



A MITEL
PRODUCT
GUIDE

Unify OpenScape Desk Phone CP Family

OpenScape Desk Phone CP Family

Administrator Documentation HFA

11/2025

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.....	7
1.1 Important Notes.....	7
1.2 Maintenance Notes.....	8
1.3 Product-oriented environmental protection.....	8
1.4 Labeling.....	9
1.5 License Information.....	9
1.6 About the Manual.....	9
1.7 Conventions for this Document.....	9
1.8 The OpenScape Desk Phone CP Family.....	9
1.8.1 OpenScape Desk Phone CP700/700X.....	10
1.8.2 OpenScape Desk Phone CP600.....	11
1.8.3 OpenScape Desk Phone CP400.....	12
1.8.4 OpenScape Desk Phone CP200/CP205.....	14
1.8.5 OpenScape Desk Phone CP100.....	15
1.9 Administration Interfaces.....	16
1.9.1 Web-based Management (WBM).....	17
1.9.2 DLS/DMS (OpenScape Deployment Service / Device Management Service).....	17
1.9.3 Local Phone Menu.....	17
2 Startup.....	18
2.1 Prerequisites.....	18
2.2 Assembling and Installing the Phone.....	18
2.2.1 Shipment.....	18
2.2.2 Connectors at the bottom side.....	19
2.2.3 Assembly.....	21
2.2.4 How to Connect the Phone.....	21
2.2.5 How to Better Use LAN Network Connections.....	22
2.2.6 Key Module.....	22
2.3 Quick Start.....	23
2.3.1 How to Access the Web Interface (WBM).....	23
2.3.1.1 Licenses.....	24
2.3.2 Access via Local Phone.....	25
2.3.2.1 OpenScape Desk Phone CP100.....	25
2.3.2.2 OpenScape Desk Phone CP200/205.....	25
2.3.2.3 OpenScape Desk Phone CP400/600/600E/700/700X.....	26
2.3.3 How to Set the Terminal Number.....	26
2.3.4 Basic Network Configuration.....	27
2.3.5 DHCP Resilience.....	27
2.3.6 Date and Time / SNTP.....	28
2.3.7 Extended Network Configuration.....	28
2.3.8 VLAN Discovery.....	29
2.3.8.1 How to Use a Vendor Class.....	29
2.3.8.2 How to Use Option #43 "Vendor Specific".....	34
2.3.9 DLS Server Address.....	35
2.3.9.1 Using Vendor Class.....	36
2.3.9.2 Using Option #43 "Vendor Specific".....	41
2.3.10 HFA Gateway Settings.....	42
2.3.11 Using the Web Interface (WBM).....	43
2.3.12 Using the Local Menu.....	43
2.3.13 Set DMS Address via DHCP.....	43
2.3.13.1 Using Option 43.....	43

2.3.13.2 Using Option 66.....	44
3 Administration.....	45
3.1 Bluetooth Interface.....	45
3.1.1 Feature Access.....	45
3.1.1.1 Disable HFU.....	45
3.2 LAN Settings.....	46
3.2.1 LAN Port Settings.....	46
3.2.2 VLAN.....	48
3.2.2.1 Automatic VLAN discovery using LLDP-MED.....	49
3.2.2.2 Automatic VLAN discovery using DHCP.....	50
3.2.2.3 Manual configuration of a VLAN ID.....	52
3.3 IP Network Parameters.....	53
3.3.1 Quality of Service (QoS).....	53
3.3.1.1 Layer 2 / 802.1p.....	53
3.3.1.2 Layer 3 / Diffserv.....	54
3.3.2 Use DHCP.....	56
3.3.3 IP Address - Manual Configuration.....	57
3.3.4 Default Route/Gateway.....	59
3.3.5 Specific IP Routing.....	61
3.3.6 DNS.....	62
3.3.6.1 DNS Domain Name.....	62
3.3.6.2 Terminal Hostname.....	63
3.3.7 IP TTL.....	64
3.3.8 Gratuitous ARP control.....	65
3.3.9 Configuration & Update Service.....	65
3.3.10 SNMP.....	67
3.4 OpenScape Service Menu.....	70
3.5 Wi-Fi Settings.....	70
3.5.1 Setting up a CP700X for the first time with WLAN connection.....	71
3.5.2 Disable LAN port.....	72
3.5.3 Advanced Wi-Fi settings.....	73
3.6 System Settings.....	75
3.6.1 System Identity.....	75
3.6.2 HFA Gateway Settings.....	75
3.6.3 HFA Emergency Gateway Settings.....	78
3.6.4 Server and Standby Server ports.....	80
3.6.5 Redundancy.....	81
3.6.6 Emergency number.....	82
3.6.7 LIN.....	83
3.6.8 Not Used Timeout.....	84
3.6.9 Allow user downloads.....	85
3.6.10 Enable telephony settings.....	86
3.6.11 Energy Saving.....	88
3.6.11.1 Energy Efficient Ethernet (OpenScape Desk Phone CP205/400/600/600E only).....	88
3.6.12 Local Features.....	88
3.6.12.1 Direct video.....	88
3.6.12.2 Door opener.....	91
3.6.13 Security.....	95
3.6.13.1 System.....	95
3.6.13.2 Access control.....	96
3.6.13.3 Security Log.....	97
3.6.13.4 Security-Related Faults.....	99
3.6.13.5 Microsoft® Exchange.....	100
3.7 Date and Time.....	102
3.7.1 SNTP is Available, but no Automatic Configuration by DHCP Server.....	102

3.8 Dialing.....	103
3.8.1 Canonical Dialing Configuration.....	103
3.8.2 Canonical Dial Lookup.....	106
3.9 Ringer.....	108
3.9.1 Local ringers.....	108
3.9.2 Ringer settings for CP100/CP200.....	109
3.9.3 Ringer settings for CP400/600/700.....	110
3.9.3.1 Ringer Mode.....	111
3.9.3.2 Ringer Volume.....	112
3.10 User Mobility.....	113
3.11 Free Programmable Keys.....	113
3.11.1 Feature Key for CP700/700X.....	113
3.12 Transferring Phone Software, Application, and Media Files.....	114
3.12.1 File name.....	114
3.12.2 FTP/HTTPS Server.....	115
3.12.3 Common FTP/HTTPS Settings (Defaults).....	116
3.12.4 Phone Application.....	117
3.12.4.1 Upgrade using File.....	118
3.12.4.2 Upgrade using FTP/HTTPS.....	118
3.12.4.3 Download/Update Phone Application.....	120
3.12.5 Picture Clips.....	122
3.12.5.1 FTP/HTTPS Access Data.....	122
3.12.5.2 Download Picture Clip.....	123
3.12.5.3 Picture Clips via LDAP.....	124
3.12.6 LDAP Template.....	126
3.12.6.1 FTP/HTTPS Access Data.....	126
3.12.6.2 Download LDAP Template.....	127
3.12.7 Screensaver.....	128
3.12.7.1 FTP/HTTPS Access Data.....	129
3.12.7.2 Download Screensaver.....	130
3.12.8 Ringer File.....	131
3.12.8.1 FTP/HTTPS Access Data.....	132
3.12.8.2 Download Ringer File.....	133
3.12.9 Company logo.....	134
3.13 UC Server.....	136
3.14 Send Request via HTTP/HTTPS.....	137
3.15 Corporate Phonebook: Directory Settings.....	138
3.15.1 LDAP.....	138
3.15.2 Contact details update.....	140
3.15.2.1 Source of the contact details.....	140
3.15.3 System Phonebook (for OpenScape Business only).....	141
3.15.4 Picture via LDAP.....	142
3.15.5 Canonical Dial Settings.....	142
3.16 Speech.....	144
3.16.1 Audio Settings.....	144
3.17 Security and Policies.....	144
3.17.1 Password.....	144
3.17.1.1 Troubleshooting: Lost Password.....	145
3.17.2 Certificates.....	145
3.17.2.1 Generic.....	145
3.17.2.2 Authentication Policy.....	146
3.17.2.3 SCEP.....	147
3.18 Restart Phone.....	151
3.19 Factory Reset.....	151
3.20 SSH — Secure Shell Access.....	152
3.21 Display License Information.....	153

Contents

3.22 Web Services Interface (WSI).....	153
3.23 HPT Interface (For Service Staff).....	154
3.24 AlertBar LED hint.....	154
3.25 Diagnostics.....	155
3.25.1 LLDP-MED.....	156
3.25.2 Fault Trace Configuration.....	157
3.25.3 EasyTrace Profiles.....	163
3.25.3.1 Phone administration problems.....	163
3.25.3.2 Audio related problems.....	164
3.25.3.3 Bluetooth problems.....	164
3.25.3.4 Call proceeding problems.....	165
3.25.3.5 Conversations / LDAP problems.....	165
3.25.3.6 Keypad problems.....	165
3.25.3.7 Mobility / DLS problems.....	166
3.25.3.8 Network problems.....	166
3.25.3.9 Security problems.....	167
3.25.4 Advanced Audio Traces.....	167
3.25.5 QoS Reports.....	168
3.25.5.1 Conditions and Thresholds for Report Generation.....	168
3.25.5.2 View Report.....	171
3.25.6 Miscellaneous.....	173
3.25.6.1 IP tests.....	173
3.25.6.2 Memory Status Information.....	174
3.25.6.3 Core dump.....	175
3.25.7 Remote Tracing — Syslog.....	176
4 Examples and HowTos.....	178
4.1 Canonical Dialing.....	178
4.1.1 Canonical Dialing Settings.....	178
4.1.2 Canonical Dial Lookup.....	178
4.1.2.1 Conversion examples.....	179
4.2 How to Set Up the Corporate Phonebook (LDAP).....	180
4.2.1 Prerequisites.....	181
4.2.2 Create an LDAP Template.....	181
4.2.3 Load the LDAP Template onto the Phone.....	184
4.2.4 Configure LDAP Access.....	185
4.3 An LLDP-Med Example.....	186
5 Technical Reference.....	188
5.1 Default Port List.....	188
5.2 Troubleshooting: Error Codes.....	189
6 Glossary.....	192
Index.....	198

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 CP200, OpenScape DeskPhone CP400 and OpenScape DeskPhone CP600 has earned the ENERGY STAR.

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

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 24.

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, 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 10
- [OpenScape Desk Phone CP600](#) on page 11

- [OpenScape Desk Phone CP400](#) on page 12
- [OpenScape Desk Phone CP200/CP205](#) on page 14
- [OpenScape Desk Phone CP100](#) on page 15

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



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 or configures the following: • Speaker/headset • Handset Volume • Ring Volume • Ring Tone • Attention Ring • Display Contrast • Controls Speakerphone Mode 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: • Release • Redial • Caller list
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. :: the speaker key activates/deactivates speakerphone mode. ;: 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.
8	Audio Keys: + and -: Increases/decreases or configures the following: • Speaker/headset • Handset Volume • Ring Volume • Ring Tone • Attention Ring • Display Contrast • Controls Speakerphone Mode 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.

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.

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 with communication 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 4000, OpenScape Business.
- 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

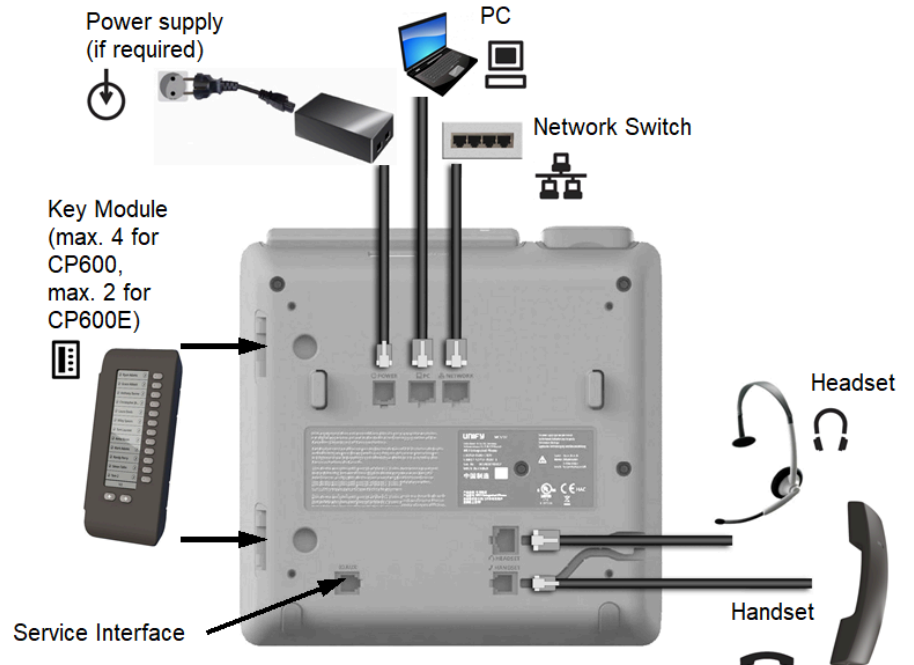
2.2 Assembling and Installing the Phone

2.2.1 Shipment

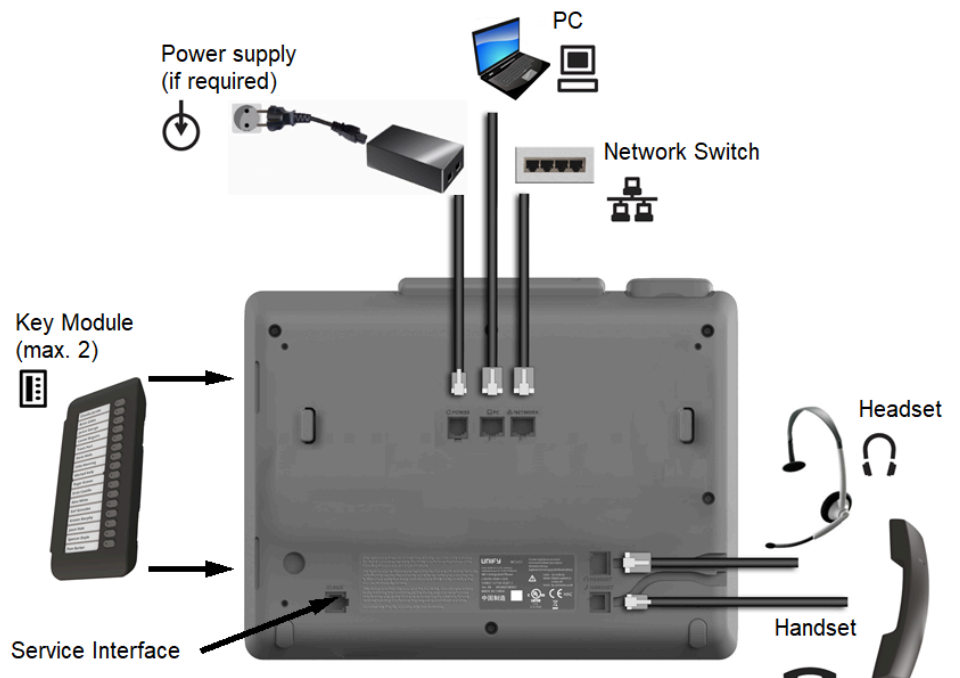
- Phone
- Handset
- Handset cable
- **Subpackage:**
 - Document "Information and Important Operating Procedures"

2.2.2 Connectors at the bottom side

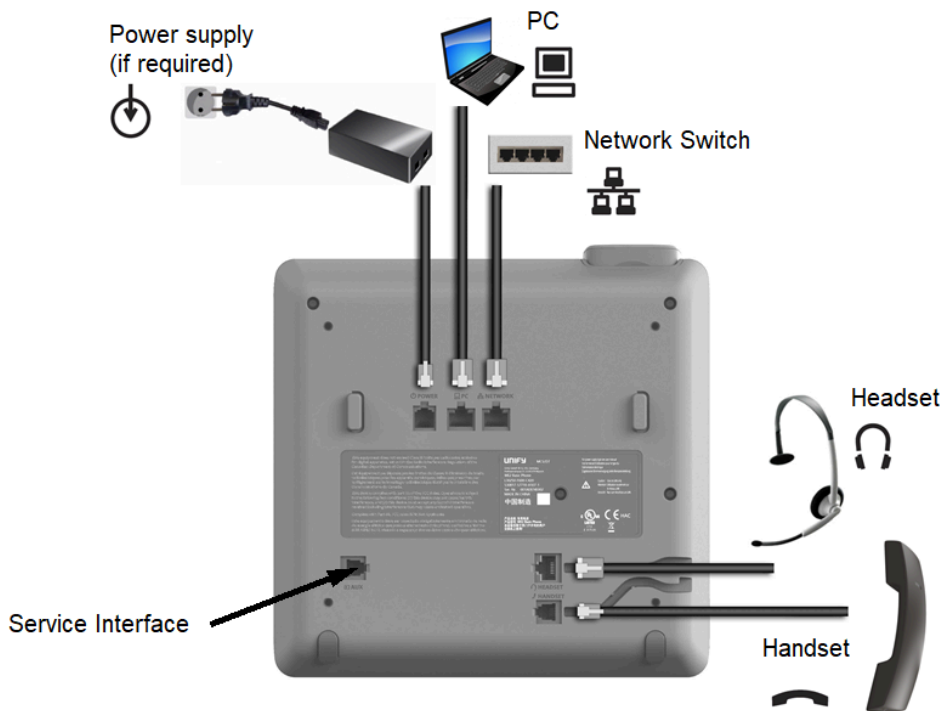
OpenScape Desk Phone CP600



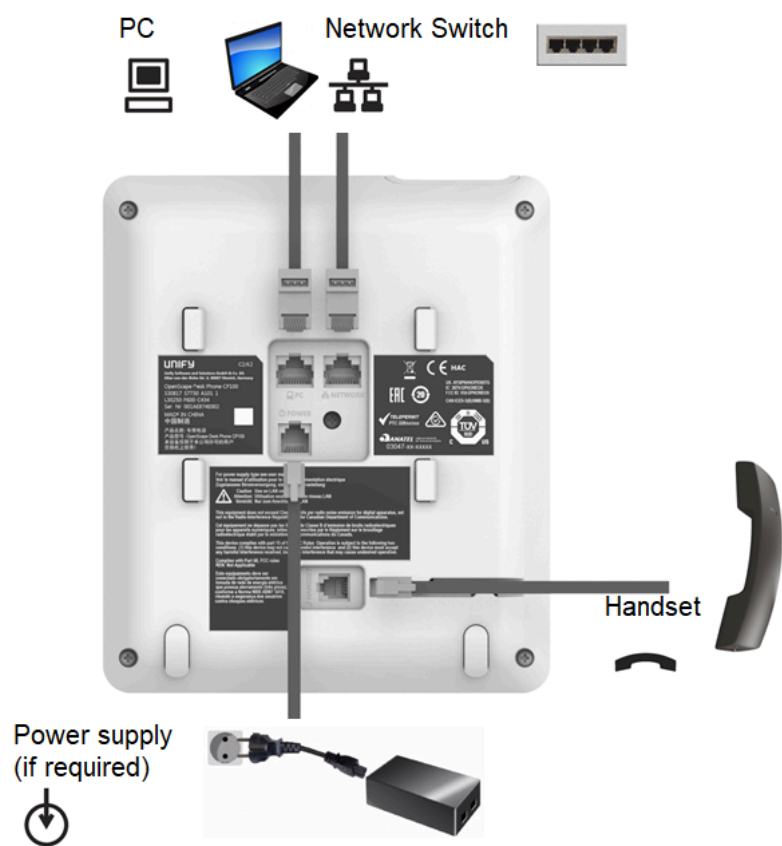
OpenScape Desk Phone CP400



OpenScape Desk Phone CP200/CP205



OpenScape 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 CP200/205	PoE (Power Class 1)
OpenScape Desk Phone CP400	PoE (Power Class 2)
OpenScape Desk Phone CP600/600E ¹	PoE (Power Class 2)
OpenScape Desk Phone CP700/700X	PoE (Power Class 2)

- 2) If Power over Ethernet (PoE) is NOT supported or an OpenScape Desk Phone CP600/600E or CP700/700X 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
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

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

Plug-in Power Supply	Order No.
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, CP600/600E and 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!



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	-	-

Phone Type	Key Modules	additional keys per module
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.

2.3 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)

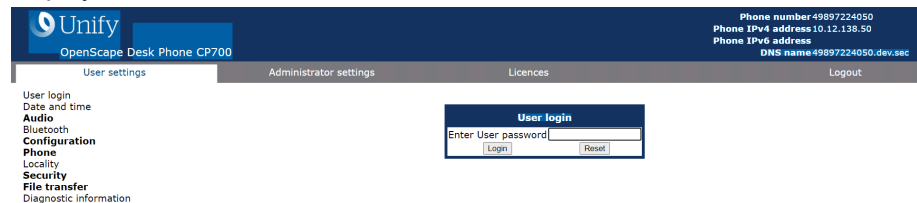
Prerequisites

- 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:**

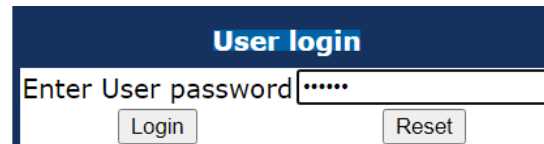
- 1) Access the local phone's Admin menu as described in Access via Local Phone.
 - **If DHCP is enabled (default):** In the Admin menu, navigate to Network > IPv4 configuration > IP address. The IP address is displayed.
 - If DHCP is disabled or if no DHCP server is available in the IP network, the 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 63.

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 Access via Local Phone

2.3.2.1 OpenScape Desk Phone CP100

- Press 1 3 0 simultaneously. You will be prompted to enter the administrator password.
- Enter the administrator password (default password is 123456). It is highly recommended to change the password (see section , [Password](#) on page 144 "Password") after your first login
- Confirm with **OK** key.

2.3.2.2 OpenScape Desk Phone CP200/205

- Press 1 3 0 simultaneously. You will be prompted to enter the administrator password.
- Enter the administrator password (default password is 123456). It is highly recommended to change the password (see section , [Password](#) on page 144 "Password") after your first login
- Confirm with **OK** key.

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

1) Access the Administration Menu

- Press 1 3 0 simultaneously. You will be prompted to enter the administrator password.
- Press the **OK** key and use the Up Arrow, Down Arrow and OK keys consecutively to select the Admin menu.

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 Section 3.15.1, "Password") after your first login. e

For entering passwords with non-numeric characters, 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) 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.	2 seconds: Ringer off 3 seconds: Beep sound instead of ringer
#	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 IP 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.

2.3.3 How to Set the Terminal Number

Prerequisites

If the user and administrator menus are needed for setup, the terminal number must be configured first. The Terminal number is by default identical with the phone number. 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 capability of the DLS is used.

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.

2.3.4 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 57 for IP address and subnet mask, and [Default Route/Gateway](#) on page 59 for the default route.

2.3.5 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.

IPv4 configuration	
LLDP-MED Enabled	☒
DHCP Enabled	☒
DHCP lease reuse	☐
IP address	192.168.1.203
Subnet mask	255.255.255.0
Default route	192.168.1.2
Route 1 IP address	
Route 1 gateway	
Route 1 mask	
Route 2 IP address	
Route 2 gateway	
Route 2 mask	
Submit Reset	

2.3.6 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 102.

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 61.

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 62.

2.3.8 VLAN Discovery

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 49). The corresponding DHCP option is vendor-specific, thus a specific procedure is necessary.

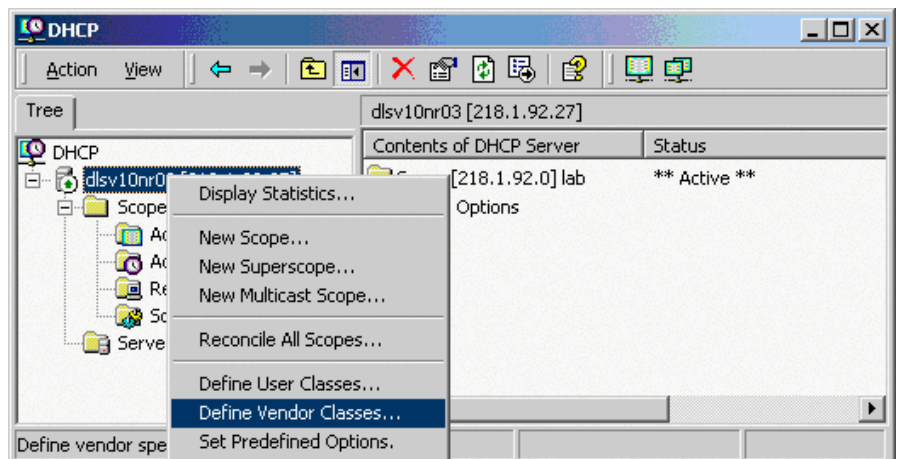
2.3.8.1 How to Use a Vendor Class

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.

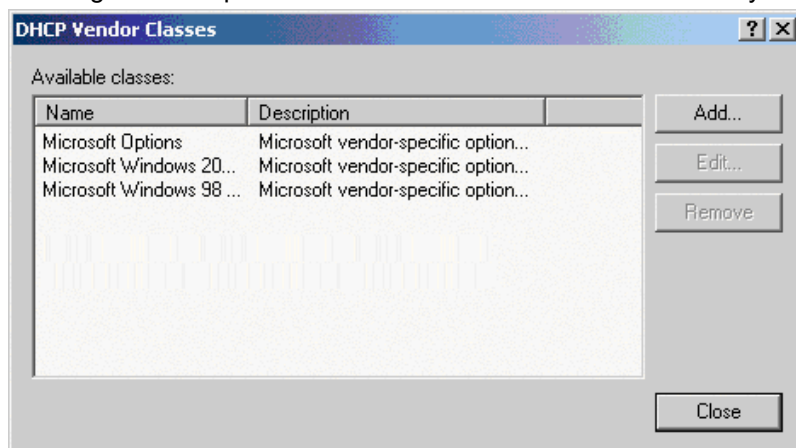
Example: Configuration of the Window DHCP Server

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 **OptiIpPhone** 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).

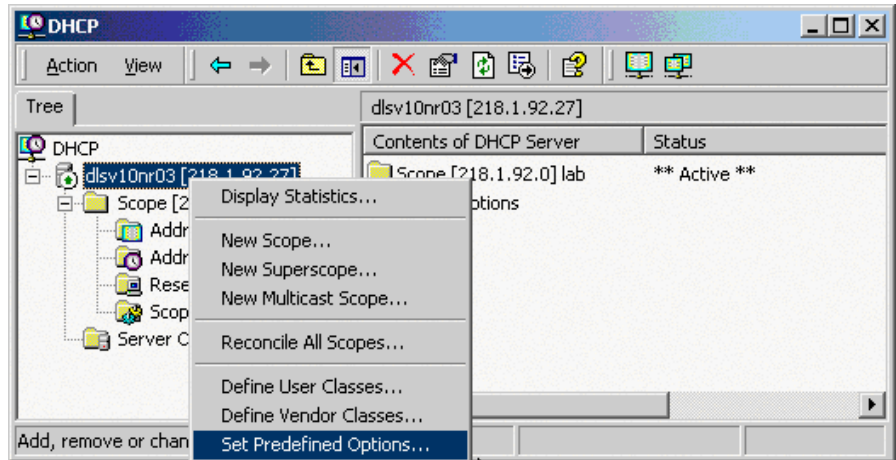
You can use the following command to configure the required option (without error message) so that it is also appears later in the DHCP console:

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

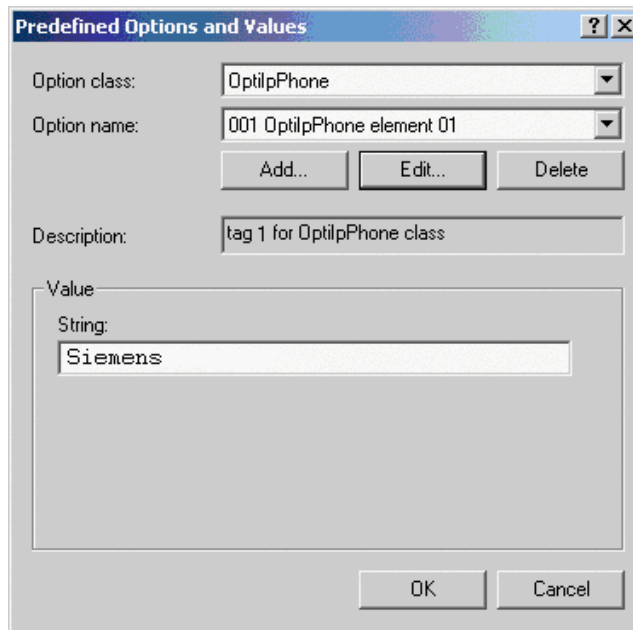
The value **SIEMENS** for optiPoint Element 1 can then be re-assigned over the DHCP console.

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.



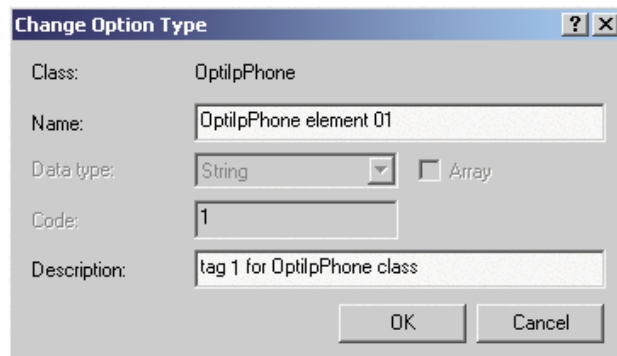
3) Enter the following data for the new option:

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.

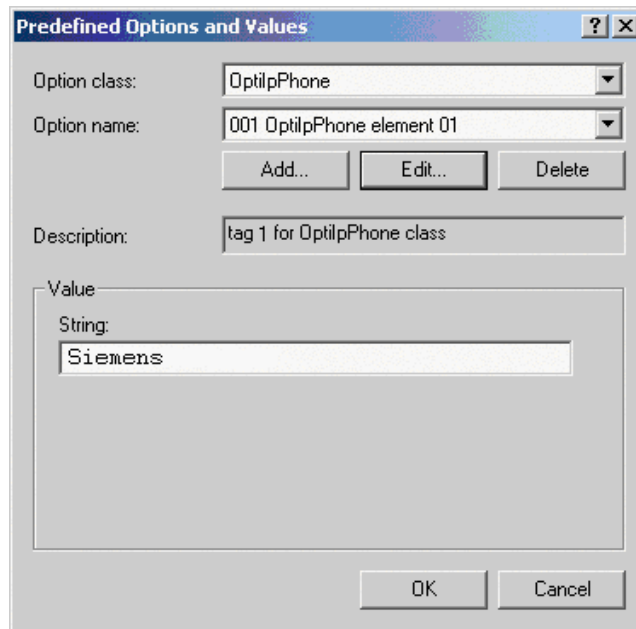


The 'Change Option Type' dialog box is shown. It has a title bar with a question mark and a close button. The fields are: Class: OptilpPhone, Name: OptilpPhone element 01, Data type: String (selected from a dropdown), Array: unchecked checkbox, Code: 1, and Description: tag 1 for OptilpPhone class. There are OK and Cancel buttons at the bottom right.

4) Enter the value for this option.

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

b) **Second Pass:** VLAN ID

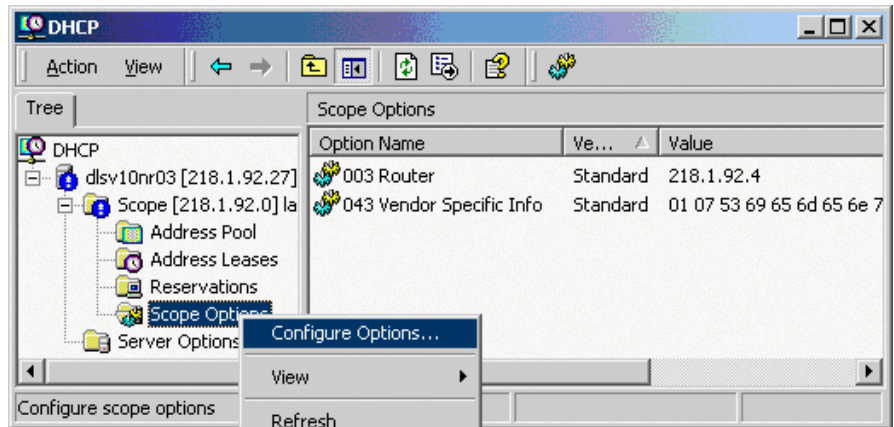


The 'Predefined Options and Values' dialog box is shown. It has a title bar with a question mark and a close button. The fields are: Option class: OptilpPhone (dropdown), Option name: 001 OptilpPhone element 01 (dropdown), Add... Edit... Delete buttons, Description: tag 1 for OptilpPhone class, and a Value section with a String field containing 'Siemens'. There are OK and Cancel buttons at the bottom right.

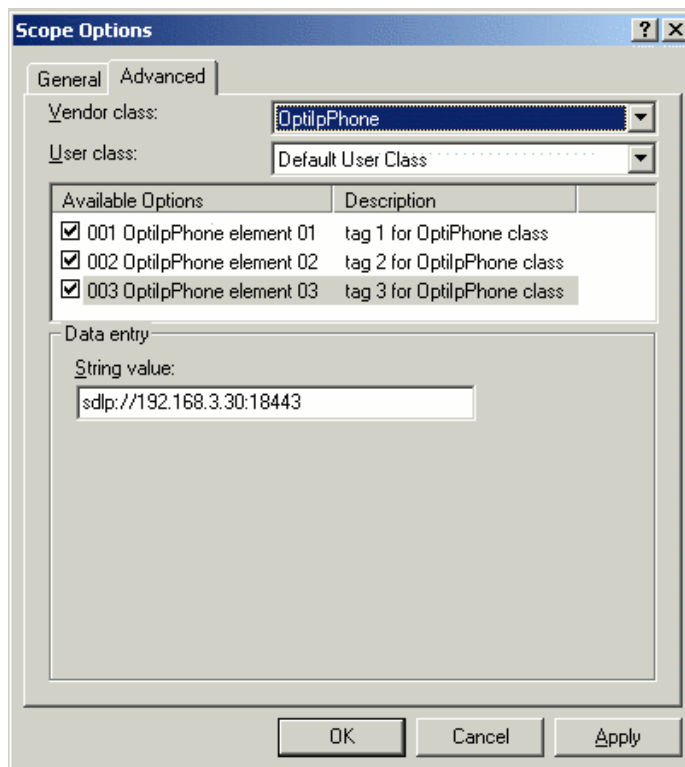
5) Press OK, repeat steps 2 to 4 for the second pass, and press OK again.

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

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":

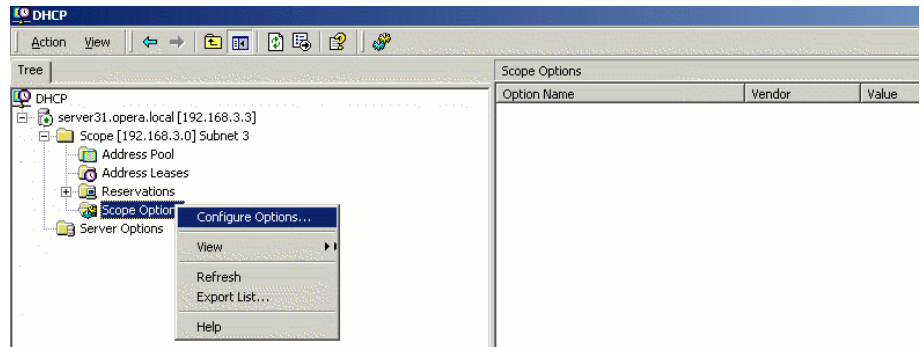
Code	Length	VLAN ID			
2	4	0	0	1	0
02	04	00	00	00	0A

For manual configuration of the VLAN ID see [Manual configuration of a VLAN ID](#) on page 52.

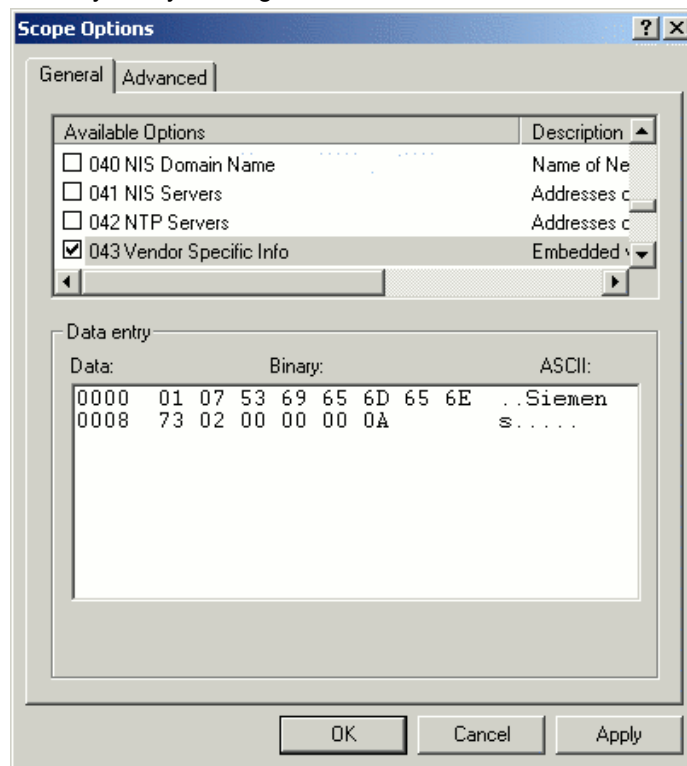
Setup Using the Windows DHCP Server

- 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 65.

For configuration of the DMS see [Set DMS Address via DHCP](#) on page 43.

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.

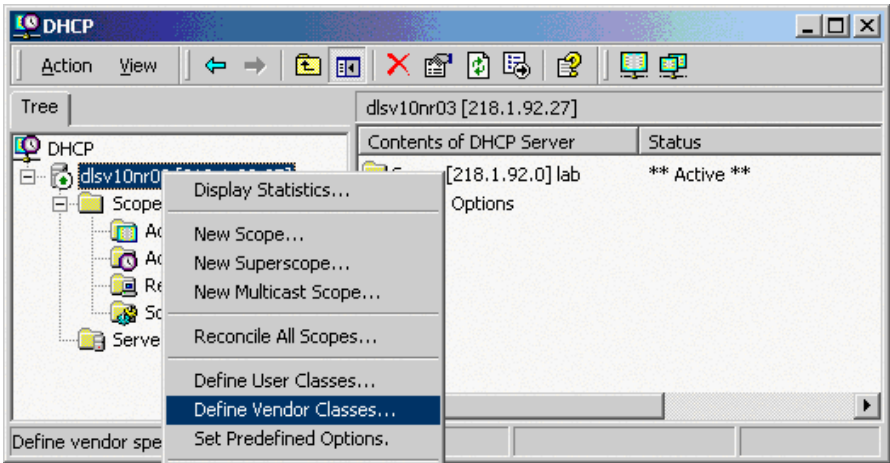
2.3.9.1 Using Vendor Class

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".

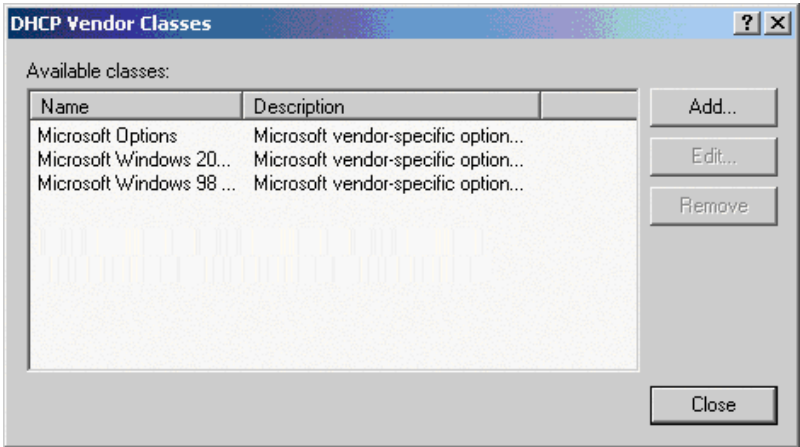
The following steps are required for the configuration of the Windows DHCP server.

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 **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 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 netsh tool in the command line (DOS shell).

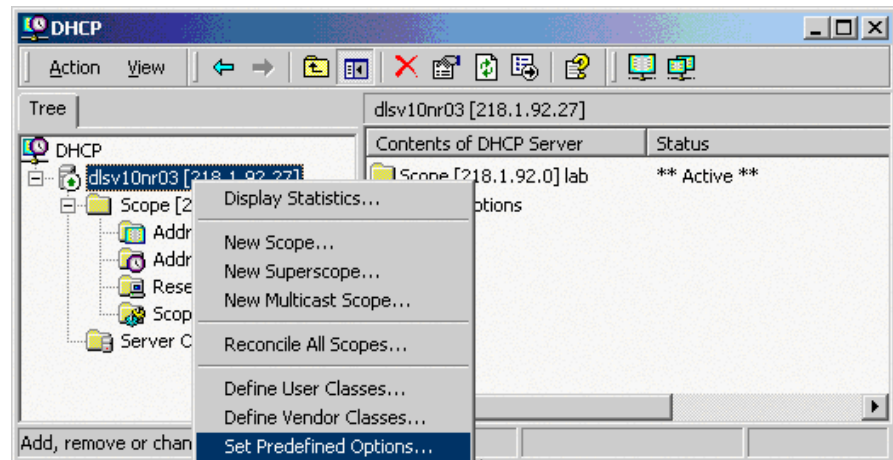
You can use the following command to configure the required option (without error message) so that it is also appears later in the DHCP console:

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

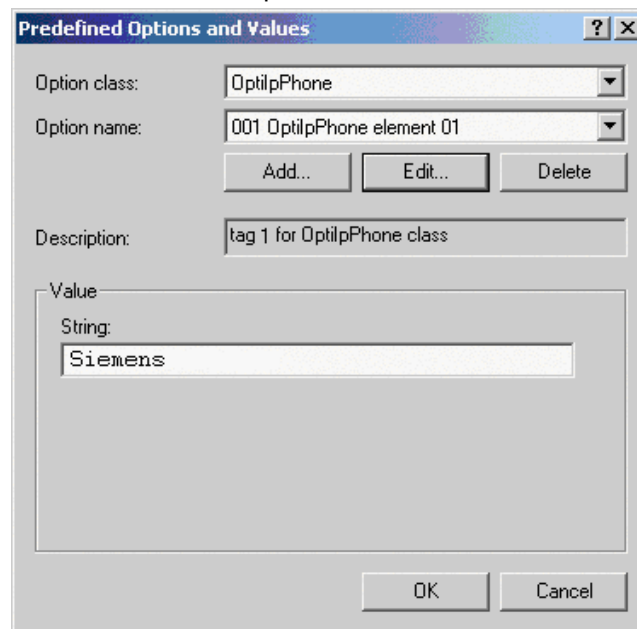
The value **SIEMENS** for optiPoint Element 1 can then be re-assigned over the DHCP console.

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 3

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

4) Enter the value for this option.

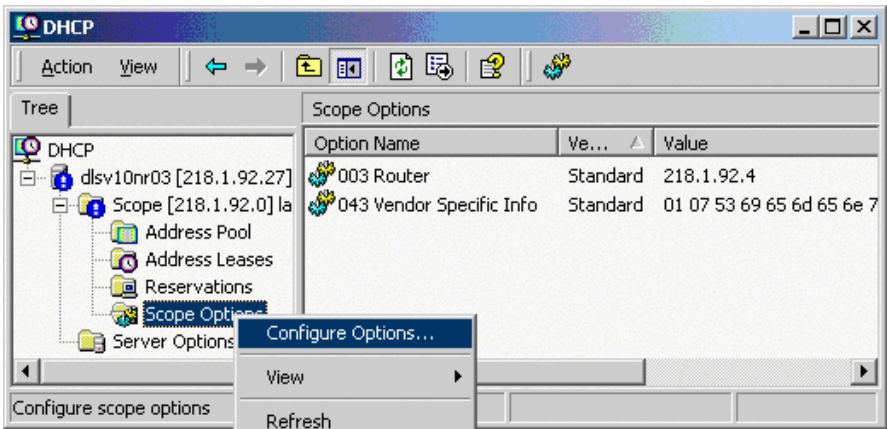
a) First Pass: "Siemens"

- 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

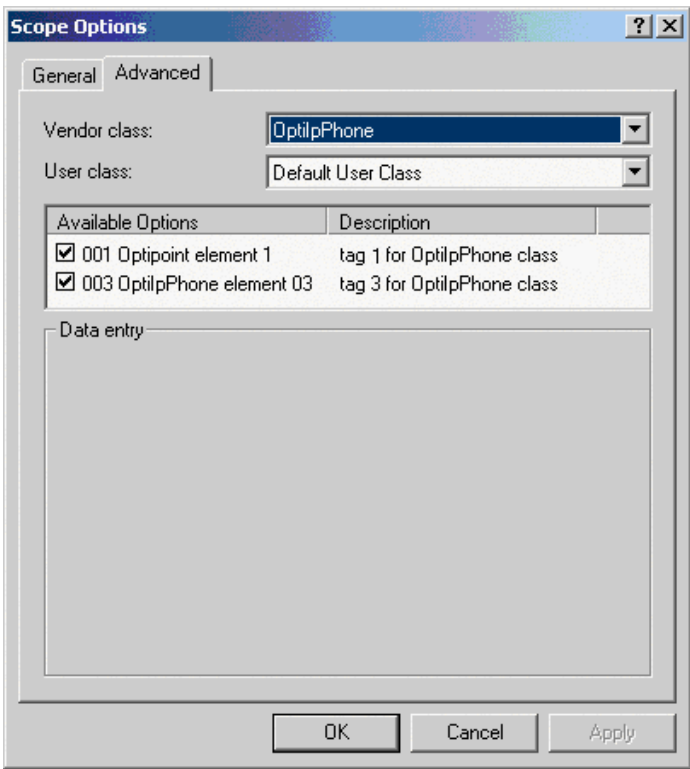
5) Press OK, repeat steps 2 to 4 for the second pass, and press OK again.

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):

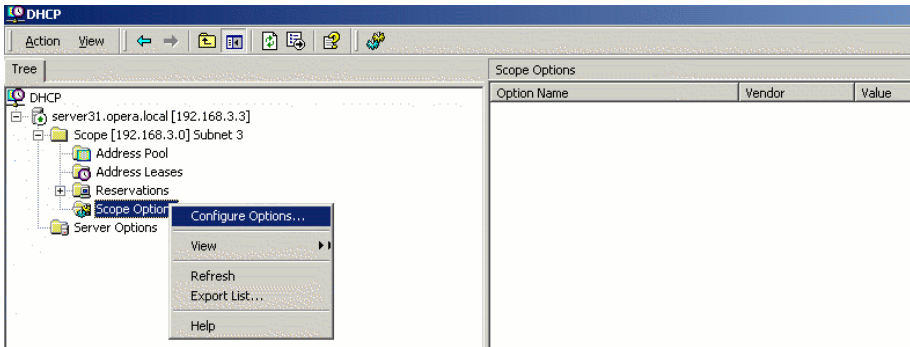
Code	Length	Vendor name						
1	7	S	i	e	m	e	n	s
01	07	53	69	65	6D	65	6E	73

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:

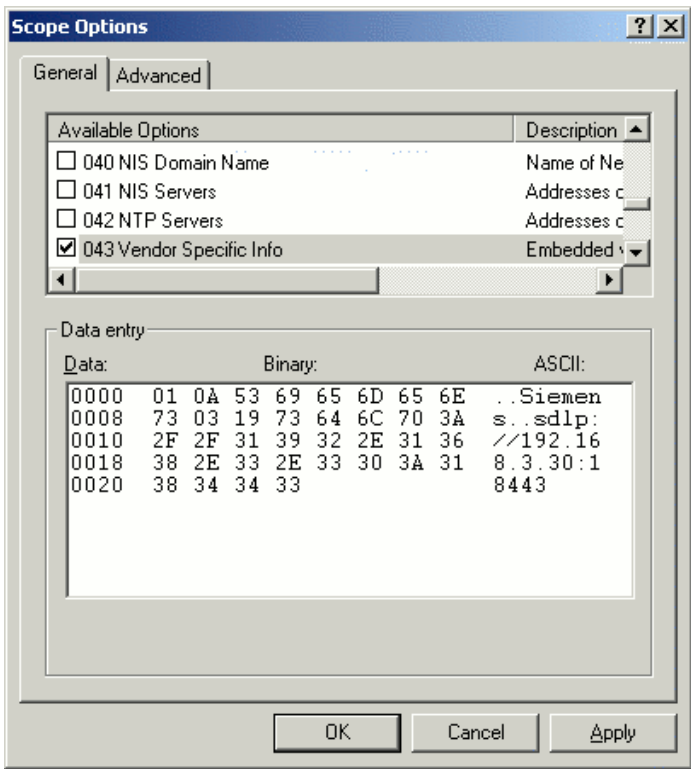
Code	Length	DLS IP address																								
3	25	s	d	i	p	:	/	/	1	9	2	.	1	6	8	.	2	.	1	9	:	1	8	4	4	3
03	19	73	64	6C	70	3A	2F	2F	31	39	32	2E	31	36	38	2E	32	2E	31	39	3A	31	38	34	34	33

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 HFA Gateway Settings

To connect the OpenScope Desk Phone CP phone to the OpenScope Business or OpenScope 4000 Communication System, the IP or DNS address of the gateway, a subscriber number and the corresponding password is needed. The subscriber number can be 1 to 24 characters long, and is used as the internal telephone number.

2.3.11 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 23.
- 2) In the menu at the lefthand side, go to System > Gateway.
- 3) Enter the IP address of the OpenScape Business or HiPath 4000 Communication System in the IP address field.
- 4) In the Subscriber number field, enter the internal extension number of the phone. It can be 1 to 24 characters long.
- 5) Enter the subscriber password in the Password field.

2.3.12 Using the Local Menu

Take the following steps to configure the access to an HFA gateway [Access via Local Phone](#):

- 1) In the administration menu, go to System > Gateway. For further instructions on entering data using the Local menu see Section 2.3.2, "Access via Local Phone".

```
|--- Administration
      |--- System
            |--- Gateway
                  |--- Syatem Type
                  |--- IP address
                  |--- Gateway ID
                  |--- Subscriber number
                  |--- Password
```

- 2) Enter the IP or DNS address of the HFA gateway provided by your OpenScape Communication System.
- 3) Enter the phone's Gateway Id, which will also serve as internal phone number.
- 4) Enter the password associated with the Gateway Id.

After the data has been entered, select **Save & exit** and press **OK**.

2.3.13 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.

2.3.13.1 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	68747470733a2f2f39332E3132322E3131342E39363a3434332f646d73
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.

2.3.13.2 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	68747470733a2f2f39332e3132322e3131342e39363a3434332f646d73

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)

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 23.

3.1 Bluetooth Interface

Bluetooth is available only on OpenScape Desk Phones CP600/CP700/CP700X.

3.1.1 Feature Access

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

Administration via WBM

Bluetooth

Administration via Local Phone

|--- Bluetooth

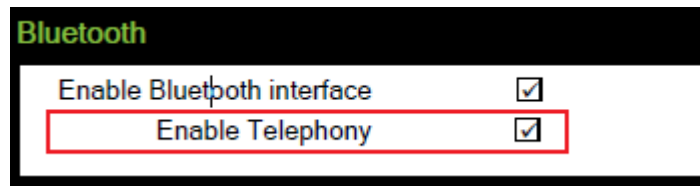
3.1.1.1 Disable HFU

With this feature, Administrator can disable HFU (carkit) functionality.

NOTICE:

If you encounter any problems, contact System Support.

Admin > Bluetooth > Feature access



3.2 LAN Settings

3.2.1 LAN Port Settings

The OpenScape Desk Phone CP phones 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) 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 Ethernet/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 CP205/400/600/700/700X 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"
- **LAN port disabled** (CP700X only): You have the option to disable the LAN port connection when a Wi-Fi network is configured.

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 Link down

PC port speed Any ▼

PC port mode disabled ▼

PC port autoMDIX ☐

Submit Reset

Administration via Local Phone

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

3.2.2 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

3.2.2.1 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

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

First, click on change mode. Afterwards, the IP configuration mode dialog opens.

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
```

3.2.2.2 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". LLDPMED 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

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
```

3.2.2.3 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 49). 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

LLDP-MED operation

Time to live (seconds)

120

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
```

52

A31003-C1000-M102-25-76A9, 11/2025
OpenScape Desk Phone CP Family, Administrator Documentation HFA

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

3.3 IP Network Parameters

3.3.1 Quality of Service (QoS)

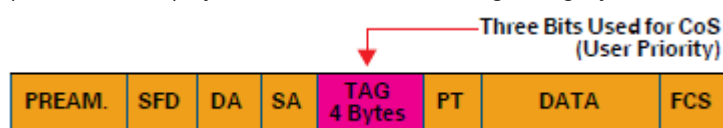
The QoS technology based on layer 2 and the two QoS technologies Diffserv and TOS/IP Precedence based on layer 3 are allowing the VoIP application to request and receive predictable service levels in terms of data throughput capacity (bandwidth), latency variations (jitter), and delay.

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

3.3.1.1 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

Layer 2	☒
Layer 2 voice	5
Layer 2 signalling	3
Layer 2 default	0
Layer 3	☐
Layer 3 voice	EF
Layer 3 signalling	AF31

Administration via Local Phone

```

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

```

3.3.1.2 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 signalling. 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 >

QoS

Layer 2 ☐

Layer 2 voice 5

Layer 2 signalling 3

Layer 2 default 0

Layer 3 ☒

Layer 3 voice EF

Layer 3 signalling AF31

Service

Administration via Local Phone

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

3.3.2 Use DHCP

If this parameter is set to "Yes" (default), the phone will 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, please deactivate this option. In this case, the IP address, subnet mask and default gateway/route must be defined manually.

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

The phone is able to maintain its IP connection even in case of DHCP server failure. For further information, please refer to DHCP Resilience.

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 Route (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)
- VLAN ID, DLS address (Vendor specific Information option 43)

Administration via WBM

Network > General IP configuration

Administration via Local Phone

```
|--- Admin
      |--- Network
            |--- General IP configuration
```

3.3.3 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 ▼
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	

- 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*

Network > IPv6 configuration

IPv6 configuration

Use LLDP-MED ☒

DHCPv6 enabled ☒

Global address

Global address prefix len

Global gateway

Link local address

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

```

3.3.4 Default Route/Gateway

If not provided by DHCP dynamically (see [Use DHCP](#) on page 56), 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

LLDP-MED Enabled

☐

DHCP Enabled

☐

DHCP lease reuse

☐

IP address

192.168.1.105

Subnet mask

255.255.255.0

Default route

192.168.1.2

Route 1 IP address

Route 1 gateway

Route 1 mask

Route 2 IP address

Route 2 gateway

Route 2 mask

Submit

Reset

Administration via Local Phone - IPv4 Configuration

```
|--- Admin
  |--- Network
    |--- IPv4 configuration
      |--- Route (Default)
```

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

Administration via Local Phone - IPv6 Configuration

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

3.3.5 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 - IPv4 Configuration

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 > IPv4 configuration

IPv4 configuration

LLDP-MED Enabled ☐

DHCP Enabled ☐

DHCP lease reuse ☐

IP address

Subnet mask

Default route

Route 1 IP address

Route 1 gateway

Route 1 mask

Route 2 IP address

Route 2 gateway

Route 2 mask

Administration via Local Phone

```
|--- Admin
    |--- Network
        |--- IPv4 Configuration
            |--- Route 1 IP
            |--- Route 1 gateway
            |--- Route 1 mask
            |--- Route 2 IP
            |--- Route 2 gateway
            |--- Route 2 mask
```

3.3.6 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.

3.3.6.1 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 > General IP configuration

Administration via Local Phone

```
|--- Admin
      |--- Network
            |--- General IP configuration
                  |--- DNS domain
```

3.3.6.2 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 > General IP configuration > DNS domain** (see [DNS Domain Name](#) on page 62).

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 > 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
```

3.3.7 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
```

3.3.8 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**.

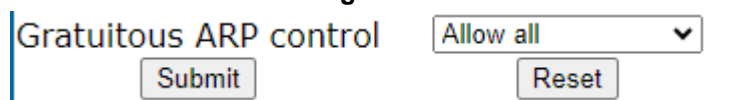
Default is **Allow all**.

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 48.

Administration via WBM

Network > Common settings



s

Administration via Local Phone

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

3.3.9 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), 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. 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.
- **Mode:** Determines 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	18443
Lock DLS address	☐
Revert to default security	☐
Mode	Default
Security PIN	
Device management service (DMS)	
DMS address	
Username	
Password	
Minimum update check (seconds)	300
Update check during working hours	☒
Ignore software update from config file	☐
Check for update	Now
Submit	Reset

Administration via Local Phone

```

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

```

3.3.10 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 specific to OpenScape Desk Phone CP

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.

Data required

- **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.
- **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"
- **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"

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

```

|--- Admin
    |--- System
        |--- SNMP
            |--- Generic traps
                |--- Trap sending enabled
                |--- Trap destination

```

```

|--- Trap destination port
|--- Trap community
|--- Queries allowed
|--- Query password
|--- Diagnostic traps
|   |--- Diagnostic sending enabled
|   |--- Diagnostic destination
|   |--- Diagnostic destination port
|   |--- Diagnostic community
|   |--- Diagnostic to generic
destination
|--- QoS report traps
|--- QoS traps to QCU
|--- QCU address
|--- QCU port
|--- QCU community
|--- QoS to generic dest.
```

3.4 OpenScape Service Menu

The phone's local menu allows for controlling functions provided the OpenScape system. For this purpose, the phone must be logged on at the system. For information on the available functions, see the phone's user manual.

Administration via Local Phone

```
|---Service Menu
```

3.5 Wi-Fi Settings

The OpenScape 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 Wi-Fi within ten seconds, it will try to connect to an unsecured network for ten seconds. If this also fails, it will continue to try these two alternatives for ten seconds each until one succeeds. 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 acquired 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 Disable LAN port

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 System Settings

3.6.1 System Identity

3.6.2 HFA Gateway Settings

To connect the OpenScape Desk Phone CP phone to the OpenScape System, the data described in the following are required.

The Gateway address is the IP address of the communication platform resp. HFA server.

The Gateway port is the port used by the HFA server for signaling messages. Usually, the default value "4060" is correct.

The Subscriber number is used as the internal extension number of the phone. It can be 1 to 24 characters long.

Administration

To log on to the HFA server, a subscriber password must be provided. A new subscriber password can be entered by the administrator.

Data required:

- IP address: IP or DNS address of the communication platform resp. HFA server.
- Subscriber number: The phone's extension.
- Password: Password for logging on to the HFA server.

Optionally, a Gateway ID can be provided. The Gateway ID refers to the PBX/ Gateway/Gatekeeper to which the phone is connected. The value is the same as the "Globid" parameter in the OpenScape 4000 resp. the "H.323 ID" in the OpenScape Business.

The System type is provided by the system the phone is connected to and therefore read-only.

Administration via WBM

System > Gateway

Gateway	
System type	OpenScape Business ▾
IP address	10.12.139.110
Gateway ID	
Subscriber number	230
Password	
Submit Reset	

Network > Port number configuration

Port number configuration

Phone port configuration

Gateway	4060
Standby gateway	4060
RTP base	5010
LDAP server	389
HTTP proxy	0

Server port configuration

System H.225	1720
System Cornet TLS	4061
System H.225 TLS	1300

Standby server port configuration

Standby H.225	1720
Standby Cornet TLS	4061
Standby H.225 TLS	1300

Administration via Local Phone

```

|--- Admin
  |--- System
    |--- Gateway
      |--- System type
      |--- IP address
      |--- Gateway ID
      |--- Subscriber number
      |--- Password
  
```

```

|--- Admin
  |--- Network
  
```

- |--- Port number configuration
- |--- Phone port configuration
- |--- **Gateway**

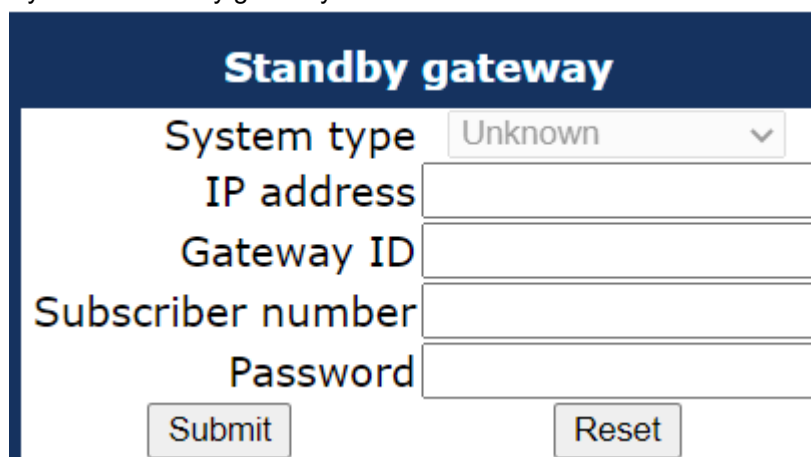
3.6.3 HFA Emergency Gateway Settings

For enabling survivability, the phone switches to a backup communications system in case the main system fails.

The settings are analog to those for the main system (see [Section 3.5.2, âHFA Gateway Settingsâ](#)).

Administration via WBM

System > Standby gateway



Standby gateway

System type

IP address

Gateway ID

Subscriber number

Password

Network > Port number configuration

Port number configuration	
Phone port configuration	
Gateway	4060
Standby gateway	4060
RTP base	5010
LDAP server	389
HTTP proxy	0
Server port configuration	
System H.225	1720
System Cornet TLS	4061
System H.225 TLS	1300
Standby server port configuration	
Standby H.225	1720
Standby Cornet TLS	4061
Standby H.225 TLS	1300
Submit Reset	

Administration via Local Phone

```
|--- Admin
  |--- System
    |--- Standby gateway
      |--- System type
      |--- IP address
      |--- Gateway ID
      |--- Subscriber number
      |--- Password
```

```
|--- Admin
  |--- Network
```

|--- Port number configuration

|--- Phone port configuration

|--- **Standby gateway**

3.6.4 Server and Standby Server ports

In this section, the server ports for signalisation and speech data transfer are determined.

H.225.0 port determines the port used for non-secure H.225 signaling. Default: 1720.

CorNet-TLS port determines the port used for secure communication by the HFA server.

H.225.0 TLS port determines the port used for secure H.225 signaling.

Administration via WBM

Network > Port number configuration

Port number configuration	
Phone port configuration	
Gateway	4060
Standby gateway	4060
RTP base	5010
LDAP server	389
HTTP proxy	0
Server port configuration	
System H.225	1720
System Cornet TLS	4061
System H.225 TLS	1300
Standby server port configuration	
Standby H.225	1720
Standby Cornet TLS	4061
Standby H.225 TLS	1300
Submit Reset	

Administration via Local Phone

```
|--- Admin
    |--- Network
        |--- Port number configuration
        |--- -----Server port configuration
        |-----System H.225
        |-----System Cornet TLS
        |-----Standby H.225 TLS
```

3.6.5 Redundancy

This section controls the switching between main HFA server and standby HFA server.

If Small remote side redundancy is activated, the phone will switch over to the standby HFA server in case the connection to the main server is lost. By default, this is disabled.

When Auto switch back is activated, the phone will switch back to the main server as soon as the connection is re-established. By default, this is disabled.

Retry count main sets the number of trials to establish a connection to the main server before the phone switches over to the standby server. The default is 1.

The Timeout main parameter determines the time interval between the last try to get a connection to the main server and the establishing of a connection to the standby server. The default is 30 seconds.

Retry **Count Standby**: Sets the number of trials to establish a connection to the standby server before the phone switches back to the main server. The default is 3.

- **Timeout Standby**: Timeout between two "Retry count standby". The default is 30 seconds.
- **Timeout main**: Timeout between two "Retry count main" The default is 30 seconds.
- **TC test retry**: TC_Test retry determines the count of how many successful TC_Tests the Main system needs to answer before the phone switches back, if Auto switchback is enabled. The default is 3.
- **TC Test Expiry**: Determines how long the Previous connection needs to timeout to actually trigger any further SRSR activities.
- How much time to wait from one unsuccessful Retry count main sequence until the next happens and in which interval the phone will send itself a TC_Test message (in idle mode). The default is 30 seconds.

Lowering this value will significantly increase network load but the phone might detect failures faster but at an increased risk of false positive detections due to short time network outage.

After changing the timing values, the SRSR needs to be deactivated and reactivated for the changes to take effect.

Administration via WBM

System > Redundancy

Redundancy	
Small remote site redundancy	☐
Auto switch back	☐
Retry count main	1
Retry count standby	3
Timeout main	30
Timeout standby	30
TC test retry	3
TC test expiry	30
Submit	Reset

Administration via Local Phone

```
|--- Admin
|--- System
|--- Redundancy
|--- Small remote site redundancy
|--- Auto switch back
|--- Retry count main
|--- Retry count standby
|--- Timeout main
|--- Retry count standby
|--- Timeout standby
|--- TC test retry
|--- TC test expiry
```

3.6.6 Emergency number

E.911 emergency number. This number establishes a connection to the PSAP (Public Safety Answering Point). If a user dials this number, and an appropriate LIN (see [Section 3.5.7, âLINâ](#)) is configured, the user's location is communicated to the PSAP. In the USA, the number is 911.

Administration via WBM

System > Features > Configuration

Configuration	
General	
Emergency number	
LIN	
Not used timeout (minutes)	2
AlertBar LED hint	☐
FPK Name	<lastname>, <firstname> ▼
Allow user downloads	☐

Administration via Local Phone

```

|--- Admin
  |--- System
    |--- Features
      |--- Configuration
        |--- General
          |--- Emergency number
          |--- LIN
          |--- Not used timeout (minutes)
          |--- AlertBar LED hint
        |--- Telephony settings
          |--- Enable telephony settings
  
```

3.6.7 LIN

The Location Identification Number is a number code which provides detailed geographic information about the phone, including e. g. the office room. On issuing an emergency call using the E.911 emergency number (see [Section 3.5.6, âEmergency numberâ](#)), this code is transferred to an ALI (Automatic Location Information) system in the public network. When the ALI has looked up the location data in its database, it transmits the data along with the call to the PSAP. The emergency operator is presented with the location data in readable form, so he can dispatch help as appropriate.

Administration via WBM

Configuration	
General	
Emergency number	
LIN	
Not used timeout (minutes)	2 ▼
AlertBar LED hint	☐
FPK Name	<lastname>, <firstname> ▼
Allow user downloads	☐

Administration via Local Phone

```

|--- Admin
  |--- System
    |--- Features
      |--- Configuration
        |--- General
          |--- Emergency number
            |--- LIN
              |--- Not used timeout (minutes)
                |--- AlertBar LED hint
                  |--- Telephony settings
                    |--- Enable telephony settings

```

3.6.8 Not Used Timeout

NOTICE: This is available only on OpenScape Desk Phone CP400/600/600E/700/700X phones

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 five minutes. The default value is 2.

Administration via WBM

System > Features > Configuration

Configuration	
General	
Emergency number	
LIN	
Not used timeout (minutes)	2 ▼
AlertBar LED hint	☐
FPK Name	<lastname>, <firstname> ▼
Allow user downloads	☐

Administration via Local Phone

```

|--- Admin
  |--- System
    |--- Features
      |--- Configuration
        |--- General
          |--- Emergency number
          |--- LIN
          |--- Not used timeout (minutes)
          |--- AlertBar LED hint
        |--- Telephony settings
          |--- Enable telephony settings

```

3.6.9 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

LIN

Not used timeout (minutes)

AlertBar LED hint

FPK Name

Allow user downloads

2

<lastname>, <firstname>

Bluetooth

Enable bluetooth interface

Enable telephony

Services

Web based manag.

USB device access

USB power using PoE

120mA (up to 4 KMs)

Telephony settings

Enable telephony settings

Submit

Reset

Administration via Local Phone

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

3.6.10 Enable telephony settings

NOTICE: This is available only on OpenScope Desk Phone CP400/600/600E/700/700X phones.

Users can access limited menu options and set basic telephony settings without the need of a password. Since the administrator enables the option "Enable telephony settings", the item "Configure telephone" appears on the telephone screen while navigating from the idle menu to Service/Settings. The user password is not required to navigate to this option. The option is disabled by default.

Administration via WBM

System > Features > Configuration

Configuration	
General	
Emergency number	
LIN	
Not used timeout (minutes)	2
AlertBar LED hint	☐
FPK Name	<lastname>, <firstname> ▼
Allow user downloads	☐
Bluetooth	
Enable bluetooth interface	☒
Enable telephony	☒
Services	
Web based manag.	☒
USB device access	☒
USB power using PoE	120mA (up to 4 KMs) ▼
Telephony settings	
Enable telephony settings	☐
Submit	Reset

Administration via Local Phone

```

|--- Admin
  |--- System
    |--- Features
      |--- Configuration
        |--- General
          |--- Emergency number
          |--- LIN
          |--- Not used timeout (minutes)
          |--- AlertBar LED hint
        |--- Telephony settings
          |--- Enable telephony settings
  
```

3.6.11 Energy Saving

3.6.11.1 Energy Efficient Ethernet (OpenScape Desk Phone CP205/400/600/600E 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.

3.6.12 Local Features

3.6.12.1 Direct video

On CP600/CP600E/700/700X phones it is possible to stream video content to the phone's display by controlling an external supported camera via a URL, triggered by Free Programmable Key or menu item. Up to 4 cameras can be configured.

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.

Data required:

- Direct video enabled (mandatory): tick to enable the feature.
- Name (mandatory): freely selectable name for the camera (can be custom name or alphanumeric).
- Protocol: protocol to transmit video, RTSP and HTTP.
- Address (mandatory): IP address or DNS name of the video server (e.g 10.10.10.1 or mycamera.local.net)
- Port (optional): target port at the server, if it is not entered 80 will be used.
- URL path (optional): URL path of the camera, e.g /videoapi/stream/
- Username: enter username for the camera.
- Password: enter password for the camera.
- Door opener (optional): name of the associated door if it configured.

Administration via WBM

System > Features > Direct video

Direct video	
Direct video enabled	☐
Camera 1	
Name	<i>Camera 1</i>
Protocol	RTSP v
Address	
URL	
Port	0
Username	
Password	
Door opener	None v
Camera 2	
Name	<i>Camera 2</i>
Protocol	RTSP v
Address	
URL	
Port	0
Username	
Password	
Door opener	None v

Camera 3

Name	Camera 3
Protocol	RTSP ▼
Address	
URL	
Port	0
Username	
Password	
Door opener	None ▼

Camera 4

Name	Camera 4
Protocol	RTSP ▼
Address	
URL	
Port	0
Username	
Password	
Door opener	None ▼

Administration via Local Phone

In the administration menu, go to **System Features > Local Features > Direct video**. The path is as follows:

```

|--- Admin
    |--- System
        |--- Features
            |--- Direct video
                |--- Direct video enabled
                |--- Name
                |--- Protocol
                |--- Address
                |--- URL
                |--- Port
                |--- Username
                |--- Password
                |--- Door opener
  
```

3.6.12.2 Door opener

OpenScape CP phones support up to 4 door openers. Each of them can be controlled independently by using one of the available control methods under the Door opener menu.

Administration via WBM

To select a control method for the door openers navigate to **System > Local features > Door opener** and click on the arrow icon to open the list of options. The available options are:

- Disabled
- Call to open door
- HTTP request to open door
- HTTPS request to open door

Once a control method is selected, click the Edit button to configure the door opener.

Door opener	
Door opener 1 - type	Disabled Edit
Door opener 2 - type	Disabled Edit
Door opener 3 - type	Disabled Edit
Door opener 4 - type	Disabled Edit

The configuration of the door openers depends on the selected control method. Fill in the required data and then click on Submit button.

Data required

If the selected control method is Call to open door fill in the following fields:

- Name (mandatory): freely selectable name for the door opener (can be custom name or alphanumeric).
- Phone Number (mandatory): the phone number controlling the door opener.
- Pin (mandatory): the PIN to open the door, same PIN as configured at Door opener device.
- FPK confirmation to open door (optional): confirmation key to open the door, default value is true.
- Associated camera: name of the associated camera.
- Automatic Door Video: 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.

DoorOpener 1	
Door opener type - Call to open door	
Name	DoorOpener 1
Phone Number	
Pin	
FPK confirmation to open door	☒
Submit	Reset

- If the selected control method is HTTP request to open door fill in the following fields:
- Name (mandatory): freely selectable name for the door opener (can be custom name or alphanumeric).
- Address (mandatory): IP address or DNS name of the door opener server e.g 10.10.10.1 or mydoor.local.net
- Port (optional): target port at the server, if it is not entered 80 will be used.
- URL path (optional): URL path of the door opener, e.g /door1/opencommand/
- URL parameters (optional): parameters inside the URL path e.g. user=name&auth=123456
- Phone Number (optional): associated door phone number, it will be used to recognize incoming call from doorphone
- FPK confirmation to open door (optional): confirmation key to open the door, default value is true.
- Associated camera: name of the associated camera.
- Automatic Door Video: 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.

DoorOpener 1	
Door opener type - HTTP request to open door	
Name	DoorOpener 1
Method	POST
Address	
Port	0
Username	
Password	
URL path	0
URL parameters	
Phone Number	
FPK confirmation to open door	☒
Submit	Reset

- If the selected control method is HTTPS request to open door fill in the following fields:
- Name (mandatory): freely selectable name for the door opener (can be custom name or alphanumeric).
- Address (mandatory): IP address or DNS name of the door opener server e.g 10.10.10.1 or mydoor.local.net
- Port (optional): target port at the server, if it is not entered 80 will be used.
- URL path (optional): URL path of the door opener, e.g /door1/opencommand/
- URL parameters (optional): parameters inside the URL path e.g. user=name&auth=123456
- Phone Number (optional): associated door phone number, it will be used to recognize incoming call from doorphone
- FPK confirmation to open door (optional): confirmation key to open the door, default value is true.
- Associated camera: name of the associated camera.
- Automatic Door Video: 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.

DoorOpener 1	
Door opener type - HTTPS request to open door	
Name	DoorOpener 1
Method	POST
Address	
Port	0
Username	
Password	
URL path	0
URL parameters	
Phone Number	
FPK confirmation to open door	☒
Submit Reset	

Administration via Local Phone

In the administration menu, go to System > Local Features > Door Opener. The path is as follows:

```
|--- Admin
    |--- System
        |--- Local Features
```

- |--- Door Opener
 - |--- Door Opener 1 -type
 - |--- Door Opener 2-type
 - |--- Door Opener 3-type
 - |--- Door Opener 4-type
 - |--- Call to open door
 - |--- Name
 - |--- Phone Number
 - |--- Pin
 - |--- FPK confirmation to open door
 - |--- Associated camera
 - |--- HTTP request to open door
 - |--- Name
 - |--- Address
 - |--- Port
 - |--- URL path
 - |--- URL parameters
 - |--- Phone Number
 - |--- FPK confirmation to open door
 - |--- Associated camera
 - |--- HTTPS request to open door
 - |--- Name
 - |--- Address
 - |--- Port
 - |--- URL path
 - |--- URL parameters
 - |--- Phone Number
 - |--- FPK confirmation to open door
 - |--- Associated camera
 - |--- Automatic Door Video

3.6.13 Security

3.6.13.1 System

OpenScape Desk Phone CP phones support the following security option:

- PKI-based SPE (Signaling and Payload Encryption)

The security settings are be configured separately for the main gateway and for the fallback gateway (standby) when using SRSR (Small Remote Site Redundancy).

The Signalling transport main/standby parameter selects the protocol to use for signalling. TCP and TLS are available.

Certificate validation main/standby shows whether the phone certificate used for encrypted logon via TLS is checked against the certificate on the gateway (read only). For configuration see [Authentication Policy](#) on page 146.

NOTICE:

For further information on deploying SPE, please refer to the manual of the OpenScape system in use, and to the Deployment Service Administration manual.

Data required

- **Validate SW upgrade:** validates if the uploaded Phone software is compatible with the phone.
- **Signalling transport main:** Protocol to use for signalling when the main gateway is in use. Value range: "TCP", "TLS".
- **Signalling transport standby:** Protocol to use for signalling when the standby gateway is in use. Value range: "TCP", "TLS".
- **Certificate validation main:** Check the phone certificate against the gateway certificate when the main gateway is in use (read only). Value range: true, false.
- **Certificate validation standby:** Check the phone certificate against the gateway certificate when the main gateway is in use (read only). Value range: true, false.
- **TLS renegotiation:** Check whether Server accepts TLS renegotiation. Value range:
 - Insecure allowed: Server without TLS renegotiation are accepted.
 - Secure (RFC5746): Only server with TLS renegotiation are allowed.
- **DoS protection:** Check to enable DoS protection. When enabled, phone will limit bandwidth to:
 - HI: 15Mbps
 - LO: 15 Mbps, 3 Mbps during media processing

Default state is Enabled. If disabled, there is no limitation.

Administration via WBM

System > Security > System

System

Validate SW upgrade	☒
Signalling transport main	TCP ▼
Signalling transport standby	TCP ▼
Certificate validation main	☐
Certificate validation standby	☐
TLS renegotiation	Insecure allowed ▼
DoS protection	☐
Submit	Reset

Administration via Local Phone

```

|--- Administration
    |--- System
        |--- Security
            |--- System
                |--- Signalling main
                |--- Signalling stdby
                |--- Certificate main
                |--- Certificate stdby
                |--- TLS renegotiation
                |--- DoS protection
  
```

3.6.13.2 Access control

The CCE access parameter controls TCP and UDP access for the CCE (CommsChannel Extender). This affects the operation of 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 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 (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. Other interfaces are 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
|
|---Disable local lock
|
|--- WBM TLS interface
|
|--- Server TLS interface
```

3.6.13.3 Security Log

A circular 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.

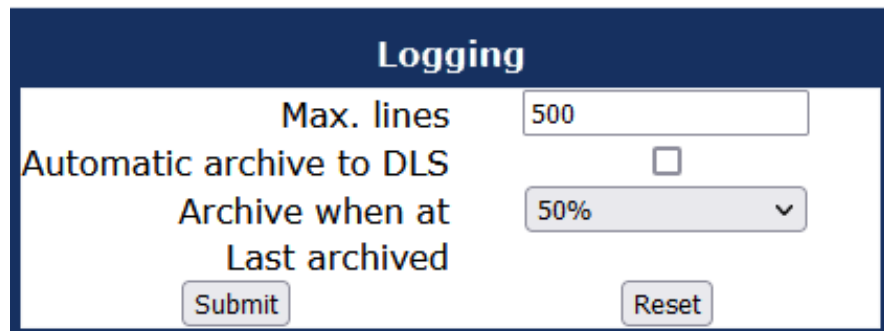
- The Max. lines parameter defines the maximum number of entry lines that can be kept in the security log before old entries are overwritten by new entries.
- Automatic archive to DLS controls whether the log is sent to the DLS. When activated, the DLS is used to automatically archive the security log 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 unachieved entries, the phone will initiate an upload.
 - If "Automatic archive to DLS" is NOT enabled and the security log reaches the threshold % for unachieved 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
        |--- Automatic archive to DLS
        |--- Archive when at
        |--- Last archived
```

3.6.13.4 Security-Related Faults

The phone reports specific security events for the DLS to display as alarms.

- **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
```

3.6.13.5 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.

3.6.13.5.1 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 successful 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	login.microsoftonline.com
Tenant ID	common
Client Id	
Client Secret	
Redirect address for user login	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

```

3.6.13.5.2 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.

✓ **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.

3.7 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.

3.7.1 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

Administration via Local Phone

```
|--- Administration
    |--- Date and Time
        |--- Time source
            |--- SNTP IP address
            |--- Timezone offset
```

3.8 Dialing

3.8.1 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 106).

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

Canonical dial	
Internal numbers	Local enterprise form ▼
External numbers	National public form ▼
External access code	For external numbers ▼
International gateway code	Leave as + ▼
Submit Reset	

- 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 106).

- **"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 dialed 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 dialed as national numbers. Numbers for a different country are dialed 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
```

3.8.2 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 103), 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 103)
- Local area code ([Canonical Dialing Configuration](#) on page 103)
- Local enterprise code ([Canonical Dialing Configuration](#) on page 103)

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	

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 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
```

3.9 Ringer

The HFA 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. A list of different ring types is maintained in the phone.

3.9.1 Local ringers

Administration via WBM

Admin > Ringer > Local ringers

Local ringers			
Name	Ringer sound	Pattern melody	Pattern sequence
Attention Emergency	Pattern	1	2
	Pattern	1	2
	Pattern	1	2
	Pattern	1	2
Submit		Reset	

Date required

- **Name:** Selects the call type to be used.

NOTICE: In OpenScape 4000, for "Speaker call" function the call type "Rollover call" is used in the CorNet AU_RINGER_START message. Value range OpenScape 4000: "Internal call", "External call", "Buzz call", "Rollover call", "Alert (simple)", "Alert (multiple)", "Special #1", "Special #2", "Special #3", "Attention ringer", "Unspecified call", " US DSN precedence ring", "US DSN routine ring", "Emergency call" Value range OpenScape Business: "Internal call", "External call", "Attention ringer" Default: "Internal call".

- **Ringer sound:** "Pattern" or the name of the selected ring tone file. Sets the distinctive ringer to use the currently set pattern (melody and sequence). This is the pattern that will be used if the configured ring tone file cannot be played for any reason.

- Value range: "Pattern", "<audio file>"
Default: "Pattern".
- **Pattern melody:** Selects the melody pattern that will be used if Ringer sound is set to "Pattern".
- Value range: "1"... "8"
Default: "2".
- **Pattern sequence:** Determines the length for the melody pattern, and the interval between the repetitions of the 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: "2".

Administration via Local Phone

There is no configuration necessary to set the names. CorNet specifies the ringer types and enumerations. Please be aware that the naming refers to the call type as sent in the CorNet message, not to be confused with a feature or a call scenario. The mapping of call type to feature or call scenario occurs in the system and this may be configurable (e.g. in HiPath 4000 by means of AMO ZAND). It is up to the administrator to configure such that the user hears the required ring tones for the various features/call scenarios. Also note that only the set of call types actually implemented by the system should be offered for configuration of the ringers.

Currently OpenScape Business only implements a subset of those in CorNet. It is assumed that this set is relatively stable.

```
|--- Admin
    |--- Settings
        |--- Ringer
            |--- Local ringer
                | |--- Name
                | |--- Ringer sound
                | |--- Ringer melody
                | |--- Pattern sequence
```

3.9.2 Ringer settings for CP100/CP200

You can select the ringer mode.

For CP100/200 Phones, any ringer sound may either be

- OpenScape specified tones
- Local ringer (selected from the pool of ringer files on the phone)

Administration via WBM

Admin > Ringer > Ringer setting

Once ringing is configured locally a system control of the ringer parameters is not possible. If system control of the ringer is desired the ringer mode must be set to "OpenScape".

Even though the ringers are configured locally the behaviour of the ringers should be the same as system controlled ones. In particular, cyclic ringers shall be played endlessly until the switch commands to stop playing (and therefore repeated if necessary), whereas single shot ringers should play for just a short period - the intention being to alert the phone user to a new state of the phone but not to hinder the ongoing conversation. This short period is defined to be 3 seconds. It should be possible to interrupt the playing of the cyclic ringer to play the single shot ringer and after timeout the cyclic ringing should resume. This behaviour is independent of whether low or high quality ringer files are played or whether the ringer is pattern generated.

The value in Octet 12 in the CorNet AU_RINGER_START message is used as an index into ringers configured on the phone. The indexed entry indicates the ringing to be used for the call.

In any cases if a distinctive ring is requested then the associated ring type is used instead of the default ringer. The ringing is played immediately when requested. If distinctive ringing is not requested or cannot be matched to a ringer then, the tone specified in the CorNet ringer message by the OpenScape system will be used to construct the ring tone.

Administration via Local Phone

```
|--- Admin
      |--- Ringer
            |--- Ringer Setting
                  |--- Ringer mode
                        |--- |--- OpenScape
                              |--- |--- Local ringer
```

3.9.3 Ringer settings for CP400/600/700

You can allow the user to change ringer settings, select the ringer mode and set an emergency ringer mode.

For CP400/600/700 Phones, any ringer sound may either be

- OpenScape specified tones
- Local ringer (selected from the pool of ringer files on the phone)

User changeable: Check the checkbox to allow user to change distinctive ringer settings, i.e. change the ringer volume.

Value range:

- Enabled
- Disabled

Default: Disabled.

Emergency ringer mode: Determines the ringer parameters.

Value range:

- "Normal": emergency ringer follows the distinctive ringing rules.
- "Always": the phone plays the emergency ringer configured as that ringer at maximum volume overriding any other ringer control settings and preventing the user from changing the ringer parameters even if User changeable is checked.

Default: "Normal".

Admin > Ringer > Ringer setting

Ringer setting

User changeable ☒

Ringer mode OpenScape ▾

Emergency ringer mode Normal ▾

Administration via Local Phone

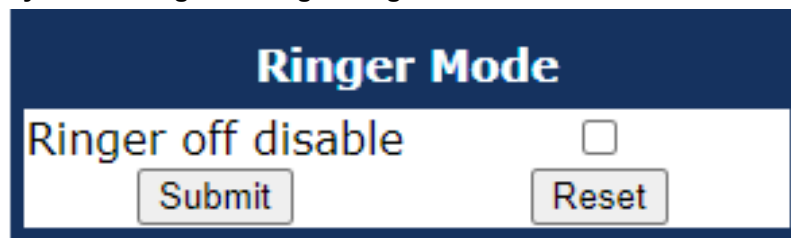
```
|--- Admin
    |--- Ringer
        |--- Options
        |--- User changeable
        |--- Ringer mode
        |--- |--- OpenScape
        |--- |--- Local ringer
        |--- Emergency ringer mode
        |--- |--- Normal
        |--- |--- Always
```

3.9.3.1 Ringer Mode

Ringer Mode allows you to disable the the "Ringer off" option.

Administration via WBM

System > Ringer Setting > Ringer Mode



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 **Key function unavailable** is displayed for a CP400/600/700 phone.

NOTICE: The temporary muting of the ringer using a short press of the * key remains functional. Only the "Ringer off" and the "Ringer silence" 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.

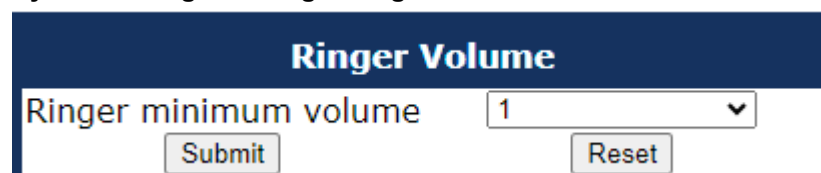
3.9.3.2 Ringer Volume

You can specify the ringer levels of the CP400/600/700 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.

3.10 User Mobility

The Set Mobility Mode parameter controls the behaviour of the phone if mobile user logs on to the phone. The following settings are possible:

- Basic (Default): When a new user logs on at the phone, all user data of the precedent user will be shown.
- Data Privacy: When a new user logs on at the phone, an empty conversation list will be presented to the mobile user. When the mobile user logs off, all conversation list entries which have been created while he was using the phone, will be deleted. No synchronization to and from DLS will happen.

3.11 Free Programmable Keys

The OpenScape Desk Phone CP700 comes with 12 free programmable keys with LED (red/green/amber), all of which can be programmed on two separate levels. The 6 first programmable keys are permanently displayed on the left panel. The 6 last programmable keys are available in Favorites. The number of programmable keys can be increased by attaching one or more OpenScape Key Module 600s to your phone.

The OpenScape Desk Phone CP400 phone provides 16 free programmable keys (FPKs) which can be associated with special phone functions. This is called „Phone keys“. On the OpenScape Desk Phone CP600 12 free programmable permanent favourites are provided, which can be associated with special phone functions.

The OpenScape Desk Phone CP400 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 phone provides four free programmable keys (FPKs). This is called „Phone keys“.

The key programming can be accessed via the WBM, via the Local Phone and via DMS.

3.11.1 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

Feature Key



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.

Feature Key

Redial

▼

Edit

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.

3.12 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/CP700X:** 100MB
 - **OpenScape Desk Phone CP600:** 100 MB
 - **OpenScape Desk Phone CP400:** 100 MB
 - **OpenScape Desk Phone CP200/CP205:** 25 MB
 - **OpenScape Desk Phone CP100:** 25MB
-

3.12.1 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 web form titled "Picture clip". It contains the following elements:

- A checkbox labeled "Use defaults" which is unchecked.
- A dropdown menu for "Download method" set to "FTP".
- A text input field for "FTP server address".
- A text input field for "FTP server port" with the value "21".
- A text input field for "FTP account".
- A text input field for "FTP username".
- A text input field for "FTP password" with masked characters ".....".
- A text input field for "FTP path" with the value "media".
- A text input field for "Filename".
- A dropdown menu for "After submit" set to "start download".
- "Submit" and "Reset" buttons at the bottom.

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

This is an identical screenshot of the "Picture clip" configuration panel as described above, showing the same fields and values.

3.12.2 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.

3.12.3 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

The screenshot shows a web interface titled "Defaults" with a dark blue header. Below the header, there are several input fields and a dropdown menu. The "Download method" is set to "FTP" with a dropdown arrow. The "FTP server address" is an empty text box. The "FTP server port" is set to "21". The "FTP account", "FTP username", "FTP password", and "FTP path" are all empty text boxes. At the bottom of the form, there are two buttons: "Submit" and "Reset".

Administration via Local Phone

```
|--- Admin
    |--- File Transfer
        |--- Defaults
            |--- Download method
            |--- FTP server address
            |--- FTP server port
            |--- FTP account
            |--- FTP username
            |--- FTP password
            |--- FTP path
```

3.12.4 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 its 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
 - **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
- If **NOT compatible**: Abandon update and return to original application

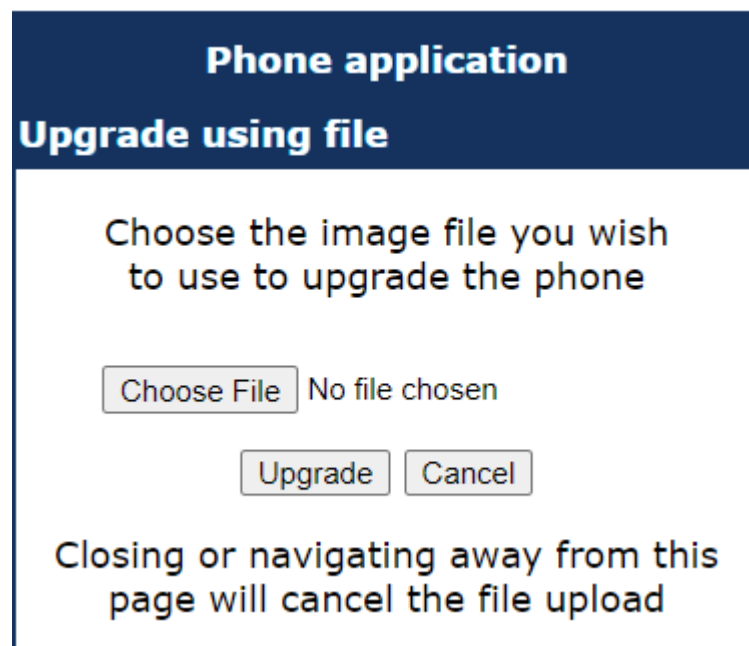
NOTICE: Do not disconnect the phone from the LAN or power unit during software update. An active update process is indicated by blinking LEDs and/or in the display.

3.12.4.1 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



The screenshot shows a web interface for upgrading a phone application. At the top, there is a dark blue header with the text 'Phone application' and 'Upgrade using file' in white. Below the header, the main content area has a light blue background. It contains the text 'Choose the image file you wish to use to upgrade the phone' in bold. Below this text is a button labeled 'Choose File' and the text 'No file chosen'. Further down are two buttons labeled 'Upgrade' and 'Cancel'. At the bottom of the main content area, there is a warning message: 'Closing or navigating away from this page will cancel the file upload'.

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.

3.12.4.2 Upgrade using FTP/HTTPS

If the default FTP/HTTPS access settings (see [Common FTP/HTTPS Settings \(Defaults\)](#) on page 116) 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**

Upgrade using FTP/HTTPS

Use defaults ☐

Download method FTP ▼

FTP server address 10.12.82.56

FTP server port 60025

FTP account

FTP username openstage

FTP password

FTP path /Images

Filename OS_WE34_HI_HFA_V1_R

After submit do nothing ▼

Submit Reset

Administration via Local Phone

```
|--- Admin
|--- File Transfer
|--- Phone application
|--- Use default
|--- Download method
|--- FTP server address
|--- FTP server port
```

```
|--- FTP account  
|--- FTP username  
|--- FTP password  
|--- FTP path  
|--- Filename  
|--- After submit
```

3.12.4.3 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

Phone application

Upgrade using file

Choose the image file you wish to use to upgrade the phone

Choose File
No file chosen

Upgrade
Cancel

Closing or navigating away from this page will cancel the file upload

Upgrade using FTP/HTTPS

☐ Use defaults

Download method

FTP ▼

FTP server address

10.12.82.56

FTP server port

60025

FTP account

FTP username

openstage

FTP password

.....

FTP path

./Images

Filename

OS_WE34_HI_HFA_V1_R

After submit

do nothing ▼

Submit
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 application
```

- **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/CP600/600E/CP700/700X:**

Press the Soft Key labeled Download. The download will start immediately.

3.12.5 Picture Clips

NOTICE: Picture clips are available only on OpenScape Desk Phone CP600/600E and CP700/700X 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.

3.12.5.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see [Common FTP/HTTPS Settings \(Defaults\)](#) on page 116) 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".
- **FTP server address:** IP address or hostname of the FTP/HTTPS server in use.
- **FTP server port:** Port number of the FTP/HTTPS server in use. 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.
- **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

FTP account

FTP username

FTP password

FTP path

Filename

After submit start download ▼

Administration via Local Phone

```

|--- Admin
|--- File Transfer
|--- Picture Clip
|--- Use defaults
|--- Download method
|--- FTP server address
|--- FTP server port
|--- FTP account
|--- FTP username
|--- FTP password
|--- FTP path
|--- Filename
|--- After submit

```

- **On OpenScape Desk Phone CP400/600/600E/700/700X:**

Press the Soft Key labeled Download. The download will start immediately.

3.12.5.2 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
```

- **On OpenScape Desk Phone CP400/600/600E/700/700X:**
- Press the Soft Key labeled Download. The download will start immediately.

3.12.5.3 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 138) 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 181).

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.

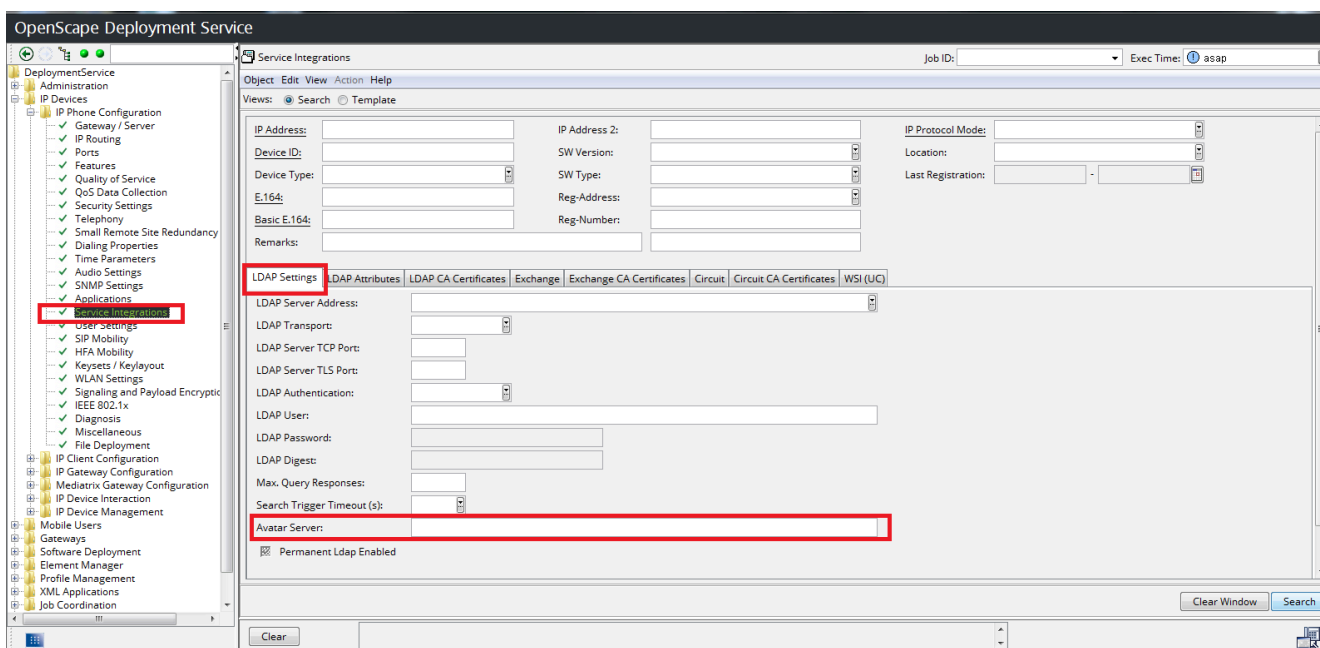
If the picture cannot be displayed (wrong format, download error, etc.) then a default avatar continues to be shown.

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	
LDAP for manual search only	☐
Submit	Reset

3.12.6 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 OpenScape Desk Phone phones support LDAPv3.

3.12.6.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see [Common FTP/HTTPS Settings \(Defaults\)](#) on page 116) are to be used, Use default must be set to "Yes", and only the Filename must be specified.

Data required (in any case)

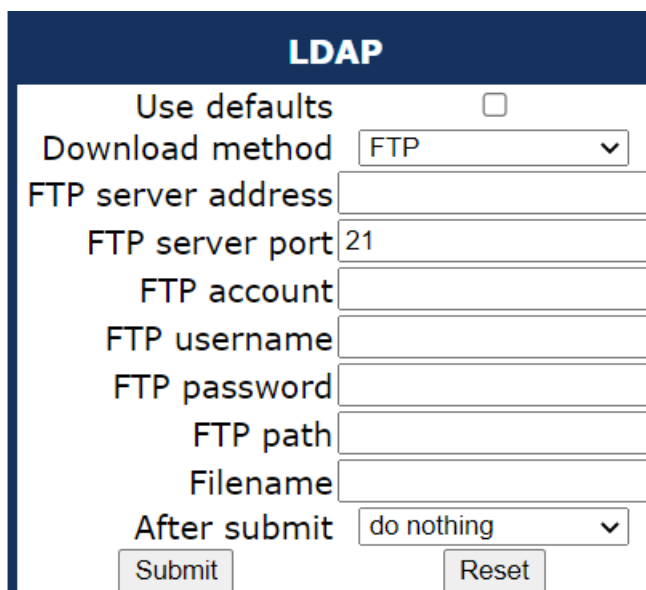
- **Use default:** Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No" Default: "No"
- **Filename:** Specifies the file name of the phone software.
- **After submit:** Specifies actions after submit button is pressed. Value range: "do nothing", "start download". Default: "do nothing".

Data required (if not derived from Defaults)

- **Download method:** Selects the protocol to be used. Value range: "FTP", "HTTPS" Default: "FTP"
- **FTP server address:** IP address or hostname of the FTP/HTTPS server in use.
- **FTP server port:** Port number of the FTP/HTTPS server in use. 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.

Administration via WBM

File transfer > LDAP



The image shows a web-based LDAP configuration form. At the top, there is a dark blue header with the word "LDAP" in white. Below the header, the form contains several fields and controls:

- Use defaults:** A checkbox that is currently unchecked.
- Download method:** A dropdown menu with "FTP" selected.
- FTP server address:** An empty text input field.
- FTP server port:** A text input field containing the number "21".
- FTP account:** An empty text input field.
- FTP username:** An empty text input field.
- FTP password:** An empty text input field.
- FTP path:** An empty text input field.
- Filename:** An empty text input field.
- After submit:** A dropdown menu with "do nothing" selected.
- Buttons:** "Submit" and "Reset" buttons are located at the bottom of the form.

Administration via Local Phone

```

|--- Admin
|--- File Transfer
|--- LDAP
|--- Use defaults
|--- Download method
|--- FTP server address
|--- FTP server port
|--- FTP account
|--- FTP username
|--- FTP password
|--- FTP path
|--- Filename
|--- After submit

```

- **On OpenScape Desk Phone CP400/600/600E/700/700X:**

Press the Soft Key labeled Download. The download will start immediately.

3.12.6.2 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

LDAP

☐

Use defaults

Download method

FTP

FTP server address

192.168.1.150

FTP server port

21

FTP account

FTP username

phone

FTP password

.....

FTP path

media

Filename

ldap_template.txt

After submit

start download

Submit

Reset

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 starts immediately.
- **On OpenScape Desk Phone CP400/600/600E/700/700X:**
Press the Soft Key labeled Download. The download starts immediately.

3.12.7 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 CP600/600E and CP700/700X.

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

3.12.7.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see [Common FTP/HTTPS Settings \(Defaults\)](#) on page 116) 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 defaults
            |--- Download method
            |--- FTP server address
            |--- FTP server port
            |--- FTP account
            |--- FTP username
            |--- FTP password
            |--- FTP path
            |--- Filename
            |--- After submit
```

- **On OpenScape Desk Phone CP400/600/600E/700/700X:**

Press the Soft Key labeled Download. The download will start immediately.

3.12.7.2 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.

3.12.8 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 (OpenScope Desk Phone CP600/600E/700/700X). The OpenScope Desk Phone CP600/600E/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

3.12.8.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see [Common FTP/HTTPS Settings \(Defaults\)](#) on page 116) 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

Ringer file

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

Administration via Local Phone

```

|--- Admin
|   |--- File Transfer
|       |--- Ringer file
|           |--- Use defaults
|           |--- Download method
|           |--- FTP server address
|           |--- FTP server port
|           |--- FTP account
|           |--- FTP username
|           |--- FTP password
|           |--- FTP path
|           |--- Filename
|           |--- After submit

```

3.12.8.2 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

Ringer file

Use defaults

Download method

FTP server address

FTP server port

FTP account

FTP username

FTP password

FTP path

Filename

After submit

Submit

Reset

☐

FTP

192.168.1.150

21

phone

.....

ring.mp3

start download

In the **File transfer > Ringer file** 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 file
```

- **On OpenScape Desk Phone CP600/600E/700/700X:**
Press the Soft Key labeled Download. The download will start immediately.

3.12.9 Company logo

NOTICE: The upload of company logo via WBM or local menu is possible only for OpenScape Desk Phone CP400/CP600/CP600E.

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 (JPEG, JPG, 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

No file chosen

Closing or navigating away from this page will cancel the file upload

Transfer using FTP/HTTPS

☐ Use defaults

Download method

FTP server address

FTP server port

FTP account

FTP username

FTP password

FTP path

Filename

After submit

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 defaults
|--- Download method
|--- FTP server address
|--- FTP server port
|--- FTP account
|--- FTP username
|--- FTP password
|--- FTP path

```

```
|--- Filename
|--- After submit
```

Format of the logo image file

The logo image file will be accepted by the phone in below formats:

- **CP600/CP600E**: PNG image
- **CP400**: BMP image

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 px
- **CP400**: 112 x 32 px

Resizing is done by keeping the aspect ratio intact.

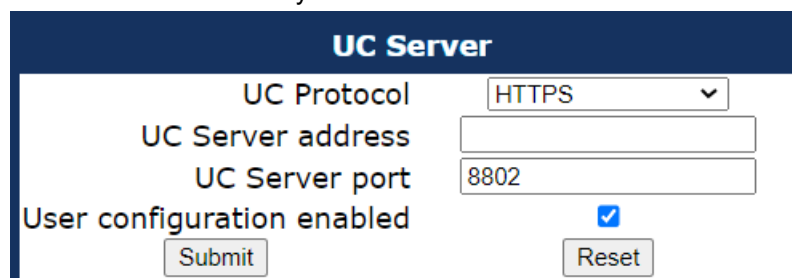
3.13 UC Server

Data required

- UC Protocol: Selects the protocol to be used. Value range: "HTTP", "HTTPS".
- UC Server address: IP address or hostname of the UC server in use.
- UC Server port: Port number of the UC server in use. Default: 8802.
- User configuration enabled: indicates whether the User configuration is enabled.

Administration via WBM

Local functions > Locality > UC Server



UC Server	
UC Protocol	HTTPS
UC Server address	
UC Server port	8802
User configuration enabled	☒
Submit Reset	

Administration via Local Phone

```
|--- Admin
  |--- Local functions
    |--- UC Server
      |--- UC Protocol
```

--- UC server address
--- UC Server port
--- User configuration enabled

3.14 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: web page /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

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 be either 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 serverside path (Path) and the additional parameters (Parameter).

Data required

- Name: name 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.

Administration via WBM

Use the Name field to define or change the name (label) of the key.

System > Local Features > Send URL

Send URL

Name

Message details

Protocol

Web server address

Port

Path

Parameters

Method

Authenticate phone

Web server user ID

Web server password

3.15 Corporate Phonebook: Directory Settings

3.15.1 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.

The user can access the LDAP directory using the 'directory->corporate' entry. The entry is displayed only, if a LDAP server configuration exists.

NOTICE: The OpenScape Desk Phone CP 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, or to use an encrypted TLS connection to a separate LDAPS port on the LDAP server, or to use an encrypted TLS connection to a separate LDAPS port on 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 180.

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. Default: "636"
- **LDAP Server port:** Port on which the LDAP server is listening for requests, when Transport is set to TCP. Default: 389
- **Authentication:** Authentication method used for connecting to the LDAP server. Value range: "Anonymous", "Simple" Default: "Anonymous"
- **User name:** User name used for authentication with the LDAP server in the LDAP bind request.
- **Password:** Password used for authentication with the LDAP server.
- **Avatar server:** HTTP/HTTPS address, where the pictures are located. The complete HTTP/HTTPS address is built from <Avatar server> + <Avatar>. <Avatar> is the attribute name from the LDAP template field <Avatar>. The specified LDAP attribute must contain the filename of the picture contained in the URL specified in <Avatar Server>. Example: <Avatar Server> = "https://mypicture.server/picturepath" <Avatar> = picturename. 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:** Allows you to control if the phone would use the search string provided by the user to search the firstname and lastname field on the LDAP server. Value range: "True", "False". Default: "False" (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

Directory settings	
LDAP server address	
Transport	TCP
Secure port	636
LDAP server port	389
Authentication	Anonymous
User name	
Password	
LDAP for manual search only	☐
Submit	Reset

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

```

3.15.2 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 CP400/600/600E/700/700X. 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)

3.15.2.1 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**Locality > Name update sources**
Administration via Local Phone

```
|--- Admin
      |--- Locality
            |--- Name update sources
                  |--- LDAP
                  |--- UC Directory
                  |--- Signalling
```

3.15.3 System Phonebook (for OpenScape Business only)

To access the System phonebook without UC configuration it is mandatory that the subscriber does have authentication activated in the System and this password is configured in the gateway settings.

Please note in case an OCAB system is used the IP of the OCAB board needs to be configured in the:

Admin --> Local functions --> UC Server to access the System Phonebook (for more information see [Section 3.11, UC Server](#)).

The user is not required to enter any UC credentials as the Gateway configuration settings are used for the System Phonebook queries.

The phone will perform a Reverse Lookup of the Number provided from the system on Outgoing and Incoming Calls so configuring of canonical dial settings (see [Section 3.13.3, Canonical Dial Settings](#) and/or [Section 4.1.1 Canonical Dialing Settings](#)) is mandatory.

Any further information available in the system Phonebook will be stored for this contact as well.

This reverse lookup is only performed if no result is returned from a configured LDAP server.

3.15.4 Picture via LDAP

In order to display centrally stored contact data the OpenScape Desk Phone CP400/600/600E/700/700X will request and retrieve the data from a server.

The OpenScape Desk Phone CP400/600/600E/700/700X requests the lookup for all numbers for which the local phonebook does not have a picture. In case the phonebook contains names for the number but without picture the name and picture from the directory server are displayed. If there is no entry for the number in the directory server the name from the local phonebook is displayed, so the directory server data overrides the local phonebook.

Currently two different mechanisms for storage of the picture shall be supported, both requiring a directory server for central storage:

- Direct retrieval of pictures stored within the ldap directory (preferred mechanism)
- Indirect (two step) retrieval in case the directory server contains a reference (url) to the picture instead- in this case the picture is retrieved from another server via http using the url.

The phones will only accept pictures encoded in jpg and max. 50K size.

3.15.5 Canonical Dial Settings

For contact data retrieval from the directory server, upon arrival of a call, the remote telephone number is converted according to the canonical dial settings (see also [Section 3.13.3, Canonical Dial Settings](#)). The format of the resulting number should match the format the numbers are stored in the directory server. It is recommended to convert the numbers to fully qualified format, i.e. adding country and area code to the subscriber number. This way it is ensured that the number used for lookup is unique.

Below is an example of settings for a company in Munich.

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	
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	☐
Submit	Reset

Administration via Local Phone

|--- Administration

|--- Local Functions

|--- Locality

|--- Canonical dial settings

|--- Local country code

|--- National prefix digit

|--- Local national code

|--- Minimum local number length

|--- Local enterprise node

|--- PSTN access code

|--- International code

|--- Operator code
|--- Emergency number
|--- Initial extension digits
|--- Expect dial number

3.16 Speech

3.16.1 Audio Settings

As an administrator, you can control the usage of microphone and speaker for speakerphone mode. Both microphone and loudspeaker can be switched on or off separately. By default, both microphone and loudspeaker are switched on.

3.17 Security and Policies

3.17.1 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.

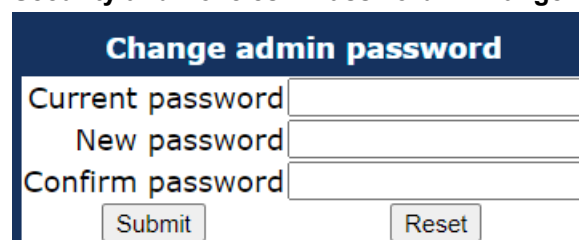
Usable characters are 0-9 A-Z a-z . " * # , ? ! ' + - () @ / : _

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



Security and Policies > Password > Change User password

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
```

3.17.1.1 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.

3.17.2 Certificates

3.17.2.1 Generic

Online Certificate Check

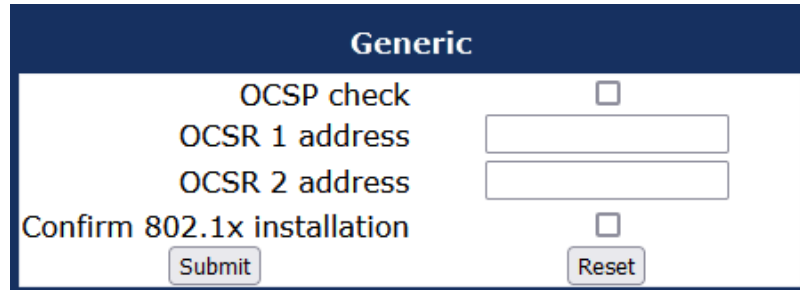
The Online Certificate Status Protocol (OCSP) is used to check if a certificate to be used has been revoked. This protocol is used to query an Online Certificate Status Responder (OCSR) at the point when the certificate is being validated. The address of an OCSR can be configured on the phone and can 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 OSCP responder.
- **OCSR 2 address:** Specifies the IP address (or FQDN) of a secondary OSCP 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



Administration via Local Phone

```
|--- Admin
  |--- Security and policies
    |--- Certificates
      |--- Generic
        |--- OCSP check
        |--- OCSR 1 address
        |--- OCSR 2 address
        |--- Confirm 802.1x Installation
```

3.17.2.2 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 [Section 3.10.3, Common FTP/HTTPS Settings \(Defaults\)](#)).

Secure HFA gateway sets the authentication level for the HFA gateway connected to the phone (see [HFA Gateway Settings](#) on page 75).

Secure 802.1x server sets the authentication level for the 802.1x authentication server.

Administration via WBM

Security and Policies > Certificates > Authentication policy

Authentication policy	
Secure file transfer	None ▼
Secure HFA gateway	None ▼
Secure 802.1x server	Trusted ▼
LDAP via TLS	None ▼
Secure Exchange server	None ▼
Secure OpenScape UC server	None ▼
Submit Reset	

Administration via Local Phone

```
|--- Admin
|
|--- Security and policies
|
|--- Certificates
|
|--- Secure File Transfer
|
|--- Secure HFA gateway
|
|--- Secure 802.1x server
|
|--- LDAP via TLS
|
|--- Secure Exchange server
|
|--- Secure OpenScape UC Server
```

3.17.2.3 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:** 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: ▼

Certificate configuration

Country (C):

Province (ST):

City (L):

Organization (O):

Common (CN):

Signature algorithm: ▼

Key length: ▼

Certificate type: ▼

Action: ▼

Certificate status:

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

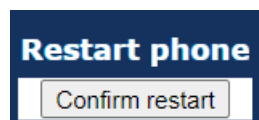
```

3.18 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

```

3.19 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
```

3.20 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 range 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

Secure shell	
Enable access	☐
Session password	
Access minutes	3 ▼
Session minutes	5 ▼
Access Phone Behind a NAT settings	
Remote SSH enable access	☐
Remote SSH server address	
Remote SSH server port	
Remote SSH username	
Remote SSH HPT port forwarding	☐
Remote SSH Webm port forwarding	☐
Remote SSH known hosts	
Submit	Reset

3.21 Display License Information

The license information for the OpenScape Desk Phone CP phone software currently loaded can be viewed via the local menu.

The license information can also be viewed by users who logged on using the phone as Admin is not permitted.

Administration via Local Phone

|--- Admin

|--- Licence information

3.22 Web Services Interface (WSI)

The Web Services interface (WSI) provides functions for Unified Communication (UC) users of OpenScape Business. It enables external applications to monitor and control devices of the UC users as well as to get information about their presence status, journal and phone book entries. For more information see the Web Services Interface Manual.

Administration via WBM

Local functions > WSI

WSI	
Protocol	HTTPS ▼
Server address	389
Server prot	8802
User configuration enabled	☐
Submit	Reset

Administration

HPT Interface (For Service Staff)

Administration via Local Phone (Disable)

```
|--- Administration
    |--- Local functions
        |--- WSI
```

3.23 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:

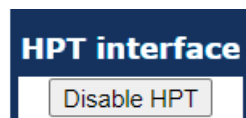
- The display shows a message indicating that remote service is active.
- Handset, microphone, speaker, headset, and microphone are disabled.

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 157).

Administration via WBM (Disable)

Maintenance > HPT interface



```
|--- Administration
    |--- Maintenance
        |--- Disable HPT / Enable HTP
```

3.24 AlertBar LED hint

The administrator can control how the Alert LED is automatically turned off in OpenScape deskphone CP400/600/600E/700/700X. When the parameter is checked, the Alert LED turned off as soon as the user enters the Conversations screen or the Call Log screen. 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

3.25 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.

3.25.1 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](#).

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 > Wired settings > LLDP-MED operation

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 ▼

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
        |--- Wired settings
            |--- LLDP-MED operation
```

3.25.2 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.

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](#) and [Example Dial Plan](#).

- 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 (only applicable for CP400/600/700/700X)

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.

- 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.

- 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.

- ConversationAPI (only applicable for CP400/600/700/700X)
The important part of the Conversation List; it combines the call history information from Call Log and the contact information in the phonebook.
- 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 (only applicable for CP400/600/700/700X)
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 processing service
This is a layer of software between the media control service, the tone generation, and voice engine services. It is also involved in the switching of audio devices such as the handset and loudspeaker.

- 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.
- 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.
- Sidecar service (only applicable for CP400/600/700)
Handles interactions between the phone and any attached sidecars.
- SWYX service (only applicable for CP400/600/700)
Traces communication between phone and the SWYX server, if configured.
- 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.
- USB backup service
Used to make backup/restore to/from USB stick by using password. This item is available in the phone GUI.
- 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.
- Video service engine (only applicable for CP600/700/700X)
Handles the video functionality.
- 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.
- WSI service (only applicable for CP400/600/700/700X)
The Web Services interface (WSI) provides functions for Unified Communication (UC) users of OpenScape Business. It enables external applications to monitor and control devices of the UC users as well as to get information about their presence status, journal and phone book entries.
- 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)	1048576	Trace timeout (minutes) 0
		Automatic clear before start ☐
Trace levels for components		
802.1x service	OFF	Administration
Application framework	OFF	Application menu
Bluetooth service	OFF	Call view
Certificate management	OFF	Clock service
Communications	OFF	Component registrar
ConversationAPI	OFF	CSTA service
Data access service	OFF	Digit analysis service
Directory service	OFF	DLS client management
Exchange service	OFF	H.323 messages
GPALAudio Core	OFF	GPALAudio Framework
Health service	OFF	HFA service agent
Instrumentation service	OFF	Journal service
Media control service	OFF	Mobility service
OBEX service	OFF	OpenScape UC service
OpenStage client management	OFF	Password management service
Performance marks	OFF	Physical interface service
Security log service	OFF	Service framework
Service registry	OFF	Sidcar service
SWYX Service	OFF	Tone generation service
Transport service	OFF	vCard parser service
Video service engine	OFF	HTTP service
Voice engine service	OFF	Web server service
WSI service	OFF	
Submit		Reset

3.25.3 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 157).

The following sections describe the EasyTrace profiles available for the phone.

3.25.3.1 Phone administration problems

Diagnostics > EasyTrace Profiles > Phone administration problems

Phone administration problems	
File size (Max 6290000 bytes)	6290000
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
Submit	Reset
Download trace file	Download saved trace file

3.25.3.2 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
H.323 messages	DEBUG
Media control service	DEBUG
Tone generation service	DEBUG
Voice engine service	DEBUG
Submit	Reset
Download trace file	Download saved trace file
Download H.323 trace file	

NOTICE: This EasyTrace profile contains the tracing of messages. Please note that after changing the level for the tracing of SIP messages, the phone must be rebooted.

3.25.3.3 Bluetooth problems

This profile is available only on OpenScope Desk Phone CP600 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
Submit	Reset
Download trace file	Download saved trace file

NOTICE: Bluetooth is only available on OpenScope Desk Phone CP600 and CP700/700X.

3.25.3.4 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 ▼
H.323 messages	DEBUG ▼
Submit	Reset
Download trace file Download saved trace file Download H.323 trace file	

NOTICE: This EasyTrace profile contains the tracing of messages. Please note that after changing the level for the tracing of SIP messages, the phone must be rebooted.

3.25.3.5 Conversations / LDAP problems

Diagnostics > EasyTrace Profiles > Conversations / LDAP problems

Conversations / LDAP problems	
File size (Max 6290000 bytes)	1048576
Trace timeout (minutes)	0
Automatic clear before start	☐
Trace levels for components	
Call view	DEBUG ▼
ConversationAPI	DEBUG ▼
CSTA service	DEBUG ▼
Digit analysis service	DEBUG ▼
Directory service	DEBUG ▼
Exchange service	DEBUG ▼
Journal service	DEBUG ▼
WSI service	DEBUG ▼
Submit	Reset
Download trace file Download saved trace file Download H.323 trace file	

3.25.3.6 Keypad problems

Diagnostics > EasyTrace Profiles > Keypad problems

Keyset 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
Sidecar service	DEBUG
Submit	Reset
Download trace file	Download saved trace file
Download H.323 trace file	

NOTICE: This EasyTrace profile contains the tracing of messages. Please note that after changing the level for the tracing of SIP messages, the phone must be rebooted.

3.25.3.7 Mobility / DLS problems

Diagnostics > EasyTrace Profiles > Mobility / DLS problems

Mobility / DLS problems	
File size (Max 6290000 bytes)	1048576
Trace timeout (minutes)	0
Automatic clear before start	☐
Trace levels for components	
Call view	DEBUG
Communications	DEBUG
DLS client management	DEBUG
Mobility service	DEBUG
OpenStage client management	DEBUG
Submit	Reset
Download trace file	Download saved trace file
Download H.323 trace file	

3.25.3.8 Network problems

Diagnostics > EasyTrace Profiles > Network problems

Network problems	
File size (Max 6290000 bytes)	1048576
Trace timeout (minutes)	0
Automatic clear before start	☐
Trace levels for components	
802.1x service	DEBUG
Transport service	DEBUG
Submit	Reset
Download trace file	Download saved trace file
Download H.323 trace file	

3.25.3.9 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
Password management service	DEBUG
Security log service	DEBUG
Submit	Reset
Download trace file	Download saved trace file
Download H.323 trace file	

3.25.4 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

3.25.5 QoS Reports

3.25.5.1 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 67) 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	OFF
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
  |--- Network
    |--- QoS
      |--- Reports
        |--- Generation
          |--- Report mode
          |--- Report interval
          |--- Observation
interval
length
values
delay
threshold values:
packets
packets
values:
...Lost packets (K)
...Consecutive lost
...Consecutive good
Compressing codec threshold
...Lost packets (K)
```

```

packets                                     |--- ...Consecutive lost
packets                                     |--- ...Consecutive good
packets                                     |--- ...Resend last report

```

3.25.5.2 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 67);
- the conditions for the generation of reports are set adequately (see [Conditions and Thresholds for Report Generation](#) on page 168).

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:

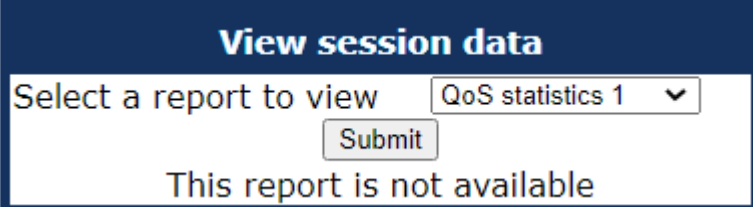
- **Start of report period - seconds:** NTP time in seconds for the start of the report period.
- **Start of report period - fraction of seconds:** Additional split seconds to be added to the seconds for an exact start time.
- **End of report period - seconds:** NTP time in seconds for the end of the 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 trap 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.
- **OpenScape 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:** Call ID.
- **MAC address:** MAC address of the local phone.

Data viewing via WBM

Diagnostics > QoS reports > View Session Data



3.25.6 Miscellaneous

3.25.6.1 IP tests

For network diagnostics, the OpenScape Desk Phone CP phone can ping any host or network device to determine whether it is reachable.

Data required

- Pre Defined Ping tests: Pings a predefined IP address. Value range: "Ping DLS", "Ping HiPath gatekeeper", "Ping standby HiPath gatekeeper"
- Ping tests: Pings the entered host's IP address or hostname.
- Pre Defined Trace tests: Pings a predefined Traceroute IP address. Value range: "Traceroute DLS", "Traceroute HiPath gatekeeper", "Traceroute standby HiPath gatekeeper"
- Traceroute: Pings the entered host's IP address or hostname.

Administration via WBM

The screenshot shows a web-based management interface for IP tests. It has a black background with green text for section headers. The first section is 'IP tests' followed by 'Pre Defined Ping tests'. Below this is a dropdown menu showing 'Ping DLS' and a 'Ping' button. The next section is 'Ping tests' with an empty input field and a 'Ping' button. The third section is 'Pre Defined Trace tests' with a dropdown menu showing 'Traceroute DLS' and a 'Traceroute' button. The final section is 'Traceroute' with an empty input field and a 'Traceroute' button.

3.25.6.2 Memory Status 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 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/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/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

[Download memory info file](#)

[Download thread info for services](#)

Device memory information

```

Mem: 157000K used, 86536K free, 5080K shrd, 0K buff, 57092K cached
CPU: 42% usr  0% sys  0% nic 57% idle  0% io  0% irq  0% sirq
Load average: 1.70 1.58 1.59 1/221 14112
PID  PPID USER  STAT  VSZ %VSZ %CPU COMMAND
213   1 root    S    22256  9% 21% eptdaemon_alsa
412  255 root    SN   72688 30%  7% {QT Gui CallView} PhoneletLauncher callviewhfa.phd V1 R6.4.2
583   1 appweb  SN   13484  6%  7% ./appWeb --config opera_appWeb_latestTlsOnly.conf
14112 214 root    R    3236  1%  7% /bin/busybox top -d 0 -a -n 1 -l 600 -b
255  214 root    S<   202m 85%  0% SvcConfig services.conf -startLogDaemon -logAll V1 R6.4.2
447  255 root    SN   54412 22%  0% {QT Gui AdminPho} PhoneletLauncher admin.phd V1 R6.4.2
643  255 root    SN   45584 19%  0% {QT Gui HiPathSt} PhoneletLauncher stimulushfa.phd V1 R6.4.2
599  255 root    SN   45072 18%  0% {QT Gui MenuPhon} PhoneletLauncher menuphonelet.phd V1 R6.4.2
214   1 root    S   32424 13%  0% SvcConfig healthservice.conf
        
```

3.25.6.3 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*

3.25.7 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/

OpenScape Desk Phone CP600;  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

4 Examples and HowTos

4.1 Canonical Dialing

4.1.1 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.)

4.1.2 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.

4.1.2.1 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

4.2 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.

NOTICE: LDAP is available only on OpenScape Desk Phone CP400, CP600/600E and CP700/700X.

4.2.1 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.
- 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 for OpenScape Voice.

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. Therefore, 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.

4.2.2 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 GUI 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.

OpenScape Desk Phone CP Field	LDAP Template Labels	LDAP Attribute	Example Value
Address 1	ATTRIB08	departmentText	0815
Address 2	ATTRIB09		
Role	ATTRIB10	mainFunction	Product Manager
Email	ATTRIB11	mail	doe@example.com
Nickname	ATTRIB12	nickname	
Avatar	ATTRIB13		jpeg image or image name, more information in the Picture Clips via LDAP on page 124

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

OpenScape Desk Phone CP Field	LDAP Template Attribute	LDAP Attribute	Example Value
Company	ATTRIB07	company	Example Inc.
Address 1	ATTRIB08	department	Administration
Address 2	ATTRIB09	l	
Job function	ATTRIB10	title	Product Manager
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="l"
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

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>alternatePhone</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>	

4.2.3 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](#) [LDAP Template \(Download\)](#) on page 126), 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" in green text. The form contains the following fields and controls:

- Use defaults:** A checkbox that is currently unchecked.
- Download method:** A dropdown menu with "FTP" selected.
- 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 "*****".
- 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 with "do nothing" selected.
- Buttons:** "Submit" and "Reset" buttons at the bottom.

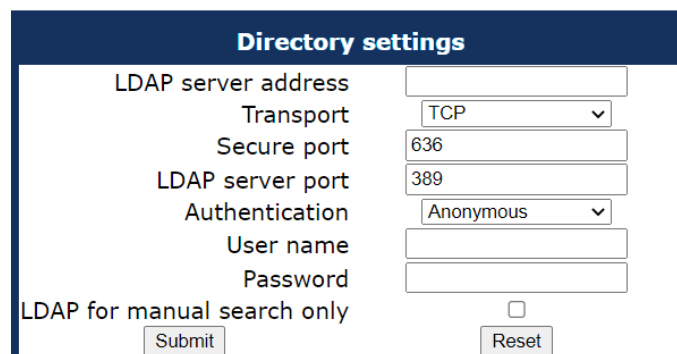
4.2.4 Configure LDAP Access

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 OpenScape Desk Phone CP600/600E.



The screenshot shows a web form titled "Directory settings" with a dark blue header. The form contains the following fields and controls:

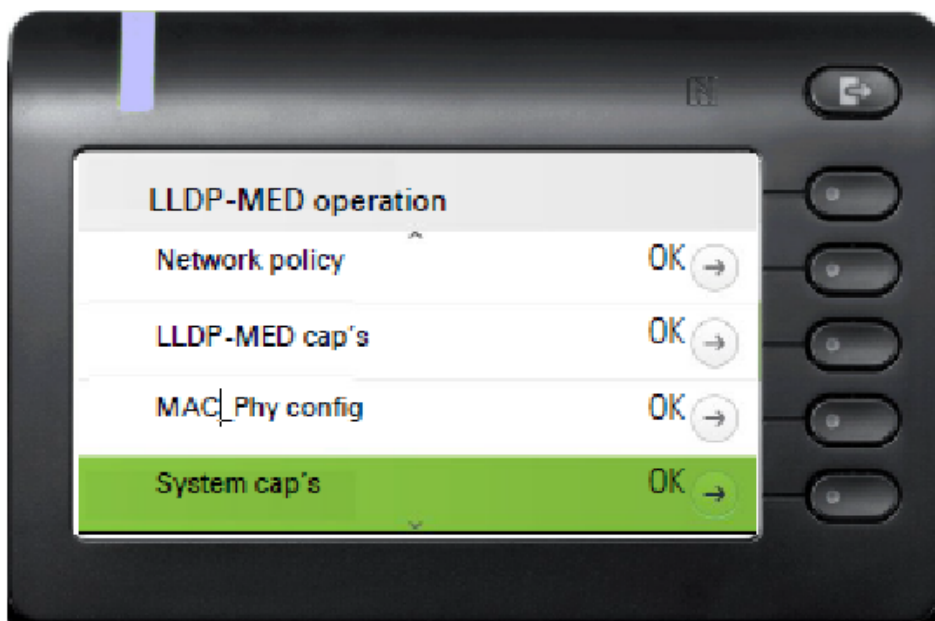
- LDAP server address: A text input field.
- Transport: A dropdown menu with "TCP" selected.
- Secure port: A text input field with "636" entered.
- LDAP server port: A text input field with "389" entered.
- Authentication: A dropdown menu with "Anonymous" selected.
- User name: A text input field.
- Password: A text input field.
- LDAP for manual search only: A checkbox that is currently unchecked.
- At the bottom, there are two buttons: "Submit" and "Reset".

3) Press Submit.

4.3 An LLDP-Med Example

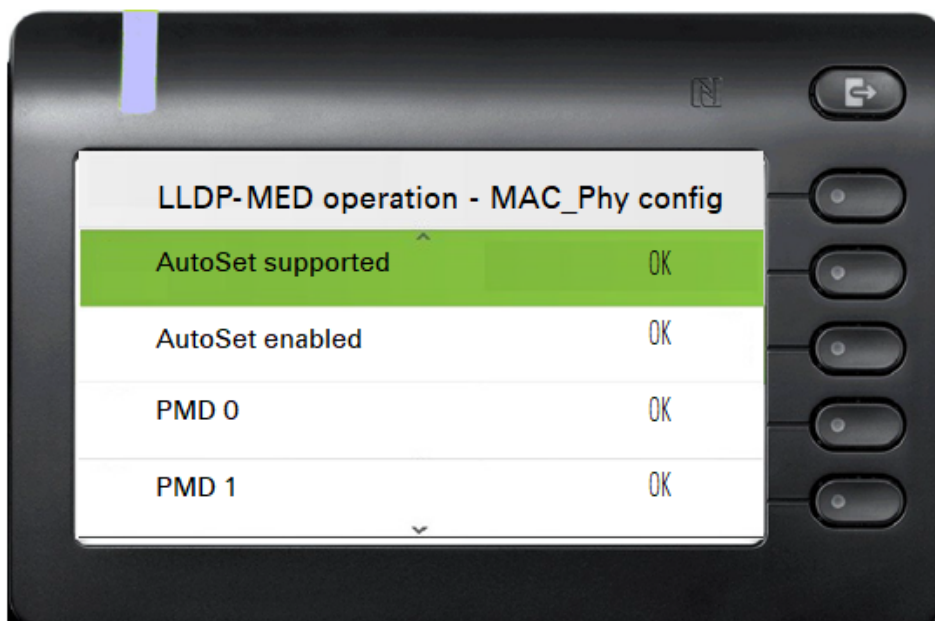
The following example illustrates the mode of operation of LLDP-MED. In order to evoke a reaction from LLDP-MED, the LAN switch has been set to auto-negotiation, whereas the phone's LAN port (see [LAN Port Settings](#) on page 46) is set to 100Mbit/s, hence a fixed value. This configuration error is 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 156). 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 > LLDP-MED Operation 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 Technical Reference

5.1 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 - 5015	5010 - 5015	RTP - RTCP
Payload transport (Secure VoIP)	5010 - 5015	5010 - 5015	SRTP - SRTCP
Directory access via LDAP	---	32786 - 61000	TCP
Directory access via LDAP (Secure)	---	32786 - 61000	TCP- SSL/TLS
DHCP Client	---	68	DHCP / UDP
DNS Client	---	32786-61000	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
Part of SNMP-Agent - receive Set/Get commands	161	---	SNMP / UDP

Service	Server Default Port	Client Default Port	Protocol Stack
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
OCSP certificate verification		80	HTTPS / TCP
H.225 (H.245)		0	TCP
H.225 - Q.931		32786 - 61000	TCP
Cornet TC	4060	1400-1719	TCP
Cornet TC	4061	1400-1719	TCP-TLS
Localization data from BT LE	8080		HTTP-TCP
CTI Service Agent Discovery	5100		
CorNet-TS based CTI	5015		
Client for Exchange access to contacts		443	EWS/SOAP/ TCP- SSL/TLS

5.2 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: âNo Telephony possible (LP)â.

Network Errors:

Table 1: Troubleshooting Error Codes: Network Errors

Error code	Priority	Problem	Description
LP	0	Unable to use LAN connection	Physical connection error
LX	1	Unable to use LAN connection	802.1x errors
L1	2	Unable to register HFA main line	No IP address - Manual config mode
L2	3	Unable to register HFA main line	No default route - Manual config mode

Error code	Priority	Problem	Description
L3	4	Unable to register HFA main line	No default route - Manual config mode
LI	5	Unable to use LAN connection	Network Configuration Error - General IP error - Manual config mode
D0	6	Unable to contact DHCP	Network Configuration Error - DHCP failure
TT	7	Unable to establish a TLS connection	No SNTP server

HFA Configuration Errors:

Table 2: Troubleshooting Error Codes: HFA Configuration Errors

Error code	Priority	Problem	Description
H4	8	Unable to register HFA main line	No gateway IP address
H5	9	Unable to register HFA main line	No subscriber number
RA	10	Unable to establish a TLS connection	Certificate error

Communication Errors:

Table 3: Troubleshooting Error Codes: Communication Errors

Error code	Priority	Problem	Description
HA	11	Unable to register HFA main line	Logon: Maintenance busy
HB	11	Unable to register HFA main line	Logon: No port available
Hb	11	Unable to register HFA main line	Logon: Rejected due to invalid LIN
Hc	11	Unable to register HFA main line	Logon: Rejected due to mobile terminal blocked
HD	11	Unable to register HFA main line	Logon: No port available (Ext)
Hd	11	Unable to register HFA main line	Logon: Rejected due to incompatible security profile
He	11	Unable to register HFA main line	Logon: Rejected due to TCP usage while TLS is required
HE	11	Unable to register HFA main line	Logon: Client not registered
HF	11	Unable to register HFA main line	Logon: Rejected due to logoff
Hf	11	Unable to register HFA main line	Logon: Reject due to PBX version not sufficient
HG	11	Unable to register HFA main line	Logon: Rejected due to logoff in progress

Error code	Priority	Problem	Description
HH	11	Unable to register HFA main line	Logon: Rejected due to shutdown
HI	11	Unable to register HFA main line	Logon: Rejected due to duplicate Logon
HJ	11	Unable to register HFA main line	Logon: Rejected due to already logged on
HK	11	Unable to register HFA main line	Logon: Rejected due to PIN not present
HL	11	Unable to register HFA main line	Logon: Rejected due to password not present
HM	11	Unable to register HFA main line	Logon: Rejected due to password not correct
HN	11	Unable to register HFA main line	Logon: Rejected due to invalid license
Ha	11	Unable to register HFA main line	Logoff: Rejected due to missing LN
HQ	11	Unable to register HFA main line	Logoff: Normal Logoff
HR	11	Unable to register HFA main line	Logoff: Client not logged on
HS	11	Unable to register HFA main line	Logoff: Client logged off
HT	11	Unable to register HFA main line	Logoff: Forced client logoff
HU	11	Unable to register HFA main line	Logoff: Timeout expired
HV	11	Unable to register HFA main line	Logoff: OMC action
HW	11	Unable to register HFA main line	Logoff: Hfa mobile user logged on
HX	11	Unable to register HFA main line	Logoff: Switch back to central system
HY	11	Unable to register HFA main line	Logoff: No bearer channel
HZ	11	Unable to register HFA main line	Logoff: New logon requested from the server
H[	11	Unable to register HFA main line	Logoff: Forced client logoff due to an incorrect PreShared secret
H0	12	Unable to register HFA main line	General Error
UC1	13	UC (WSI) server not accessible	Invalid UC server access configuration
UC2	14	UC logon rejected/not available	No access to UC service (UC mode)
EX	15	Exchange failure	• Exchange: please check username and password • Exchange: untrusted server • connection to Exchange server failed
CI	16	Circuit failure	• Circuit: please check username and password • Circuit: untrusted server • connection to Circuit server failed
NT	17	SNTP server unavailable	No SNTP connection

http://wiki.unify.com/wiki/OpenScape_Desk_Phone_CP_FAQ#Error_Codes

6 Glossary

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 192, 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 192 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 192) guarantees on Glossary on page 192 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 192es.
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 192. It requires a 64 kBit/s bandwidth.
G.722	ITU-T standard for audio encoding using split band Glossary on page 192. 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 192 or fax tones cannot be transported reliably with this codec.
Gateway	Mediation components between two different network types, e. g., Glossary on page 192 network and ISDN network.
HTTP	Hypertext Transfer Protocol. A standard protocol for data transfer in Glossary on page 192 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 192 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 192 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 192.
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 192, 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 192es: 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 192 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 192-based network

WBM

Web Based Management. A web interface which enables configuration of the device using a standard web browser.

Index

A

Advanced Audio Traces [167](#)
AlertBar LED hint [154](#)
Audio
 advanced traces [167](#)
Audio Settings [144](#)

B

Bluetooth
 handsfree profile [164](#)
 headset profile [165](#)

C

Canonical Dial Lookup [106](#)
Connectors [19](#)
Core dump [175](#)
Corporate Phonebook [138](#)
CSTA [192](#)
CTI [192](#)

D

Date and Time (SNTP) [102](#)
Daylight Saving [102](#)
Default Route [59](#)
DFT [192](#)
DHCP [56](#), [192](#)
Diffserv [54](#)
Directory Settings [138](#)
DLS (Deployment Service) [17](#), [35](#), [65](#), [192](#)
DNS [62](#), [192](#)
 Domain Name [62](#)
DST Zone (Daylight Saving Time Zone) [102](#)

E

Easy Trace Profiles [163](#)
 Bluetooth handsfree profile [164](#)
 Bluetooth headset profile [165](#)
 Call Connection [165](#)
 Call Log [166](#), [166](#)
 DAS Connection [167](#)
Emergency Number [104](#)
Energy Saving [87](#)
Error Codes [189](#)
External Access Code [106](#)
External Numbers [105](#)

F

Factory Reset [151](#)
Fault Trace Configuration [157](#)
FTP Settings [116](#)

G

Gateway [59](#)

H

HPT Interface [154](#)

I

Initial Digits [105](#)
Internal Numbers [105](#)
International Code (Local Country Code) [104](#)
International Gateway Code [106](#)
International Prefix (International Access Code) [104](#)
IP
 Address [27](#), [57](#)
 Address (Manual configuration) [57](#)
 IP [193](#)
 Specific Routing [61](#)

K

Key module (phone types) [22](#)
Keys
 programmable [113](#)

L

LAN [194](#)
 Port [46](#)
LAN port [47](#)
Layer 2 [53](#)
Layer 3 [54](#)
LDAP [138](#), [180](#), [194](#)
LDAP Template (Download) [126](#)
License Information [153](#)
LLDP-MED [156](#)
Local Country Code (International Code) [104](#)
Local Enterprise Number [104](#)
Local National Code (Local Area Code) [104](#)

M

MAC Address [194](#)
MDI-X [46](#), [194](#)
MIB [194](#)

MWI (Message Waiting Indicator) [194](#)

N

National Prefix (Trunk Prefix) [104](#)

Network port configuration [47](#)

O

OCSP [145](#)

OCSR failure [99](#)

Operator Code [104](#)

P

Password

Change [144](#)

Lost [145](#)

PBX [194](#)

PC port [46](#)

Phone

Restart [151](#)

Phone application

Download/Update [120](#)

Upgrade using File [118](#)

Upgrade using FTP/HTTPS [118](#)

Phone software (Download) [117](#)

Phonebook [138](#)

Picture Clips (Download) [122](#)

PoE (Power over Ethernet) [21](#), [195](#)

Port configuration [47](#), [47](#)

Port List [188](#)

Power Consumption/Supply [21](#)

Programmable Keys [113](#)

PSTN [195](#)

PSTN Access Code [104](#)

Q

QCU [68](#), [68](#)

QoS [53](#)

Quick Start [23](#)

R

Remote Tracing — Syslog [176](#)

Reset Factory [151](#)

Restart Phone [151](#)

Ringer File [131](#)

RTP [195](#)

S

Screensaver (Download) [128](#)

Secure

file transfer [146](#)

Shipment [18](#)

SNMP [67](#), [195](#)

SSH — Secure Shell Access [152](#)

Subnet Mask [27](#)

Subnet Mask (Manual configuration) [57](#)

T

TCP [196](#)

Timezone Offset [102](#)

TLS [196](#)

Trace Configuration [157](#)

Trace Profiles [163](#)

Traps [68](#)

U

UDP [196](#)

Update Service [65](#)

V

Vendor Class (DHCP) [29](#), [36](#)

View Report [171](#)

VLAN [48](#)

W

WBM (Web Based Management) [17](#), [23](#), [197](#)

Wi-Fi settings [70](#)

