To assign a new function to a key, select from the drop down list box. To view or modify the parameters associated with the key, use the Edit button. All keys of Key Module 1 appear on favourites if no KM is attached/functioning.

Page 1		Key		Page 2		
Unallocated	▼	Edit	1	Unallocated	▼	Edit
Unallocated	▼	Edit	2	Unallocated	▼	Edit
Unallocated	▼	Edit	3	Unallocated	▼	Edit
Unallocated	▼	Edit	4	Unallocated	▼	Edit
Unallocated	▼	Edit	5	Unallocated	▼	Edit
Unallocated	▼	Edit	6	Unallocated	▼	Edit
Unallocated	▼	Edit	7	Unallocated	▼	Edit
Unallocated	▼	Edit	8	Unallocated	▼	Edit
Unallocated	▼	Edit	9	Unallocated	▼	Edit
Unallocated	▼	Edit	10	Unallocated	▼	Edit
Unallocated	▼	Edit	11	Unallocated	▼	Edit
Unallocated	▼	Edit	12	Unallocated	▼	Edit

The configured keys can be either in Normal or Shifted level. When switching to the Shifted level the phone doesn't switch automatically back to the Normal level, unless you configure it to do so.

Administration via WBM

System > Features > Configuration

To configure the phone to automatically switch back to the Normal level, enable the **Automatic key module switchback** checkbox. The phone will start a 15 seconds timer and then switch to the non shifted level on all the attached KM400/KM600.

To switch to shifted level (or back) simultaneously on every attached Key module (and permanent Favourites on CP700), enable the **Simultaneous key module switching** checkbox.

Configuration	
General	
Emergency number	
Voice mail number	
MWI LED	AlertBar LED ▼
Missed call LED	AlertBar LED ▼
AlertBar LED hint	☐
Allow refuse	☒
Hot/Warm phone	No action ▼
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☒
Server features	☐
Not used timeout (minutes)	2 ▼
Transfer on hangup	☐
Bridging enabled	☐
Dial plan enabled	☐
FPK program timer	On ▼
Selected Dial Action on calls	No action ▼
DSS monitored	☐
Show icon for all forwarding types	☒
Automatic key module switchback	☒
Simultaneous key module switching	☒

3.17 Dialing

3.17.1 Canonical Dialing Configuration

Call numbers taken from a directory application, LDAP for instance, are mostly expressed in canonical format. Moreover, call numbers entered or imported (e.g. from Outlook) into the local phone book are automatically converted and stored in canonical format, thereby adding "+", local country code, local national code, and local enterprise number as prefixes.

The system uses the length of a number to be canonized to determine if it is a locally dialable number (e.g. local PSTN) when the number had not been recognized by earlier canonical rules. For this check a new configuration item is required to specify the maximum length for a locally dialable number (this complements the existing configuration item that specifies the minimum length for such a number).

NOTICE: A number that had not been canonized but matches the new rule is canonized as a local dialable number

If the number to be canonized is longer than the maximum local number that could be dialed then it already contains additional addressing digits and hence is treated as a national dialable number. Otherwise it is locally dialable and needs to be prefixed with the local access codes.

- 49171558765432 exceeds the length for a local dialable number (example 11) and is simply canonized as +49171558765432
- | 4917155876 fits the length for a local dialable number and is canonized as +498951594917155876

Example

The user enters the extension "1234", the local country code is "49", the local national code is "89", and the local enterprise number is "722". The resulting number in canonical format is "+49897221234".

NOTICE: To enable the number conversion, all parameters not marked as optional must be provided, and the canonical lookup settings must be configured (see [Canonical Dial Lookup](#) on page 245).

Changes to these parameters can impact the phone's ability to match calls to contacts.

Administration via WBM

Local functions > Locality > Canonical dial settings

Canonical dial settings	
 Warning – changes to these settings could prevent calls being matched to existing conversations	
Use	Value
Local country code	33
National prefix digit	0
Local national code	1
Minimum local number length	6
Local enterprise node	4192
PSTN access code	0
International access code	00
Operator codes	9
Emergency numbers	015,017,018,0112,0115,01
Initial extension digits	1,23,24,25,26,27,28,29,3,4
Expect dial number	☐
Submit	Reset

Data required

- **Local country code:** E.164 Country code, e.g. "49" for Germany, "44" for United Kingdom. Maximum length: 5.
- **National prefix digit:** Prefix for national connections, e.g. "0" in Germany and United Kingdom. Maximum length: 5.
- **Local national code:** Local area code or city code, e.g. "89" for Munich, "20" for London. Maximum length: 6.
- **Minimal local number length:** Minimum number of digits in a local PSTN number, e.g. 3335333 = 7 digits.
- **Local enterprise node:** Number of the company/PBX wherein the phone is residing. Maximum length: 10. (Optional)

- **Local enterprise node:** number of the company / PBX in which the phone is residing. Maximum length: 10.
- **PSTN access code:** Access code used for dialing out from a PBX to a PSTN. Maximum length: 10. (Optional)
- **International access code:** International prefix used to dial to another country, e.g. "00" in Germany and United Kingdom. Maximum length: 5.
- **Operator codes:** List of extension numbers for a connection to the operator. The numbers entered here are not converted to canonical format. Maximum length: 50. (Optional)
- **Emergency numbers:** List of emergency numbers to be used for the phone. If there are more than one numbers, they must be separated by commas. The numbers entered here are not converted to canonical format. Maximum length: 50. (Optional)
- **Initial extension digits:** List of initial digits of all possible extensions in the local enterprise network. When a call number could not be matched as a public network number, the phone checks if it is part of the local enterprise network. This is done by comparing the first digit of the call number to the value(s) given here. If it matches, the call number is recognized as a local enterprise number and processed accordingly. If, for instance, the extensions 3000-5999 are configured in the OpenScape Desk Phone CP100/200/205/400/600/600E, each number will start with 3, 4, or 5. Therefore, the digits to be entered are 3, 4, 5.
- **Expect dial number:** Indicates when PSTN access code and national prefix digit is retained and not converted into the international access code.

Administration via WBM

Local functions > Locality > Canonical dial

- Internal numbers

NOTICE: To enable the phone to discern internal numbers from external numbers, it is crucial that a canonical lookup table is provided ([Canonical Dial Lookup](#) on page 245).

- **"Local enterprise form":** Default value. Any extension number is dialed in its simplest form. For an extension on the local enterprise node, the node ID is omitted. If the extension is on a different enterprise node, then the appropriate node ID is prefixed to the extension number. Numbers that do not correspond to an enterprise node extension are treated as external numbers.
- **"Always add node":** Numbers that correspond to an enterprise node extension are always prefixed with the node ID, even those on the local node. Numbers that do not correspond to an enterprise node extension are treated as external numbers.

- **"Use external numbers"**: All numbers are dialled using the external number form.
- External numbers
 - **"Local public form"**: Default value. All external numbers are dialed in their simplest form. Thus a number in the local public network region does not have the region code prefix. Numbers in the same country but not in the local region are dialled as national numbers. Numbers for a different country are dialled using the international format.
 - **"National public form"**: All numbers within the current country are dialled as national numbers, thus even local numbers will have a region code prefix (as dialling from a mobile). Numbers for a different country are dialled using the international format.
 - **"International form"**: All numbers are dialled using their full international number format.
- External access code
 - **"Not required"**: The access code to allow a public network number to be dialled is not required.
 - **"For external numbers"**: Default value. All public network numbers will be prefixed with the access code that allows a number for a call to be routed outside the enterprise network. However, international numbers that use the + prefix will not be given access code.
- International gateway code:
 - **"Use national code"**: Default value. All international formatted numbers will be dialled explicitly by using the access code for the international gateway to replace the "+" prefix.
 - **"Leave as +"**: All international formatted numbers will be prefixed with "+".

Administration via Local Phone

```
|--- Admin
    |--- Local Functions
        |--- Locality
            |--- Canonical settings
                |--- Local country code
                |--- National prefix digit
                |--- Local national code
                |--- Minimum local number length
                |--- Local enterprise node
                |--- PSTN access code
                |--- International access code
                |--- Operator codes
                |--- Emergency numbers
                |--- Initial extension digits
                |--- Expect dial number
|--- Admin
    |--- Local Functions
        |--- Locality
            |--- Canonical dial
                |--- Internal numbers
                |--- External numbers
                |--- External access code
                |--- International gateway code
```

3.17.2 Canonical Dial Lookup

The parameters given here are important for establishing outgoing calls and for recognizing incoming calls.

In the local phonebook, and, mostly, in LDAP directories, numbers are stored in canonical format. In order to generate an appropriate dial string according to the settings in Internal numbers and External numbers ([Canonical Dialing Configuration](#) on page 241), internal numbers must be discerned from external numbers. The canonical lookup table provides patterns which allow for operation.

Furthermore, these patterns enable the phone to identify callers from different local or international telephone networks by looking up the caller's number in the phone book. As incoming numbers are not always in canonical format, their composition must be analyzed first. For this purpose, an incoming number is matched against one or more patterns consisting of country codes, national codes, and enterprise nodes. Then, the result of this operation is matched against the entries in the local phone book.

NOTICE: To make sure that canonical dial lookup works properly, at least the following parameters of the phone must be provided:

- Local country code ([Canonical Dialing Configuration](#) on page 241)
 - Local area code ([Canonical Dialing Configuration](#) on page 241)
 - Local enterprise code ([Canonical Dialing Configuration](#) on page 241)
-

You can view and edit the first five entries via the WBM. The Local code 1 ... 5 parameters define up to 5 different local enterprise nodes, whilst International code 1... 5 define up to 5 international codes, that is, fully qualified E.164 call numbers for use in a PSTN. The whole list of entries are not visible on the phone but can be seen and handled using the DLS.

A number that contains the 'International code 1' series of digits may translate these digits to that of 'Local code 1' or vice-versa.

Administration via WBM

Locality > Canonical dial lookup

Canonical dial lookup

Warning – changes to these settings could prevent calls being matched to existing conversations

Equivalent number forms

Local code 1	3314070	International code 1	+3314070
Local code 2	3314192	International code 2	+3314192
Local code 3	3335982	International code 3	+3335982
Local code 4	3342683	International code 4	+3342683
Local code 5		International code 5	

Submit

Reset

Data required

- **Local code 1 ... 5:** Local enterprise code for the node/PBX the phone is connected to. Example: "7007" for Unify office in Munich.
- **International code 1 ... 5:** Sequence of "+", local country code, local area code, and local enterprise node corresponding to to one or more phone book entries. Example: "+49897007" for Unify office in Munich.

Administration via Local Phone

```
|--- Administrator settings
  |--- Local Functions
    |--- Locality
      |--- Canonical dial lookup
        |--- Local code 1
        |--- International code1
        |--- Local code 2
        |--- International code 2
        |--- Local code 3
        |--- International code 3
        |--- Local code 4
        |--- International code4
        |--- Local code 5
        |--- International code5
```

3.17.3 Phone location

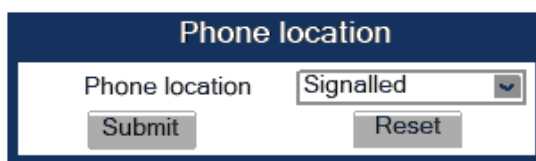
This parameter specifies if phone location information are included in appropriate SIP messages or not included in any SIP messages but such information are allowed to be configured.

Data required

- **Phone location:** .
- Value range: "Signalled", "Not signalled" Default: "Signalled"

Administration via WBM

Locality > Phone Location



The image shows a 'Phone location' configuration window. It has a title bar 'Phone location'. Inside, there is a label 'Phone location' followed by a dropdown menu currently showing 'Signalled'. Below the dropdown are two buttons: 'Submit' and 'Reset'.

Administration via Local Phone

```
|--- Admin
    |--- Local Functions
        |--- Locality
            |--- Phone location
                |--- Phone location
```

3.17.4 Dial Plan

OpenScape Desk Phone CP phones may optionally use a dial plan residing on the phone. By means of the dial plan, the phone can infer from the digits entered by the user that a complete call number has been entered, or that a particular prefix has been entered. Thus, the dialing process can start without the need to confirm after the last digit has been entered, without delay or with a configurable delay. The standard timer, which is found on the WBM under **User menu > Configuration > Outgoing calls > Autodial delay (seconds)**, is overridden if a dial plan rule is matched.

A dial plan consists of rules defining patterns, timeouts and actions to be performed when a pattern is matched and/or a timeout has expired. The phone can store one dialplan, which can contain up to 48 different rules.

It is very important that the phone's dial plan does not interfere with the dial plan in the SIP server, PBX, or public network.

The dial plan can be created and uploaded to the phone using the DLS (please refer to the Deployment Service Administration Manual). The DLS can also export and import dial plans in .csv format. For details about the composition of a dial plan, please refer to [Example Dial Plan](#) on page 336.

The current dial plan, along with its status (enabled/disabled) and error status can be displayed on the WBM via **Diagnostics > Fault trace configuration > Download dial plan file**.

The Dial plan ID and the Dial plan status is displayed in the local menu.

To make use of the dial plan facility, the following requirements must be met:

- A correct dial plan is loaded to the phone.
- In the user menu, Allow immediate dialing is enabled. This condition is only necessary for on-hook dialing, but not for off-hook dialing.
- Dial plan enabled is checked.

Administration via WBM (User menu)

User > Configuration > Outgoing calls > Allow immediate dialing

Outgoing calls

Autodial delay (seconds)

6

Allow callback

☒

Allow busy when dialling

☐

Allow transfer on ring

☒

Allow immediate dialling

☐

Submit

Reset

System > Features > Configuration > Dial plan enabled

General

Emergency number

3335

Voice mail number

MWI LED

AlertBar LED

Missed call LED

AlertBar LED

Allow refuse

☒

Hot/Warm phone

No action

Hot/Warm destination

Initial digit timer (seconds)

30

Allow uaCSTA

☒

Server features

☐

Not used timeout (minutes)

2

Transfer on hangup

☐

Bridging enabled

☒

Dial plan enabled

☐

FPK program timer

On

DSS monitored

☐

Show icon for all forwarding types

☐

Administration via Local Phone

```
|--- User
  |--- Configuration
    |--- Outgoing calls
      |--- Immediate dialling
|--- Admin
  |--- System
    |--- Features
      |--- Configuration
        |--- General
          |--- Dial plan
|--- Admin
  |--- General Information
    |--- Dial plan ID
    |--- Dial plan status
```

3.18 Ringer Setting

3.18.1 Distinctive

The SIP server may provide information indicating a specific type of call within an incoming call. The phone can use this information to choose a ring tone according to the call type from the "Distinctive ringer table".

The relevant information is carried as a string in the SIP Alert-Info header. This string is configured in the OpenScape Voice system; please refer to the relevant OpenScape Voice documentation. When the string sent via alert-info matches the string specified in the Name parameter, the corresponding ringer is triggered. For instance, the OpenScape Voice system may send the string `Bellcore-dr1` to indicate that a call is from within the same business group, and the Name parameter is set to "Bellcore-dr1". To select a specific ring tone for calls from the same business group, the other parameters corresponding to that Name must be set accordingly.

The Ringer sound parameter determines whether a pattern, i. e. melody, or a specific sound file shall be used as ringer.

Pattern melody selects the melody pattern that will be used if Ringer sound is set to "Pattern".

Pattern sequence determines the length for the melody pattern, and the interval between the repetitions of the pattern. There are 3 variants:

- **"1"**: 1 sec ON, 4 sec OFF
- **"2"**: 1 sec ON, 2 sec OFF
- **"3"**: 0.7 sec ON, 0.7 sec OFF, 0.7 sec ON, 3 sec OFF

The Duration parameter determines how long the phone will ring on an incoming call. The range is 0-300 sec.

With the Audible parameter, the ringer can be muted. In this case, an incoming call will be indicated only visually.

Special Ringers can be configured for the following call types:

- Internal
- External
- Recall
- Emergency
- Special1
- Special2
- Special3

NOTICE: To make the special ringers available and configurable to the user, the administrator needs to map the call types to specific ringers via the **Ringer setting** mapping table in **Admin > Ringer setting > Distinctive**. Each call type can be mapped to a specific Ringer sound, Pattern Melody, and Pattern sequence.

Abstract names used for Special Ringers:

- "Bellcore-dr1" - normal (internal) alerting or ring-back;
- "Bellcore-dr2" - external alerting or ring-back;
- "Bellcore-dr3" - recall alerting or ring-back (e.g., following transfer).
- "alert-internal" - normal (internal) alerting or ring-back;

- "alert-external" - external alerting or ring-back;
- "alert-recall" - recall alerting or ring-back (e.g., following transfer)
- "alert-emergency" - emergency alerting or ring-back.
- "Line-<DN of Line>-Reserved" - distinctive alerting for a line with number <DN of Line>

Once made available (by the administrator) to the user, the **Special Ringers** for the call types listed can be selected and configured via the **User** menu as shown in [Special Ringers](#) on page 252.

NOTICE: Please keep in mind that the ringer settings might be locked by DLS and therefore also the special ringers will not be available for the user. See DLS Documentation for details.

Administration via WBM

Admin > Ringer setting > Distinctive

Distinctive

This page allows you to set up interworking with other IP phone systems that support distinctive ringing

Name	Ringer sound	Pattern melody	Pattern sequence	Duration (sec)	Audible
Belcore-dr1	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
Belcore-dr2	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
Belcore-dr3	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
alert-emergency	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼
	Pattern ▼	2 ▼	2 ▼	60	Ring ▼

Administration via Local Phone

```

|--- Admin
    |--- Ringer setting
        |--- Distinctive
            |--- <1 .... 15>
                |--- Name
                    |--- Ringer sound
                    |--- Pattern melody
                    |--- Pattern sequence
                    |--- Duration
                    |--- Audible

```

3.18.2 Map to Specials

The "Mapping table" is accessible by local menu, WBM, or DLS but is predefined with Ringer name defaults. Only the special ringers for the default types will be shown in the local menu and WBM. If a default Ringer name is not

configured in the "Distinctive ringer table" then the mapped entry in the "Special ringer table" will be greyed and read-only.

The "Mapping table" has been configured to identify the distinctive ringer names as a special ringer type and the User has access to configure a different audio file or pattern for this distinctive ringer via their "Special ringer table". Any change made by the User to this special ringer will be reflected in the "Distinctive ringer table" and any change made by Admin in the "Distinctive ringer table" will be reflected in the "Special ringer table".

Administration via WBM

Admin > Ringer setting > Map To Specials

Map to specials	
Internal	Bellcore-dr1 ▼
External	Bellcore-dr2 ▼
Recall	Bellcore-dr3 ▼
Emergency	alert-emerge ▼
Special1	▼
Special2	▼
Special3	▼
Submit Reset	

3.18.3 Ringer Mode

Ringer Mode allows you to disable the "Ringer off" option.

Administration via WBM

System > Ringer Setting > Ringer Mode

Ringer Mode

Ringer off disable ☐

When the "Ringer off " function is disabled, it becomes read-only on the user's phone, preventing the user from changing the phone's ringer by long-pressing the * key. If pressed, a toast message (for CP400/600/700) or a popup (for CP100/200) **Key function unavailable** is displayed.

NOTICE: The temporary muting of the ringer using a short press of the * key remains functional. Only the "Ringer off" and the "Ringer beep" options are disabled.

Additionally, the function can no longer be allocated to an FPK. If a CP400/600/700 FPK has been configured with the "Ringer off" function before the Admin disables it, the Admin should inform the user that the function is no longer available.

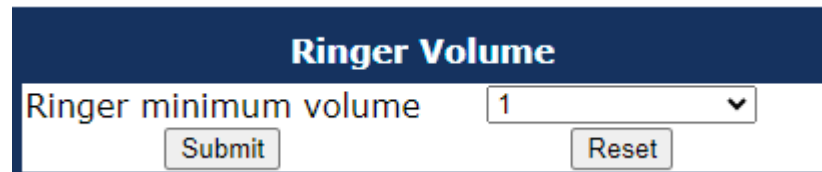
3.18.4 Ringer Volume

You can specify the ringer levels of the CP Phones.

The ringer volume has ten levels, ranging from 1 (minimum) to 10 (maximum) by default. Admin can limit the lowest volume that the user is able to select (i.e. to ensure that the ringer is always heard above background noise).

Administration via WBM

System > Ringer setting > Ringer volume



When the ringer volume is limited, the user can not reduce the slider below the limited volume level. The slider bar color will be changed to gray to indicate the disabled ringer volume level. The slider position will still be visible even when it's set to the minimum volume level.

Example

If the minimum volume is set to 4, the user will be able to adjust the ringer volume between levels 4 and 10. Volume levels 3, 2 and 1 will not be accessible.

3.18.5 Special Ringers

Special Ringers can be configured via the **User** menu for the following call types:

- Internal
- External
- Recall
- Special1
- Special2
- Special3

Administration via WBM (User menu)

User > Audio > Special ringers

The **Special ringers** dialog allows the user to change the ring tones for the special call types listed below, provided that the call type is signaled to the phone.

NOTICE: To make the special ringers available and configurable to the user, the administrator needs to map the call types to specific ringers via the **Ringer setting** mapping table in **Admin > Ringer setting > Distinctive**. Each call type can be mapped to a specific Ringer sound, Pattern melody, and Pattern sequence.

NOTICE: Please note, that User cannot change the Ringer sound, Pattern melody and/or Pattern sequence of Emergency call type. This can be set only by an Administrator. Emergency ringer is always played (regardless of ringer settings) at maximum volume.

Special Ringer Call Types

- Internal
- External
- Recall
- Emergency
- Special1
- Special2
- Special3

Special ringers

This page allows you to change the ringer played for a limited range of special incoming calls where the type of call has been signalled to the phone

Call type	Ringer sound	Pattern melody	Pattern sequence
Internal	Pattern ▼	2 ▼	1.0 sec. ON, 2.0 sec. OFF ▼
External	Pattern ▼	2 ▼	1.0 sec. ON, 2.0 sec. OFF ▼
Recall	Pattern ▼	2 ▼	1.0 sec. ON, 2.0 sec. OFF ▼
Emergency	Pattern ▼	2 ▼	1.0 sec. ON, 2.0 sec. OFF ▼
Special 1	Ringer 1.mp3 ▼	1 ▼	1.0 sec. ON, 4.0 sec. OFF ▼
Special 2	Ringer 1.mp3 ▼	1 ▼	1.0 sec. ON, 4.0 sec. OFF ▼
Special 3	Ringer 1.mp3 ▼	1 ▼	1.0 sec. ON, 4.0 sec. OFF ▼

Submit
Reset

Administration via Local Phone

```

|--- User
    |--- Audio
        |--- <Special Ringers>
            |--- Internal
                |--- External
                |--- Recall
                |--- Emergency
                |--- Special 1
                |--- Special 2
                |--- Special 3
  
```

For each call type, except Emergency, the following parameters can be configured:

The Ringer sound parameter determines whether a pattern, i. e. melody, or a specific sound file shall be used as ringer.

Pattern melody selects the melody pattern that will be used if Ringer sound is set to "Pattern".

Pattern sequence determines the length for the melody pattern, and the interval between the repetitions of the pattern. There are 3 variants:

- "1": 1 sec ON, 4 sec OFF
- "2": 1 sec ON, 2 sec OFF

- "3": 0.7 sec ON, 0.7 sec OFF, 0.7 sec ON, 3 sec OFF

3.19 Mobility

The Mobility feature requires the OpenScape Deployment Service (DLS). If the phone is mobility enabled by the DLS, a mobile user can log on to the phone and thereby have his own user settings transferred to the phone. These user data are stored in the DLS database and include, for instance, SIP registration settings, dialing properties, key layouts, as well as the user's phonebook and call records.

If the mobile user changes some settings, the changed data is sent to the DLS server. This ensures that his user profile is updated if necessary.

If Unauthorized Logoff Trap is set to "Yes", a message is sent to the SNMP server if an unauthorized attempt is made to log off the mobile user.

Logoff Trap Delay defines the timespan in seconds between the unauthorized logoff attempt and the trap message to the SNMP server.

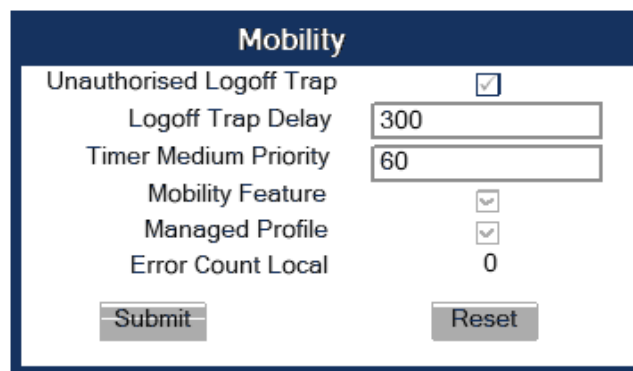
Timer Medium Priority determines the timespan in seconds between a change of user data in the phone and the transfer of the changes to the DLS server.

The Mobility Feature parameter indicates whether the mobility feature is enabled by the DLS or not.

Data required

- **Unauthorized Logoff Trap:** An SNMP trap is sent on an unauthorized logoff attempt. Value range: "Yes", "No" Default: "No"
- **Logoff Trap Delay:** Timespan in seconds between the unauthorized logoff attempt and the SNMP trap. Default: 300
- **Timer Medium Priority:** Timespan in seconds between a data change in the phone and its transfer to the DLS server. Default: 60
- **Mobility feature:** Indicates whether the mobility feature is enabled.
- **Managed Profile:** Display only field.
- **Error Count Local:** Display only field.

Administration via WBM



Mobility	
Unauthorised Logoff Trap	☒
Logoff Trap Delay	300
Timer Medium Priority	60
Mobility Feature	☒
Managed Profile	☒
Error Count Local	0
Submit Reset	

Administration via Local Phone

```
|--- Admin
      |--- Mobility
            |--- Unauthorized Logoff Trap
```

```

|--- Logoff Trap Delay
|--- Timer Medium Priority
|--- Mobility Feature
|--- Managed Profile
|--- Error Count Local

```

3.20 Transferring Phone Software, Application, and Media Files

New software images, hold music, picture clips for phonebook entries, LDAP templates, company logos, screensaver images, and ring tones can be uploaded to the phone via DLS (Deployment Service) or WBM (Web Based Management).

NOTICE: For all user data, which includes files as well as phonebook content, the following amounts of storage place are available:

- **OpenScape Desk Phone CP700/700X:** 100 MB
 - **OpenScape Desk Phone CP600/600E:** 100 MB
 - **OpenScape Desk Phone CP400:** 100 MB
 - **OpenScape Desk Phone CP200/CP205:** 25 MB
 - **OpenScape Desk Phone CP100:** 25MB
-

3.20.1 File name

In Linux based file systems, the null character and the path separator "/" are prohibited. Other characters may have an adverse effect during the creation or deletion of the particular file in the Linux operating system.

Prevent invalid file names

Saving a file with an invalid filename on the phone could lead to operational or security issues. To protect against this the phone will ensure that the filename for the file to be saved does not contain non-allowed characters.

The set of allowed characters are:

- 0 to 9
- a to z
- A to Z
- "-" (hyphen)
- "_" (underscore)

A space character is explicitly not allowed in a Linux filename. Any non-allowed characters are replaced with an "_" (underscore) character. The filename must not start with a "-" (hyphen) character.

The solution is to replace invalid characters in the names of files to be downloaded onto the phone with a dummy character.

This should cover any download mechanism:

- WBM download of user files (such as ringers)
- WBM download of binds

- FTP or HTTPS download of files to the phone

When a file is downloaded to the phone, sanity checks are carried out to ensure there are no operational or security impacts on the phone.

WBM checks the filename entered in any FTP/HTTPS file transfer panel only contains characters that are valid in a filename.

- If a file path character is detected in the filename then an error is displayed and the file transfer is not allowed.

Example: Picture clip

The screenshot shows a configuration panel titled "Picture clip". It contains the following elements: a "Use defaults" checkbox (unchecked); a "Download method" dropdown menu set to "HTTPS"; an "HTTPS base URL" text field containing "172.23.37.195:8080"; a "Filename" text field containing "tra..in1.jpg"; an "After submit" dropdown menu set to "do nothing"; and an error message "Filename contains path character" displayed in red. At the bottom are "Submit" and "Reset" buttons.

WBM checks that the file extension is valid for the type of file transfer

- If an invalid file extension is detected in the filename then an error is displayed and the file transfer is not allowed.

Example: Picture clip

The screenshot shows a configuration panel titled "Picture clip". It contains the following elements: a "Use defaults" checkbox (unchecked); a "Download method" dropdown menu set to "HTTPS"; an "HTTPS base URL" text field containing "172.23.37.195:8080"; a "Filename" text field containing "train1.xml"; an "After submit" dropdown menu set to "do nothing"; and an error message "File extension is not allowed" displayed in red. At the bottom are "Submit" and "Reset" buttons.

3.20.2 FTP/HTTPS Server

There are no specific requirements regarding the FTP server for transferring files to the OpenScape Desk Phone CP. Any FTP server providing standard functionality will do.

3.20.3 Common FTP/HTTPS Settings (Defaults)

For each one of the various file types, e.g. phone software, or logos, specific FTP/HTTPS access data can be defined. If some or all file types have the

parameters Download method, FTP Server, FTP Server port, FTP Account, FTP Username, FTP path, and HTTPS base URL in common, they can be specified here. These settings will be used for a specific file type if its Use defaults parameter is set to "Yes".

NOTICE: If Use defaults is activated for a specific file type, any specific settings for this file type are overridden by the defaults.

Additional log messages are issued for the following scenarios:

- Update has been allowed due to override flag being set
- Whole part number is not recognized
- Block 4 of part number is not recognized
- Downloaded software does not have a hardware level included

Data required

- **Download method:** Selects the protocol to be used. Value range: "FTP", "HTTPS". Default: "FTP".
- **FTP Server:** IP address or hostname of the FTP server in use.
- **FTP Server port:** Port number of the FTP server in use. For HTTPS, port 443 is assumed, unless a different port is specified in the HTTPS base URL. Default: 21.
- **FTP Account:** Account at the server (if applicable).
- **FTP Username:** User name for accessing the server.
- **FTP Password:** Password corresponding to the user name.
- **FTP path:** Path of the directory containing the files.
- **HTTPS base URL:** IP address or hostname of the HTTPS server in use. If no port number is specified here, port 443 is used. Only applicable if Download method is switched to "HTTPS".

Administration via WBM

File transfer > Defaults

Administration via Local Phone

```
|--- Admin
    |--- File Transfer
        |--- Defaults
```

```

|--- Download method
|--- Server
|--- Port
|--- Account
|--- Username
|--- Password
|--- FTP path
|--- HTTPS base URL

```

3.20.4 Phone Application

The firmware for the phone can be updated by downloading a new software file to the phone.

If an incorrect software image is being attempted to be loaded onto the phone, the phone will reject the request and return to normal operation without reboot. As part of this security mechanism, new software binds are identified by a "Supported Hardware Level" information built into the header.

Prerequisite: The phone knows it's own hardware level (from the part number and/or by a dynamical check of its HW level).

When a new software bind is downloaded to the phone, the following verification is performed:

1) If new software bind has hardware level header included (in the bind header): Hardware level of new bind is compared with phone's hardware level.

- **If compatible (or if Override is set):** Proceed with update

NOTICE: The options about override and protection can be found by the administrator via the WBM under **Administrator settings > System > Security > System**

- **If NOT compatible:** Abandon update and return to original application

2) If new software bind does NOT have hardware level header included (in the bind header): Software version of new bind is compared with minimum known supported SW level.

- **If compatible (or if Override is set):** Proceed with update

NOTICE: The options about override and protection can be found by the administrator via the WBM under **Administrator settings > System > Security > System**

- **If NOT compatible:** Abandon update and return to original application

NOTICE: Do not disconnect the phone from the LAN or power unit during software update. An active update process is indicated by blinking LEDs and/or in the display.

3.20.4.1 Upgrade using File

You can upgrade the phone application by uploading a local file. This can be done only by WBM administration.

Administration via WBM

File transfer > Phone application

Click on **Browse...**, select the file you want to install and click Upgrade.

Wait until the upgrade process is finished.

Please note that the "Cancel" functionality will not work once the process is in burn state.

3.20.4.2 Upgrade using FTP/HTTPS

If the default FTP/HTTPS access settings (see [Common FTP/HTTPS Settings \(Defaults\)](#) on page 256) are to be used, Use defaults must be set to "Yes", and only the Filename must be specified.

Data required (in every case)

- **Use defaults:** Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No".
- **Filename:** Specifies the file name of the phone software.

Data required (if not derived from Defaults)

- **Download method:** Selects the protocol to be used. Value range: "FTP", "HTTPS". Default: "FTP".
- **Server:** IP address or hostname of the FTP/HTTPS server in use.
- **Server port:** Port number of the FTP/HTTPS server in use. Default: 21.
- **Account:** Account at the server (if applicable).
- **Username:** User name for accessing the server.
- **Password:** Password corresponding to the user name.
- **FTP path:** Path of the directory containing the files.
- **HTTPS base URL:** IP address or hostname of the HTTPS server in use; only applicable if Download method is switched to "HTTPS".

- **After submit:** Specifies actions after submit button is pressed. Value range: "do nothing", "start download". Default: "do nothing".

Administration via WBM

File transfer > Phone application

Phone application

Use defaults

☐

Download method

FTP

FTP Server address

FTP Server port

21

FTP account

FTP username

FTP password

FTP path

HTTPS base URL

Filename

After submit

do nothing

Submit

Reset

Administration via Local Phone

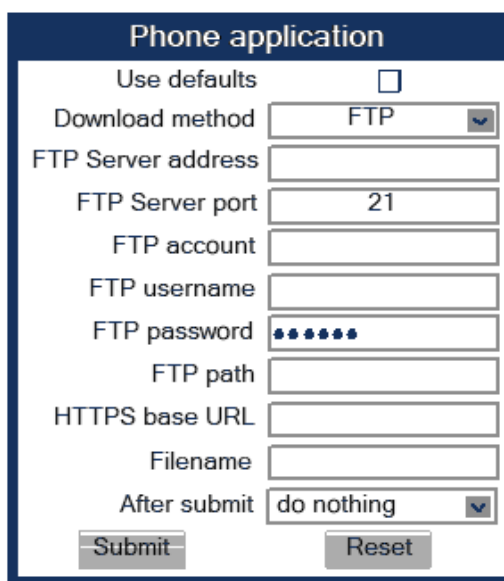
```
|--- Admin
  |--- File Transfer
    |--- Phone application
      |--- Use default
      |--- Download method
      |--- Server
      |--- Port
      |--- Account
      |--- Username
      |--- Password
      |--- FTP path
      |--- HTTPS base URL
      |--- Filename
```

3.20.4.3 Download/Update Phone Application

If applicable, phone software should be deployed using the Deployment Service (DLS). Alternatively, the download can be triggered from the WBM interface or from the Local phone menu. When the download has been successful, the phone will restart and boot up using the new software.

Start Download via WBM

File transfer > Phone application



The image shows a 'Phone application' configuration dialog box. It has a title bar 'Phone application'. Inside, there is a 'Use defaults' checkbox which is unchecked. Below it are several input fields: 'Download method' (a dropdown menu showing 'FTP'), 'FTP Server address' (empty), 'FTP Server port' (containing '21'), 'FTP account' (empty), 'FTP username' (empty), 'FTP password' (masked with dots), 'FTP path' (empty), 'HTTPS base URL' (empty), and 'Filename' (empty). At the bottom, there is an 'After submit' dropdown menu showing 'do nothing'. There are two buttons at the bottom: 'Submit' and 'Reset'.

In the **File transfer > Phone application** dialog, set After submit to "start download" and press the Submit button.

Start Download via Local Phone

In the administration menu, set the focus to Phone app.

```
|--- Admin
    |--- File Transfer
        |--- Phone app
```

- **On OpenScape Desk Phone CP200/CP205:**
Press the OK key. A context menu opens. In the context menu, select Download. The download will start immediately.
- **On OpenScape Desk Phone CP400/600/700/700X:**
Press the Soft Key labeled Download. The download will start immediately.

3.20.5 Picture Clips

Picture clips are provided in an LDAP lookup but may also be provided manually and linked to a contact.

NOTICE: Picture clips are available only on OpenScape Desk Phone CP600 phones.

NOTICE: The file size for a picture clip is limited to 300 KB.

Picture Clips are small images used for displaying a picture of a person that is calling on a line. The supported file formats for picture clips are JPEG, BMP and PNG. The file extensions supported for JPEG are jpeg and jpg.

3.20.5.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see [Common FTP/HTTPS Settings \(Defaults\)](#) on page 256) are to be used, Use default must be set to "Yes", and only the Filename must be specified.

Data required (in any case)

- **Use default:** Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No".
- **Filename:** Specifies the file name of the image file.
- **Download method:** Selects the protocol to be used. Value range: "FTP", "HTTPS". Default: "FTP".
- **Server:** IP address or hostname of the FTP/HTTPS server in use.
- **Server port:** Port number of the FTP/HTTPS server in use. Default: 21.
- **Account:** Account at the server (if applicable).
- **Username:** User name for accessing the server.
- **Password:** Password corresponding to the user name.
- **FTP path:** Path of the directory containing the files.
- **HTTPS base URL:** IP address or hostname of the HTTPS server in use; only applicable if Download method is switched to "HTTPS".
- **After submit:** Specifies actions after submit button is pressed. Value range: "do nothing", "start download". Default: "do nothing".

Administration via WBM

File transfer > Picture clip

Picture clip

Use defaults☐

Download method

FTP

FTP Server address

FTP Server port

21

FTP account

FTP username

FTP password

FTP path

HTTPS base URL

Filename

After submit

do nothing

Submit

Reset

Administration via Local Phone

```
|--- Admin
  |--- File Transfer
    |--- Picture Clip
      |--- Use default
      |--- Download method
      |--- Server
      |--- Port
```

```

|--- Account
|--- Username
|--- Password
|--- FTP path
|--- HTTPS base URL
|--- Filename

```

- **On OpenScape Desk Phone CP400/600/700:**

Press the Soft Key labeled Download. The download will start immediately.

3.20.5.2 Download Picture Clip

If applicable, picture clips should be deployed using the Deployment Service (DLS). Alternatively, the download can be triggered from the web interface or from the local phone menu.

Start Download via WBM

File transfer > Phone application

In the **File transfer > Picture clip** dialog, set After submit to "start download" and press the Submit button.

Start Download via Local Phone

In the administration menu, set the focus to Picture clip.

```

|--- Admin
    |--- File Transfer
        |--- Picture clip

```

3.20.5.3 Picture Clips via LDAP

conversation, so that he can easily recognize his conversation partners. The LDAP template identifies if avatars are available for LDAP entries and how they are accessed by the phone.

The LDAP directory must contain avatar pictures in JPEG/JIFF format (plain or base 64 encoded) or a URL that points to a web-server that can provide a picture for the contact.

Example: Plain JPEG picture attributes are "jpegPhoto" or "thumbnailPhoto". URL attribute can be "photoURL".

For best display the square format is recommended. Maximum picture size is 100 kB. The phone shows an avatar in two sizes:

- 32x32 for Conversation List and Contact Details (header)
- 64x64 for Conversation and Call screens

If another size provided, the phone will automatically resize the picture to needed dimensions.

Until a JPEG image is available a default avatar is used for the LDAP contact.

The LDAP has to be configured (for more information, see [LDAP](#) on page 275) and a suitable LDAP template has to be available on the phone. The LDAP template must support a 13th attribute to allow access to a contact's picture (for more information, see [Create an LDAP Template](#) on page 329).

If the configured address of the web server (Avatar server) is not empty, the attribute content is treated as the variable part of the URL to access the picture from a WEB server — see Configuration via DLS and WBM in this chapter. The phone then constructs a full path to the picture file on the web server, i.e. adds the attribute value to the Avatar server field value. The photoURL attribute may be a direct URL which ends up with <filename>.jpg. The address can include a HTTP address or a HTTPS address. HTTPS is assumed by default.

If configured address of the web server (Avatar server) is empty, the attribute value is treated as a LDAP DN and the LDAP server will be asked for the content of the attribute. The content must be plain JPEG or base64 encoded.

Example: Avatar server value is „https://my.image.server.com/internal“ . The photoURL attribute is „employee1.jpg“. Phone will sent http request for https://my.image.server.com/internal/employee1.jpg.

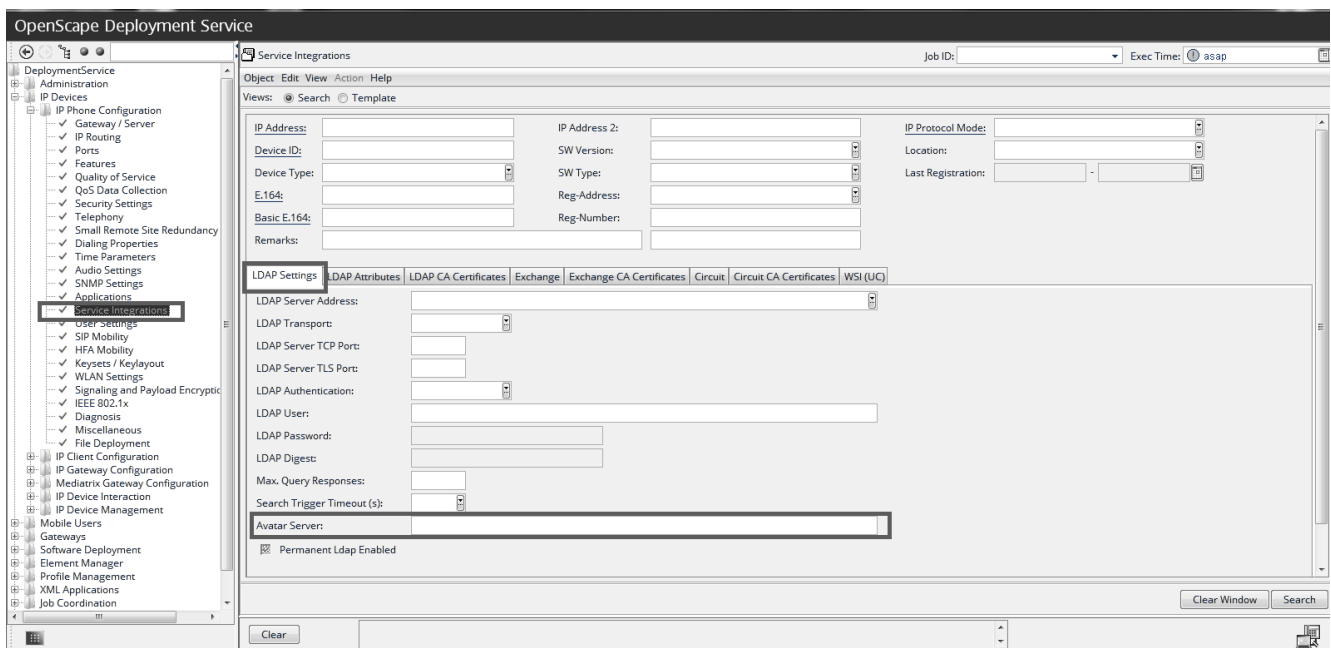
If the picture cannot be displayed (wrong format, download error, etc.) then a default avatar continues to be shown.

Configuration via Admin menu:

Settings -> Administrator -> Local functions -> LDAP -> Avatar server

Configuration via DLS:

DeploymentService -> IP Devices -> IP Phone Configuration -> Service Integrations -> LDAP Settings -> Avatar Server



Configuration via WBM:

Location: Admin -> Local functions -> Directory settings

Label: Avatar server.

Directory settings

LDAP server address	
Transport	TCP ▼
Secure port	636
LDAP server port	389
Authentication	Anonymous ▼
User name	
Password	
Permanent LDAP Enabled	☐
Avatar server	

3.20.6 LDAP Template

The LDAP template is an ASCII text file that uses an allocation list to assign directory server attributes to input and output fields on an LDAP client. The LDAP template must be modified correctly for successful communication between the directory server and the LDAP client.

NOTICE: The OpenScope Desk Phone
CP100/200/205/400/600/600E phones support LDAPv3.

3.20.6.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see [Common FTP/HTTPS Settings \(Defaults\)](#) on page 256) are to be used, Use default must be set to "Yes", and only the Filename must be specified.

Data required (in any case)

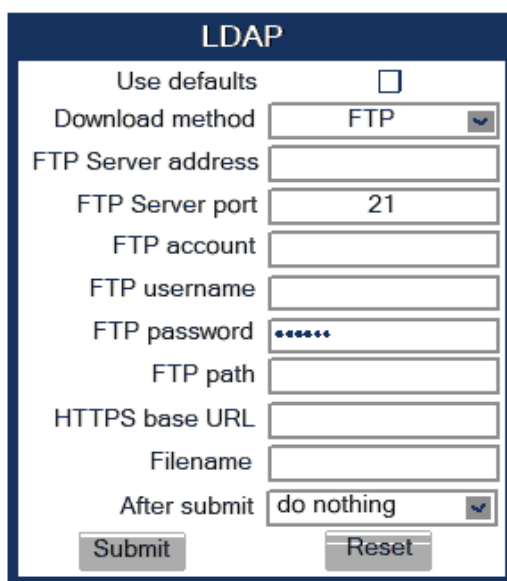
- **Use default:** Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No" Default: "No"
- **Filename:** Specifies the file name of the phone software.
- **After submit:** Specifies actions after submit button is pressed. Value range: "do nothing", "start download". Default: "do nothing".

Data required (if not derived from Defaults)

- **Download method:** Selects the protocol to be used. Value range: "FTP", "HTTPS" Default: "FTP"
- **Server address:** IP address or hostname of the FTP/HTTPS server in use.
- **Server port:** Port number of the FTP/HTTPS server in use. Default: 21
- **Account:** Account at the server (if applicable).
- **Username:** User name for accessing the server.
- **Password:** Password corresponding to the user name.
- **FTP path:** Path of the directory containing the files.
- **HTTPS base URL:** IP address or hostname of the HTTPS server in use; only applicable if Download method is switched to "HTTPS".

Administration via WBM

File transfer > LDAP



The image shows a web-based configuration form titled "LDAP" within a dark blue border. At the top, there is a checkbox labeled "Use defaults" which is currently unchecked. Below this, the form contains several input fields and dropdown menus: "Download method" is a dropdown menu with "FTP" selected; "FTP Server address" is a text input field; "FTP Server port" is a text input field with "21" entered; "FTP account" is a text input field; "FTP username" is a text input field; "FTP password" is a text input field with masked characters (dots); "FTP path" is a text input field; "HTTPS base URL" is a text input field; "Filename" is a text input field; and "After submit" is a dropdown menu with "do nothing" selected. At the bottom of the form, there are two buttons: "Submit" and "Reset".

Administration via Local Phone

```
|--- Admin
    |--- File Transfer
        |--- LDAP
            |--- Use default
            |--- Download method
            |--- Server
            |--- Port
            |--- Account
            |--- Username
            |--- Password
            |--- FTP path
            |--- HTTPS base URL
            |--- Filename
```

3.20.6.2 Download LDAP Template

If applicable, LDAP templates should be deployed using the DLS (Deployment Service). Alternatively, the download can be triggered from the web interface or from the Local phone menu.

NOTICE: The OpenScape Desk Phone CP phone supports LDAPv3.

Start Download via WBM

The image shows a web-based configuration dialog titled "LDAP". It contains the following fields and controls:

- Use defaults:** A checkbox that is currently unchecked.
- Download method:** A dropdown menu set to "FTP".
- FTP Server address:** A text input field containing "192.168.1.150".
- FTP Server port:** A text input field containing "21".
- FTP account:** An empty text input field.
- FTP username:** A text input field containing "phone".
- FTP password:** A text input field with masked characters "*****".
- FTP path:** A text input field containing "media".
- HTTPS base URL:** An empty text input field.
- Filename:** A text input field containing "ldap_template.txt".
- After submit:** A dropdown menu set to "start download".
- Buttons:** "Submit" and "Reset" buttons at the bottom.

In the **File transfer > LDAP** dialog, set After submit to "start download" and press the Submit button.

Start Download via Local Phone

In the administration menu, set the focus to LDAP.

```
|--- Admin
    |--- File Transfer
        |--- LDAP
```

- **On OpenScape Desk Phone CP100/200/205:**

Press the OK key. A context menu opens. In the context menu, select Download. The download will start immediately.

- **On OpenScape Desk Phone CP400/
OpenScape Desk Phone CP600/700/700X:**

Press the Soft Key labeled Download. The download will start immediately.

3.20.7 Screensaver

The screensaver is displayed when the phone is in idle mode. It performs a slide show consisting of images which can be uploaded using the web interface.

NOTICE: Screensavers are available only on OpenScape Desk Phone CP600/CP700/CP700X.

NOTICE: The file size for a screensaver image is limited to 300 KB. If the file is too large or the contents of the file are not valid, the file will not be stored in the phone.

For screensaver images, the following specifications are valid:

- **Data format:** JPEG, BMP or PNG. JPG is recommended. The file extensions supported for JPEG are jpeg and jpg.
- **Screen format:** 4:3. The images are resized to fit in the screen, so that images with a width/height ratio differing from 4:3 will appear with deviant proportions.
- **Resolution:** The phone's screen resolution is the best choice for image resolution:
 - **OpenScape Desk Phone CP600/600E/700/700X:** 320x240 px

3.20.7.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see [Common FTP/HTTPS Settings \(Defaults\)](#) on page 256) are to be used, Use default must be set to "Yes", and only the Filename must be specified.

Data required (in any case)

- **Use default:** Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No" Default: "No"
- **Filename:** Specifies the file name of the phone software.
- **After submit:** Specifies actions after submit button is pressed. Value range: "do nothing", "start download". Default: "do nothing".

Data required (if not derived from Defaults)

- **Download method:** Selects the protocol to be used. Value range: "FTP", "HTTPS" Default: "FTP"
- **Server address:** IP address or hostname of the FTP/HTTPS server in use.

- **Server port:** Port number of the FTP/HTTPS server in use. Default: 21
- **Account:** Account at the server (if applicable).
- **Username:** User name for accessing the server.
- **Password:** Password corresponding to the user name.
- **FTP path:** Path of the directory containing the files.
- **HTTPS base URL:** IP address or hostname of the HTTPS server in use; only applicable if Download method is switched to "HTTPS".

Administration via WBM

File transfer > Screensaver

Administration via Local Phone

```

|--- Admin
|   |--- File Transfer
|       |--- Screensaver
|           |--- Use default
|           |--- Download method
|           |--- Server
|           |--- Port
|           |--- Account
|           |--- Username
|           |--- Password
|           |--- FTP path
|           |--- HTTPS base URL
|           |--- Filename

```

3.20.7.2 Download Screensaver

If applicable, screensavers should be deployed using the DLS (Deployment Service). Alternatively, the download can be triggered from the web interface or from the Local phone menu.

Start Download via WBM

In the **File transfer > Screensaver** dialog, set After submit to "start download" and press the Submit button.

Start Download via Local Phone

In the administration menu, set the focus to Screensaver.

```
|--- Admin
      |--- File Transfer
            |--- Screensaver
```

- **On OpenScape Desk Phone CP600/600E/700/700X:**

Press the Soft Key labeled Download. The download will start immediately.

3.20.8 Ringer File

NOTICE: The download of ringer files via WBM or local menu is possible for all CP phone models.

Custom ring tones can be uploaded to the phone.

NOTICE: The file size for a ringer file is limited to 1 MB. If the file is too large or the contents of the file are not valid, the file will not be stored in the phone. This limitation is only enforced on WBM.

The following file formats are supported:

- **WAV format. The recommended specifications are:**
 - **Audio format:** PCM
 - **Bitrate:** 16 kB/sec
 - **Sampling rate:** 8 kHz
 - **Quantization level:** 16 bit

- MIDI format.
- MP3 format (OpenScape Desk Phone CP400/600/700/700X only). The OpenScape Desk Phone CP400/600/700/700X phones are able to play MP3 files from 32 kbit/s up to 320 kbit/s. As the memory for user data is limited to 8 MB, a constant bitrate of 48 kbit/sec to 112 kbit/s and a length of max. 1 minute is recommended. Although the phone software can play stereo files, mono files are recommended, as the phone has only 1 loudspeaker. See the following table for estimated file size (mono files).

Length	64 kbit/s	80 kbit/s	96 kbit/s	112 kbit/s
0:15 min	0.12 MB	0.15 MB	0.18 MB	0.21 MB
0:30 min	0.23 MB	0.29 MB	0.35 MB	0.41 MB
0:45 min	0.35 MB	0.44 MB	0.53 MB	0.62 MB
1:00 min	0.47 MB	0.59 MB	0.70 MB	0.82 MB

3.20.8.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see [Common FTP/HTTPS Settings \(Defaults\)](#) on page 256) are to be used, Use default must be set to "Yes", and only the Filename must be specified.

Data required (in every case)

- **Use default:** Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No" Default: "No"
- **Filename:** Specifies the file name of the phone software.
- **After submit:** Specifies action after submit button is pressed. Value range: "do nothing", "start download". Default: "do nothing".

Data required (if not derived from Defaults)

- **Download method:** Selects the protocol to be used. Value range: "FTP", "HTTPS" Default: "FTP"
- **Server address:** IP address or hostname of the FTP/HTTPS server in use.
- **Server port:** Port number of the FTP/HTTPS server in use. Default: 21
- **Account:** Account at the server (if applicable).
- **Username:** User name for accessing the server.
- **Password:** Password corresponding to the user name.
- **FTP path:** Path of the directory containing the files.
- **HTTPS base URL:** IP address or hostname of the HTTPS server in use; only applicable if Download method is switched to "HTTPS".

Administration via WBM

File transfer > Ringer file

Administration via Local Phone

```
|--- Admin
    |--- File Transfer
        |--- Ringer
            |--- Use default
            |--- Download method
            |--- Server
            |--- Port
            |--- Account
            |--- Username
            |--- Password
            |--- FTP path
            |--- HTTPS base URL
            |--- Filename
```

3.20.8.2 Download Ringer File

If applicable, ring tone files should be deployed using the DLS (Deployment Service). Alternatively, the download can be triggered from the web interface or from the Local phone menu.

Start Download via WBM

In the **File transfer > Ringer** dialog, set After submit to "start download" and press the Submit button.

Start Download via Local Phone

In the administration menu, set the focus to Ringer.

```
|--- Admin
      |--- File Transfer
            |--- Ringer
```

- **On OpenScape Desk Phone CP600/700/700X:**

Press the Soft Key labeled Download. The download will start immediately.

3.20.9 Company logo

NOTICE: The upload of company logo via WBM or local menu is possible only for OpenScape Desk Phone CP400/CP600/CP600E/700/700X.

Custom company logo can be uploaded to the phone.

NOTICE: There can only be a single logo image on the phone. When a new logo image is uploaded, the old one is deleted if there is one existing.

By default, there is no logo image file on the phone. Admin can upload a custom logo image with appropriate file extension (PNG or BMP), which would be displayed on Menu and Phone Lock screens. The Time and Date information are shown in small format below the status bar when the logo is being displayed.

Administration via WBM

File transfer > Logo

Logo

Transfer using file

Choose the image file you wish to use as a logo

Choose File

No file chosen

Submit

Cancel

Closing or navigating away from this page will cancel the file upload

Transfer using FTP/HTTPS

Use defaults

☐

Download method

FTP

FTP server address

FTP server port

21

FTP account

FTP username

FTP password

FTP path

Filename

After submit

do nothing

Submit

Reset

If there was a logo uploaded, an additional option "delete logo file" appears under the option "After submit".

Administration via Local Phone

```
|--- Admin
  |--- File Transfer
    |--- Logo
      |--- Use default
      |--- Download method
```

```
|--- Server  
|--- Port  
|--- Account  
|--- Username  
|--- Password  
|--- FTP path  
|--- HTTPS base URL  
|--- Filename
```

Format of the logo image file

The logo image file will be accepted by the phone in below formats:

- **CP600/700**: PNG image 24-bit with alpha
- **CP400**: BMP image format

Image file size must not exceed 10 MBytes.

Resizing logo image file

After successful transfer of the new logo file, the phone will check the image resolution size in pixels and decide if it needs to be resized so that the image fits in the logo image placeholder.

The maximum size of logo image placeholder is as below:

- **CP600/CP600E**: 220 x 70
- **CP400/700/700X**: 112 x 32

Resizing is done by keeping the aspect ratio intact.

3.21 Corporate Phonebook: Directory Settings

3.21.1 LDAP

The Lightweight Directory Access Protocol enables access to a directory server via an LDAP client. Various personal information is stored there, e.g. the name, organization, and contact data of persons working in an organization.

When the LDAP client has found a person's data, e. g. by looking up the surname, the user can call this person directly using the displayed number.

NOTICE: Direct access to LDAP by the user is only available on CP100/CP200/CP205 phones. For CP400/CP600/CP600E/CP700/CP700X phones, the access to LDAP is part of the **Conversations** screen and especially of its *Search* feature.

NOTICE: The OpenScape Desk Phone CP100/200/205/400/600/600E phones support LDAPv3.

For connecting the phone's LDAP client to an LDAP server, the required access data must be configured. The parameter Server address specifies the IP address of the LDAP server. The parameter Transport defines whether the

phone has to continue to use an unencrypted TCP connection to the LDAP server. Depending on the setting of Transport the Secure Port (for TLS) or the Server port (for TCP) are to be defined. If the Authentication is not set to "Anonymous", the user must authenticate himself with the server by providing a User name and a corresponding Password. The user name and password are defined by the administrator. The user name is the string in the LDAP bind request, e. g. "C=GB,O=SIEMENS COMM,OU=COM,L=NTH,CN=BAYLIS MICHAEL". The internal structure will depend on the specific corporate directory.

For a quick guide on setting up LDAP on an OpenScape Desk Phone CP100/200/205/400/600/600E phone, please refer to [How to Set Up the Corporate Phonebook \(LDAP\)](#) on page 328.

A search field for LDAP requests is supported. The search string is submitted to the LDAP server as soon as the OK key is pressed or when the Search trigger timeout expires.

Data required

- **LDAP Server address:** IP address or hostname of the LDAP server.
- **Transport:** Defines Transport mode, whether LDAP interface uses TCP and is unencrypted, or uses TLS and is encrypted.
 - **Value range:** "TCP", "TLS".
 - **Default:** "TCP".
- **Secure Port:** Defines the port of the appropriate TLS interface on LDAP server when Transport is set to TLS. The default value is "636".
- **LDAP Server port:** Defines the port on which the LDAP server listens for requests when Transport is set to TCP. The default value is "389".
- **Authentication:** Defines the authentication method used for connecting to the LDAP server.
 - **Value range:** "Anonymous", "Simple".
 - **Default:** "Anonymous".
- **User name:** The username used for authentication with the LDAP server in the LDAP bind request.
- **Password:** The password used for authentication with the LDAP server.
- **Avatar server:** HTTP/HTTPS address, where the pictures are stored. The complete HTTP/HTTPS address is built from <Avatar server> + <Avatar>, where <Avatar> is the attribute name in the LDAP template that contains the filename of the picture.
 - Example: <Avatar Server> = "https://mypicture.server/picturepath"
 - <Avatar> = "UserA.jpg"

When the phone does an LDAP lookup for user A, the field **picturename** returns `picturename = UserA.jpg`. The phone will look for the picture at: `https://mypicture.server/picturepath/UserA.jpg`.
- **LDAP for manual search only:** Allows you to disable the automatic LDAP lookup when an LDAP server is configured. If checked, the user can search LDAP only manually.
 - Value range: "True", "False".
 - Default: "False".

NOTICE: This item is available only for CP400/600/700.

- **Firstname and lastname for quick search:** Defines whether the phone searches both **Firstname** and **Lastname** or only **Lastname**.
 - Value range: "True", "False".
 - Default: "False".

NOTICE: The default value indicates that the search string provided by the user is used to search the **Lastname** field only on the LDAP server.

Administration via WBM

Local functions > Directory Settings

Administration via Local Phone

```
|--- Admin
  |--- Local Functions
    |--- LDAP
      |--- Server address
      |--- Transport
      |--- LDAP Secure port
      |--- LDAP Server port
      |--- Authentication
      |--- User name
      |--- Password
      |--- LDAP for manual search only
      |--- Firstname and lastname for quick
search
```

3.21.2 Contact details update

It is possible to update the source used to obtain call party names from one place.

NOTICE: Contact details update is possible only for CP phone models: 600, 600E & 400. Not applicable for Broadsoft.

The phone can be configured by Admin such that

- Existing contact names are updated for new calls (if one or more sources are specified and matched)
- Existing contact names are not updated (if the Local source is used, i.e. no sources set)

3.21.2.1 Source of the contact details

The update source can be set as one or more of the following:

1) Directory

- LDAP (if an LDAP entry matches the call then the contact is update to match the LDAP entry)

2) Signalling

- Via SIP (if set then the contact is updated based on the call party name in signaling)

3) Local

- Alternatively the source may be local, meaning that the existing number matching rules are applied but the matched contact is not updated

When an update source has been specified then the phone will try to match the call party number signalled for a call to an entry in the update source(s). If more than one source is specified then they will be used in the following order:

- LDAP
- Signalling

Administration via WBM

Local functions > Name update sources

Administration via Local Phone

```
|--- Admin
    |--- Local Functions
        |--- LDAP
            |--- Server address
            |--- Transport
            |--- LDAP secure port
            |--- LDAP server port
            |--- Authentication
            |--- User name
            |--- Password
            |--- Avatar server
        |--- Name update sources
```

3.22 XSI access

The BroadSoft Xtended Services Interface (Xsi) provides access to various user features like caller lists and directories.

Administration via WBM

Local functions > XSI access

Administration via Local Phone

```
|--- Admin
    |--- Local Functions
        |--- XSI access
            |--- Server address
            |--- Use SIP credentials
            |--- User name
            |--- Password
```

3.23 RingCentral API connection

You can sync call log data and phonebook from RingCentral backend to your Desk Phone CP device (phone). You can also enable the Server DND feature to make the DND status reflect on the user's phone display.

To enable the sync features, you have to establish a connection between your phone device and the RingCentral API.

Administration via WBM

The path to this configuration is: **Admin > Local functions > RingCentral API**

Enter manually the API server address (URL) under **Server address**, including the port, if port is not the default https port (default: empty).

3.23.1 Syncing call log data

You can enable call log data sync to ensure the RingCentral user's call history is up-to-date.

When the option to sync the call log from the API is enabled, the phone will stop logging calls locally. When enabled for the first time, the phone will clear the local call log and delete all call history data from existing conversations. If disabled again, the local call logging will be resumed.

Administration via WBM

The path to this configuration is: **Admin > Local functions > RingCentral API**

Check the option **Sync call log**. Default is disabled.

NOTICE: The connection to the API server is done via TLS and will use the existing mechanisms for validating the connection by using a new RingCentral API specific authentication policy. Please refer to [RingCentral Certificates](#) for more details regarding RingCentral certificates.

NOTICE: When a server address is provided and synchronisation of call log data is enabled, the phone will try to download call log data from the API server at RingCentral.

Additional Notes

On DeskPhone CP devices supporting Conversations, the phone will display each call log record as a single conversation:

- Every missed call item can be marked as viewed separately or using the "Mark all calls as read" functionality from the options menu.
- Every call item can be deleted separately or using the "Delete all calls" functionality from the options menu.
- No item on the list can be edited.
- The conversation list options provided will be "Delete all conversations" and "Mark all conversations as read".

On DeskPhone CP devices NOT supporting conversations, the phone will display all call log records in the corresponding list of missed, received or dialled calls:

- On leaving the missed call list, all calls will be marked as viewed.

- Calls cannot be deleted speratly, only one of the missed, received or dialled call lists can be deleted at once.

On entering the call log list, the phone will attempt to refresh the data from the API. This must be done because there is no mechanism allowing the server to tell the phone that the call log has been changed and needs to be updated. A refresh will attempt to download the incremental changes of call log data since the last synchronisation. Other mechanisms to update the call log:

- On changing the server address or enabling the sync call log feature.
- On startup of the phone.
- When a call has finished.

3.23.2 Syncing the phonebook

You can enable phonebook sync to ensure the RingCentral user has access to their contacts.

Administration via WBM

The path to this configuration is: **Admin > Local functions > RingCentral API**

Check the option **Sync phonebook**. Default is disabled.

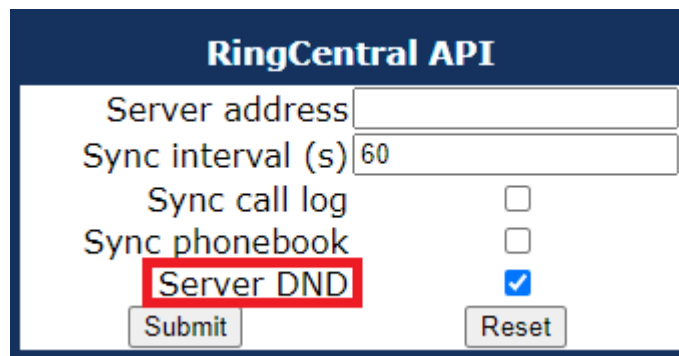
When enabled, the user can access the phonebook data via the main menu screen and view, add, edit or delete a phonebook record. Any change made in the phonebook data is synchronized via the API.

3.23.3 Syncing the DND settings

You can integrate the server-side DND settings with the CP Phone. This allows the user to manage a single DND setting that is synchronized and indicates their availability across all endpoints.

Administration via WBM

The path to this configuration is: **Admin > Local functions > RingCentral API**



The image shows a web form titled "RingCentral API". It contains the following fields and controls:

- Server address**: A text input field.
- Sync interval (s)**: A text input field containing the value "60".
- Sync call log**: A checkbox, currently unchecked.
- Sync phonebook**: A checkbox, currently unchecked.
- Server DND**: A checkbox, currently checked. This label is highlighted with a red rectangular box.
- Submit**: A button located below the "Server DND" checkbox.
- Reset**: A button located to the right of the "Submit" button.

Check the option **Server DND**. Default is disabled.

When enabled, server DND state is reflected on the user's phone display. Otherwise Local DND is used and the setting is not shared with other users.

When disabled, the user's presence state and menu is reverted back to local DND setting.

To apply configuration parameters, you need to trigger a resync manually:

- via **Phone System > Phones & Devices > User Phones** : Select a phone which is assigned and provisioned and then select the **Resync** option.
- Reassign the CP Phone to another user, remove or edit a phone number.

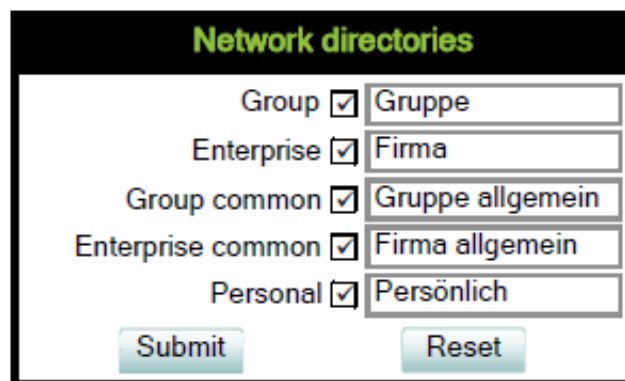
3.24 Network directories

Available network directories (accessible by BroadSoft Xtended Services Interface) can be activated/deactivated and supplied with customized names.

To synchronize Network directories, the XSI has to be activated.

Administration via WBM

Local functions > Network directories



The image shows a web form titled "Network directories". It contains the following fields and controls:

- Group**: A checkbox (checked) followed by a text input field containing "Gruppe".
- Enterprise**: A checkbox (checked) followed by a text input field containing "Firma".
- Group common**: A checkbox (checked) followed by a text input field containing "Gruppe allgemein".
- Enterprise common**: A checkbox (checked) followed by a text input field containing "Firma allgemein".
- Personal**: A checkbox (checked) followed by a text input field containing "Persönlich".
- Submit**: A button located below the "Personal" checkbox.
- Reset**: A button located to the right of the "Submit" button.

Administration via Local Phone

```
|--- Admin
|--- Local Functions
|--- Network directories
|--- Group
|--- Enterprise
|--- Group common
|--- Enterprise common
```

|--- Personal

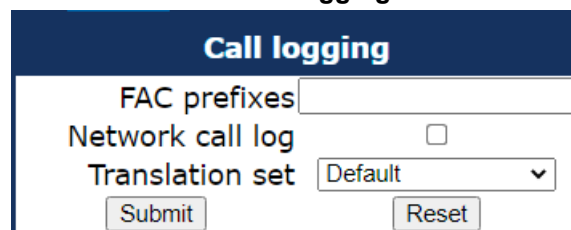
3.25 Call log

The Network directories and the XSI has to be activated.

NOTICE: The **Network call log** option is specific to Broadsoft.

Administration via WBM

Local functions > Call logging



On OpenScape Desk Phone CP100/CP200/CP205 also available on 2nd level.
For more information, see [Enable "Long Press" for Free Programmable Keys on second level for CP20X Broadsoft](#).

For more information, see [Call logging](#) on page 114.

3.26 Speech

3.26.1 RTP Base Port

The port used for RTP is negotiated during the establishment of a SIP connection. The RTP base port number defines the starting point from which the phone will count up when negotiating. The default value is 5010.

The number of the port used for RTCP will be the RTP port number increased by 1.

Administration via WBM

Network > Port Configuration

Port configuration

SIP server5060

SIP registrar5060

SIP gateway5060

SIP local5060

Backup proxy5060

RTP base5010

Download server (default)21

LDAP server389

HTTP proxy0

LAN port status100 Mbps half duplex

LAN port speedAny

PC port statusLink down

PC port speedAny

PC port modedisabled

PC port autoMDIX☐

SubmitReset

Administration via Local Phone

```
|--- Admin
  |--- Network
    |--- Port configuration
      |--- RTP base
```

3.26.2 Codec Preferences

If Silence suppression is activated, the transmission of data packets is suppressed when there is no conversation, that is, if the user doesn't speak.

The OpenScape Desk Phone CP phone provides the codecs G.722, OPUS (both not applicable for OpenScape Desk Phone CP100), G.711 and G.729. When a SIP connection is established between two endpoints, the phones negotiate the codec to be used. The result of the negotiation is based on the general availability and ranking assigned to each codec. The administrator can allow or disallow a codec as well as assign a ranking number to it.

The Packet size, i. e. length in milliseconds, of the RTP packets for speech data, can be set to 10ms, 20ms, 30ms, 40ms, 60ms or to automatic detection.

Data required

The Packet size, i. e. length in milliseconds, of the RTP packets for speech data, can be set to 10ms, 20ms, 30ms, 40ms, 60ms or to automatic detection.

Data required

- **Silence suppression:** Suppression of data transmission on no conversation. Value range: "On", "Off"
Default: "Off"
- **Allow "HD" icon:** If "On" an additional icon is shown when codec OPUS (or G.722) is used. Value range: "On", "Off"
Default: "On"
- **Packet size:** Size of RTP packets in milliseconds. Value range: "10 ms", "20ms", "30ms", "40ms", "60ms", "Automatic"
Default: "Automatic"
- **OPUS:** Parameters for the OPUS codec. Value Range: "Choice 1", "Choice 2", "Choice 3", "Choice 4", "Disabled", "Enabled"
Default: "Choice 1"
- **G.711:** Parameters for the G. 711 codec. Value Range: "Choice 1", "Choice 2", "Choice 3", "Choice 4", "Disabled", "Enabled"
Default: "Choice 2"
- **G.729:** Parameters for the G. 729 codec. Value Range: "Choice 1", "Choice 2", "Choice 3", "Choice 4", "Disabled", "Enabled"
Default: "Choice 3"
- **G.722:** Parameters for the G. 722 codec. Value Range: "Choice 1", "Choice 2", "Choice 3", "Choice 4", "Disabled", "Enabled"
Default: "Disabled"

OPUS settings

- **Max bandwidth:** Determines the bandwidth that OPUS encoder should operate on. The OPUS codec may decrease the bandwidth from Wideband to Narrowband as it see fit. However if set to Narrowband, it will never increase to Wideband by itself. The bandwidth also determines the optimum bitrate if encoder is in CBR mode (12 kb/s at NB, 20 kb/s at WB).
Value Range: "Narrowband" (8kHz), "Wideband" (16kHz)
Default: "Wideband"
- **Bitrate type:** Configures if OPUS encoder should work in VBR or CBR modes.
Value Range: "CBR", "VBR"
Default: "VBR"
- **Max complexity:** Determines the maximum computational complexity of the codec. Lower values indicate worse quality.
Value Range: 0 to 10
Default: 10
- **FEC:** Forward Error Correction (FEC) is used to include redundant payload data for better quality in lossy networks, but increases computational complexity and bandwidth.
Value Range: "On", "Off"
Default: "Off"

Administration

- **DTX**: Discontinuous Transmission (DTX) determines whether to send empty payload frames during silence periods.

Value Range: "On", "Off"

Default: "Off"

- **PLR**: Packet loss rate (PLR) provides packet loss percentage of the network as an input to encoder.

Value Range: 0 to 100

Default: 0

Administration via WBM

Speech > Codec preferences

The screenshot shows a web interface for configuring codec preferences and OPUS settings. The 'Codec preferences' section includes checkboxes for 'Silence suppression' and 'Allow "HD" icon', a dropdown for 'Packet size' set to 'Automatic', and ranking controls for OPUS, G.711, G.729, and G.722 using up/down arrows and a red 'X' icon. The 'OPUS settings' section includes dropdowns for 'Max bandwidth' (Wideband) and 'Bitrate type' (VBR), a text input for 'Max complexity' (10), and checkboxes for 'FEC' and 'DTX'. A 'PLR' text input is set to 0. 'Submit' and 'Reset' buttons are at the bottom.

Codec preferences	
Silence suppression	☐
Allow "HD" icon	☒
Packet size	Automatic
OPUS ranking	Down arrow, Red X
G.711 ranking	Up arrow, Down arrow, Red X
G.729 ranking	Up arrow, Down arrow, Red X
G.722 ranking	Up arrow, Checkmark

OPUS settings	
Max bandwidth	Wideband
Bitrate type	VBR
Max complexity	10
FEC	☐
DTX	☐
PLR	0

Submit Reset

Administration via Local Phone

```
|--- Admin
  |--- Speech
    |--- Codec Preferences
      |--- Silence suppression
      |--- Allow 'HD' icon
      |--- Packet size
        |--- OPUS
        |--- G.711
        |--- G.729
        |--- G.722
```

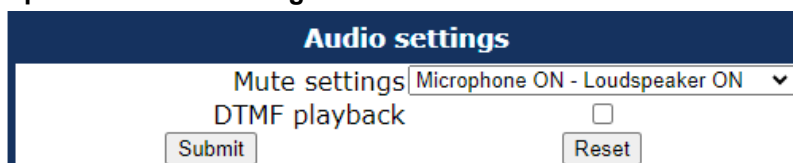
```
|--- OPUS settings
```

3.26.3 Audio Settings

The usage of microphone and speaker for speakerphone mode can be controlled by the administrator. Both microphone and loudspeaker can be switched on or off separately. By default, both microphone and loudspeaker are switched on.

Administration via WBM

Speech > Audio Settings



Administration via Local Phone

```
|--- Admin
    |--- Speech
        |--- Audio Settings
            |--- Disable microphone
                |--- Disable loudspeaker
                    |--- DTMF playback
```

The DTMF playback feature aims at the capability to play DTMF digits received using [RFC2833](#) coding (i.e. Rtp events) in the current active audio device (headset / loudspeaker / handset).

3.27 Password

The passwords for user and administrator can be set here. They have to be confirmed after entering. The default factory setting for the administrator password is "123456"; it should be changed after the first login (see Change Admin and User password). The factory setting for the user password is "not set", i. e. no password.

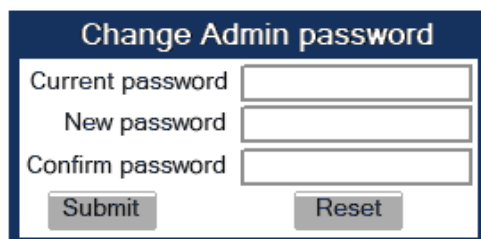
Usable characters are 0-9 A-Z a-z . " * # , ? ! ' + - () @ / : _

Default Passwords

- **Admin menu:** 123456
- **User menu:** no password
- **Factory Reset:** 124816
- **Soft Restart:** Press keys 1-4-7 simultaneously and enter Admin password.
- **Factory Reset:** Press keys 2-8-9 simultaneously and enter Reset password.

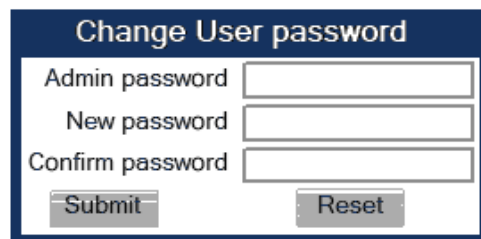
Administration via WBM

Security and Policies > Password > Change Admin password



A screenshot of a web form titled "Change Admin password". It contains three input fields: "Current password", "New password", and "Confirm password". Below the fields are two buttons: "Submit" and "Reset".

Security and Policies > Password > Change User password



A screenshot of a web form titled "Change User password". It contains three input fields: "Admin password", "New password", and "Confirm password". Below the fields are two buttons: "Submit" and "Reset".

Administration via Local Phone

```
|--- Admin
    |--- Security and policies
        |--- Change admin password
            |      |--- Current admin
                |      |--- Admin
                |      |--- Confirm admin
            |--- Change user password
                |--- Admin password
                |--- New user password
                |--- Confirm new user
```

3.27.1 Troubleshooting: Lost Password

If the administration and/or user password is lost, and there is no DLS available, new passwords must be provided. In case of lost administration password, a factory reset is necessary. In case of lost user password, the administrator may reset the user password. Take the following steps to initiate a factory reset:

- 1) On the phone, press the Service/Settings key to activate the administration menu (the Menu key toggles between the user's configuration menu and the administration menu).
- 2) Press the number keys 2-8-9 simultaneously. The factory reset menu opens. If not, the key combination is deactivated due to security reason.
- 3) In the input field, enter the special password for factory reset "124816".
- 4) Confirm by pressing OK.

3.28 Restart Phone

If necessary, the phone can be restarted from the administration menu or via pressing number keys 1-4-7 simultaneously.

Administration via WBM

Maintenance > Restart Phone



Administration via Local Phone

```
|--- Admin
      |--- Maintenance
          |--- Restart
```

3.29 Factory Reset

This function resets all parameters to their factory settings. A special reset password is required for this operation: "124816".

Administration via WBM

Maintenance > Factory reset



Administration via Local Phone

```
|--- Admin
      |--- Maintenance
          |--- Factory reset
```

3.30 SSH — Secure Shell Access

The phone's operating system can be accessed via SSH for special troubleshooting tasks. Hereby, the administrator is enabled to use the built-in Linux commands. As soon as SSH access has been enabled using the WBM, the system can be accessed by the user "admin" for a specified timespan. When this timespan has expired, no connection is possible any more. The user "admin" has the following permissions:

- **Log folder and files:** read only
- **User data folder and files:** read/write access
- **Opera deploy folders and files:** read only
- **Version folder:** read/write access; version files: read only

NOTICE: It is not possible to logon as root via SSH.

When Enable access is enabled, and the parameters described underneath are specified, SSH access is activated. By default, SSH access is disabled.

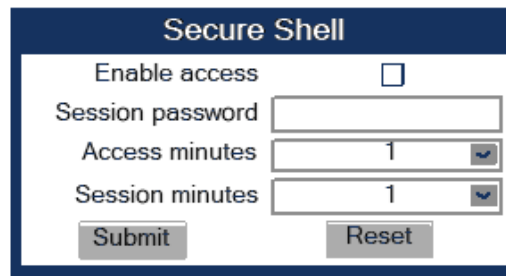
With the Session password parameter, a password for the "admin" user is created. This password is required. It will be valid for the timespan specified in the parameters described underneath.

Access minutes defines the timespan in minutes within which the SSH connection must be established. After it has expired, a logon via SSH is not possible. The possible values ranges from 1 to 10.

Session minutes defines the maximum length in minutes for an SSH connection. After it has expired, the "admin" user is logged out. The possible values are 5, 10, 20, 30, 60.

Administration via WBM

Maintenance > Secure Shell



3.31 Diagnostics

NOTICE: Some of the diagnostic tools and functions may reveal personal data of the user, such as caller lists. Thus, with regards to data privacy, it is recommended to inform the user when diagnostic functions are to be executed.

3.31.1 Display General Phone Information

General information about the status of the phone can be displayed if desired.

Displayed Data

- MAC address: Shows the phone's MAC address.
- Software version: Displays the version of the phone's firmware.
- Last restart: Shows date and time of the last reboot.
- Backlight type: Indicates whether the phone has a backlight, and, if applicable, the type of backlight. Value range: 0 (no backlight); 1 (cathode tube backlight); 2 (LED backlight)
- Part Number: Shows the part number of this telephone.
- UBoot version: Shows the software version of the UBoot loader.
- Audio parameter set
- Number of KMs

Display on the WBM

General information

General information	
MAC address	001ae8761022
Software version	V1 R9.4.80 SIP 220505
Last restart	2022-05-05T14:12:34
Backlight type	2
Part number	S30817-S7722-A101-04
UBoot version	U-Boot 1.0.0.31.201019
Audio parameter set	Standard
Number of KMs	0

Display on the Local Phone

```
|--- Admin
|--- General Information
|--- MAC address
|--- Software version
|--- Last restart
|--- Backlight type
|--- Part Number
|--- UBoot version
|--- Audio parameter set
|--- Number of KMs
```

3.31.2 View Diagnostic Information

In addition to the general phone information (see [Display General Phone Information](#) on page 290), extended data can be viewed.

NOTICE: The Diagnostic Information can also be viewed by the administrator on the local phone by selecting **Diagnostic information > View**.

Display on the WBM

Diagnostics > Diagnostic information > View

View	
2011-10-16 20:22:33	
00 Terminal number:	3339
01 SIP server:	192.168.1.230
02 SIP port:	5060
03 SIP registrar:	192.168.1.230
04 SIP registrar port:	5060
05 SIP gateway:	192.168.1.230
06 SIP gateway port:	5060
07 SIP transport:	UDP
08 SIP local:	5060
09 Server features:	No
10 DNS results:	5060
11 Multiline:	No
12 Registered lines:	5060
13 Backup active:	Yes
14 Backup proxy:	192.168.1.148
15 Use secure calls:	No
16 SDES status:	0
17 Secure SIP server:	0
18 Software version:	V3R0.50.0 110924
19 Display message:	None
20 Last restart:	2011-10-10T23:59:01
21 Memory free:	65733K free
22 Protocol mode:	IPv4
23 IP4 address:	192.168.1.235

3.31.3 User Access to Diagnostic Information

If this option is enabled, extended phone data is also displayed to the user. To view the data, the user must click on the "Diagnostic information" link in the user menu.

NOTICE: The Diagnostic Information can also be viewed by the user on the local phone by selecting **User > Diagnostic information**.

Administration via WBM

Diagnostics > Diagnostic information > User access

3.31.4 Diagnostic Call

The feature "Rapid Status Diagnostic Call" will provide the possibility to place a diagnostic call, for example by the user, which starts call related tracing on the phone and on involved OpenScope Voice and collect these traces at OpenScope Voice Trace Manager (OSVTM). With all these traces available, a call can be followed throughout the voice system and a possible problem can be detected faster. As all traces from all involved components are available at the first level support, the analysis of a possible problem can be started immediately.

A so-called diagnostic scenario will enable traces on all involved SIP components of the OSC Voice solution and store all traces at a central server. A tool will help service to follow a call through the traces and determine the point of problem.

The approach is to use a SIP Header ([1]) to indicate, whether a call is a diagnostic call or not. Presence of this header will mean that related call is a diagnostic call. Absence of this field means a non-diagnostic call. This header will either switch on traces in the solution component or be ignored, if it isn't supported. If the call is recognized as a diagnostic call, the traces will be sent to DLS as a first step and then DLS will forward them to OSVTM. Collected traces will either be sent after a successful end of diagnostic scenario or trace file is full.

For enabling tracing on all involved solution components, a call must be recognized to be a "diagnostic" call. Therefore, a special SIP header will be added to the signalling messages. All components which are able to support such a call will then switch on traces and send the traces to DLS server (which will forward them to a pre-defined OSVTM server).

A dial-prefix has been chosen, as the dialled number should be identical to a number, where the user identified a possible problem. This prefix will be filtered before placing a call, so that the SIP messages will be similar to the ones for the problematic destination.

The SIP header "X-Siemens-Trace-ID" has been chosen, as this is a special SIP field created for this feature. Existence of the diagnostic call, start and finish of a diagnostic call can be determined via this field [1].

Trace id will be unique throughout the system and the following format will be used to generate trace id:

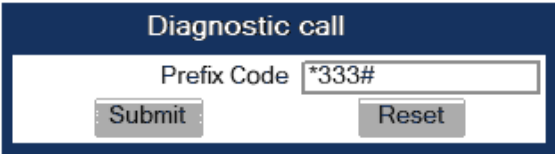
TraceId: <UNIX_Timestamp>_<Last 6 bytes of MAC Address>

If related calls (diagnostic or not) are established following the start of the diagnostic call, then it turns to be a diagnostic scenario. Related calls become diagnostic (if they are not already) and traces are collected until the last diagnostic call ends plus a predefined timer. This timer guarantees capturing related information regarding to a problematic scenario.

The diagnostic call can only be determined during the call so initial traces might get lost. For this reason, user may need to do additional call. This is completely user related and user should be informed about the process. There will not be any restriction to prevent user to dial the prefix. If the prefix is configured by admin, user can always dial the prefix and start a diagnostic call. The prefix has to consist of the leading asterisk followed by three digits and the hash. Example: *333#.

Administration via WBM

Maintenance > Diagnostic call



Diagnostic call

Prefix Code

Administration via Local Phone

```
|--- Admin
      |--- Maintenance
```

```
|--- Diagnostic Call
```

Admin will not be able to change trace settings or can not clear the existing phone traces during an active diagnostic tracing. If admin tries to change trace configuration or delete existing traces this will not be allowed and admin will get the following error: **Change not allowed: Diagnostic tracing is active!**

3.31.5 LAN Monitoring

The LAN port mirror facility allows for monitoring all network traffic at the phone's LAN port.

Additionally, there is a possibility to monitor LAN traffic and port settings in the Local user menu:

```
|--- User
    |--- Network information
        |--- Phone address
        |--- Web address
        |--- IPv4 address
        |--- IPv6 Global Address
        |--- IPv6 Linklocal Address
        |--- LAN RX
        |--- LAN TX
        |--- PC RX
        |--- PC TX
        |--- LAN autonegotiated
        |--- LAN information
        |--- PC autonegotiated
        |--- PC information
```

3.31.6 LLDP-MED

When the phone is connected to a switch with LLDP-MED capabilities, it can receive a VLAN ID and QoS parameters and advertise its own network-related properties. The data is exchanged in TLV (Type-Length-Value) format.

Both sent and received LLDP-MED data can be monitored at the administrator interface.

NOTICE: For details on LLDP-MED, please refer to the ANSI/TIA-1057 standard.

For a network configuration example that shows LLDP-MED in operation, please refer to [Example Dial Plan](#) on page 336.

Displayed Data

- **Extended Power:** Power Consumption; relevant for PoE.
- **Network policy (voice):** VLAN ID and QoS (Quality of Service) parameters for voice transport.
- **Network policy (signalling):** VLAN ID and QoS (Quality of Service) parameters for signalling.

- **LLDP-MED capabilities:** The LLDP-MED TLVs supported by the phone and the switch as well as the specific device class they belong to.
- **MAC_Phy configuration:** Identifies the possible duplex and bit-rate capability of the sending device, its current duplex and bit-rate capability, and whether these settings are the result of auto-negotiation during the initialization of the link, or of manual set override actions.
- **System capabilities:** The devices advertise their potential and currently enabled functions, e. g. "Bridge", "Telephone".
- **TTL:** Time To Live. This parameter determines how long the TLVs are valid. When expired, the device will send a new set of TLVs.
- **Inventory:** Inventory information of a CP phone such as "Manufacturer Name", "Model Name", "Hardware Revision", "Firmware Revision", "Software Revision", "Serial Number", "Asset ID"

View Data From WBM

Network > Wires settings

Wired settings	
LAN connection	
Use LLDP-MED	☒
Use DHCP	☒
DHCPv6 enabled	☒
Use DHCP reuse	☐
VLAN discovery	LLDP-MED v
VLAN ID	
LLDP-MED operation	
Time to live (seconds)	120 v
LAN port	
LAN port status	100 Mbps full duplex
LAN port speed	Any v

S

View Data From Local Menu

If both sent and received values are concordant, OK is appended to the parameter. If not, an error message is displayed.

```
|--- Admin
    |--- Network
        |--- Wires settings
            |--- Use
            |--- Network policy (voice)
            |--- Network policy (signaling)
            |--- LLDP-MED cap's
            |--- MAC_Phy config
            |--- System cap's
            |--- TTL
```

3.31.7 IP Tests

For network diagnostics, the OpenScope Desk Phone CP phone can ping any host or network device to determine whether it is reachable. Additionally, the IP route to a host or network device can be traced using the traceroute tool contained in the phone software.

The Pre Defined Ping tests provide ping for a pre-defined selection of servers: DLS, SIP server, and SIP registrar.

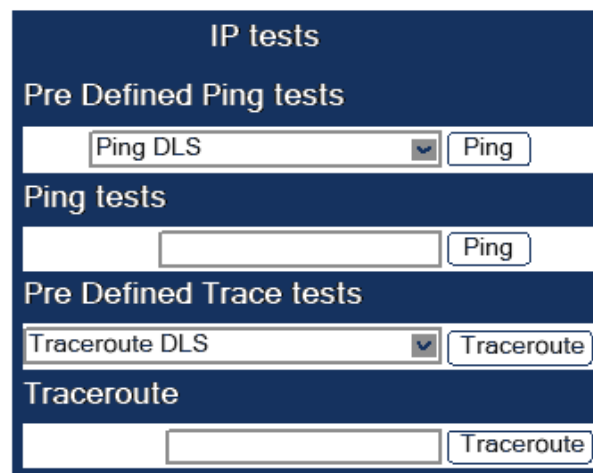
Ping tests enables the ping of a random IP address.

The Pre Defined Trace tests provide traceroute tests for a pre-defined selection of servers: DLS, SIP server, and SIP registrar.

Traceroute enables traceroute tests for a random IP address.

Administration via WBM

Diagnostics > Miscellaneous > IP tests



The screenshot shows a web interface titled "IP tests". It contains four sections: "Pre Defined Ping tests" with a dropdown menu showing "Ping DLS" and a "Ping" button; "Ping tests" with an empty input field and a "Ping" button; "Pre Defined Trace tests" with a dropdown menu showing "Traceroute DLS" and a "Traceroute" button; and "Traceroute" with an empty input field and a "Traceroute" button.

3.31.8 Process and Memory Information

The processes currently running on the phone's operating system as well as their CPU and memory usage can be monitored here. 100 processes are monitored on the web page. For further information, please refer to the manual of the "top" command for Unix/Linux systems, or to the related documentation.

The amount of free memory is checked on a regular basis in order to prevent problems caused by low memory. This check determines whether a recovery is necessary.

When **Disable reboot** is checked, no automatic reboot takes place when a memory problem has been found. However, recovery requires a manual reboot, which is preferable after working hours.

The recovery process will be triggered when the available main memory (RAM) falls below a given threshold value. There are two thresholds parameters, indicating how much space memory is available:

- **The High Threshold (MBs):**

This parameter defines the threshold for out of working hours.

NOTICE:

For OpenScape Desk Phone CP100, the default value is 13 MB.

For OpenScape Desk Phone CP100/CP200/CP205, the default value is 20 MB.

For OpenScape Desk Phone CP400/600/700/700X, the default value is 30 MB.

- **The Low Threshold (MBs):**

This parameter defines the threshold for working hours.

NOTICE:

For OpenScape Desk Phone CP100, the default value is 11 MB.

For OpenScape Desk Phone CP200/CP205, the default value is 17 MB.

For OpenScape Desk Phone CP400/600, the default value is 20 MB.

The beginning and end of the working hours are defined in 24 hours format with Working Hour Start (Default: 5) and Working Hour End (Default: 24).

When memory shortage has occurred, information about the incident is written to a log file which can be viewed via the Download memory info file link. If there has been a previous case of memory shortage, the corresponding log file can be viewed via Download memory info file.

Administration via WBM

Diagnostics > Miscellaneous > Memory information

Memory information

Memory monitor configuration

Disable reboot

High threshold(MBs)

Low threshold(MBs)

Working hour start

Working hour end

13

11

5

24

Submit

Reset

Download memory info file

Download thread info for services

Download old memory info file

Download thread info for callview

Download thread info for admin

Device memory information

Mem: 154392K used, 89144K free, 5376K shrd, 0K buff, 73108K cached

CPU: 0% usr 0% sys 0% nic 100% idle 0% io 0% irq 0% irq

Load average: 1.05 1.10 1.07 1/207 16859

PID	PPID	USER	STAT	VSZ	WSS	PCPU	COMMAND
263	1	root	S	25300	10K	0%	epddaemon_alsa
16859	264	root	R	3236	1K	0%	/bin/busybox top -d 0 -a -n 1 -l 600 -b
304	264	root	S	1969	0K	0%	svcConfig services.conf -startLogDaemon -logAll V1 R9.4.80
459	304	root	RN	72820	30K	0%	[Qt Gui CallView] PhoneletLauncher callview.phd V1 R9.4.80
612	304	root	SN	55140	23K	0%	[Qt Gui AdminPho] PhoneletLauncher admin.phd V1 R9.4.80
264	1	root	S	32944	14K	0%	svcConfig healthservice.conf
10354	1	appweb	SN	13904	6K	0%	/appweb --config opera_appweb_latest!IsOnly.conf
16854	10354	appweb	SN	12208	5K	0%	/Opera_Deploy/appweb/web/page.cnd
381	1	root	S	8092	3K	0%	/usr/sbin/stunnel /Opera_Deploy/stunnel_server_all!Versions.conf
10219	304	root	S	4220	2K	0%	/sbin/dhclient -d -q -0 li -sf /Opera_Deploy/networking/dhcpv4Event.sh -lf /tmp/networking/dhcpv4Leases.none -cf /data/networking/dhcpv4.conf eth0
10209	304	root	S	4220	2K	0%	/sbin/dhclient -d -q -sf /Opera_Deploy/networking/dhcpv4Event.sh -lf /data/networking/dhcpv4Leases.none -cf /data/networking/dhcpv4.conf eth0
372	1	root	S	3240	1K	0%	/bin/sh
1	0	root	S	3236	1K	0%	init
8995	1	root	S	3236	1K	0%	/sbin/syslogd -L -s 2000 -O /tmp/logs/messages
85	1	root	S	3236	1K	0%	/sbin/klogd
262	1	root	S	3236	1K	0%	/wd_trap.sh /bin/sh /etc/init.d/wd_trap.sh
268	262	root	S	3104	1K	0%	sleep 86400000
445	2	root	DW	0	0K	0%	sidecar_thread]
22	2	root	SW	0	0K	0%	[spi32!65]
7	2	root	SW	0	0K	0%	[rcu_preempt]
3	2	root	SW	0	0K	0%	[ksoffirqd!0]
16465	2	root	SW	0	0K	0%	[kworker!0:1]
18	2	root	SW	0	0K	0%	[spi32!66]
120	2	root	SW	0	0K	0%	[ubifs_bgt!0]
32	2	root	SW	0	0K	0%	[khungtaskd]
2	0	root	SW	0	0K	0%	[kthread]
117	2	root	SW	0	0K	0%	[ubi_bgt!d]
59	2	root	SW	0	0K	0%	[ubi_bgt!0d]
15947	2	root	SW	0	0K	0%	[kworker!u2!0]
60	2	root	SW	0	0K	0%	[ubifs_bgt!0]
16468	2	root	SW	0	0K	0%	[kworker!u2!2]
5	2	root	SW	0	0K	0%	[kworker!0!0H]
8	2	root	SW	0	0K	0%	[rcu_bh]
9	2	root	SW	0	0K	0%	[rcu_sched]
10	2	root	SW	0	0K	0%	[khalper]
11	2	root	SW	0	0K	0%	[kdevtmpfs]
12	2	root	SW	0	0K	0%	[netns]
14	2	root	SW	0	0K	0%	[writeback]
15	2	root	SW	0	0K	0%	[blisect]
16	2	root	SW	0	0K	0%	[crypto]
17	2	root	SW	0	0K	0%	[kblockd]
25	2	root	SW	0	0K	0%	[spi32!64]
28	2	root	SW	0	0K	0%	[spi32!63]
31	2	root	SW	0	0K	0%	[cfg80211]
33	2	root	SW	0	0K	0%	[kswapd0]
34	2	root	SW	0	0K	0%	[fsmotify_mark]
44	2	root	SW	0	0K	0%	[irq!176-180af00]
44	2	root	SW	0	0K	0%	[irq!177-180ac00]

3.31.9 Fault Trace Configuration

Error tracing and logging can be configured separately for all components, i. e. the services and applications running on the OpenScape Desk Phone CP. The resulting files can be viewed in the WBM web pages over the Download links.

The File size (bytes) parameter sets the maximum file size. When it is reached, the data is saved as old file, and a new file is generated. From then on, the trace data is written to the new file. When the maximum file size is reached again, the data is saved as old file once more, thereby overwriting the previous old file. The default value is 1048576.

NOTICE: The absolute maximum file size is 6290000 bytes. However, on OpenScape Desk Phone CP phones, a maximum size not greater than 1000 000 bytes is recommended due to the amount of available memory.

The Trace timeout (minutes) determines when to stop tracing. When the timeout is reached, the trace settings for all components are set to OFF, but ERROR and STATUS messages are still written to the trace file ad infinitum. When the trace file has reached its maximum size, the data is saved, and a new file is created (for more information, see File size (bytes) above). If the value is 0, the trace data will be written without time limit.

If Automatic clear before start is checked, the existing trace file will be deleted on pressing the Submit button, and a new, empty trace file will be generated. By default, it is unchecked.

298

A31003-C1000-M101-23-76A9, 10/2025

Administration SIP, Administrator Documentation SIP

You can read the log files by clicking on the appropriate hyperlinks (the hyperlinks work only if the file in question has been created). The following logs can be viewed:

- Download trace file

The trace data according to the settings specified for the services.

- Download old trace file

The trace file is stored in permanent memory. When the file has reached its size limit, it will be saved as old trace file, and the current exception file is emptied for future messages. The old trace file can be viewed here.

- Download saved trace file

Normally, the trace file is saved only in the phone RAM. When the phone restarts in a controlled manner, the trace file will be saved in permanent memory.

- Download syslog file

Messages from the phone's operating system, including error and exception messages.

- Download old syslog file

Old messages from the phone's operating system.

- Download saved syslog file

Saved messages from the phone's operating system.

- Download exception file

If an exceptions occurs in a process running on the phone, a message is written to this file. These messages are incorporated in the syslog file (see [Download syslog file](#) also).

- Download old exception file

The exception file is stored permanent memory. When the file has reached its size limit, it will be saved as old exception file, and the current exception file is emptied for future messages. The old exception file can be viewed here.

- Download upgrade trace file

The trace log created during a software upgrade.

- Download upgrade error file

The error messages created during a software upgrade. These messages are incorporated in the syslog file (see [Download syslog file](#) also).

- Download dial plan file

If a dial plan has been uploaded to the phone, it is displayed here, along with its status (enabled/disabled) and error status. For details, please refer to [Dial Plan](#) on page 247 and [Example Dial Plan](#) on page 336.

- Download Database file

Configuration parameters of the phone in SQLite format.

- Download HPT remote service log file

Log data from the HPT service.

- Download security log file

Log data from the Security Log Service.

By pressing Submit, the trace settings are submitted to the phone. With Reset, the recent changes can be canceled.

The following trace levels can be selected:

- **OFF**: Default value. Only error messages are stored.
- **FATAL**: Only fatal error messages are stored.
- **ERROR**: Error messages are stored.
- **WARNING**: Warning messages are stored.
- **LOG**: Log messages are stored.
- **TRACE**: Trace messages are stored. These contain detailed information about the processes taking place in the phone.
- **DEBUG**: All types of messages are stored.

Brief Descriptions of the Components/Services

- Administration

Deals with the changing and setting of parameters within the phone database, from both the User and Admin menus.

- Application framework

All applications within the phone, e.g. Call view, Call log, or Phonebook, are run within the application framework. It is responsible for the switching between different applications and bringing them into and out of focus as appropriate.

- Application menu

This is where applications to be run on the phone can be started and stopped.

- Bluetooth service (only applicable for CP600/700/700X)

This handles the Bluetooth interactions between external Bluetooth devices and the phone.

- Broadsoft service

Traces communication between phone and the XSI server, if configured.

- Call Log

The Call log application displays the call history of the phone.

- Call View

Handles the representation of telephony calls on the phone screen.

- Certificate management

Handles the verification and exchange of certificates for security and verification purposes.

- Clock Service

Handles the phone's time and date, including daylight saving and NTP functionality.

- CPE service

Customer Premises Equipment (CPE) traces TR-069 protocol communication.

- Communications
Involved in the passing of call related information and signaling to and from the CSTA service.
- Component registrar
Handles data relating to the type of phone, e.g. OpenScape Desk Phone CP100/200/205/400/600/600E.
- CSTA service
Any CSTA messages are handled by this service. CSTA messages are used within the phone by all services as a common call progression and control protocol.
- Data Access service
Allows other services to access the data held within the phone database.
- Desktop
Responsible for the shared parts of the phone display. Primarily these are the status bar at the top of the screen and the FPK labels.
- Digit analysis service
Analyses and modifies digit streams which are sent to and received by the phone, e.g. canonical conversion.
- Directory service
Performs a look up for data in the phonebook, trying to match incoming and outgoing numbers with entries in the phonebook.
- DLS client management
Handles interactions with the DLS (Deployment Service).
- Exchange service (only applicable for CP400/600/700/700X)
Traces communication between phone and the exchange server, if configured.
- GPALAudio Core
Core audio component traces with low-level information.
- GPALAudio Framework
Advanced audio component traces with low-level information.
- Health service
Monitors other components of the phone for diagnostic purposes and provides a logging interface for the services in the phone.
- HTTP Service
Handles the HTTP Service messages.
- Instrumentation service
Used by the HPT phone tester to exchange data with the phone for remote control, testing and monitoring purposes.
- Journal service
Responsible for saving and retrieving call history information, which is used by the Call log application.
- Media control service
Provides the control of media streams (voice, tones, ringing etc.) within the phone.

- Media recording service
Logs the data flow generated with call recording.
- Mobility service
Handles the mobility feature whereby users can log onto different phones and have them configured to their own profile.
- OBEX service (only applicable for CP600/700/700X)
The Object Exchange (OBEX) service traces functionality related to exchanging objects via Bluetooth. It is used for features like sending/receiving vCards or contacts synchronization via BT.
- OpenScape UC service (only applicable for CP400/600/700/700X)
Traces communication and events between phone and the OpenScape UC server, if configured.
- OpenStage client management
Provides a means by which other services within the phone can interact with the database.
- Password management service
Verifies passwords used in the phone.
- Phonebook
Responsible for the phonebook application.
- Performance Marks
Aid for measuring the performance of the phone. For events triggered by the user, a performance mark is written to the trace file, together with a timestamp in the format hh:mm:ss yyyy.milliseconds, and information about the event. The timespan between two performance marks is an indicator for the performance of the phone.

NOTICE: The trace level must be set to "TRACE" or "DEBUG".

- Physical interface service
Handles any interactions with the phone via the keypad, mode keys, fixed feature buttons, clickwheel and slider.
- RingCentral service
Traces communication between phone and the RingCentral server, if configured.
- Security Log Service
Handles Security Log Service messages.
- Service framework
This is the environment within which other phone services operate. It is involved in the starting and stopping of services.
- Service registry
Keeps a record of all services currently running inside the phone.
- SIP call control
Contains the call model for the phone and is associated with telephony and call handling.

- SIP messages

Traces the SIP messages exchanged by the phone.

NOTICE: After changing the level for the tracing of SIP messages, the phone must be rebooted. Otherwise the changes would have no effect.

- SIP M5T stack

SIP stack internal trace messages.

- SIP signalling

Involved in the creation and parsing of SIP messages. This service communicates directly with the SIP stack.

- Team service

Primarily concerned with keyset operation.

- Tone generation service

Handles the generation of the tones and ringers on the phone.

- Transport service

Provides the IP (LAN) interface between the phone and the outside world.

- vCard parser service (only applicable for CP600/700/700X)

Provides detailed traces related to the parsing process for vCards (i.e. token detection). Usually these traces are enabled only if there is some specific problem with vCard parsing (i.e. wrong information in transferred contacts). Otherwise generic OBEX service traces should be enough.

- Voice engine service

Provides a switching mechanism for voice streams within the phone. This component is also involved in QDC, Music on hold and voice instrumentation.

- Voice mail

Handles the voice mail functionality.

- Web server service

Provides access to the phone via web browser.

- 802.1x service

Provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. The service is used for certain closed wireless access points.

Administration via WBM

Diagnostics > Fault trace configuration

Fault trace configuration

File size (Max 6290000 bytes)6290000

Trace timeout (minutes)0

Automatic clear before start☐

Trace levels for components

802.1x serviceOFF

Application frameworkOFF

Broadsoft serviceOFF

Call viewDEBUG

Circuit serviceOFF

CommunicationsOFF

ConversationAPIOFF

CSTA serviceDEBUG

Digit analysis serviceOFF

DLS client managementOFF

GPALAudio CoreOFF

Health serviceOFF

Journal serviceOFF

Media recording serviceOFF

OBEX serviceOFF

OpenStage client managementOFF

Performance marksOFF

RingCentral ServiceOFF

Service frameworkDEBUG

Sidecar serviceOFF

SIP messagesDEBUG

SIP M5T stackOFF

Tone generation serviceOFF

vCard parser serviceOFF

HTTP serviceOFF

Web server serviceOFF

AdministrationOFF

Application menuOFF

Bluetooth serviceOFF

Certificate managementOFF

Clock serviceOFF

Component registrarOFF

CPE ServiceOFF

Data access serviceOFF

Directory serviceOFF

Exchange serviceOFF

GPALAudio FrameworkOFF

Instrumentation serviceOFF

Media control serviceOFF

Mobility serviceOFF

OpenScape UC serviceOFF

Password management serviceOFF

Physical interface serviceOFF

Security log serviceOFF

Service registryOFF

SIP call controlDEBUG

SIP signallingDEBUG

Team serviceOFF

Transport serviceOFF

Video service engineOFF

Voice engine serviceOFF

Submit

Reset

3.31.10 EasyTrace Profiles

In order to simplify tracing for a specific problem, the tracing levels can be adjusted using predefined settings. The EasyTrace profiles provide settings for a specific area, e. g. call connection. On pressing Submit, those pre-defined settings are sent to the phone. If desired, the settings can be modified anytime using the general mask for trace configuration under Diagnostics > Fault Trace Configuration (see [Fault Trace Configuration](#) on page 298).

The following sections describe the EasyTrace profiles available for the phone.

3.31.10.1 Phone administration problems

Diagnostics > EasyTrace Profiles > Phone administration problems

Phone administration problems	
File size (Max 6290000 bytes)	1048576
Trace timeout (minutes)	0
Automatic clear before start	☐
Trace levels for components	
Administration	DEBUG ☐
Clock service	DEBUG ☐
Data access service	DEBUG ☐
OpenStage client management	DEBUG ☐
Password management service	DEBUG ☐
Web server service	DEBUG ☐
Download trace file	Download saved trace file
Submit	Reset

3.31.10.2 Audio related problems

Diagnostics > EasyTrace Profiles > Audio related problems

Audio related problems	
File size (Max 6290000 bytes)	1048576
Trace timeout (minutes)	0
Automatic clear before start	☐
Trace levels for components	
GPALAudio Core	DEBUG ☐
GPALAudio Framework	DEBUG ☐
Media control service	DEBUG ☐
SIP messages	DEBUG ☐
Tone generation service	DEBUG ☐
Voice engine service	DEBUG ☐
Download trace file	Download saved trace file
Submit	Reset

NOTICE: This EasyTrace profile contains the tracing of SIP messages. Please note that after changing the level for the tracing of SIP messages, the phone must be rebooted.

3.31.10.3 Bluetooth problems

This profile is available only on OpenScape Desk Phone CP600/700/700X telephones.

Diagnostics > EasyTrace Profiles > Bluetooth problems

Bluetooth problems	
File size (Max 6290000 bytes)	1048576
Trace timeout (minutes)	0
Automatic clear before start	☐
Trace levels for components	
Bluetooth service	DEBUG ☐
CSTA service	DEBUG ☐
OBEX service	DEBUG ☐
vCard parser service	DEBUG ☐
<u>Download trace file</u>	<u>Download saved trace file</u>
Submit	Reset

3.31.10.4 Call proceeding problems

Diagnostics > EasyTrace Profiles > Call proceeding problems

Call proceeding problems	
File size (Max 6290000 bytes)	1048576
Trace timeout (minutes)	0
Automatic clear before start	☐
Trace levels for components	
Call view	DEBUG
Communications	DEBUG ☐
CSTA service	DEBUG ☐
SIP call control	DEBUG ☐
SIP messages	DEBUG ☐
SIP signalling	DEBUG ☐
<u>Download trace file</u>	<u>Download saved trace file</u>
Submit	Reset

NOTICE: This EasyTrace profile contains the tracing of SIP messages. Please note that after changing the level for the tracing of SIP messages, the phone must be rebooted.

3.31.10.5 Conversations / LDAP problems

Diagnostics > EasyTrace Profiles > Conversations / LDAP problems

Conversations / LDAP problems

File size (Max 6290000 bytes)

Trace timeout (minutes)

Automatic clear before start ☐

Trace levels for components

Call log	DEBUG	v
Call view	DEBUG	v
ConversationAPI	DEBUG	v
CSTA service	DEBUG	v
Digit analysis service	DEBUG	v
Directory service	DEBUG	v
Exchange service	DEBUG	v
Journal service	DEBUG	v

[Download trace file](#)
[Download saved trace file](#)

3.31.10.6 Keyset problems

Diagnostics > EasyTrace Profiles > Keyset problems

Keyset problems

File size (Max 6290000 bytes)

Trace timeout (minutes)

Automatic clear before start ☐

Trace levels for components

Call View	DEBUG	v
Communications	DEBUG	v
CSTA service	DEBUG	v
Sidecar services	DEBUG	v
SIP messages	DEBUG	v
Team service	DEBUG	v

[Download trace file](#)
[Download saved trace file](#)

NOTICE: This EasyTrace profile contains the tracing of SIP messages. Please note that after changing the level for the tracing of SIP messages, the phone must be rebooted.

3.31.10.7 Mobility / DLS problems

Diagnostics > EasyTrace Profiles > Mobility / DLS problems

Mobility / DLS problems

File size (Max 6290000 bytes)

Trace timeout (minutes)

Automatic clear before start

☐

Trace levels for components

Call view	DEBUG	☒
Communications	DEBUG	☒
DLS client management	DEBUG	☒
Mobility service	DEBUG	☒
OpenStage client management	DEBUG	☒

Download trace file

Download saved trace file

Submit

Reset

3.31.10.8 Network problems

Diagnostics > EasyTrace Profiles > Network problems

Network problems

File size (Max 6290000 bytes)

Trace timeout (minutes)

Automatic clear before start

☐

Trace levels for components

802.1x service	DEBUG	☒
Transport service	DEBUG	☒

Download trace file

Download saved trace file

Submit

Reset

3.31.10.9 Security problems

Diagnostics > EasyTrace Profiles > Security problems

Security problems	
File size (Max 6290000 bytes)	1048576
Trace timeout (minutes)	0
Automatic clear before start	☐
Trace levels for components	
Certificate management	DEBUG v
Password management service	DEBUG v
Security log service	DEBUG v
<u>Download trace file</u>	<u>Download saved trace file</u>
Submit	Reset

3.31.11 Bluetooth Advanced Traces

This trace is available only on OpenScape Desk Phone CP600/700/700X telephones.

Diagnostics > Bluetooth Advanced Traces

Bluetooth Advanced Traces	
Automatic clear before start	☒
File size (Max 6290000 bytes)	0
Extended dump	☒
Verbose decoding	☒
Tracing is stopped	Start
<u>Download trace file</u>	
Submit	Reset

3.31.12 Advanced Audio Traces

This feature allows the admin to turn on EPT (Broadcom EndPoint) traces, so that audio related issues can be collected directly from the users' phones. This helps to analyze those audio issues faster and come to a solution.

The following information can be collected:

- EPT traces
- The status of the EPT component
- The existence of the eptMsg thread that processes the microphone packets (available only for CP100 and CP20x)

Data required

- **EPT trace level:** can be configured from 0 (tracing disabled) up to 5 (maximum trace level).
- **Automatic clear before start:** if checked, the ept file will be cleared after pressing the Submit button.
- **Capture and stop (only available for CP100/20x):**
 - if checked, tracing will continue until the maximum number of lines is reached and then it will stop. Also, this feature will remain enabled after restart.
 - if unchecked, the trace file will continuously wrap around, overwriting the older lines.
- **Number of lines (Max 100000)(only available for CP100/20x):** the maximum number of lines in the eptlog file.
- **Download eptlog file:** opens a new web page presenting the contents of the trace file "eptlog.txt".
- **Download saved eptlog file:** saves the trace file "eptlog.txt.save.gz" captured before the last reboot, if there was any. In order to save the flash memory space, this file is compressed.
- **Download audio status:** the current status of the audio devices, streams and the gain setting. The origin of the information differs according to the platform:
 - **CP_LO phone models:** information from /proc/ept filesystem and from pxcon tool.
 - **CP_HI phone models:** information from mxcon tool.

Administration via WBM

Diagnostics > Advanced audio traces

Advanced audio traces

EPT trace level 0

Automatic clear before start ☐

Capture and stop ☐

Number of lines(Max 100000) 1000

Submit Reset

[Download eptlog file](#) [Download saved eptlog file](#)

[Download audio status](#)

3.31.13 M5T Advanced Traces

Diagnostics > M5T Advanced Traces

M5T Advanced Traces

SIP M5T stack

M5T trace components

3.31.14 QoS Reports

3.31.14.1 Conditions and Thresholds for Report Generation

NOTICE: For details about the functionality, please refer to the Release Notes.

The generation of QoS (Quality of Service) reports which are sent to a QCU server (see [SNMP](#) on page 84) is configured here.

Data required

- **Report mode:** Sets the conditions for generating a QoS report. Value range:
 - **"OFF":** No reports are generated.
 - **"EOS Threshold exceeded":** Default value. A report is created if a) a telephone conversation longer than the Minimum session length has just ended, and b) a threshold value has been exceeded during the conversation.
 - **"EOR Threshold exceeded":** A report is created if a) the report interval has just passed, and b) a threshold value has been exceeded during the observation interval.
 - **"EOS (End of Session)":** A report is created if a telephone conversation longer than the Minimum session length has just ended.
 - **"EOR (End of Report Interval)":** A report is created if the report interval has just passed.
- **Report interval (seconds):** Time interval between the periodical observations. Default: 60
- **Observation interval (seconds):** During this time interval, the traffic is observed. Value: 10
- **Minimum session length (100 millisecond units):** When the Report mode is set to "EOS Threshold exceeded" or "EOS (End of Session)", a report can be created only if the duration of the conversation exceeds this value. Default: 20
- **Maximum jitter (milliseconds):** When the jitter exceeds this value, a report is generated. Default: 20
- **Average round trip delay (milliseconds):** When the average round trip time exceeds this value, a report is generated. Default: 100

Non-compressing codecs:

The following threshold values apply to non-compressing codecs.

- **Lost packets (per 1000 packets):** When the number of lost packets exceeds this maximum value during the observation interval, a report is created. Default: 10.
- **Consecutive lost packets:** When the number of lost packets following one another exceeds this maximum value during the observation interval, a report is created. Default: 2.
- **Consecutive good packets:** When the number of good packets following one another falls below this minimum value, a report is created. Default: 8.

Compressing codecs:

The following threshold values apply to compressing codecs.

- **Lost packets (per 1000 packets):** When the number of lost packets exceeds this maximum value during the observation interval, a report is created. Default: 10.
- **Consecutive lost packets:** When the number of lost packets following one another exceeds this maximum value during the observation interval, a report is created. Default: 2.
- **Consecutive good packets:** When the number of good packets following one another falls below this minimum value, a report is created. Default: 8.

General:

- **Resend last report:** If checked, the previous report is sent once again on pressing Submit. By default, this is unchecked.

The transmission of report data can be triggered manually by pressing Send now in the local menu.

Administration via WBM

Diagnostics > QoS Reports > Generation

Generation	
Report mode	EOS Threshold exceeded
Report interval (seconds)	60
Observation interval (seconds)	10
Minimum session length (100 millisecond units)	20
Codec independent threshold values	
Maximum jitter (milliseconds)	20
Average round trip delay (milliseconds)	100
Non-compressing codec threshold values	
Lost packets (per 1000 packets)	10
Consecutive lost packets	2
Consecutive good packets	8
Compressing codec threshold values	
Lost packets (per 1000 packets)	10
Consecutive lost packets	2
Consecutive good packets	8
Resend last report	☐
Submit	Reset

Administration via Local Phone

| --- Admin

```

length
|--- Network
|   |--- QoS
|       |--- Reports
|           |--- Generation
|               |--- Mode
|               |--- Report interval
|               |--- Observe interval
|               |--- Minimum session
|           |--- Send now
|               |--- Thresholds
|                   |--- Maximum jitter
|                   |--- Round-trip delay
|               |--- Non-compressing:
|                   |--- ...Lost packets (K)
|                   |--- ...Lost consecutive
|                   |--- ...Good consecutive
|               |--- Compressing:
|                   |--- ...Lost packets (K)
|                   |--- ...Lost consecutive
|                   |--- ...Good consecutive

```

3.31.14.2 View Report

OpenScape Desk Phone CP phones generate QoS reports using a HiPath specific format, QDC (QoS Data Collection). The reports created for the last 6 sessions, i. e. conversations, can be viewed on the WBM.

To enable the generation of reports, please ensure that:

- the switch QoS traps to QCU (System > SNMP) is activated (see [SNMP](#) on page 84);
- the conditions for the generation of reports are set adequately (see [Conditions and Thresholds for Report Generation](#) on page 311).

For details about QoS reports on OpenScape Desk Phone CP devices, see the HiPath QoS Data Collection V 1.0 Service Manual.

A QoS report contains the following data:

- **Start of report period - seconds:** NTP time in seconds for the start of the report period.
- **Start of report period - fraction of seconds:** Additional split seconds to be added to the seconds for an exact start time.
- **End of report period - seconds:** NTP time in seconds for the end of the report period.
- **End of report period - fraction of seconds:** Additional split seconds to be added to the seconds for an exact end time.
- **SNMP specific trap type:** The trap type is a 5 bit value calculated from a list of threshold-exceeding bits. Every time a threshold is exceeded, the associated bit is set, otherwise it is cleared. The trace type bits are defined as follows:
 - **Bit 0:** Jitter threshold was exceeded.
 - **Bit 1:** Delay threshold was exceeded.
 - **Bit 2:** Threshold for lost packets was exceeded.

- **Bit 3:** Threshold for consecutive lost packets was exceeded.
- **Bit 4:** Threshold for consecutive good packets was exceeded.
- **IP address (local):** IP address of the local phone.
- **Port number (local):** RTP receiving port of the local phone.
- **IP address (remote):** IP address of the remote phone that took part in the session.
- **Port number (remote):** RTP sending port of the local phone.
- **SSRC (receiving):** RTP Source Synchronization Identifier of the local phone.
- **SSRC (sending):** RTP Source Synchronization Identifier of the remote phone.
- **Codec:** Number of the Payload Type applied in the session; see RFC 3551 (Table 4 and 5).
- **Maximum packet size:** Maximum size (in ms) of packets received during the report interval.
- **Silence suppression:** Number of silence suppression activation objects found in the RTP stream received. A silence suppression activation object is defined as a period of silence when no encoded voice signals were transmitted by the sender.
- **Count of good packets:** Total amount of good packets.
- **Maximum jitter:** Maximum jitter (in ms) found during the report interval.
- **Maximum inter-arrival jitter:** Maximum of the interarrival jitter values (in ms). The interarrival jitter is the smoothed absolute value of the jitter measurements. It is calculated continuously. For details about the calculation, see RFC 3550.
- **Periods jitter threshold exceeded:** Number of observation intervals in which the threshold for maximum jitter was exceeded.
- **Round trip delay:** Average value of delay calculated for each RTCP packet. The first value is available after about 15 sec.
- **Round trip delay threshold exceeded:** Set to "true" if the average round trip delay threshold value was exceeded in the report interval.
- **Count of lost packets:** Number of packets lost in the course of speech decoding.
- **Count of discarded packets:** Number of the packets discarded without transferring the contents.
- **Periods of lost packets:** Number of observation intervals in which the threshold for lost packets was exceeded.
- **Consecutive packet loss (CPL):** List of sequences consecutive packets that were all lost, grouped according to the amount of packets per sequence. The first number in the list counts single lost packets, the second number counts sequences of two lost packets, and so on. The last number counts sequences of more than 10 lost packets.
- **Periods of consecutive lost packets:** Number of observation intervals in which the threshold for consecutive lost packets was exceeded.
- **Consecutive good packets (CGP):** List of sequences consecutive packets that were all processed, grouped according to the amount of packets per sequence. The first number in the list counts single good packets, the second number counts sequences of two good packets, and so on. The last number counts sequences of more than 10 good packets. All values are reset to 0 after an interval without packet loss.
- **Periods of consecutive good packets:** Number of intervals in which the count of lost packets went below the threshold.

- **Count of jitter buffer overruns:** Number of packets rejected because the jitter buffer was full.
- **Count of jitter buffer under-runs:** Increased by one whenever the decoder requests new information on decoding and finds an empty jitter buffer.
- **Codec change on the fly:** The value is 1, if there has been a codec or SSRC change during the observation period, and 0, if there has been no change.
- **Periods with at least one threshold exceeded:** Number of observation intervals with at least one threshold exceedance. If there is no data, the value is 255. The threshold values included are:
 - maximum jitter;
 - lost packets;
 - consecutive lost packets;
 - consecutive good packets.
- **HiPath Switch ID:** Unique number identifying the HiPath switch to which the endpoints are assigned.
- **LTU number:** In HiPath 4000 only, the shelf identification is taken from the shelf containing a gateway.
- **Slot number:** The slot number where the phone is connected in the shelf.
- **Endpoint type :** Type of the local phone.
- **Version:** Software version of the local phone.
- **Subscriber number type:** Type of subscriber number assigned to the local phone. The possible types are:
 - 1: local number, extension only
 - 2: called number, network call
 - 3: E.164 number of the local phone
- **Subscriber number:** Subscriber number of the local phone.
- **Call ID:** SIP call id.
- **MAC address:** MAC address of the local phone.

Data viewing via WBM

Diagnostics > QoS reports > View Session Data

3.31.15 Core dump

If Enable core dump is checked, a core dump will be initiated in case of a severe error. The core dump will be saved to a file. By default, this function is activated.

If Delete core dump is activated, the current core dump file is deleted on Submit. By default, this is not activated.

If one or more core dump file exist, hyperlinks for downloading will be created automatically.

Administration via WBM

Diagnostics > Miscellaneous > Core Dump

Core Dump

Enable core dump*

☒

Delete core dump

☐

*Changes to this item do not take effect until the phone is restarted

Submit

Reset

3.31.16 Remote Tracing — Syslog

All trace messages created by the components of the phone software can be sent to a remote server using the syslog protocol. This is helpful especially for long-term observations with a greater number of phones.

To enable remote tracing, Remote trace status must be set to "Enabled". Furthermore, the IP address of the server receiving the syslog messages must be entered in Remote ip, and the corresponding server port must be given in Remote port.

With version V2, the User notification parameter controls whether the user is notified about the remote tracing or not. If user notification is enabled, a

blinking symbol ( on OpenScape Desk Phone CP400/600/700/700X;  on OpenScape Desk Phone CP200/CP205) will inform the user when remote tracing is active, that is, when Remote trace status is set to "Enabled".

Administration via Local Phone

```
|--- Admin
  |--- Maintenance
    |--- Remote trace
      |--- Remote trace status
      |--- User notification
      |--- Remote ip
      |--- Remote port
```

Administration via WBM

Remote trace

Remote trace status

☐

User notification

☐

Remote server

Remote server port

Submit

Reset

3.31.17 HPT Interface (For Service Staff)

For special diagnosis and maintenance tasks, the service staff may employ the HPT tool, which is able to control and observe an OpenScape Desk Phone CP100/200/205/400/600/600E phone remotely.

There are 2 types of HPT sessions, control session and observation session.

A control session allows for activating phone functions remotely. When a control session is established, the following changes will occur:

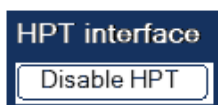
- The display shows a message indicating that remote service is active.
- Handset, microphone, speaker, headset, and microphone are disabled.

An observation session allows for supervising events on the phone, like, for instance, pressing a key, incoming calls or navigating in the menus. Before an observation session is started, the user is prompted for allowing the observation. During an observation session, the phone operates normally, including loudspeaker, microphone and ringer. Thus, the local user can demonstrate an error towards the service staff that is connected via HPT.

The session data is written to a log file on the phone. It can be downloaded from the **Diagnostics > Fault trace configuration** menu (see [Fault Trace Configuration](#) on page 298).

Administration via WBM (Disable)

Maintenance > HPT interface



```
|--- Administration
      |--- Maintenance
            |--- Disable HPT / Enable HTP
```

3.32 MWI LED

This configurable item is added to the Administrator settings to allow the Administrator to control how new VoiceMails are indicated to the user; via the "Envelope" mode key LED only, via the Top LED only or via both LEDs.

The selection field offers the choice between:

- "Key only" (default)
- "Key & AlertBar"
- "AlertBar only"

Administration via WBM

System > Features > Configuration

Configuration	
General	
Emergency number	
Voice mail number	
MWI LED	AlertBar LED ▼
Missed call LED	AlertBar LED ▼
AlertBar LED hint	☐
Allow refuse	☒
Hot/Warm phone	No action ▼
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☒
Server features	☐
Not used timeout (minutes)	2 ▼
Transfer on hangup	☐
Bridging enabled	☐
Dial plan enabled	☐
FPK program timer	On ▼
DSS monitored	☐
Show icon for all forwarding types	☒
Alerting	
BLF alert	Beep ▼
Group pickup alert	Off ▼
Group pickup tone interval	15
Group pickup visual alert	Prompt ▼
MLPP ringer	▼
Callback ringer	▼
Impact level ringer	▼
Call recording	
Recorder address	
Recording mode	Disabled ▼
Audible notification	Single-shot ▼
Submit	Reset

Administration via Local Phone

```
|--- Admin
  |--- System
    |--- Features
      |--- Configuration
        |--- MWI LED
```

3.33 Missed Call LED

This configurable item is added to the Administrator settings to allow the Administrator to control how new Missed Calls are indicated to the user; via the "Envelope" mode key LED only, via the Top LED only, via both LEDs or no LED.

The selection field offers the choice between:

- "Key only" (default)
- "Key & AlertBar"
- "AlertBar only"
- "No LED"

Administration via WBM

System > Features > Configuration

Configuration	
General	
Emergency number	
Voice mail number	
MWI LED	AlertBar LED ▼
Missed call LED	AlertBar LED ▼
AlertBar LED hint	☐
Allow refuse	☒
Hot/Warm phone	No action ▼
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☒
Server features	☐
Not used timeout (minutes)	2 ▼
Transfer on hangup	☐
Bridging enabled	☐
Dial plan enabled	☐
FPK program timer	On ▼
DSS monitored	☐
Show icon for all forwarding types	☒
Alerting	
BLF alert	Beep ▼
Group pickup alert	Off ▼
Group pickup tone interval	15
Group pickup visual alert	Prompt ▼
MLPP ringer	▼
Callback ringer	▼
Impact level ringer	▼
Call recording	
Recorder address	
Recording mode	Disabled ▼
Audible notification	Single-shot ▼
Submit	Reset

3.34 AlertBar LED hint

This configurable item is added to the Administrator settings to allow the Administrator to control how will the Alert LED be extinguished. When this

item is checked, the Alert LED will extinguish as soon as the user enters the Conversations screen or the Call Log screen (if they use a CP200 phone). The Conversations screen and the Main menu screen will continue to indicate the existence of a new missed call. The default option is False.

Administration via WBM

System > Features > Configuration

Configuration	
General	
Emergency number	
Voice mail number	
MWI LED	AlertBar LED ▼
Missed call LED	AlertBar LED ▼
AlertBar LED hint	☐
Allow refuse	☒
Hot/Warm phone	No action ▼
Hot/Warm destination	
Initial digit timer (seconds)	30
Allow uaCSTA	☒
Server features	☐
Not used timeout (minutes)	2 ▼
Transfer on hangup	☐
Bridging enabled	☐
Dial plan enabled	☐
FPK program timer	On ▼
DSS monitored	☐
Show icon for all forwarding types	☒
Alerting	
BLF alert	Beep ▼
Group pickup alert	Off ▼
Group pickup tone interval	15
Group pickup visual alert	Prompt ▼
MLPP ringer	▼
Callback ringer	▼
Impact level ringer	▼
Call recording	
Recorder address	
Recording mode	Disabled ▼
Audible notification	Single-shot ▼
Submit	Reset

3.35 Impact Level Notification

Communications for the Public Sector Network (PSN) is seen as originating from or terminating to zones with differing 'impact' levels (the impact level indicates how the phone user should handle the call

conversation). The purpose is to notify the OpenScape Desk Phone CP100/200/205/400/600/600E/700/700X phone users when they are connecting or in a call where another party in the call is in a lower Impact Level (IL) zone.

This feature uses a UI mechanism to notify/remind the phone user that the call may require special treatment. This involves special icons, text indications, and special audio (ringer or tone as appropriate). There are no restrictions on call handling as a result of any special status for the call.

Thus the Impact Level Notification feature only involves UI changes that are triggered by receiving new SIP headers and affects the following:

- Prompts presented to alert for incoming calls
- Prompts presented to monitor progress for outgoing calls
- Connected call displays
- Call scenarios involving multiple calls
- Retrieving a held call

However, since there are no call restrictions explicit for the Impact Level Notification feature the solution needs to consider some additional scenarios:

- Group pickup
- Directed pickup
- Callback
- CTI action
- Shared lines on a Keypad

This feature cannot be turned off at the phone since it is driven solely by the OSV.

The OSV is responsible for being aware of the impact level of the phone (the phone does not have control of its own level) and the impact levels of all other endpoints that are participating in a call with the phone. The OSV uses this information to signal (via a new SIP header) the phone when the call is to be treated as from a lower impact level. It does this during the start of a call or anytime during a call.

Data required

- **Impact level ringer:** Identifies one of the named distinctive ringers to be used in place of the normal ringer for calls from a lower impact level. Value range: the offered values are those defined in "Ringer Settings" > Distinctive", e.g. "Bellcore-dr1" or any arbitrary name

Administration via WBM

System > Features > Configuration > Impact level ringer

Alerting	
BLF alert	Beep
Group pickup alert	Off
Group pickup tone interval	15
Group pickup visual alert	Prompt
MLPP ringer	
Callback ringer	
Impact level ringer	

The phone plays the configured Impact Level Notification ringer when the call is from a lower impact level. The ringer has to be configured in the ringer setting table (see [Ringer Setting](#) on page 248).

Administration via Local Phone

```
|--- Admin
    |--- System
        |--- Features
            |--- Configuration
                |--- Alerting
                    |--- Impact level ringer
```

4 Technical Reference

4.1 Default Port List

The following table contains all default ports, resp. port ranges, and protocols used by the services running on OpenScape Desk Phone CP100/200/205/400/600/600E/600E phones.

Service	Server Default Port	Client Default Port	Protocol Stack
Payload transport (VoIP)	5010 - 5059	5010 - 5059	RTP - RTCP
Payload transport (VoIP)	5010 - 5059	5010 - 5059	SRTP - SRTCP
SIP subscriber - TCP is used	5060	32786 - 61000	SIP / TCP
SIP subscriber - TLS is used	5061	32786 - 61000	SIP / TLS
SIP subscriber - UDP is used	5060	5060	SIP / UDP
Directory access via LDAP	---	32786 - 61000	TCP
Directory access via LDAP	---	32786 - 61000	TCP- SSL/TLS
DHCP Client	---	68	DHCP / UDP
DNS Client	---	1024 - 65535	DNS / TCP_UDP
DLS contact me service - workpoint side	8085	---	HTTP / TCP
Default communication with the DLS workpoint interface	---	18443	HTTPS / TCP - SSL / TLS
Secure communication with the DLS workpoint interface	---	18444	HTTPS / TCP - SSL / TLS
Connection to the control port of FTP server	21	32786 - 61000	FTP / TCP
FTP client; uses the FTP server in active mode	32786 - 61000	20	FTP / TCP
HTTPS file download server	443	32786 - 61000	HTTPS / TCP - SSL/TLS
Client application which sends QDC data to the QCU	---	32786 - 61000	SNMP / UDP
Part of SNMP-Agent - sending Traps	---	32786 - 61000	SNMP / UDP

Service	Server Default Port	Client Default Port	Protocol Stack
Part of SNMP-Agent - receive Set/Get commands	161	---	SNMP / UDP
SNTP client - queries time information in unicast operation	---	123	SNTP / UDP
SNTP client - receives time information in broadcast operation	123	---	SNTP / UDP
Web server for WBM access	8085	---	HTTP / TCP
Secure Web Server for WBM access	443	---	HTTPS / TCP - SSL / TLS

4.2 Troubleshooting: Error Codes

For a set of error cases, specific error codes are defined. These error codes are shown in brackets on the display, following a general error note. Example: „No Telephony (LP1)“.

NOTICE:

On CP700X/700/600/600E/400 the codes are shown in a 'sausage' notification at the bottom of the display.

On CP20X/100 they are shown as an Idle screen error.

Text part	Error code	Scenario	Reason
No telephony	LP1	Unable to use LAN	Physical connection missing (Link Protocol)
	LX1	Unable to use LAN	802.1x error
	LI1	Link problem	No network connection
	RS2	Unable to Register	No server address configured
	RN2	Unable to Register	No number configured
	RI2	Unable to Register	No phone IP address set
	RA2	Unable to Register	Authentication failed

Text part	Error code	Scenario	Reason
	RF2	Unable to Register	Server failed
Limited keyset	W5	Limited Keyset support	Waiting to subscribe
Limited service	NT	Network Time	No NTP source
	B8	Unable to Register	Backup route active
Limited service	DF	DNS failure	SIP related DNS lookups fail
Exchange: please check username and password	EX	Exchange failure	Wrong username/ password
Exchange: untrusted server			Cert validation failure
connection to Exchange server failed			Other failure
Circuit: please check username and password	CI	Circuit failure	Wrong username/ password
Circuit: untrusted server			Cert validation failure
connection to Circuit server failed			Other failure

NOTICE: A special “fast-busy” tone (also called congestion tone) is played if a temporary network problem causes a user-initiated call action to fail. Typical call actions: making an outgoing call; picking up a call from Manual Hold; or Group pickup. Phone users include keyset users and mobile users logged on to the phone. The special tone is triggered if one of the following SIP response codes is received from the server: 606, 408, or 503.

5 Examples and HowTos

5.1 Canonical Dialing

5.1.1 Canonical Dialing Settings

The following example shows settings suitable for the conversion of given dial strings to canonical format. The example phone is located in Nottingham, UK.

Parameter	Example value	Explanation
Local country code	44	International country code for the UK.
National prefix digit	0	Used in front of national codes when dialled without international prefix.
Local national code	115	Area code within the UK (here: Nottingham).
Minimum local number length	7	Minimum number of digits in a local PSTN number (e. g. 3335333 = 7 digits).
Local enterprise node	780	Prefix to access Nottingham numbers from within the Siemens network.
PSTN access code	9	Prefix to make an international call in the UK.
Operator codes	0,7800	Set of numbers to access the local operators. (No blank after comma, or else the subsequent entry is ignored.)
Emergency numbers	999,555	Set of numbers to access emergency services. (No blank after comma, or else the subsequent entry is ignored.)
Initial extension digits	2,3,4,5,6,8	1st digits of numbers that are used for extension numbers on the local node. (No blank after comma, or else the subsequent entry is ignored.)

5.1.2 Canonical Dial Lookup

The following example shows settings suitable for recognizing incoming numbers and assigning them to entries in the local phonebook, and for generating correct dial strings from phone book entries, depending on whether the number is internal or external.

Parameter	Example value	Explanation
Local code <1>	780	Enterprise node prefix (here: Nottingham).
International code <1>	+44115943	Equivalent prefix to access numbers on this node from the PSTN. Here, the prefix used by the PSTN (DID/DDI: direct inward dialing) is 943, which differs from the enterprise node prefix used within the enterprise network.
Local code <2>	7007	Enterprise node prefix (here: Munich).
International code <2>	+49897007	Equivalent prefix to access numbers on this node from the PSTN. Here, the prefix used by the PSTN for direct inward dialing is identical to the enterprise node prefix.

5.1.2.1 Conversion examples

In the following examples, numbers entered into the local phonebook by the user are converted according to the settings given above.

Example 1: Internal number, same node as the local phone

User entry	2345	
External numbers	Local public form	
External access code	Not required	
International gateway code	Use national code	
Number stored in the phonebook	+441159432345	
Dial string sent when dialing from the phonebook	Internal numbers = Local enterprise form	1234
	Internal numbers = Always add node	7802345
	Internal numbers = Use external numbers	9432345

Example 2: Internal number, different node

User entry	70072345	
External numbers	Local public form	

Examples and HowTos

How to Set Up the Corporate Phonebook (LDAP)

External access code		Not required
International gateway code		Use national code
Number stored in the phonebook		+498970072345
Dial string sent when dialing from the phonebook	Internal numbers = Local enterprise form	2345
	Internal numbers = Always add node	7802345
	Internal numbers = Use external numbers	9432345

Example 3: External number, same local national code as the local phone

User entry		011511234567
External numbers		Local public form
External access code		Not required
International gateway code		Use national code
Number stored in the phonebook		+4411511234567
Dial string sent when dialing from the phonebook	External numbers = Local public form	234567
	External numbers = National public form	011511234567
	External numbers = International form	004411511234567

5.2 How to Set Up the Corporate Phonebook (LDAP)

The Corporate Phonebook function is based on an LDAP client that can be connected to the company's LDAP service. A variety of LDAP servers can be used, for instance Microsoft Active Directory, OpenLDAP, or Apache Directory Server.

5.2.1 Prerequisites

- 1) An LDAP server is present and accessible to the phone's network. The standard Server port for LDAP is 389, the standard transport for LDAP is TCP. There is also the secure interface for LDAPS using TLS.
- 2) Query access to the LDAP server must be provided. Unless anonymous access is used, a user name and password must be provided. It might be

feasible to use a single login/password for all OpenScape Desk Phone CP phones.

- 3) To enable dialing internal numbers from the corporate phonebook, an LDAP entry must be provided that contains the proper number format required by OpenScape Desk Phone CP.

In Microsoft Active Directory, the standard LDAP attribute `telephoneNumber` is typically populated as follows: `+1<area code><call number>`. However, in a standard configuration, OpenScape Desk Phone CP will not handle this dial string correctly, due to the `+1` prefix, if Canonical Dial is not configured. In this case, it is recommended to use the `ipPhone` field, which is typically unused in Active Directory. It can be found in the Telephones tab of the Active Directory User Manager.

5.2.2 Create an LDAP Template

The task of an LDAP template is to map the phone's search and display fields to LDAP attributes that can be delivered by the server. In the LDAP template, the fields are represented by hard-coded names: `ATTRIB01`, `ATTRIB02`, and so on. These field names are assigned to LDAP attributes, as appropriate.

The following examples show the relations between Contact field names, the attribute labels used in the template, and exemplary mappings to LDAP attributes.

NOTICE: In an LDAP template for OpenScape Desk Phone CP, the entries must be sorted according to the sequential number of the template labels, as shown in the example underneath.

Generic Example (Standard Attributes)

OpenScape Desk Phone CP Field	LDAP Template Labels	LDAP Attribute	Example Value
Last name	ATTRIB01	<code>surnameNational</code>	Doe
First name	ATTRIB02	<code>givenNameNational</code>	John
Work 1	ATTRIB03	<code>telephoneNumber</code>	9991234
Work 2	ATTRIB04	<code>alternatePhone</code>	9992345
Mobile	ATTRIB05	<code>mobile</code>	017711223344
Home	ATTRIB06	<code>otherTelephone</code>	441274333444
Company	ATTRIB07	<code>ou</code>	Example Inc.
Address 1	ATTRIB08	<code>departmentText</code>	0815
Address 2	ATTRIB09		
Role	ATTRIB10	<code>mainFunction</code>	Product Manager
Email	ATTRIB11	<code>mail</code>	doe@example.com

OpenScape Desk Phone CP Field	LDAP Template Labels	LDAP Attribute	Example Value
Nickname	ATTRIB12	nickname	
Avatar	ATTRIB13		jpeg image or image name, more information in the Picture Clips via LDAP on page 264

Given "example.com" as the LDAP subtree to be searched, the LDAP template file looks like this:

```
OpenScape Desk Phone CP LDAP TEMPLATE (v.1)
SEARCHBASE="O=SIEMENS COMM, C=GB"
ATTRIB01="surnameNational"
ATTRIB02="givenNameNational"
ATTRIB03="telephonenumber"
ATTRIB04="alternatePhone"
ATTRIB05="mobile"
ATTRIB06="otherTelephone"
ATTRIB07="ou", READONLY
ATTRIB08="departmentText", READONLY
ATTRIB09=""
ATTRIB10="mainFunction"
ATTRIB11="mail"
ATTRIB12="nickname"
ATTRIB13=""
EOF
```

Microsoft Active Directory Specific Example

OpenScape Desk Phone CP Field	LDAP Template Attribute	LDAP Attribute	Example Value
Last name	ATTRIB01	sn	Doe
First name	ATTRIB02	givenName	John
Business 1	ATTRIB03	ipPhone	9991234
Business 2	ATTRIB04	otherTelephone	9992345
Mobile	ATTRIB05	mobile	017711223344
Private	ATTRIB06	homePhone	441274333444
Company	ATTRIB07	company	Example Inc.
Address 1	ATTRIB08	department	Administration
Address 2	ATTRIB09	l	
Job function	ATTRIB10	title	Product Manager

OpenScape Desk Phone CP Field	LDAP Template Attribute	LDAP Attribute	Example Value
Email	ATTRIB11	mail	doe@example.com
Nickname	ATTRIB12	nickname	
Avatar	ATTRIB13		jpeg image

Given "example.com" as the LDAP subtree to be searched, the LDAP template file looks like this:

```
OpenScape Desk Phone CP LDAP TEMPLATE (v.1)
SEARCHBASE="dc=example,dc=com"
ATTRIB01="sn"
ATTRIB02="givenName"
ATTRIB03="ipPhone"
ATTRIB04="otherTelephone"
ATTRIB05="mobile"
ATTRIB06="homePhone"
ATTRIB07="company"
ATTRIB08="department"
ATTRIB09="1"
ATTRIB10="title"
ATTRIB11="mail"
ATTRIB12="nickname"
ATTRIB13=""
EOF
```

Administration via WBM

The LDAP template can be configured via path:

Administration setting > Local functions > LDAP template

Examples and HowTos

Administrator settings
User settings

Admin login
Network
System
File transfer
Defaults
Phone application
LDAP
Ringer file
Dongle key
Local functions
Directory settings
LDAP template
Locality
UC Server
Date and time
Speech
General information
Security and policies
Ringer
User mobility
Diagnostics
Maintenance

LDAP template


This page allows you to specify the LDAP attribute fields that will be used by the phone, plus how the field is used.

Use	Field name	Usage type
Search base		
Last name		▼
First name		▼
Work 1		▼
Work 2		▼
Mobile		▼
Home		▼
Company		▼
Address 1		▼
Address 2		▼
Role		▼
Email		▼
Nickname		
Avatar		

Submit
Reset

Example of the LDAP configuration:

LDAP template


This page allows you to specify the LDAP attribute fields that will be used by the phone, plus how the field is used

Use	Field name	Usage type
Search base	<u>O=UNIFY,C=GB</u>	
Last name	<u>surnameNational</u>	▼
First name	<u>givenNameNational</u>	▼
Work 1 number	<u>telephonenumber</u>	▼
Work 2 number	<u>alternatPhone</u>	▼
Mobile number	<u>mobile</u>	▼
Home number	<u>otherTelephone</u>	▼
Company name	<u>ou</u>	READONLY ▼
Address	<u>departmentText</u>	READONLY ▼
Address contd.		▼
Role	<u>mainFunction</u>	▼
Email	<u>mail</u>	▼
Nickname search	<u>nickname</u>	
Avatar	<u>jpegPhoto</u>	

NOTICE: if the **Usage type** field is set to **READONLY** means then this specific LDAP field will not be part of the search.

5.2.3 Load the LDAP Template onto the Phone

When you have configured the LDAP template, you can upload it to the phone:

- 1) Save the template under a suitable name, for example, ldap-template.txt.
- 2) Copy the template file to the FTP server designated for deploying LDAP templates.
- 3) Upload the file using the WBM (see [LDAP Template](#) (Download) on page 265), or, alternatively, the Local menu, or the DLS (see the Deployment Service Administration Manual). For an example configuration, see the following WBM screenshot (path: File transfer > LDAP):

The screenshot shows a web form titled "LDAP" with a dark blue header. The form contains the following fields and controls:

- Use defaults:** A checkbox that is currently unchecked.
- Download method:** A dropdown menu set to "FTP".
- FTP Server address:** An empty text input field.
- FTP Server port:** A text input field containing the value "21".
- FTP account:** An empty text input field.
- FTP username:** A text input field containing the value "phone".
- FTP password:** A text input field with masked characters (dots).
- FTP path:** A text input field containing the value "media".
- HTTPS base URL:** An empty text input field.
- Filename:** A text input field containing the value "ldap-template.txt".
- After submit:** A dropdown menu set to "do nothing".
- Buttons:** "Submit" and "Reset" buttons at the bottom.

5.2.4 Configure LDAP Access

To enter the access data using the WBM, take the following steps:

- 1) Navigate to Local Functions > Directory Settings.

2) Enter the following parameters:

- LDAP Server address (IP address or hostname of the LDAP server)
- Transport (allows the LDAP interface to be encrypted using TLS (via LDAPS) or unencrypted using TCP, typically TCP)
- Secure port (port used by the LDAP for encrypted (TLS) transport, typically 636)
- LDAP Server port (port used by the LDAP for unencrypted (TCP) transport, typically 389)
- Authentication (authentication method for the connection to the LDAP server)
- User name (only required if simple authentication is selected); Password (relating to the user name).
- Permanent LDAP enabled
- Avatar server (holds a contact picture for each entry). Available only for OpenScope Desk Phone CP600/600E/700/700X.

Directory settings

LDAP server address

Transport

Secure port

LDAP server port

Authentication

User name

Password

LDAP for manual search only

Firstname and lastname for quick search

Submit

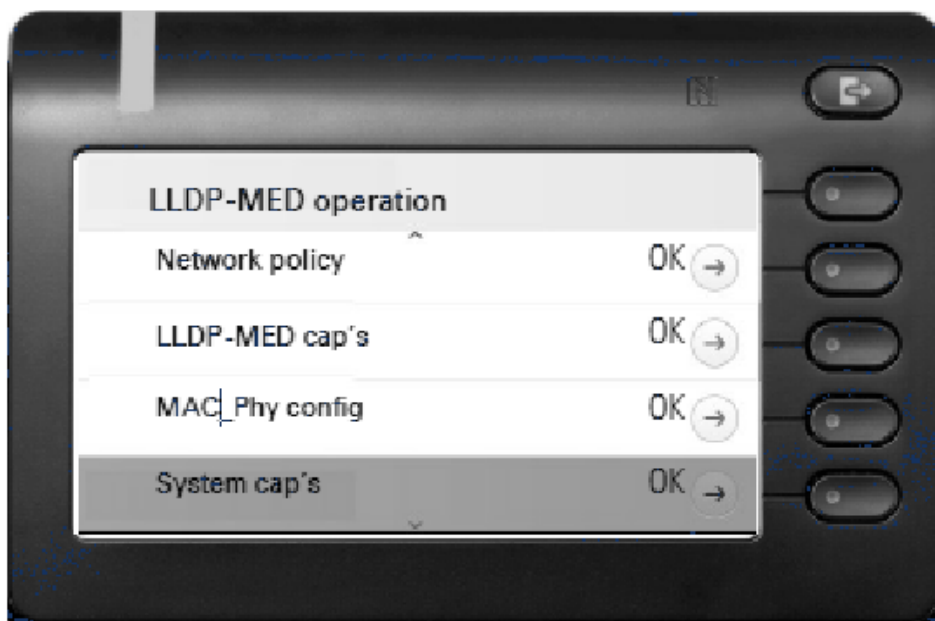
Reset

3) Press Submit.

5.3 An LLDP-Med Example

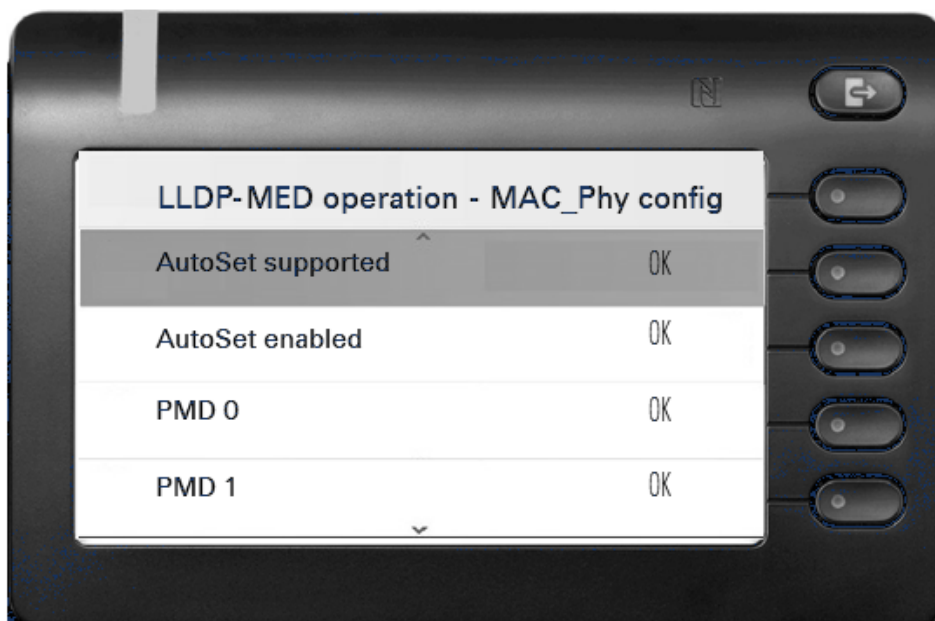
The following example illustrates the mode of operation of LLDP-MED. In order to evoke a reaction from LLDP-MED, the LAN switch has been set to auto-negotiation, whereas the phone's LAN port (see [LAN Port Settings](#) on page 55) is set to 100Mbit/s, hence a fixed value. This configuration error is discovered by LLDP-MED. The following screenshots from the phone's local menu will show the error messages.

This screenshot shows the LLDP-MED operation submenu (see [LLDP-MED](#) on page 294). Please note the status of MAC_Phy config.



When MAC_Phy config is selected, the details are displayed.

- 1) Log in as administrator on the local phone's Admin menu.
- 2) In the Admin menu, navigate to Network >Wired settings, select LLDP-MED Operation by using the navigation keys, and click OK.
- 3) In the LLDP-MED Operation submenu (see LLDP-MED Operation), navigate to MAC_Phy config and note the status displayed.
- 4) **Select the MAC_Phy config submenu by pressing OK and navigate to the parameters displayed by using the navigation keys. The following status is displayed for the MAC_Phy config parameters:** AutoSet enabled = Incompatible MAU = Incompatible



5.4 Example Dial Plan

5.4.1 Introduction

A dial plan is a set of rules that determine the phone's behaviour on digit entry by the user. Up to 48 rules are possible. With OpenScape Desk Phone CP, a dial plan rule is constructed from 9 parameters. In the following, the setup of a dial plan is explained.

The dial plan entries are preceded by a title line. This is a free format string, e. g. a descriptive name or version number, which can be used by the administrator for version control purposes.

5.4.2 Dial Plan Syntax

NOTICE: The phone will not perform any checking on the title; ensuring that different dial plans are given different titles is part of the administration process.

A dial plan rule is built from the parameters described underneath.

- **Digit string:** A pattern of digits or "*", "#", or "x" characters that is to be matched for starting an action. The maximum length is 24 characters. The "x" character is a wildcard character that represents any of the other digits (it may be upper or lower case).
- **Action :** The action to be taken when the criteria are met. The following options are available:
 - **"S" (Send digits):** The digits entered are sent to the server when one of the following three conditions is satisfied:
 - a) the maximum digits have been received, or
 - b) the timer expires after the minimum digits have been received, or
 - c) on receipt of the terminator after the minimum digits.
 - **"C" (Check for other actions):** If the the digit sequence entered by the user matches Digit string, Maximum length, and Minimum length, the timer starts. On timer expiry, the digit string will be sent to the server. If further digits are received before timer expiry, further entries will be checked. If the timer is set to 0, the dial string will be sent immediately. This option is used when there are more than one rules which start with the same digits.
- **Minimum length:** The dial plan rule will not initiate the sending of digits until at least this number of digits have been entered. However, the digits will be sent after the delay configured in User menu > Configuration > Outgoing calls > Autodial delay (seconds).
- **Maximum length:** Automatic sending will occur when this number of digits have been dialed. If not specified, then the digits will be sent when the timer expires, or a terminating character is entered.

- **Timer:** This indicates the timeout to be used for subsequent digit handling. If not specified, the default timer value is used (User menu > Configuration > Outgoing calls > Autodial delay (seconds)).
- **Terminating character:** A "*" or "#" character which indicates that the preceding digits should be considered complete, even though the maximum length may not be reached. However, the reach the minimum length must be reached by the string built from the digits entered and the terminating characters.
- **Special indication:**
 - **"E" (Emergency):** If this character is entered here, the digits matching this rule will be sent even if the phone is locked. The number will be dialed immediately even when immediate dialing is disabled, and the phone is on-hook.
 - **"b" (bypass):** The phone lock is bypassed. The number will be dialed immediately even when immediate dialing is disabled, if the phone is off-hook.
- **Comment:** A remark on this dial plan entry.
- **Terminator sent:** If set to true, the terminating character is sent to the server along with the dial string proper. If set to false, the dial string is sent without the terminating character.

5.4.3 How To Set Up And Deploy A Dial Plan

For creating and deploying a dial plan to an OpenScape Desk Phone CP, a working installation of the DLS (version V2R4 onwards) is required. This HowTo describes the creation of a simple dial plan for OpenScape Desk Phone CP by example. Unless otherwise stated, the actions described underneath are made in the DLS.

- 1) Log on to the DLS with an account that has suitable rights for deploying a dial plan. For details, please refer to the Deployment Service Administration Manual.
- 2) Navigate to IP Devices > IP Phone Configuration > Features > "Dialplan" tab.
- 3) Check Dialplan, if not checked already.
- 4) Enter a suitable Dialplan ID.
- 5) Click on  to create the first dial plan rule.
- 6) **Enter the following data:**

Parameter	Value	Description/Remarks
Digit string	3	This rule matches numbers beginning with 3. For instance, theses might be internal numbers.
Action	S	When all criteria are met, the number is sent to the server.
Minimum length	4	This rule matches numbers with a length of 4 digits.
Maximum length	4	

Parameter	Value	Description/Remarks
Timer	0	The specified Action will take place without delay when all other criteria are met.

Summary: This rule determines that digit strings which begin with 3 and have a length of 4 digits are sent to the server without delay after the last digit has been entered.

- 7) Click on  to create the second dial plan rule.

- 8) **Enter the following data:**

Parameter	Value	Description/Remarks
Digit string	0	This rule matches numbers beginning with 0. In the USA, this number calls the operator.
Action	C	When Minimum length, Maximum length, and the length of the digit string entered by the user match, the Timer is started. When it expires, the digits are sent to the server. When another digit is entered before expiry, the next dial plan entry will come into operation.
Minimum length	1	This rule matches numbers with a length of 1 digits.
Maximum length	1	
Timer	1	The phone waits 1 second for further digits. If the user does not enter any further digits, the action specified in Action is initiated.

Summary: When 0 is entered as first digit, the phone will wait 1 second. After this, 0 will be sent to the server, which might result in a call to an operator, for instance. When further digits are entered during the 1 second timespan, the next dial plan rule will take control.

- 9) Click on  to create the third dial plan rule.

- 10) **Enter the following data:**

Parameter	Value	Description/Remarks
Digit string	011	This rule matches numbers beginning with 011. In the USA, this digit string is the prefix international calls.
Action	S	When the entered digit string reaches the Minimum length, the Timer is started. On expiry, the digit string is sent.
Minimum length	4	When the length of the digit sequence entered by the user reaches this value, the Timer is started.

Parameter	Value	Description/Remarks
Maximum length	13	When the length of the digit sequence entered by the user reaches this value, the digits are sent to the server immediately. The Timer is overridden.
Timer	3	When the length of the digit sequence entered by the user reaches the Minimum length, the phone waits 3 seconds for further digits. If the user does not enter any further digits, the Action is triggered.
Terminating Character	#	When this character is entered, the digits are sent to the server immediately, regardless of the criteria contained in this rule.

Summary: Any numbers that start with 011 and have a length of 13 digits are sent to the server immediately. Shorter numbers with a length from 4 digits onwards are sent after a 3 seconds delay.

11) The example dial plan is completed; it should look like this:

☒ Dialplan
 Dialplan ID:
 Dialplan Error:

☒ Table
 ☐ Selected entry
 1 / 3

Digit String	Action	Min Length	Max Length	Timer	Terminating Character	Special Indication	Comment	Terminator sent
3	-S- Send digits	4	4	0				☐
0	-C- Action for digits	1	1	1				☐
011	-S- Send digits	4	13	3	#			☐

12) You can check the dial plan using the phone's web interface; navigate to Diagnostics > Fault trace configuration > Download dial plan file.

6 Glossary

Address of Record (AoR)	A SIP URI that represents the "public address" of a SIP user resp. a phone or line. The format is similar to an E-mail address: "username@hostname".
ADPCM	Adaptive Differential Pulse Code Modulation. A compressed encoding method for audio signals which are to be transmitted by a low bandwidth. As opposed to regular Glossary on page 340, a sample is coded as the difference between its predicted value and its real value. As this difference is usually smaller than the real, absolute value itself, a lesser number of bits can be used to encode it.
CSTA	Computer Supported Telecommunications Applications. An abstraction layer for telecommunications applications allowing for the interaction of Glossary on page 340 computer applications with telephony devices and networks.
CTI	Computer Telephony Integration. This term denotes the interaction of computer applications with telephony devices and networks.
DFT	Digital Feature Telephone. A phone with no line keys.
DHCP	Dynamic Host Configuration Protocol. Allows for the automatic configuration of network endpoints, like IP Phones and IP Clients.
DiffServ	Differentiated Services. Specifies a layer 3 mechanism for classifying and managing network traffic and providing quality of service (Glossary on page 340) guarantees on Glossary on page 340 networks. DiffServ can be used to provide low-latency, guaranteed service for e. g. voice communication.
DLS	The Deployment Service (DLS) is a OpenScape management application for the administration of workpoints, i. e. IP Phones and IP Clients, in both HiPath- and non-HiPath networks.
DNS	Domain Name System. Performs the translation of network domain names

	and computer hostnames to Glossary on page 340es.
DTMF	Dual Tone Multi Frequency. A means of signaling between a phone and e. g. a voicemail facility. The signals can be transmitted either in-band, i. e. within the speech band, or out-band, i. e. in a separate signaling channel.
EAP	Extensible Authentication Protocol. An authentication framework that is frequently used in WLAN networks. It is defined in RFC 3748.
FTP	File Transfer Protocol. Used for transferring files in networks, e. g., to update telephone software.
G.711	ITU-T standard for audio encoding, used in ISDN and Glossary on page 340. It requires a 64 kBit/s bandwidth.
G.722	ITU-T standard for audio encoding using split band Glossary on page 340. The audio bandwidth is 7 kHz at a sampling rate of 16 kHz. There are several transfer rates ranging from 32 to 64 kBit/s, which correspond to different compression degrees. The voice quality is very good.
G.729	ITU-T standard for audio encoding with low bandwidth requirements, mostly used in VoIP. The standard bitrate is 8 kBit/s. Music or tones such as Glossary on page 340 or fax tones cannot be transported reliably with this codec.
Gateway	Mediation components between two different network types, e. g., Glossary on page 340 network and ISDN network.
HTTP	Hypertext Transfer Protocol. A standard protocol for data transfer in Glossary on page 340 networks.
IP	Internet Protocol. A data-oriented network layer protocol used for transferring data across a packet-switched internetwork. Within this network layer, reliability is not guaranteed.
IP address	The unique address of a terminal device in the network. It consists of

	four number blocks of 0 to 255 each, separated by a point.
Jitter	Latency fluctuations in the data transmission resulting in distorted sound.
LAN	Local Area Network. A computer network covering a local area, like an office, or group of buildings.
Layer 2	2nd layer (Data Link Layer) of the 7-layer OSI model for describing data transmission interfaces.
Layer 3	3rd layer (Network Layer) of the 7-layer OSI model for describing the data transmission interfaces.
LCD	Liquid Crystal Display. Display of numbers, text or graphics with the help of liquid crystal technology.
LDAP	Lightweight Directory Access Protocol. Simplified protocol for accessing standardized directory systems, e.g., a company telephone directory.
LED	Light Emitting Diode. Cold light illumination in different colours at low power consumption.
MAC Address	Media Access Control address. Unique 48-bit identifier attached to network adapters.
MDI-X	Media Dependent Interface crossover (X). The send and receive pins are inverted. This MDI allows the connection of two endpoints without using a crossover cable. When Auto MDI-X is available, the MDI can switch between regular MDI and MDI-X automatically, depending on the connected device.
MIB	Management Information Base. A type of database used to manage the devices in a communications network.
MWI	Message Waiting Indicator. A signal, typically a LED, to notify the user that new mailbox messages have arrived.
PBX	Private Branch Exchange. Private telephone system that connects the internal devices to each other and to the ISDN network.
PCM	Pulse Code Modulation. A digital representation of an analog signal, e. g. audio data, which consists of

	quantized samples taken in regular time intervals.
PING	Packet Internet Gro(u)per. A program to test whether a connection can be made to a defined IP target. Data is sent to the target and returned from there during the test.
PoE	Power over Ethernet. The IEEE 802.3af standard specifies how to supply power to compliant devices over Ethernet cabling (10/100Base-T).
Port	Ports are used in Glossary on page 340 networks to permit several communication connections simultaneously. Different services often have different port numbers.
PSTN	Public Switched Telephone Network. The network of the world's public circuit-switched telephone networks.
QoS	Quality of Service. The term refers to control mechanisms that can provide different priority to different users or data flows, or guarantee a certain level of performance to a data flow in accordance with requests from the application program. The OpenScape Desk Phone CP phone allows for the setting of QoS parameters on layer 2 and layer 3 (DiffServ).
RAM	Random Access Memory. Memory with read / write access.
ROM	Read Only Memory. Memory with read only access.
RTCP	Realtime Transport Control Protocol. Controls the Glossary on page 340 stream and provides information about the status of the transmission, like QoS parameters.
RTP	Realtime Transport Protocol. This application layer protocol has been designed for audio communication.
SDP	Session Description Protocol. Describes and initiates multimedia sessions, like web conferences. The informations provided by SDP can be processed by Glossary on page 340.
SNMP	Simple Network Management Protocol. Used for monitoring,

	controlling, and administration of network and network devices.
SNTP	Simple Network Time Protocol. Used to synchronize the time of a terminal device with a timeserver.
Subnet Mask	To discern the network part from the host part of an Glossary on page 340, a device performs an AND operation on the IP address and the network mask. The network classes A, B, and C each have a subnet mask that demasks the relevant bits: 255.0.0.0 for Class A, 255.255.0.0 for Class B and 255.255.255.0 for Class C. In a Class C network, for instance, 254 IP addresses are available.
Switch	Network device that connects multiple network segments and terminal devices. The forwarding of data packets is based on Glossary on page 340es: data targeted to a specific device is directed to the switch port that device is attached to.
TCP	Transfer Control Protocol. The protocol belongs to the transport layer and establishes a connection between two entities on the application layer. It guarantees reliable and in-order delivery of data from sender to receiver.
TLS	Transport Layer Security. Ensures privacy between communicating applications. Typically, the server is authenticated, but mutual authentication is also possible.
URI	Uniform Resource Identifier. A compact string of characters used to identify or name a resource.
URL	Uniform Resource Locator. A special type of Glossary on page 340 which provides means of acting upon or obtaining a representation of the resource by describing its primary access mechanism or network location.
VLAN	Virtual Local Area Network. A method of creating several independent logical networks within a physical network. For example, an existing network can be separated into a data and a voice VLAN.

VoIP

Voice over IP. A term for the protocols and technologies enabling the routing of voice conversations over the internet or through any other [Glossary](#) on page 340-based network

WBM

Web Based Management. A web interface which enables configuration of the device using a standard web browser.

Index

Numerics

2nd Alert [214](#)

A

Administration Menu (Local Menu) [53](#), [54](#), [54](#), [54](#)

Advanced Audio Traces [309](#)

Advanced Traces (Bluetooth) [309](#)

AlertBar LED hint [320](#)

Alternate [197](#)

Audio

 advanced traces [309](#)

Audio Settings [287](#)

Authenticated Registration [121](#)

B

Backlight time [113](#)

Backlight type [290](#)

Backup SIP Server [142](#)

Blind Transfer [197](#)

Bluetooth

 advanced traces [309](#)

 handsfree profile [306](#)

 headset profile [306](#)

 Interface activation/deactivation [55](#)

Built-in Forwarding [213](#)

C

Call

 Accept via Headset [200](#)

 Forwarding [192](#), [193](#)

 Recording [181](#)

 Transfer [159](#)

 Waiting [207](#)

Callback [204](#)

Cancel Callbacks [205](#)

Canonical Dial Lookup [245](#)

Codec Preferences [284](#)

Conference

 Phone-Based [199](#)

 System based [164](#)

Connectivity Check (TLS) [137](#)

Connectors [22](#)

Consult [206](#)

Consultation [206](#)

Core dump [315](#)

Corporate Phonebook [275](#)

CSTA [179](#), [340](#)

CTI [340](#)

D

Date and Time (SNTP) [117](#)

Daylight Saving [117](#)

Default Route [73](#)

Deflect a Call [198](#)

DFT [340](#)

DHCP [69](#), [340](#)

Diagnostic [291](#)

Dial Plan [247](#), [336](#)

Dialing

 Repeat [192](#)

 Selected [191](#)

Diffserv [64](#)

Direct Station Select (DSS) [232](#)

Directory Settings [275](#)

Display Identity [112](#)

Distinctive Ringing [248](#)

DLS (Deployment Service) [19](#), [38](#), [82](#), [340](#)

DNS [79](#), [341](#)

 Domain Name [79](#)

 Primary/Secondary [79](#)

 Servers [79](#)

Do Not Disturb (DND) [200](#)

DSS key settings [233](#)

DST Zone (Daylight Saving Time Zone) [117](#)

DTMF playback [287](#)

E

Early 183 response [129](#), [129](#), [130](#)

Easy Trace Profiles [304](#)

 Bluetooth handsfree profile [306](#)

 Bluetooth headset profile [306](#)

 Call Connection [307](#)

 Call Log [308](#), [308](#)

 DAS Connection [308](#)

 DLS Data Errors [309](#)

Emergency Number [112](#), [243](#)

Error Codes [324](#)

External Access Code [244](#)

External Numbers [244](#)

F

Factory Reset [289](#)

Fault Trace Configuration [298](#)

Features

 Server Based [173](#)

Forward indication [229](#)

Forwarding [192](#), [193](#)

FTP Settings [257](#)

G

G.711 [285](#)
G.722 [285](#)
G.729 [285](#)
Gateway [73](#)
General Information [290](#)
Group Pickup [156](#)

H

Hold [197](#)
Hot Phone [152](#)
Hot warm
 action [225](#)
 destination [225](#)
HPT Interface [317](#)
Hunt Group [202](#)

I

ICE (Interactive Connectivity Establishment) [144](#)
Identity
 Display [112](#)
 Terminal and User [111](#)
Immediate Ring [231](#)
Initial digit timer [152](#)
Initial Digits [243](#)
Interactive Connectivity Establishment [144](#)
Internal Numbers [243](#)
International Code (Local Country Code) [242](#)
International Gateway Code [244](#)
International Prefix (International Access Code) [243](#)
IP
 Address [29](#), [71](#)
 Address (Manual configuration) [71](#)
 IP [341](#)
 Specific Routing [75](#)

J

Join Two Calls [198](#)

K

Key module (phone types) [26](#)
Key Modules [240](#)
Keyset Operation [228](#)

L

LAN [342](#)
 Monitoring [294](#)
 Port [56](#)
LAN port [56](#)
Last restart [290](#)
Layer 2 [63](#)

Layer 3 [64](#)
LDAP [275](#), [328](#), [342](#)
LDAP Template (Download) [265](#)
Line action mode [229](#)
Line Key Configuration [224](#)
Line Preview [231](#)
LLDP-MED [294](#)
Local Country Code (International Code) [242](#)
Local Enterprise Number [242](#)
Local National Code (Local Area Code) [242](#)

M

MAC address [290](#)
MAC Address [342](#)
MDI-X [56](#), [342](#)
Memory Information [296](#)
Messages settings [164](#)
MIB [342](#)
Missed Call LED [318](#)
Mobile User [203](#)
Mobility [254](#)
Monitoring [294](#)
Multiline / Keyset [224](#)
Multiline Appearance/Keyset [224](#)
MWI [162](#)
MWI (Message Waiting Indicator) [342](#)
MWI LED [317](#)

N

National Prefix (Trunk Prefix) [242](#)
Network port configuration [57](#)
Non-INVITE [140](#)
NonCall trans [140](#)

O

OCSP [105](#)
OCSR failure [99](#)
Operator Code [243](#)
OPUS [285](#)
Originating line preference [228](#)
Outbound Proxy [123](#)

P

Part Number [290](#)
Password
 Change [287](#)
 enter [47](#)
 Lost [288](#)
PBX [342](#)
PC port [56](#)
Phone
 Restart [288](#)

- Phone application
 - Download/Update [260](#)
 - Upgrade using File [259](#)
 - Upgrade using FTP/HTTPS [259](#)
- Phone software (Download) [258](#)
- Phonebook [275](#)
- Pickup alert [157](#)
- Picture Clips (Download) [261](#)
- PoE (Power over Ethernet) [24](#), [343](#)
- Port configuration [56](#), [57](#)
- Port List [323](#)
- Power Consumption/Supply [24](#)
- Process
 - Information [296](#)
- PSTN [343](#)
- PSTN Access Code [243](#)

Q

- QCU [86](#), [86](#)
- QoS [63](#)
- QoS Reports [310](#)
- Quick Start [27](#)

R

- Realm [225](#)
- Refuse [150](#)
- Registration
 - Authenticated [121](#)
- Registration Backoff Timer [141](#)
- Release [215](#)
- Remote Tracing — Syslog [316](#)
- Repeat Dialing [192](#)
- Repertory Dial [201](#)
- Reservation timer [229](#)
- Reset Factory [289](#)
- Response Timer [139](#)
- Restart Phone [288](#)
- Ringer
 - Off [196](#)
- Ringer File [270](#)
- RTP [343](#)
 - Base Port [283](#)

S

- Screensaver (Download) [268](#)
- Secure
 - file transfer [105](#)
 - SIP server [105](#)
- Selected Dialing [191](#)
- Send Request [211](#)
- Server Based Features [173](#)
- Shared type [225](#)
- Shift Level [199](#)
- Shipment [21](#)

- Show phone screen [215](#)
- Silence suppression [284](#)
- SIP
 - Addresses [118](#)
 - Connection [125](#)
 - Ports [118](#)
 - Server Addresses [118](#)
 - Server Ports [120](#)
 - Transport Protocol [124](#)
- SNMP [84](#), [344](#)
- Software version [290](#)
- SSH — Secure Shell Access [289](#)
- Start Phonebook [214](#)
- Subnet Mask [29](#)
- Subnet Mask (Manual configuration) [71](#)
- Survivability [136](#)

T

- TCP [344](#)
- Terminal
 - Number [111](#)
- Terminal Identity [111](#)
- Timeout (Not used) [180](#)
- Timezone Offset [117](#)
- TLS [344](#)
 - Connectivity Check [137](#)
- Trace Configuration [298](#)
- Trace Profiles [304](#)
- Transaction timer [140](#)
- Transfer on hangup [160](#)
- Transfer on Ring [159](#)

U

- uaCSTA [179](#)
- UBoot version [290](#)
- UDP [344](#)
- Unauthenticated RegistrationRegistration
 - Unauthenticated [121](#)
- Update Service [82](#)
- User Identifier [225](#)
- User Identity [111](#)

V

- Vendor Class (DHCP) [32](#), [39](#)
- View Report [313](#)
- VLAN [31](#), [58](#)
- Voice Mail Number [112](#)

W

- Warm Phone [152](#)
- WBM (Web Based Management) [19](#), [27](#), [345](#)
- Wi-Fi settings [88](#)

Z

Zip Tone [208](#)

