



A MITEL
PRODUCT
GUIDE

OpenScape Desk Phone




CP Family

Administrator Documentation HFA

10/2024

Important information

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.

	<p>For safety reasons, the telephone should only be supplied with power:</p> <ul style="list-style-type: none">• using the original power supply unit.• over a LAN with PoE (Power over Ethernet), which complies with the IEEE 802.3af standard.
	<p>Never open the telephone. Should you encounter any problems, consult your administrator.</p>
	<p>Use only original accessories. The use of other accessories is hazardous and will render the warranty, extended manufacturer's liability and the CE and other markings invalid.</p>

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. Contact our legal department at iplegal@mitel.com for additional information.

For a list of the worldwide Mitel and Unify registered trademarks, refer to the website: <http://www.mitel.com/trademarks>.

Software update

During a software update, the phone must not be disconnected from the power supply unit or the LAN. An update action is indicated by messages on the display and by flashing LEDs.

Online documentation

This document along with additional information is available online at:
<https://www.unify.com/> → Support.

Technical notes, current information about firmware updates, frequently asked questions and lots more can be found on the Internet at: <https://wiki.unify.com/>.

Location of the telephone

- The telephone may only be operated using the LAN cabling internally in the building. The device should be connected to the IP infrastructure using a shielded LAN cable: Cat-5 for 100 Mbps or Cat-6 for 1000 Mbps. Make sure in the building installation that this cable shielding is earthed.
- When using the additional Wi-Fi dongle CP10 when connecting the phone to the network, make sure that the network security standards (e.g. encryption) and availability are met
- The telephone is designed for operation in a protected environment within a temperature range of 5 °C to 40 °C.
- Do not install the telephone in a room where large quantities of dust accumulate; this can considerably reduce the service life of the telephone.
- Do not expose the telephone to direct sunlight or any other source of heat, as this is liable to damage the electronic components and the casing.
- Do not install the telephone in bathrooms or shower rooms.

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.

Special setting instructions for energy-efficient use of telephones can be found in section "Energy saving" → page 86.

Energy Star



ENERGY STAR is a US 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 US Environmental Protection Agency.

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

The Unify products OpenScape Desk Phones have earned the ENERGY STAR. Learn more at energystar.gov

License information

For further information about EULA (End User License Agreement) and Open Source licenses, consult your administrator or the web-based management (WBM, see "How to access the web interface (WBM)" → page 28).

Contents

Important information.....	2
Trademarks.....	2
Software update.....	3
Online documentation.....	3
Location of the telephone.....	3
Product-oriented environmental protection.....	3
License information.....	4
Overview.....	10
About this manual.....	10
Maintenance notes.....	10
Conventions for this document.....	10
The OpenScape Desk Phone CP family.....	11
OpenScape Desk Phone CP110.....	11
OpenScape Desk Phone CP210.....	13
OpenScape Desk Phone CP410.....	15
OpenScape Desk Phone CP710.....	17
Administration interfaces.....	18
Web-based management (WBM).....	18
Local phone menu.....	19
DLS/DMS (OpenScape Deployment Service / Device Management Service).....	19
Startup.....	20
Prerequisites.....	20
Assembling and installing the phone.....	20
Shipment.....	20
Connectors at the bottom side.....	21
Assembly.....	25
How to connect the phone via LAN cable.....	25
How to use LAN connections.....	26
How to connect the phone via USB Wi-Fi dongle.....	27
Key modules.....	27
Quick start.....	27
How to access the web interface (WBM).....	28

Access via local phone.....	29
How to configure the Terminal number.....	30
Basic network configuration.....	30
DHCP resilience.....	31
Date and time / SNTP.....	31
Extended Network configuration.....	32
Vendor-specific VLAN discovery and DLS address.....	32
HFA gateway settings.....	39
Manual registration.....	40
Using the local menu.....	40
Setting the DMS address via DHCP.....	41
Cloud deployment.....	42
Administration.....	46
Bluetooth interface.....	46
Configuring the USB access.....	47
LAN settings.....	47
LAN port settings.....	47
VLAN.....	49
IP Network parameters.....	54
Quality of Service (QoS).....	54
Use DHCP.....	57
Manual configuration of the IP address.....	58
Default router / gateway.....	60
Specific IP routing.....	60
DNS.....	61
IP TTL.....	64
Gratuitous ARP control.....	65
Configuration & update service.....	65
SNMP.....	68
OpenScape service menu.....	70
Wi-Fi settings.....	70
Setting up a WiFi connection.....	73
Disable LAN port.....	74
Advanced Wi-Fi settings.....	74
System.....	77
HFA gateway settings.....	78

HFA emergency gateway settings.....	80
Server and standby server ports.....	81
Redundancy.....	82
Emergency number.....	83
LIN.....	84
Not used timeout.....	85
Enable telephony settings.....	86
Energy saving.....	86
System.....	87
Date and time.....	90
Settings via SNTP.....	91
Dialing.....	92
Canonical dialing configuration.....	92
Canonical dial look-up.....	96
Ringer setting.....	98
Local ringers.....	98
Ringer settings CP100 / CP200.....	100
Ringer settings CP400 / CP600 / CP700.....	101
Ringer mode.....	102
User mobility.....	102
Free programmable keys.....	103
Enabling "Long Press" for FPKs.....	103
Selected dial action on calls.....	104
Transferring phone software, application, and media files.....	104
Linux file name issues.....	104
FTP / HTTPS server.....	105
Common FTP / HTTPS settings (defaults).....	105
Phone application.....	107
Picture clips.....	111
LDAP template.....	114
Screen Saver.....	117
Ringer file.....	120
Company logo.....	123
UC server.....	125
Send request via HTTP / HTTPS.....	125
Settings of the corporate directory.....	128
LDAP.....	128

Contact details update.....	130
Picture via LDAP.....	131
Canonical dial settings.....	132
Speech.....	133
RTP base port.....	133
Codec preferences.....	134
Security and policies.....	135
Changing a password.....	135
Retrieve a lost password.....	137
Certificates.....	137
Restart phone.....	143
Factory reset.....	143
SSH — secure shell access.....	144
Display license information.....	145
HPT interface (for service staff).....	146
AlertBar LED hint.....	146
Diagnostics.....	147
LLDP-MED.....	147
Fault trace configuration.....	149
EasyTrace profiles.....	153
Advanced audio traces.....	157
QoS reports.....	158
Miscellaneous.....	163
Remote tracing — syslog.....	165
Key modules.....	166

Examples and how-tos.....168

Canonical dialing.....	168
Canonical dialing settings.....	168
Canonical dialing look-up.....	168
Conversion examples.....	169
How to set up the “Corporate directory” (LDAP).....	171
Prerequisites.....	171
Create an LDAP template.....	171
Upload the LDAP template to the phone.....	175
Configure LDAP access.....	176
Mapping the LDAP fields.....	176

LLDP-Med example.....	177
Technical reference.....	179
Default port list.....	179
Troubleshooting error codes.....	180
Glossary.....	185

Overview

About this manual

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

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

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

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

Maintenance notes

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

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

Note	Never open the telephone or a key module. If you encounter any problems, contact system support.
-------------	--

Conventions for this document

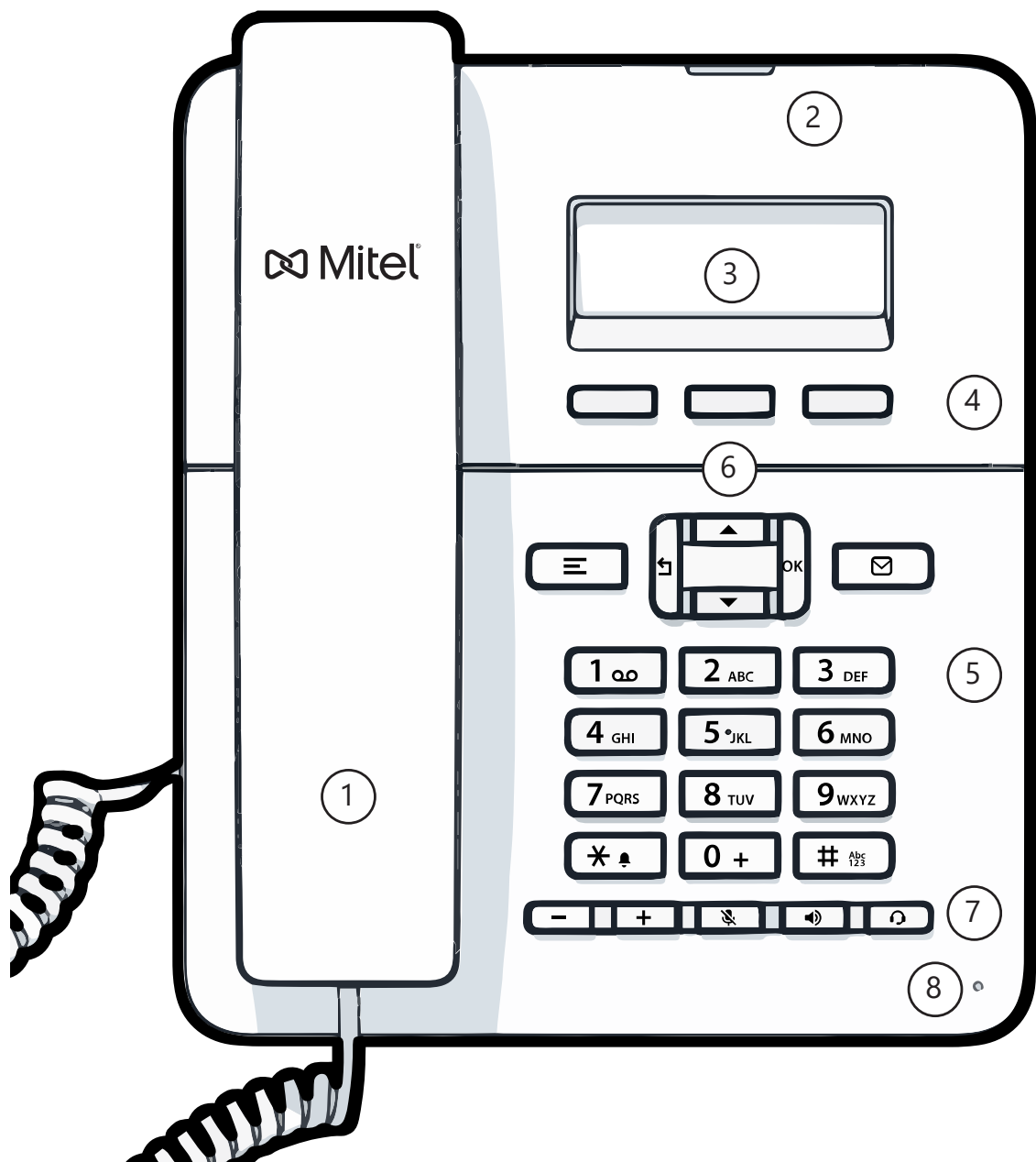
The terms for parameters and functions used in this document are derived from the web interface (WBM). In some cases, the phone's local menu uses shorter, less specific terms and abbreviations. In a few cases the terminologies differ in wording. If so, the local menu term is added with a preceding "/".








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

This document describes the software version 3.0.

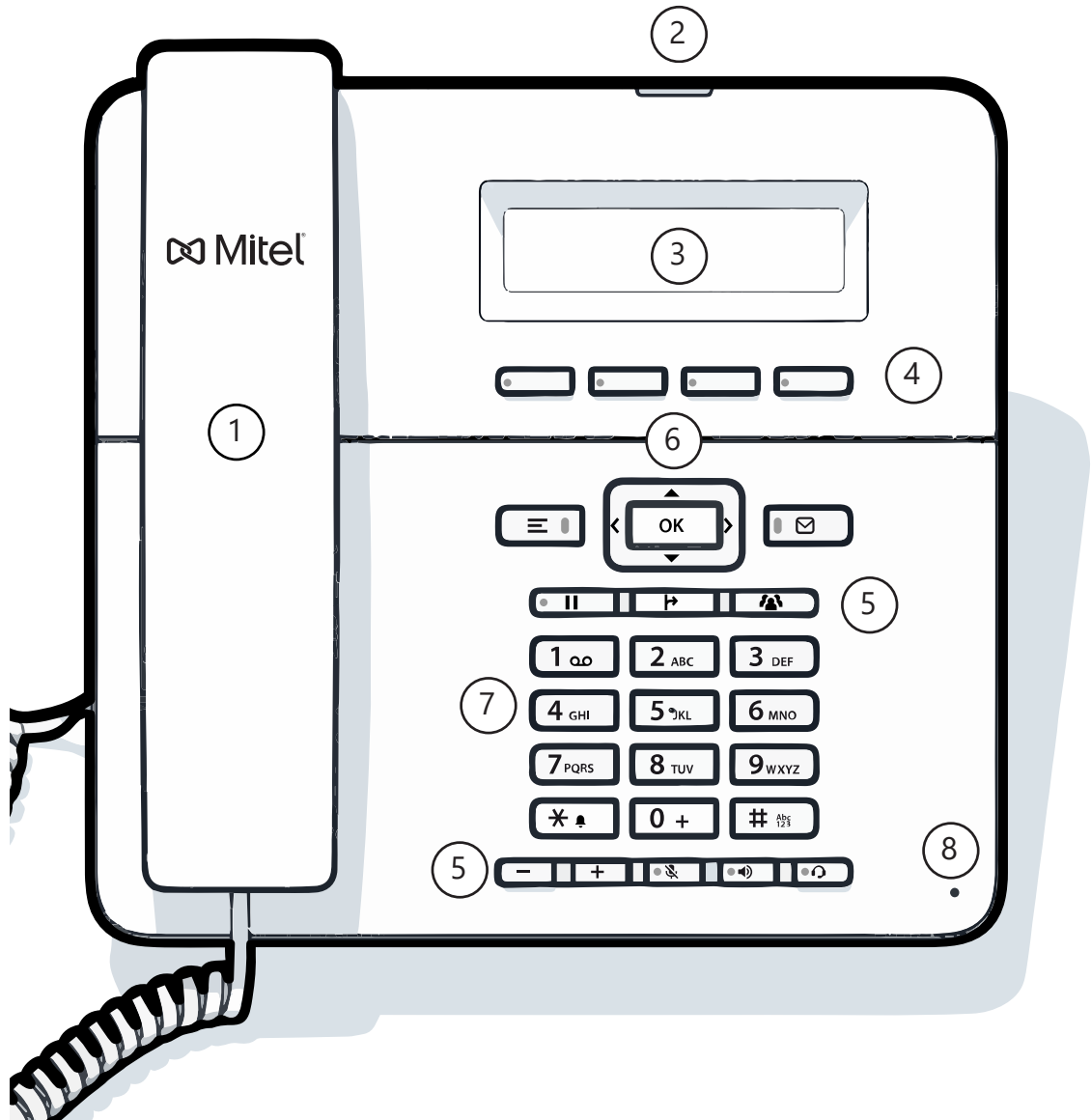
The OpenScape Desk Phone CP family

OPENSCAPE DESK PHONE CP110












1	You can make and receive calls as normal using the handset .
2	The Notification LED ("AlertBar LED") displays the phone connection status. Incoming calls and new voice mails are visually signalled.
3	The display shows information during telephone operation (three lines with up to 32 characters each).
4	The programmable function keys can be set to various functions.
5	<p>The function keys (non-programmable) are assigned to the following functions during a call:</p> <p>: Provides access to the user menu for locally controlling the phone settings.</p> <p>: Allows voicemails to be managed.</p> <p> : Increases or decreases the speaker or headset volume.</p> <p>: Activates or deactivates the microphone.</p> <p>: Activate or deactivates the speakerphone during an active call.</p> <p>: Activates or deactivates the headset.</p>
6	The navigation keys help you navigating through the various phone functions, applications and configuration menus.
7	The dialpad can be used to enter phone numbers and write text.
8	You can speak without the handset using the microphone .

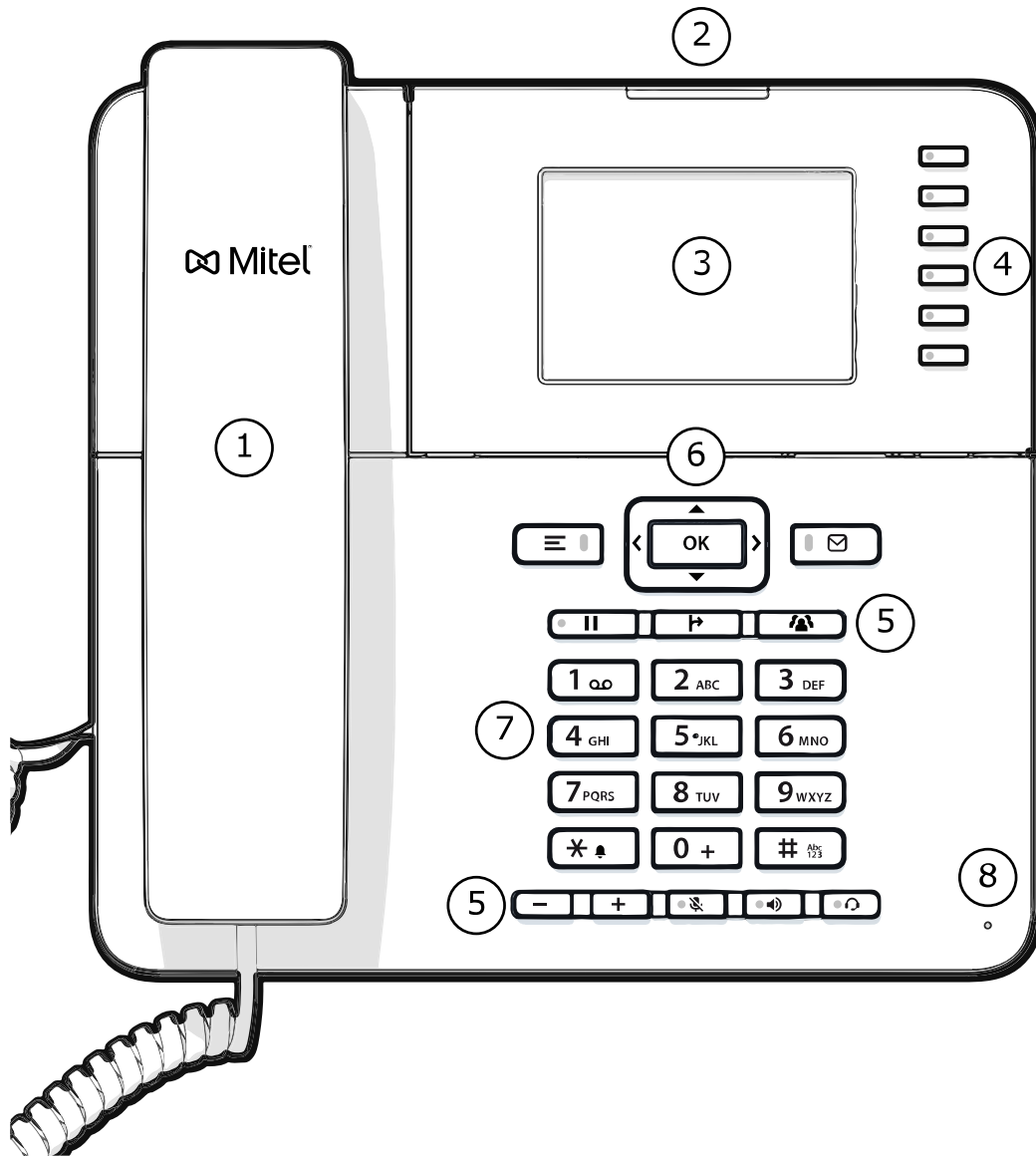
OPENScape DESK PHONE CP210












1	You can make and receive calls as normal using the handset .
2	The Notification LED ("AlertBar LED") displays the phone connection status. Incoming calls and new voice mails are visually signalled.
3	The display shows information during telephone operation (three lines with up to 32 characters each).
4	The programmable function keys can be set to various functions.

5	<p>The function keys (non-programmable) are assigned to the following functions during a call:</p> <p>: Provides access to the user menu for locally controlling the phone settings.</p> <p>: Allows voice mails to be managed.</p> <p>: Hold or retrieve the active call.</p> <p>: Transfer a call to another contact.</p> <p>: Enable access to the conference functions.</p> <p>: Increases or decreases the speaker or headset volume.</p> <p>: Activates or deactivates the microphone.</p> <p>: Activate or deactivates the speakerphone during an active call.</p> <p>: Activates or deactivates the headset.</p>
6	<p>The navigation keys help you navigating through the various phone functions, applications and configuration menus.</p>
7	<p>The dialpad can be used to enter phone numbers and write text.</p>
8	<p>You can speak without the handset using the microphone.</p>

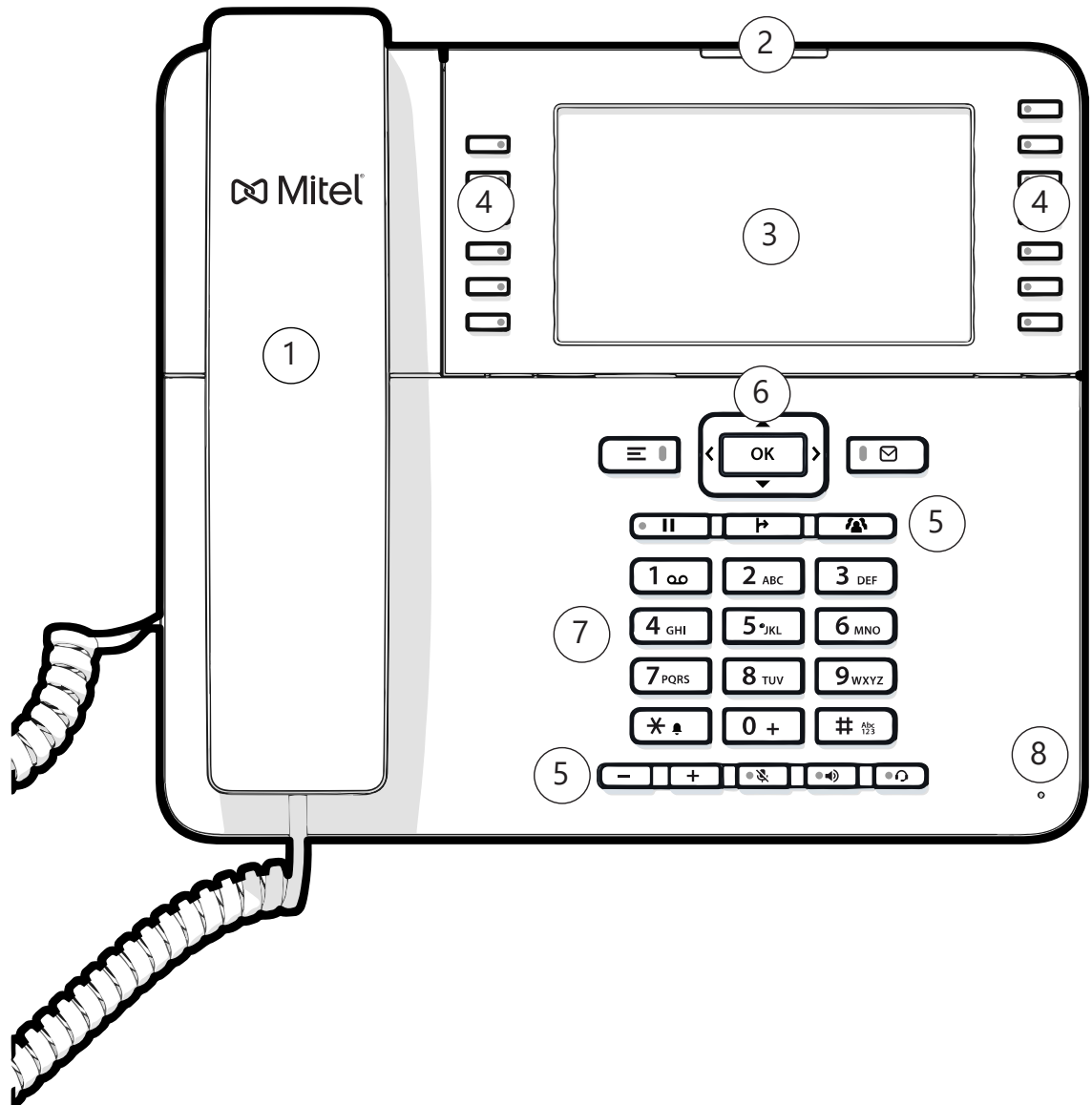
OPENScape DESK PHONE CP410












1	You can make and receive calls as normal using the handset .
2	The Notification LED ("AlertBar LED") displays the phone connection status. Incoming calls and new voice mails are visually signalled.
3	The display shows information during telephone operation.
4	The fixed function keys on the right of the display correspond to the fixed functions on the display.

5	<p>The function keys (non-programmable) are assigned to the following functions during a call:</p> <p>: Provides access to the user menu for locally controlling the phone settings.</p> <p>: Allows voice mails to be managed.</p> <p>: Hold or retrieve the active call.</p> <p>: Transfer a call to another contact.</p> <p>: Enable access to the conference functions.</p> <p>: Increases or decreases the speaker or headset volume.</p> <p>: Activates or deactivates the microphone.</p> <p>: Activate or deactivates the speakerphone during an active call.</p> <p>: Activates or deactivates the headset.</p>
6	The navigation keys help you navigating through the various phone functions, applications and configuration menus.
7	The dialpad can be used to enter phone numbers and write text.
8	You can speak without the handset using the microphone .

OPENScape DESK PHONE CP710



1	You can make and receive calls as normal using the handset .
2	The Notification LED ("AlertBar LED") displays the phone connection status. Incoming calls and new voice mails are visually signalled.
3	The display shows information during telephone operation.
4	The programmable function keys on the left of the display can be set to various functions. The fixed function keys on the right of the display correspond to the fixed functions on the display.

5	<p>The function keys (non-programmable) are assigned to the following functions during a call:</p> <ul style="list-style-type: none"> : Provides access to the user menu for locally controlling the phone settings. : Allows voice mails to be managed. : Hold or retrieve the active call. : Transfer a call to another contact. : Enable access to the conference functions. : Increases or decreases the speaker or headset volume. : Activates or deactivates the microphone. : Activate or deactivates the speakerphone during an active call. : Activates or deactivates the headset.
6	The navigation keys help you navigating through the various phone functions, applications and configuration menus.
7	The dialpad can be used to enter phone numbers and write text.
8	You can speak without the handset using the microphone .

Administration interfaces

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

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.

Note

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

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 (see "Manual registration" → page 40).

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.

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

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.

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

For further information, refer to the DLS or DMS Administration Guide.

Startup

Prerequisites

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

- An Ethernet connection to a Network with communication servers.

Note

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

Any secure interface, such as IEEE_802.1x, will require a reliable time source. Thus an SNTP server is essential for these interfaces. For additional information see: https://wiki.unity.com/wiki/IEEE_802.1x

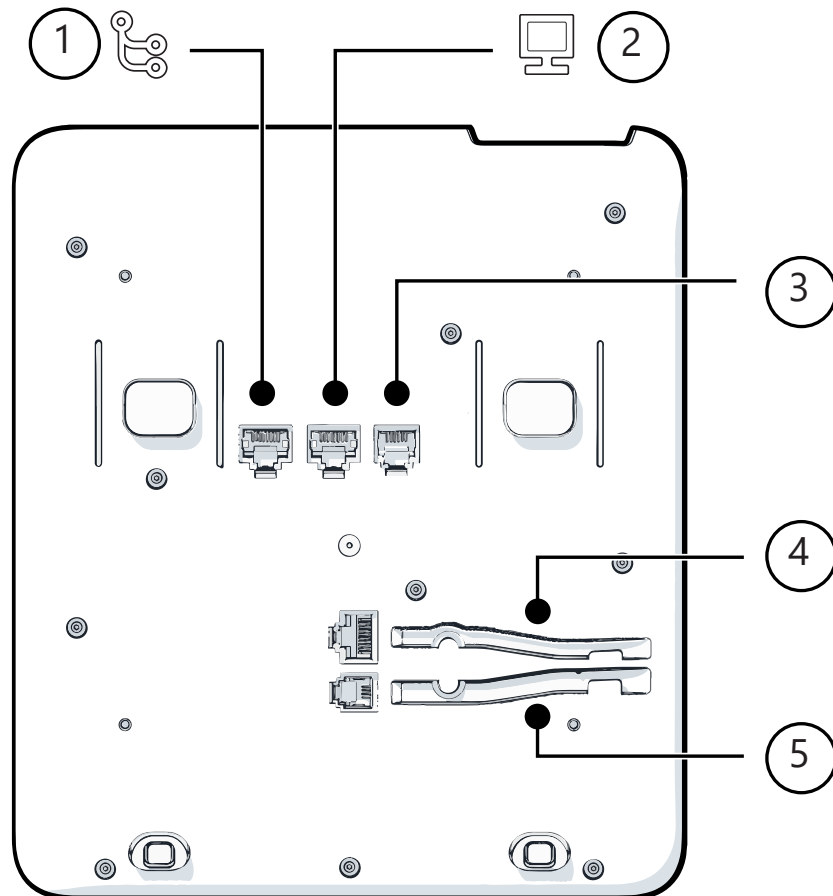
Assembling and installing the phone

SHIPMENT

- Phone
- Handset
- Handset cable
- Placement supports
- **Sub-package:** Document "Information and Important Operating Procedures"

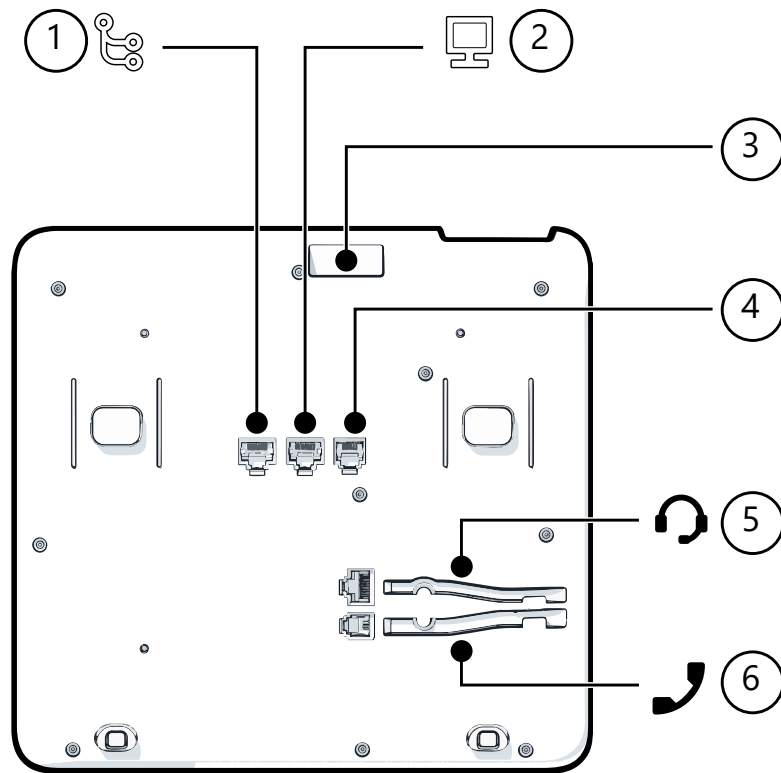
CONNECTORS AT THE BOTTOM SIDE

OpenScape Desk Phone CP110



1	Network LAN port	2	PC LAN port
3	Optional power supply	4	Headset port
5	Handset port		

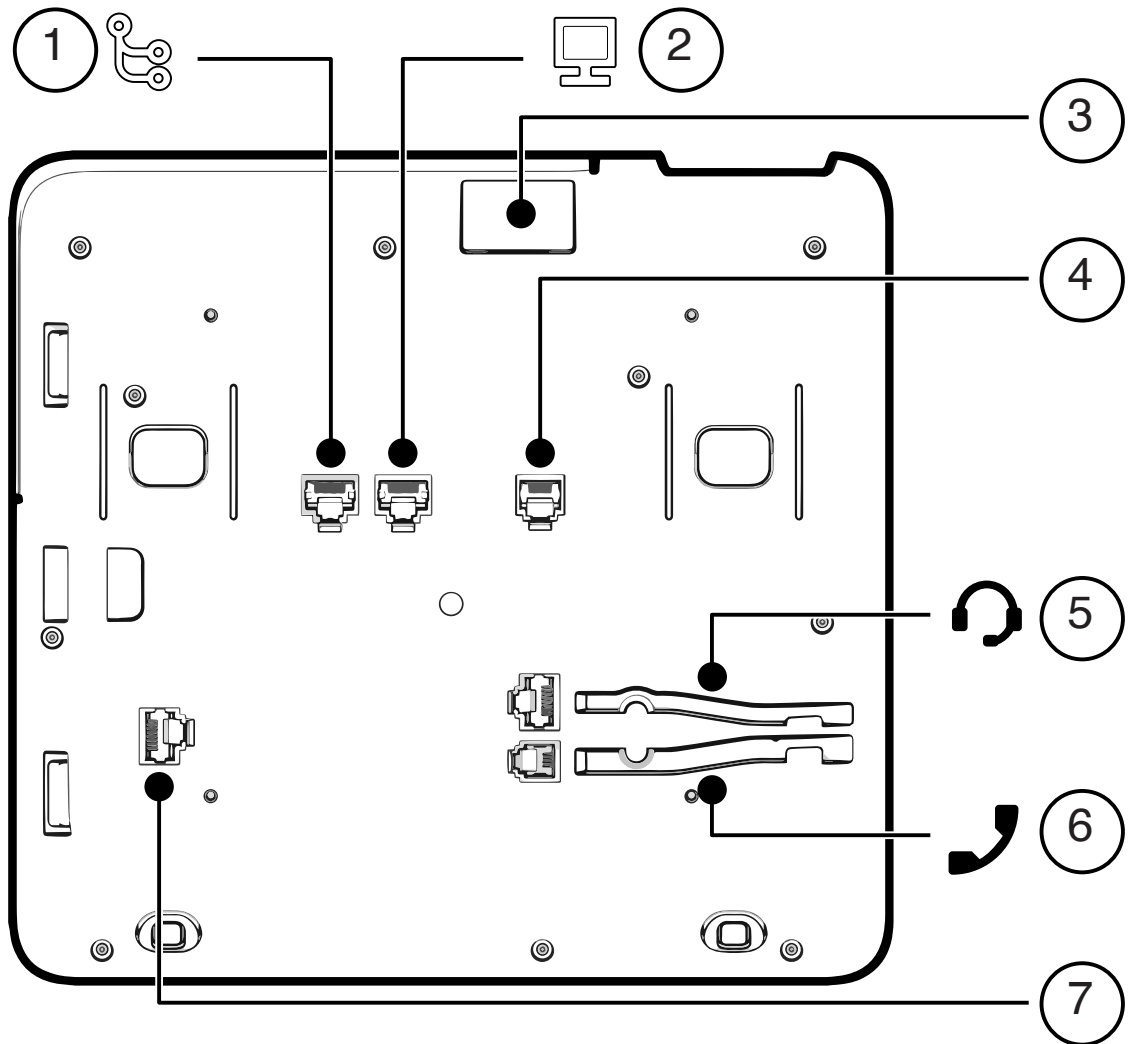
OpenScape Desk Phone CP210



1	Network LAN port	2	PC LAN port
3	USB-A port	4	Optional power supply
5	Headset port	6	Handset port
7	Key module port		

Note The key module is not “hot-swappable”: Always switch off the phone before removing or connecting a key module.

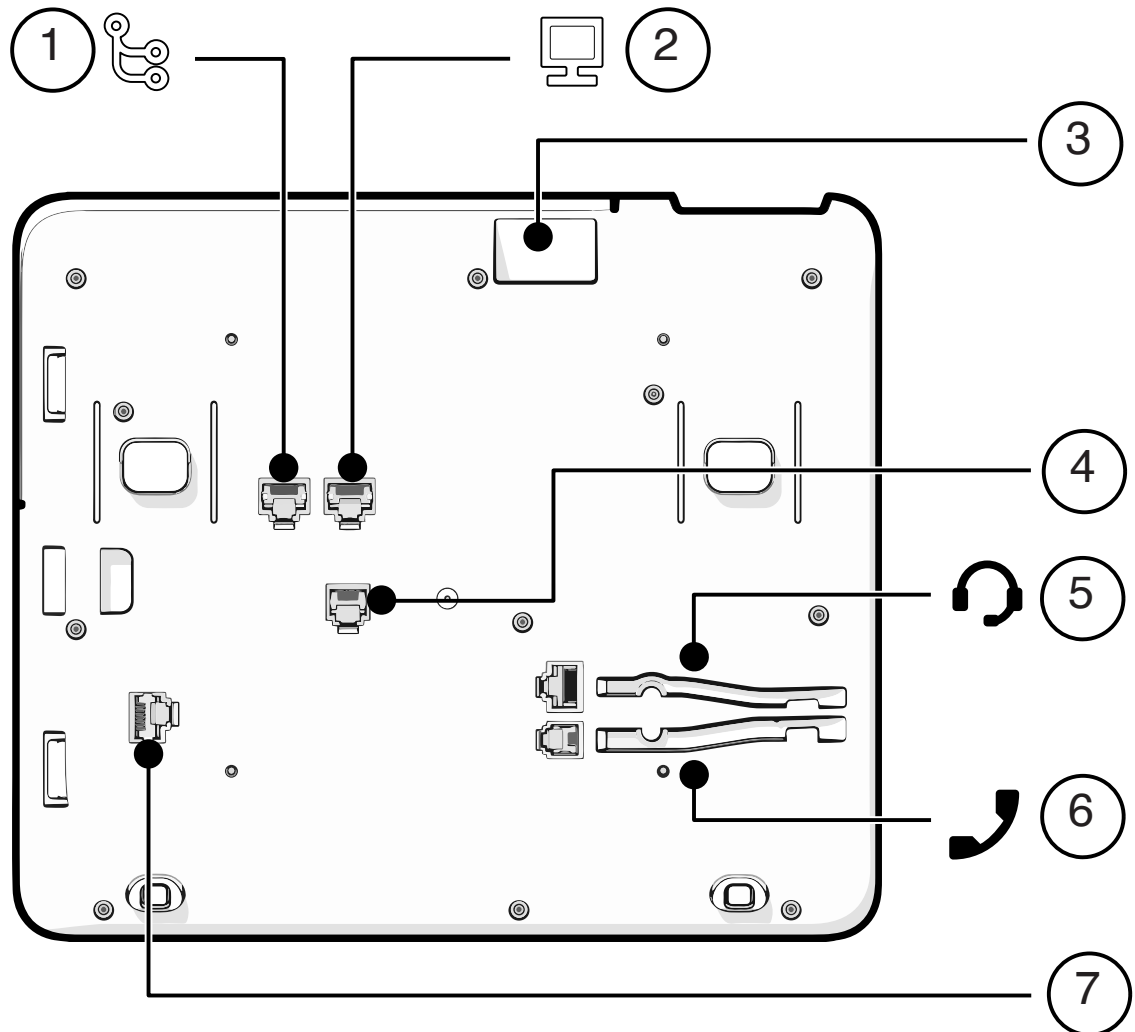
OpenScape Desk Phone CP410



1	Network LAN port	2	PC LAN port
3	USB-A port	4	Optional power supply
5	Headset port	6	Handset port
7	Key module port		

Note The key module is not “hot-swappable”: Always switch off the phone before removing or connecting a key module.


OpenScape Desk Phone CP710



1	Network LAN port	2	PC LAN port
3	USB-A port	4	Optional power supply
5	Headset port	6	Handset port
7	Key module port		


Note The key module is not "hot-swappable": Always switch off the phone before removing or connecting a key module.

ASSEMBLY

1. Insert the plug on the long end of the handset cable into the jack  on the base of the telephone.
2. Press the cable into the groove provided.
3. Insert the plug on the short end of the handset cable into the jack on the handset.

HOW TO CONNECT THE PHONE VIA LAN CABLE

When using a CP10 connector, all phones can be connected to the network via WiFi. They may require a Power-over-Ethernet (PoE) connection to power them if not connected to a power source via the power connection.


1. Plug the LAN cable into the connector  at the bottom of the telephone and connect the cable to the LAN or switch.

Note

If PoE (Power over Ethernet) is 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 supply
OpenScape Desk Phone CP110	<ul style="list-style-type: none"> • PoE (Power Class 1) • Power chord
OpenScape Desk Phone CP210	<ul style="list-style-type: none"> • PoE (Power Class 2) • Power chord
OpenScape Desk Phone CP410 <ul style="list-style-type: none"> • Only 1 key module can be connected using PoE 	<ul style="list-style-type: none"> • PoE (Power Class 2) • Power chord
OpenScape Desk Phone CP710 <ul style="list-style-type: none"> • When the power supply for the USB port is set to 120 mA, up to 4 key modules can be connected. • When the power supply for the USB port is set to 500 mA, only up to 2 key modules can be connected. 	<ul style="list-style-type: none"> • PoE (Power Class 3) • Power chord

2. If Power over Ethernet (PoE) is **not** provided by the system, plug the power supply unit into the mains.
3. Connect the power supply unit to the power connector  at the bottom of the phone (see "[Connectors at the bottom side](#)" → [page 21](#)). Up to 4 key modules can be connected to CP710 or CP410 when using a mains power supply.

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
Power supply, power cable and plug for South Africa	L30250-F600-C185
Power supply without power cable	L30250-F600-C148

4. If applicable, connect the following optional jacks:

- LAN connection to PC 
- Headset (accessory) 

HOW TO USE LAN CONNECTIONS

You may 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 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.

Note Do not use this connection to connect additional OpenScope Desk Phone CP phones, OpenScope Desk Phone IP phones, or OpenStage phones!

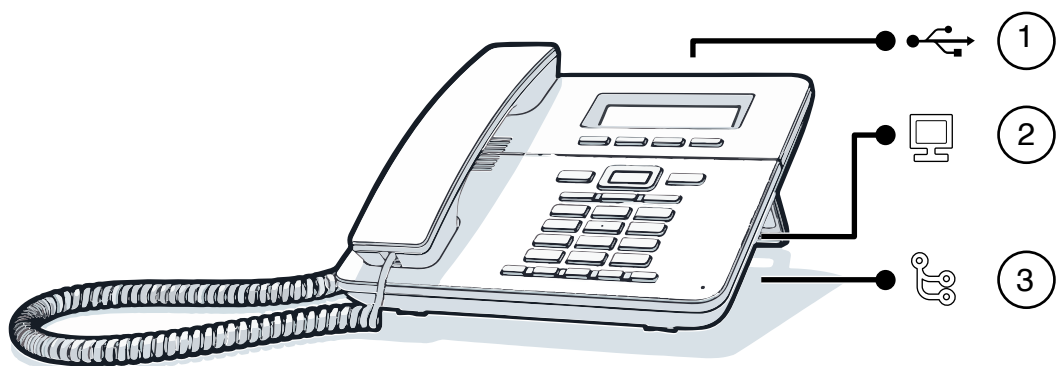


Fig.: 4-1: LAN connections (example)

HOW TO CONNECT THE PHONE VIA USB WI-FI DONGLE

Note Configuring the USB access is possible only for phones with a USB port (see "Connectors at the bottom side" → page 21).

The phone can also be connected to a wireless network via the USB type A port with the Wi-Fi USB dongle CP10 (see "The OpenScape Desk Phone CP family" → page 11).

Do not unplug the USB dongle during calls, as this disrupts the network connection.

1. Insert the USB Wi-Fi dongle into the USB port.
2. Check that USB is enabled (see "Configuring the USB access" → page 47).
3. Check that Wi-Fi is enabled (see "Wi-Fi settings" → page 70).
4. If applicable, connect the following optional jacks:
 - Headset (accessory)

KEY MODULES

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 module (KM)	Number of key modules (max.)	Additional keys per module
OpenScape Desk Phone CP410	KM410	4	16
OpenScape Desk Phone CP410	KM710	4	12
OpenScape Desk Phone CP710	KM410	4	16
OpenScape Desk Phone CP710	KM710	4	12

The configuration of a key on the key module is identical to the configuration of a phone key.

Quick start

This section describes the typical 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 information of the administration sections are given.

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.

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

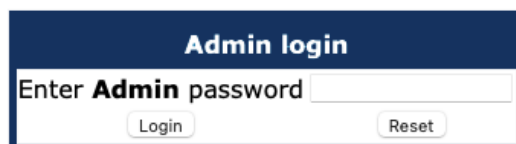
HOW TO ACCESS THE WEB INTERFACE (WBM)

Prerequisites

- The phone IP address or URL is required for accessing the phone web interface via a web browser. By default, the phone will automatically search for a DHCP server on start-up 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 /router must be defined manually.

Procedure

1. Access the local phone admin menu (see "Access via local phone" → page 29).
 - 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 router or gateway must be defined (see "Basic network configuration" → page 30).
2. Open a web browser and enter the IP address, e.g. `https://192.168.1.15` or `https://myphone.phones`. For configuring the phone DNS name, refer to "Terminal host name" → page 63.
3. If the browser displays a certificate notification, accept it.
4. Click the tab "Administrator settings".
5. Enter the admin password. The default password is "123456".



A screenshot of the 'Admin login' form. It has a dark blue header with the text 'Admin login' in white. Below the header is a white input field with the placeholder text 'Enter Admin password'. At the bottom of the form are two buttons: 'Login' and 'Reset'.

The main page of the "Administrator settings" page is displayed. The left column contains the menu tree.



- Clicking on an item printed in normal style opens the corresponding page.
- Clicking on an item printed in bold letters opens a sub-menu containing further items.

ACCESS VIA LOCAL PHONE

OpenScape Desk Phone CP110



1. Press the key for "Settings" .
2. Enter the administrator password (default password is "123456"). It is highly recommended to change the password after your first login (see section "Changing a password" → page 135).
3. Confirm with the key **OK** .

OpenScape Desk Phone CP210

1. Press the key for "Settings" .
2. Enter the administrator password (default password is "123456"). It is highly recommended to change the password after your first login (see section "Changing a password" → page 135).
3. Confirm with the key **OK** .

OpenScape Desk Phones CP410 / CP710

1. Access the administration menu:
 - Press "1 3 0" simultaneously.
 - Use the Up arrow, Down arrow and **OK** keys consecutively to select the administration menu.
2. Enter the administrator password. The default password is "123456". It is recommended to change the password after first login.
For changing the mode, press "#" once or repeatedly, depending on the desired character. The "#" key cycles around the input modes as follows: (Abc) -> (abc) -> (123) -> (ABC) -> back to start.
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 is displayed in the selected parameter field.
5. Press **OK** to enter the selective list. Use the Up Arrow and Down Arrow keys to scroll up and down in the selection list.
6. To select a list entry, press **OK**.
7. Enter the parameter value for selecting numbers and characters, use special keys.

Key	Key function during text input	Key function when held down
	Enter special characters.	<ul style="list-style-type: none"> • 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.	Phone lock on / off.

1. Use the keypad for entering parameter values. Use the navigation keys or navigation block to navigate and execute administrative actions in the administration menu.
2. Select **Save & exit** and click **OK**.

HOW TO CONFIGURE 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.

Procedure

With the WBM, the terminal number is configured as follows:

1. Log on as administrator to the WBM by entering the access data for your phone.
2. In the Administrator menu (left column), select System > System Identity to open the "System Identity" dialog.
3. Enter the terminal number.

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 "Manual configuration of the IP address" → page 58 for IP address and subnet mask, and "Default router / gateway" → page 60 for the default route.

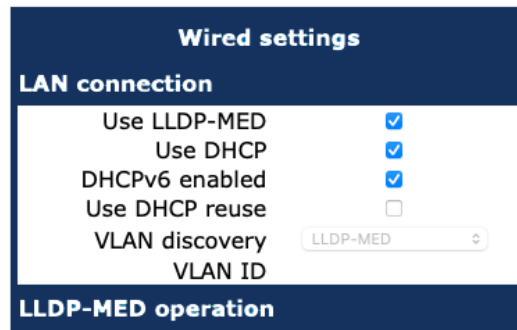
DHCP RESILIENCE

Prerequisites

It is possible to sustain Network connectivity in case of DHCP server failure. If "DHCP 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.

Procedure

1. Open Network > Wired settings.
2. Select the checkbox to enable DHCP lease reuse.



DATE AND TIME / SNTP

A SNTP (Simple Network Time Protocol) server provides the current date and time for Network clients. The IP address of a SNTP server can be given by DHCP or can be configured manually (see "Settings via SNTP" → page 91).

Consistent time for peer entities is required to allow secure interfaces to operate correctly. 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" → page 90.

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:

- **Static Routing Table** (Option #33): For manual configuration of specific/static routing, see "Specific IP routing" → page 60.

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

- **Domain Name** (Option #15): For manual configuration of the DNS domain name, see "DNS domain name" → page 62.

VENDOR-SPECIFIC VLAN DISCOVERY AND DLS ADDRESS

Note

The VLAN ID can also be configured by LLDP-MED (see "Automatic VLAN discovery using LLDP-MED" → page 50).

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

- For manual configuration of the DLS server address see "Configuration & update service" → page 65.
- For the configuration of vendor-specific settings by DHCP, there are two alternative methods:
 - Using a vendor class (see "Using vendor class" → page 35)
 - Using the DHCP option #43 (see "Using option #43 "Vendor Specific"" → page 34)
- For DMS follow the instructions in "Setting the DMS address via DHCP" → page 41.

VLAN discovery

If the phone is located in a VLAN (Virtual LAN), a VLAN ID must be assigned, see "VLAN" → page 49.

If the VLAN is provided by DHCP, VLAN Discovery must be set to "DHCP". The corresponding DHCP option is vendor-specific, thus a specific procedure is necessary.

- For automatic configuration via LLDP-MED see "Automatic VLAN discovery using LLDP-MED" → page 50.
- For automatic configuration via DHCP see "Automatic VLAN discovery using DHCP" → page 51.
- For manual configuration see "Manual configuration of a VLAN ID" → page 53.

For information on how to use a vendor class, refer to "Using vendor class" → page 35

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 is used. If no appropriate TLV is received, DHCP is used for VLAN discovery.

Administration via WBM

1. Open Network > Wired settings.

Wired settings	
LAN connection	
Use LLDP-MED	<input type="checkbox"/>
Use DHCP	<input checked="" type="checkbox"/>
DHCPv6 enabled	<input type="checkbox"/>
Use DHCP reuse	<input checked="" type="checkbox"/>
VLAN discovery	DHCP
VLAN ID	
LLDP-MED operation	
Time to live (seconds)	120

Wired settings	
LAN connection	
Use LLDP-MED	<input checked="" type="checkbox"/>
Use DHCP	<input checked="" type="checkbox"/>
Use DHCP reuse	<input type="checkbox"/>
VLAN discovery	LLDP-MED
VLAN ID	
LLDP-MED operation	
Time to live (seconds)	120

1. Enable "Use LLDP-MED".
2. Select "LLDP-MED" in the option "VLAN discovery".

Administration via local phone

```
|--- Administration
    |--- Network
        |--- Wired settings
            |--- LAN connection
                |--- Use LLDP-MED
```

Manual configuration of a VLAN ID

Note If you configure a phone to an incorrect VLAN, the phone may not connect to the network.

Administration via WBM

1. Open Network > Wired settings.

Wired settings

LAN connection

Use LLDP-MED ☐

Use DHCP ☒

DHCPv6 enabled ☒

Use DHCP reuse ☐

VLAN discovery

VLAN ID

LLDP-MED operation

2. In "LAN connection", set "VLAN discovery" to "Manual".
3. Click **Submit**.

Please select mode

VLAN discovery

VLAN ID

4. Set a VLAN ID between 1 and 4095.
5. Click **Submit**.

Administration via local phone

```
|--- Administration
  |--- Network
    |--- Wired settings
      |--- LAN connection
        |--- Use LLDP-MED
          ...
        |--- VLAN ID
```

Using 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

DLS server address

This setting only applies if a DLS / 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" → page 65](#).
- For configuration of the DMS, see ["Setting the DMS address via DHCP" → page 41](#).
- For the configuration of vendor-specific settings by DHCP, there are two alternative methods:
 - the use of DHCP option #43
 - the use of a vendor class

For information on how to use a vendor class, refer to ["Using vendor class" → page 35](#)

Setting up the DLS Server

1. In the Windows Start menu, select Start > Programs > Administrative Tools > DHCP.
2. Select the DHCP server and the scope.
3. Select "Configure Options" in the context menu using the right mouse button.
4. Enter the IP address and port number of the DLS server.
5. Click **Apply**.
6. Click **OK**.

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.

Setup 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 required DHCP server and select **Define Vendor Classes...** in the context menu.
3. Click **Add**.

4. Define a new vendor class with the name **OptiIpPhone** and enter a description of this class.
5. Click **OK**. The new vendor class now appears in the list.
6. Close the window.

Add options to the new vendor class

Two options or tags is added to the vendor class. Two passes are needed:

- In the first pass, tag #1 with the required value "Siemens" is entered.
- In the second pass, the DLS address is entered as tag #3.

Note 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).

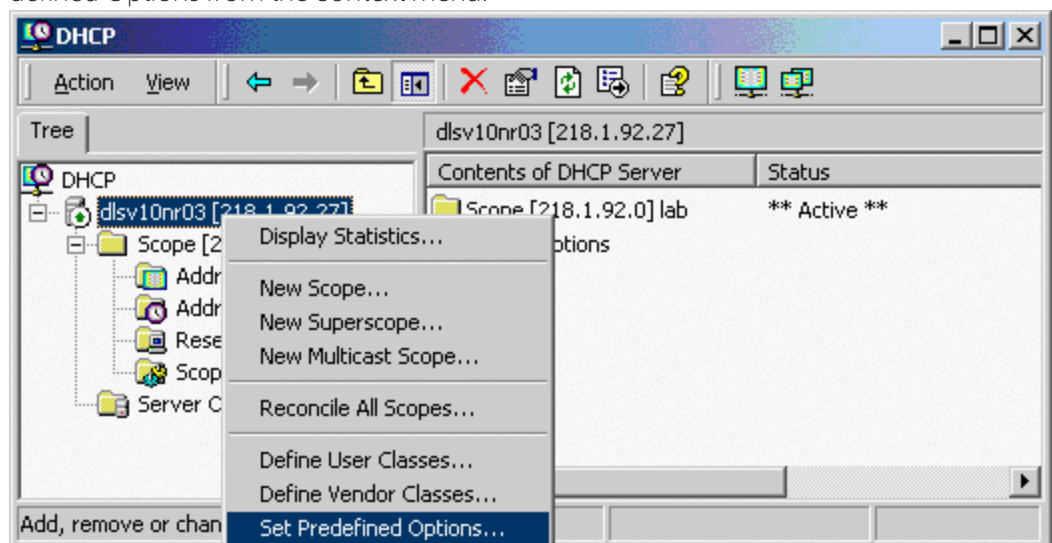
You can use the following command to configure the required option (without error message) so that it also appears later in the DHCP console:

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

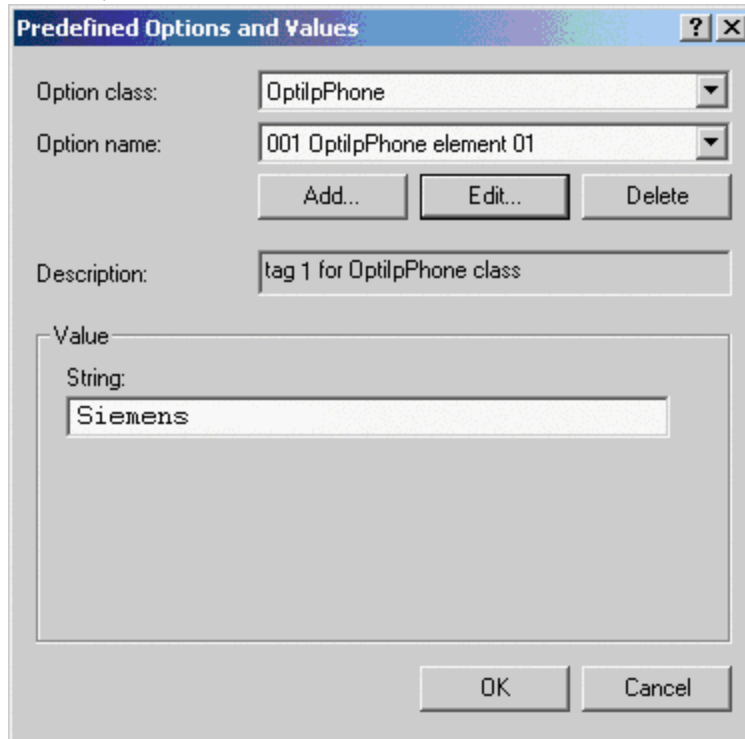
The value **SIEMENS** for optiPoint Element 1 can then be re-assigned over the DHCP console.

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 Pre-defined Options from the context menu.



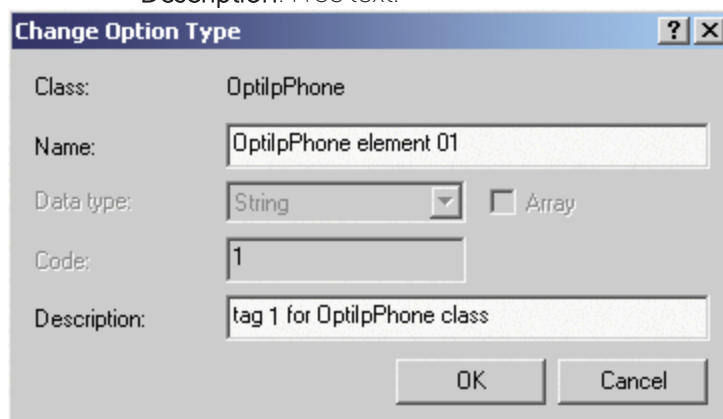
2. In the dialogue, select the previously defined OptilpPhone class and click on Add... to add a new option.



The dialog box titled "Predefined Options and Values" contains the following fields and controls:

- Option class:** A dropdown menu with "OptilpPhone" selected.
- Option name:** A dropdown menu with "001 OptilpPhone element 01" selected.
- Buttons:** "Add...", "Edit...", and "Delete" buttons are located below the option name dropdown.
- Description:** A text field containing "tag 1 for OptilpPhone class".
- Value section:** A container with a "String:" label and a text field containing "Siemens".
- Buttons:** "OK" and "Cancel" buttons are at the bottom right.

3. Enter the following data for the new option:
 - First Pass: Option 1
 - Name: Free text, e. g. "OptilpPhone element 01"
 - Data type: "String"
 - Code: "1"
 - Description: Free text.
 - Second Pass: Option 3
 - Name: Free text, e. g. "OptilpPhone element 03"
 - Data type: "String"
 - Code: "3"
 - Description: Free text.

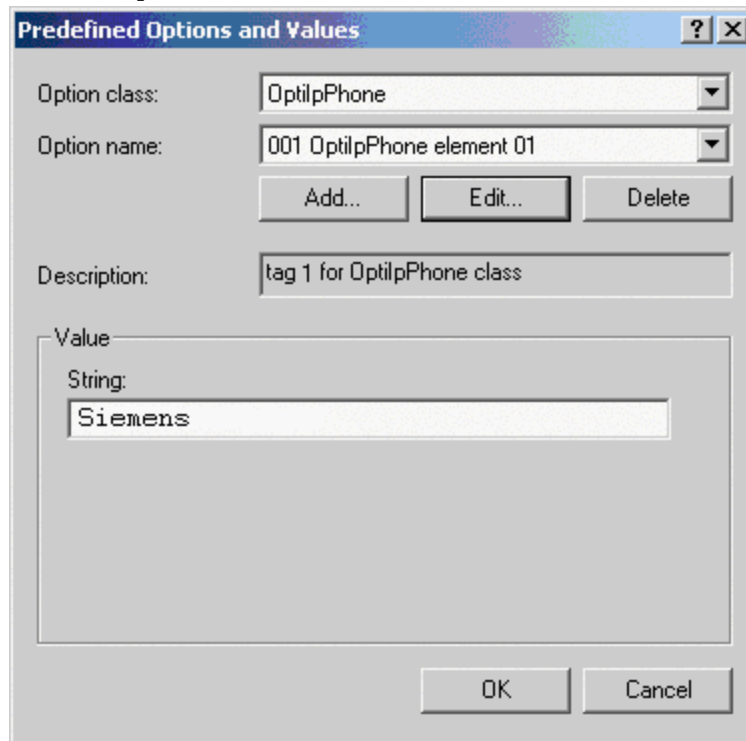


The dialog box titled "Change Option Type" contains the following fields and controls:

- Class:** A text field containing "OptilpPhone".
- Name:** A text field containing "OptilpPhone element 01".
- Data type:** A dropdown menu with "String" selected, and an unchecked checkbox labeled "Array".
- Code:** A text field containing "1".
- Description:** A text field containing "tag 1 for OptilpPhone class".
- Buttons:** "OK" and "Cancel" buttons are at the bottom right.

4. Enter the value for this option.

- **First Pass:** "Siemens"
- **Second Pass:** DLS address The DLS address has the following format:
 PROTOCOL:://IP ADDRESS OF DLS SERVER:PORT NUMBER Example:
 sd1p://192.168.3.30:18443

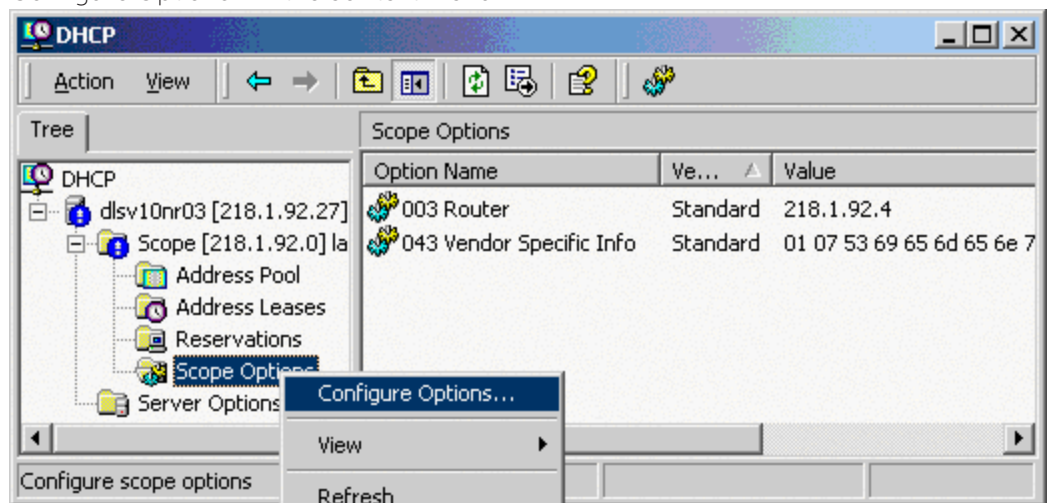


5. Click OK.

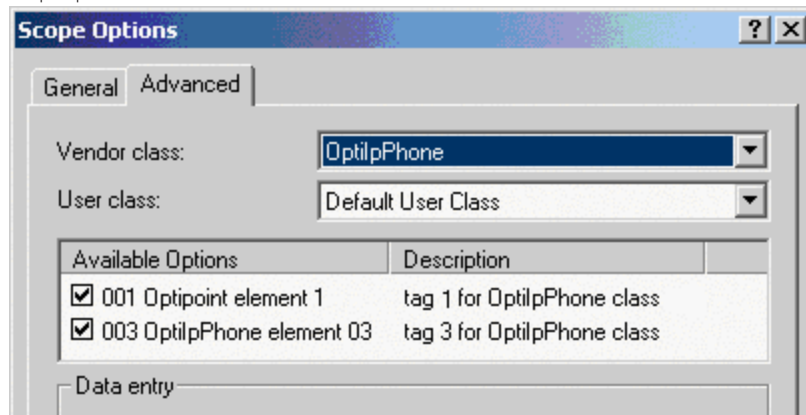
6. Repeat steps 2 to 5 for the second pass.

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.



3. Activate the options that you want to assign to the scope (in this example, 001 and 003).
4. The DHCP console shows the information that is 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 i 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";
}
```

HFA GATEWAY SETTINGS

To connect the OpenScape Desk Phone CP phone to the OpenScape Business or OpenScape 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.

MANUAL REGISTRATION

1. Open the web interface of the phone using its IP address.
2. Open the tab "Administration" and enter the admin password.
3. Open System > Gateway.

Gateway	
System type	OpenScape Business ▼
IP address	10.12.139.110
Gateway ID	DEFAULTH323ID
Subscriber number	723
Password	
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

4. Select the system type from the drop-down menu.
5. Enter the IP address and the name of the gateway server.
6. Enter the subscriber number.
7. Enter the user password of the subscriber.
8. Click **Submit**.

USING THE LOCAL MENU

1. In the administration menu, go to System > Gateway. For further instructions on entering data using the Local menu see "Access via local phone" → page 29.

```

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

2. Enter the IP or DNS address of the HFA gateway provided by the 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.
5. Select **Save & exit** and click **OK**.

SETTING THE 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.

Note The DMS address is mutually exclusive with a possibly provided DLS address. A phone can either connect to a DLS or DMS server.

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.

Example

Tag	Length	Content (Example)
01	07	5369656d6556e73
02	04	00000065
03	1d	68747470733a2f2f3933 ... 3131342E39363a3434332f646d73
ff		

Each tag has an explicit length value and is closed by the 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
 - 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. You can find details for configuration of a VLAN ID here: http://wiki.unify.com/wiki/VLAN_ID_Discovery_over_DHCP.

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	68747470733a2f2f39332e3132322e3131342e39363a3434332f646d7-3

Option #66 does not have specific tags, only 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)

CLOUD DEPLOYMENT

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

The phone determines that a cloud deployment process is to be used based on the IP settings it receives from the DHCP at the customer site. The "Unify Redirect" server redirects the phone to a DLS-WPI based management system operated by the cloud service provider. This management system completes the configuration of the phone with all the information required for it to be usable and may also customize the phone for the cloud service provider's "house" style.

If zero touch deployment is available the phone is automatically connected to the management system. However, if zero touch deployment is not possible, then a cloud deployment pin must be entered at the phone. This PIN is a code that determines which cloud service provider is responsible for the phone. The code is provided as part of a pin supplied from the cloud organization to the user.

Process of cloud deployment

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

Preconditions:

- The phone is not running
- The phone is set to factory default values
- The phone has a LAN connection
- The LAN connection provides access to the public internet

Start

Phone broadcasts a DHCP request	The phone has all the information that it needs to contact a DNS server. A DLS address is not
---------------------------------	---

	provided.
--	-----------

A DHCP server responds with IP addresses	
--	--

The phone detects that a cloud deployment is required	<ul style="list-style-type: none"> • DHCP is available • IP address allocated to the phone • DNS address is available • Subnet mask is available • Router address is available • No DLS address available • No SIP addresses available
---	---

The phone starts the zero touch cloud deployment process	The phone is locked so that the mode keys and FPKs etc cannot be used
--	---

The phone obtains the IP address of the Unify Redirect server ("cloud-setup.com") from the DNS	
--	--

Phone contacts the Unify Redirect server using DLS-WPI	
--	--

Phone displays the Progress prompt	
------------------------------------	--

Phone receives configuration items from the Unify Redirect server	<ul style="list-style-type: none"> • DLS address (set to the name of the Deployment server) • Language (optional) • DLS port (optional)
---	--

Phone saves the configuration data	If the language is changed the display is updated
------------------------------------	---

Phone updates, and displays the progress prompt	
---	--

The phone obtains the IP address of the deployment server from the DNS by looking up the DLS address if appropriate.	<p>The stored DLS address is not changed by the result of the DNS look-up.</p> <p>NOTE: <i>For zero touch deployment, the redirect server must already know the MAC address of the phone and uses it to identify the DLS address to provide to the phone. If the redirect server does not recognize the phone by its MAC address then it expects a pre-distributed pin to be provided by the phone.</i></p>
--	--

Phone contacts the deployment server using DLS-WPI	The hash of the pin is provided as an inventory item to the deployment server
--	---

Deployment server configures the phone and the phone saves the changes	
--	--

Deployment server terminates the DLS-WPI session

The phone exits the cloud deployment process and enables the mode keys and FPKs etc. to act as normal



Phone removes the progress prompt and displays a timed success pop-up, indicating that cloud deployment is done

The phone verifies that it now has an e164 number

registered

Reducing deployment time with a deployment parameter

To reduce the installation time of a phone connected to a DLS, the administrator enters a deployment parameter and leaves the installation process to the DLS.

1. Press the key  and connect the phone to the power supply or PoE.
2. When the phone displays the screen for entering the PIN, enter one of the following numbers:
 - The e164-number of the phone that enables the DLS to recognise it.
 - The deployment pin of the redirect server to identify the appropriate DLS that can provide the correct plug & play data for installation.
 - A security pin if the DLS needs to bootstrap the phone into secure mode communication with the DLS.
3. Conclude input with . The installation proceeds.

Aborting cloud deployment process by user

The phone detects that a cloud deployment is required and starts the cloud deployment process. The phone expects the input of the PIN by the user. At this point the user has the option to cancel the process. If the user confirms his decision, the deployment process is aborted.

Re-trigger cloud deployment

Cloud deployment may be restarted by triggering a factory reset:

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

Deployment errors

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

- It is shown to notify the phone User that deployment failed to complete as expected.
- It is a non-timed warning popup
- It is non-dismissible by user action

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

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

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 section.
- For access using the web interface (WBM), see ["How to access the web interface \(WBM\)"](#) → page 28.

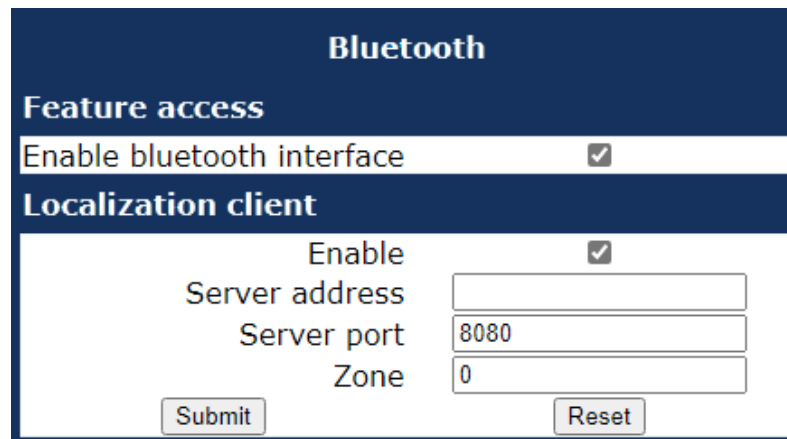
Bluetooth interface

Note This feature is available only on OpenScape Desk Phone CP710.

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

Administration via WBM

1. Open Bluetooth.



The screenshot shows a web interface titled "Bluetooth". Under the heading "Feature access", there is a checkbox labeled "Enable bluetooth interface" which is checked. Below this, under the heading "Localization client", there is another checked checkbox labeled "Enable". To the right of the "Enable" checkbox are three input fields: "Server address" (empty), "Server port" (containing "8080"), and "Zone" (containing "0"). At the bottom left is a "Submit" button and at the bottom right is a "Reset" button.

2. Enable or disable the Bluetooth interface.
3. If the phone is used to detect BLE advertisements, enable the localization client.
4. Provide the server address and port number, as well as the zone.
5. Click **Submit**.

Administration via local phone

|--- Bluetooth

Configuring the USB access

Note Configuring the USB access is possible only for phones with a USB port (see "Connectors at the bottom side" → page 21).

Administration via WBM

1. Open Admin > System > Features > Feature access.

Services	
Bluetooth	<input checked="" type="checkbox"/>
USB device access	<input checked="" type="checkbox"/>
USB power using PoE	120mA (up to 4 KMs) ▼
Web based manag.	120mA (up to 4 KMs)
Feature toggle	500mA (up to 2 KMs)
Phone lock	<input checked="" type="checkbox"/>
Limited FPK set	No limitation ▼
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

2. In "Services", enable "USB device access". When enabled, the user is able to use the USB port for communication and data exchange (see "How to connect the phone via USB Wi-Fi dongle" → page 27).
3. Select "USB power using PoE" to configure the power supply options when powering the phone via PoE. The power supply via PoE is limited and can only supply the following combinations when USB is enabled (refer to "How to connect the phone via LAN cable" → page 25).
 - When the power supply for the USB port is set to 120 mA, up to 4 key modules can be connected.
 - When the power supply for the USB port is set to 500 mA, only up to 2 key modules can be connected.
4. Click **Submit**.

LAN settings

LAN PORT SETTINGS

The OpenScape Desk Phone CP phones provide an integrated switch that connects the LAN, the phone and a PC port. By default, the switch will auto negotiate the transfer rate (10/100/1000 Mbps), autosensing, configurable, and duplex method (full or half duplex) with the equipment connected. Optionally, the required transfer rate and duplex mode can be specified manually using the LAN port speed parameter.

Note 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", the PC port is active.
- If set to "Mirror", the data traffic at the LAN port is mirrored at the PC port. This setting is for diagnostic purposes. If, for instance, a PC running Ethereal / Wireshark is connected to the PC port, all network activities at the phone's LAN port can be captured.

Note Do not use this connection for further phones!

Note Removing the power from the phone or a phone reset or 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.

Administration via WBM

1. Open Network > Wired settings.

- **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", "Gbps full duplex"
 - 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", "Gbps full duplex"
 - 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** (only with CP10): You have the option to disable the LAN port connection when a Wi-Fi network is configured.

Administration via local phone

```
|--- Admin
    |--- Network
        |--- Wired settings
            |--- LAN port configuration
                |--- LAN port disabled
                |--- LAN port status
                |--- LAN port speed
            |--- PC port configuration
                |--- PC port status
                |--- PC port speed
                |--- PC port mode
                |--- PC port autoMDIX
```

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.

Note

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 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 (with fallback to DHCP)
- By DHCP
- Manually

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 is used. If no appropriate TLV is received, DHCP is used for VLAN discovery.

Administration via WBM

1. Open Network > Wired settings.

Wired settings

LAN connection

Use LLDP-MED ☐

Use DHCP ☒

DHCPv6 enabled ☐

Use DHCP reuse ☒

VLAN discovery DHCP

VLAN ID

LLDP-MED operation

Time to live (seconds) 120

2. Enable "Use LLDP-MED".
3. Set "VLAN discovery" to "LLPD-MED".
4. Select the "Time to live" (TTL) in seconds.
 - Value range: 40...400 seconds
 - Default: 120 seconds
5. Click **Submit**.

Administration via local phone

```
|--- Administration
    |--- Network
        |--- Wired settings
            |--- LAN connection
                |--- Use LLDP-MED
            |--- LLDP-MED operation
                |--- TTL
                    |--- TTL (secs)
```

Automatic VLAN discovery using DHCP

To automatically discover a VLAN ID using DHCP (except LLDP-MED), the phone must be configured as "DHCP". The DHCP server is configured to supply the Vendor Unique Option in the correct VLAN over DHCP format (see "Using option #43 "Vendor Specific" → page 52).

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 not be correct.

Administration via WBM

1. Open Network > Wired settings.

Wired settings

LAN connection

Use LLDP-MED ☐

Use DHCP ☒

DHCPv6 enabled ☐

Use DHCP reuse ☒

VLAN discovery DHCP

VLAN ID

LLDP-MED operation

Time to live (seconds) 120

2. Deselect "Use LLDP-MED".
3. Select "DHCP" in the VLAN discovery option.
4. Click **Submit**.

Administration via local phone

```
|--- Administration
    |--- Network
        |--- Common settings
            |--- Protocol mode
        |--- Wired settings
            |--- LAN connection
                |--- Use LLDP-MED
                |--- VLAN discovery
```

Using option #43 "Vendor Specific"

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

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

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

- **Tag 004:** DLS hostname

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

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

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

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

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

Cod- e	Length	DLS IP address																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																
-----------	--------	----------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Manual configuration of a VLAN ID

To configure VLAN manually, the phone must be provided with a VLAN ID between 1 and 4095.

Note If you misconfigure a phone to an incorrect VLAN, the phone will not connect to the network. If in static IP mode, no server connections is possible.

Administration via WBM

1. Open Network > Wired settings.

2. Deselect "Use LLDP-MED".
3. Set "VLAN discovery" to "Manual".
4. Click **Submit**.

5. Enter the VLAN ID.
6. Click **Submit**.

Administration via local phone

```
|--- Administration
    |--- Network
        |--- Wired settings
            |--- LAN connection
                |--- Use LLDP-MED
                |--- VLAN discovery
```

IP Network parameters

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.

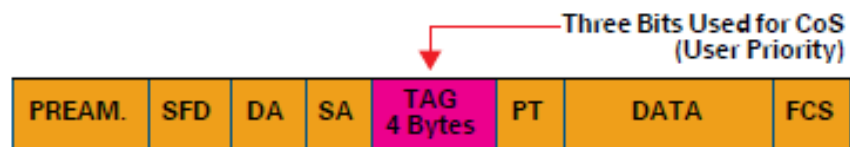
Note

Layer-2 and -3 QoS for voice and signaling transmission can be set via LLDP-MED (see "Automatic VLAN discovery using LLDP-MED" → page 50). The value cannot be changed by another interface.

Layer 2 / 802.1p

QoS on layer-2 is using 3 Bits in the 802.1q/p 4-Byte VLAN tag which must 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.



Administration via WBM

1. Open Network > QoS.

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

Administration via local phone

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

Layer-3 / Diffserv

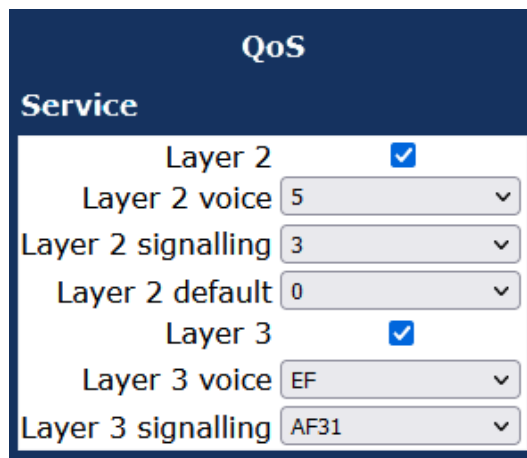
Diffserv assigns a class of service to an IP packet by adding an entry in the IP header.

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

- 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".
- 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".
- 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: AFX 1 (low drop probability), AFX 2 and AFX 3 (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.

Administration via WBM

1. Open Network > QoS.



QoS	
Service	
Layer 2	<input checked="" type="checkbox"/>
Layer 2 voice	5
Layer 2 signalling	3
Layer 2 default	0
Layer 3	<input checked="" type="checkbox"/>
Layer 3 voice	EF
Layer 3 signalling	AF31

- **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 signaling:** Sets the CoS (Class of Service) value for signaling.
 - Value range: "BE", "AF11", "AF12", "AF13", "AF21", "AF22", "AF23", "AF31", "AF32", "AF33", "AF41", "AF42", "AF43", "EF", "CS7", "CS3", "CS4", "CS5", 0, 1, 2 ... through 63.
 - Default: "AF31"

Administration via local phone

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

USE DHCP

If this parameter is set to "Yes" (default), the phone will search for a DHCP server on start-up and try to obtain IP data and further configuration parameters from that central server.

Note The data obtained via DHCP cannot be changed with DHCP enabled. Also, when DHCP is enabled, the data read from the server overwrites current values on the phone

If no DHCP server is available in the IP network, deactivate this option. In this case, the IP address, subnet mask, and default gateway / route must be defined manually.

Note 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.

DHCP parameters

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)
 - SIP Addresses / SIP Server & Registrar (SIP Server option 120)
 - VLAN ID, DLS address (Vendor specific Information option 43)

Administration via WBM

1. Open Network > Wired settings.

2. Select "Use DHCP".
3. Click **Submit**.

Administration via Local Phone

```
|--- Admin
    |--- Network
        |--- Wired settings
            |--- LAN connection
```

MANUAL CONFIGURATION OF THE IP ADDRESS

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

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, 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. Open Network > Wired settings.

2. Deselect "Use LLDP-MED", "Use DHCP", and "DHCPv6 enabled".

3. In the tab "IPv4 routing", enter the IP address, the gateway, and the (subnet) mask for Route 1.
4. If applicable, enter the data for route 2.
5. Click **Submit**.

Administration via local phone

```
|--- Admin
    |--- Network
        |--- Wired settings
            |--- LAN connection
                |--- Protocol mode

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

DEFAULT ROUTER / GATEWAY

If not provided by DHCP dynamically, enter the IP address of the router that links your IP network to other networks. If the value was assigned by DHCP, it is read-only.

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

Administration via WBM - IPv4

1. Open Network > Wired settings.

IPv4 routing	
Route 1 IP address	<input type="text"/>
Route 1 gateway	<input type="text"/>
Route 1 mask	<input type="text"/>
Route 2 IP address	<input type="text"/>
Route 2 gateway	<input type="text"/>
Route 2 mask	<input type="text"/>

2. Enter the default route, i.e. the IP address of the router that links your IP network to other networks.
3. Click **Submit**.

Administration via local phone - IPv4

```
|--- Admin
    |--- Network
        |--- Wired settings
            |--- LAN connection
                |--- IPv4 routing
```

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

- 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

1. Open Network > IPv4 configuration.

IPv4 routing	
Route 1 IP address	<input type="text"/>
Route 1 gateway	<input type="text"/>
Route 1 mask	<input type="text"/>
Route 2 IP address	<input type="text"/>
Route 2 gateway	<input type="text"/>
Route 2 mask	<input type="text"/>

2. 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.
3. Click **Submit**.

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
```

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.

DNS domain name

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

Administration via WBM

1. Open Network > Common settings.

2. Enter the DNS domain the phone belongs to.
3. Click **Submit**.

Administration via local phone

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

DNS servers

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

When DHCP is enabled, the DNS server is read-only.

Note Depending on the configuration chosen for survivability, DNS SRV is required. For details, refer to "Resilience and survivability" →1.

Administration via WBM

1. Open Network > Common settings.

2. Enter the name of the DNS domain.

3. Enter the IP addresses of the Primary DNS and the Secondary DNS server.
 - **Primary DNS:** IP address of the primary DNS server.
 - **Secondary DNS:** IP address of the secondary DNS server.
4. Click **Submit**.

Administration via local phone

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

Terminal host name

The phone host name can be customized.

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

Note 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 is 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:

Administration via WBM

1. Open System > System Identity.

2. Select the DNS name construction.
 - **None:** No host name 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 string entered in Web name.
 - **Only number:** The DNS name is set to the Terminal number, i.e. the phone's call number (E.164).

- **Prefix number:** The DNS name is constructed from the string entered in Web name, followed by the Terminal number.
3. Click **Submit**.

Administration via local phone

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

IP TTL

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

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

Administration via WBM

1. Open Network > Common settings.

Common settings	
Protocol mode	IPv4_IPv6
DNS domain	fritz.box
Primary DNS	192.168.178.1
Secondary DNS	
HTTP proxy	
IP TTL	64
Parse DHCP option 43	<input checked="" type="checkbox"/>
Parse DHCP option 66	<input checked="" type="checkbox"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

2. Select the desired value for “IP TTL”.
 - Values: 64 or 128 (seconds)
3. Click **Submit**.

Administration via local phone

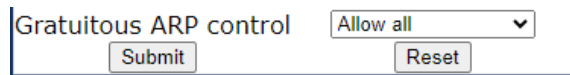
```
|--- Admin
    |--- Network
        |--- Common settings
            |--- IP Time to live
```


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.

Administration via WBM



Gratuitous ARP control Allow all ▼

- To drop gratuitous ARP frames before they can be used in an ARP attack, set option Gratuitous ARP control to "Block all".
 - Default: Allow all.
- Click **Submit**.

Note Blocking of gratuitous ARP frames is available only in an IPv4 network. If protocol mode IPv6 is configured, the 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" → page 49.

Administration via local phone

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

CONFIGURATION & UPDATE SERVICE

All items can be administered by management applications in both OpenScape and non OpenScape networks. Among the most important features are:

- Security (e.g. PSS generation and distribution within an SRTP security domain)
- Mobility for OpenScape SIP phones
- Software deployment
- Plug & play support
- Error and activity logging.

OpenScape Deployment Service (DLS) address, i.e. the IP address or host name 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.

The mode (labeled "Mode" in the local phone administration 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.

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:

- The DLS server requests the phone to contact it by sending a HTTP "Contact-Me" request or by leaving a request at the DCMP poll server for the phone to check periodically.
- The phone always establishes the connection to the DLS server.

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, which is placed outside of the phone 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.

Note 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.

Administration via WBM

1. Open Network > Update Service (DLS).

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	<input type="checkbox"/>
DLS address	<input type="text"/>
Default mode port	18443
Lock DLS address	<input type="checkbox"/>
Revert to default security	<input type="checkbox"/>
Mode	Default
Security PIN	<input type="text"/>
Device management service (DMS)	
DMS address	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Minimum update check (seconds)	300
Update check during working hours	<input checked="" type="checkbox"/>
Ignore software update from config file	<input type="checkbox"/>
Check for update	Now
Submit	Reset

Deployment service (DLS)

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.

- **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.).

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

- **DLS address:** IP address or host name of the server on which the Deployment Service is running.
- **Default mode port:** Port on which the DLS Deployment Service is listening.
 - Default: 18443.
- **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.

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

- **Revert to default security** disables mutual authentication and returns to DEFAULT mode. SECURE mode related settings are reset and certificates are removed.
- **Revert to default security:** When set, security mode is set to default. When using local phone administration, this is set by selection option "Default security".
- **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.

Note A security PIN can be provided which is used for decrypting data provided by the DLS during bootstrap.

Bootstrapping is the process by which an initial non-secure connection to the DLS is elevated to a secure connection. Once the connection has been elevated to secure mode it will stay in that mode for subsequent connections to the same DLS.

For further information, refer to the DLS documentation.

Device management service (DMS)

The DMS is a configuration file based deployment service which can be used instead of a DLS. The DMS address can be provided manually or via DHCP for a full plug & play installation (see "Setting the DMS address via DHCP" → page 41).

The DMS is compatible to the Broadsoft DMS and the RingCentral provisioning server. A detailed description can be found here: https://wiki.unify.com/wiki/Device_Management_System

- **DMS address:** IP address or host name of the server on which the DMS is running.
- **Username:** User name for authentication.
- **Password:** Password for authentication.
- **Minimum update check (seconds):** Time between two configuration requests to the DMS.
- **Update check during working hours:** Enables checking for updates during office hours, which may decrease performance.
- **Ignore SW update from config file:** Any software link provided by the DMS will be ignored.
- **Check for Update: Now** forces the phone to an immediate check for a new configuration.

Administration via local phone

```
|--- Admin
    |--- Network
        |--- Deployment Service
            |--- Disable DLS-WPI
            |--- DLS address
            |--- Default mode port
            |--- Revert to default security
```

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.

Note OpenScape Desk Phone CP phones support SNMPv1.

Trap categories

There are currently 3 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 phones.** 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.

Administration via WBM

1. Open System > SNMP.

The image shows a web-based configuration interface for SNMP. It is divided into three main sections: Generic traps, Diagnostic traps, and QoS report traps. Each section contains several configuration options with checkboxes and text input fields. At the bottom, there are 'Submit' and 'Reset' buttons.

SNMP	
Generic traps	
Trap sending enabled	<input type="checkbox"/>
Trap destination	<input type="text"/>
Trap destination port	<input type="text" value="162"/>
Trap community	<input type="text" value="....."/>
Queries allowed	<input type="checkbox"/>
Query password	<input type="text"/>
Diagnostic traps	
Diagnostic sending enabled	<input type="checkbox"/>
Diagnostic destination	<input type="text"/>
Diagnostic destination port	<input type="text"/>
Diagnostic community	<input type="text"/>
Diagnostic to generic destination	<input type="checkbox"/>
QoS report traps	
QoS traps to QCU	<input type="checkbox"/>
QCU address	<input type="text"/>
QCU port	<input type="text" value="12010"/>
QCU community	<input type="text" value="....."/>
QoS to generic destination	<input type="checkbox"/>
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

- **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 host name 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 host name 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 host name 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 local phone

```
|--- Admin
    |--- System
        |--- SNMP
            |--- Queries allowed
                |--- Query password
                |--- Traps enabled
                |--- Trap destination
            |--- Trap destination port
            |--- Trap community
            |--- Diag sending enabled
                |--- Diag destination
            |--- Diag destination port
            |--- Diag community
                |--- QoS traps to QCU
                |--- QCU address
                |--- QCU port
                |--- QoS to generic dest.
```

OpenScape service menu

The phone 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
```

Wi-Fi settings

Note

Wi-Fi operation requires a CP10 to be plugged in to the USB port of CP710, CP410 and CP210, and the USB port must be enabled (see "Feature access" → page 1).

Wi-Fi parameters can be configured via WBM and local settings. You can activate or deactivate Wi-Fi network access and set up new Wi-Fi networks that is 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. Only the EAP-TLS authentication protocol is supported.

Wi-Fi connections with no encryption type, WEP or WPA are characterized as non-secure 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 is 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.

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

Administration via WBM

1. Open Network > Wi-Fi settings.

Wi-Fi settings

Enable Wi-Fi interface ☐

Wi-Fi MAC address ""

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
No saved Wi-Fi networks				

- 2.
3. Enable the Wi-Fi interface. If disabled or without an inserted CP10 USB dongle, the phone can only connect via Ethernet cable.
 - **Wi-Fi MAC Address:** MAC address of the Wi-Fi interface, normally the LAN MAC address + 2.
 - Read from the device and read-only
 - **Last connected Wi-Fi network name:** SSID of last connected WLAN network.
 - Read-only
 - **Wi-Fi link status:** "down", "up", "connected", "failure".
 - Read-only
 - **Wi-Fi country settings:** ISO 3166 2 letter country code used to customise the Wi-Fi operation (independent of the phone's country setting)
 - For **Advanced** settings see "Advanced Wi-Fi settings" → page 74

Add new Wi-Fi network: Allows a WLAN network to be defined and saved

- **Wi-Fi SSID:** The Service Set Identifier that is your network's name.
- **Hidden SSID:** Enable this to not show the SSID in the list of saved networks.
- **Wi-Fi password:** The encryption type is either "None" or "EAP".
- **IP settings:** Sets the discovery mode as "DHCP" or "manual".
- **IP address / Subnet mask / Default route:** The discovery mode is "manual".
- **Authentication protocol:** Either "None", "PEAP", "TLS", "LEAP" or "FAST"(when the Encryption type is "EAP").
- **EAP anonymous identity:** Name to display rather than real identity, when authentication is one of "PEAP", "TLS" or "FAST".
- **EAP identity:** Full user name when authentication is "NONE".
- **EAP password:** When authentication is one of "PEAP", "TLS" or "FAST".
- **Stored Wi-Fi networks:** A summary list of saved WLAN networks.

Administration via local phone

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

SETTING UP A WIFI CONNECTION

When a Wi-Fi-enabled phone is set up for the first time using only Wi-Fi to establish a LAN connection, a temporary Wi-Fi connection is used. The device is connected to a predefined Wi-Fi 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).

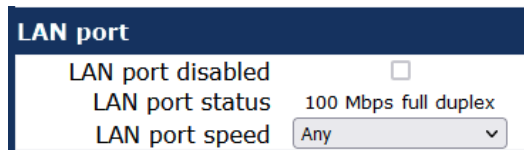
Once the phone has acquired a DLS address, it will open up a secure connection to DLS for downloading configuration parameters using the WPI protocol. Any certificates needed for Wi-Fi authentication or SIP/TLS will also be downloaded as a part of this process. If a DLS address is specified in the downloaded configuration, that DM is used subsequently. If not, the DLS discovery procedure is 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.

DISABLE LAN PORT

The OpenScape Desk Phones CP210, CP410, and CP710 provide the option to disable the LAN port connection when a Wi-Fi network is configured.

Administration via WBM

1. Open Network > Wired settings.



2. Enable or disable the LAN port.
 - When the LAN port is disabled, the Ethernet connection is not supported.
 - The LAN port may be disabled whether Wi-Fi LAN is enabled or disabled. When the LAN port is disabled the Wi-Fi LAN is automatically enabled, if not already enabled, and cannot be disabled.
3. Click **Submit**.

Administration via local phone

```
|--- Admin
    |--- Network
        |--- LAN port configuration
```

ADVANCED WI-FI SETTINGS

The OpenScape Desk Phones CP210, CP410, and CP710 provide advanced Wi-Fi options to reduce downtime during Wi-Fi roaming process.

Advanced Wi-Fi options

1. Select one of the following options to set the frequency band:
 - All (5 GHz + 2.4 GHz)
 - 5 GHz
 - 2.4 GHz

2. Select one of the following options to configure only a specific subset of allowed frequencies during Network scan and Wi-Fi operation:
 - All
 - Non DFS
 - UNII-1
 - UNII-3
 - UNII-1, UNII-2
 - UNII-1, UNII-2, UNII-3
 - 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)

1. Select one of the following options to configure only a specific subset of allowed frequencies during Network scan and Wi-Fi operation:
 - All
 - 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)" is valid, the new value is rejected and the previous value is kept (to prevent from invalid configuration).
- If new input is invalid and previous value is 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:

- True
- False

Roaming RSSI threshold

1. Edit the text field to configure the roaming RSSI threshold. Value can be set as a negative integer (RSSI value in dBm).

Invalid inputs is 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 WBM

1. Open Network > Wi-Fi settings > Advanced settings.

Advanced settings

Frequency band	All (5 GHz + 2.4 GHz) ▾
Allowed channels (5 GHz)	All ▾
Manual selection of allowed channels (5 GHz)	<input type="text"/>
Allowed channels (2.4 GHz)	All ▾
Manual selection of allowed channels (2.4 GHz)	<input type="text"/>
Enable 802.11r (Fast BSS Transition)	<input checked="" type="checkbox"/>
Roaming RSSI threshold	<input type="text" value="-75"/>
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

Fields are the same as in Local, except:

- “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).
- If “Allowed channels (5 GHz)” is not set to “Manual selection”, any input in “Manual selection of allowed channels (5 GHz)” is ignored.
- If field “Allowed channels (2.4 GHz)” is not set to “Manual selection”, any input in field “Manual selection of allowed channels (2.4 GHz)” is ignored.

Administration via local phone

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

System

OpenScope 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).

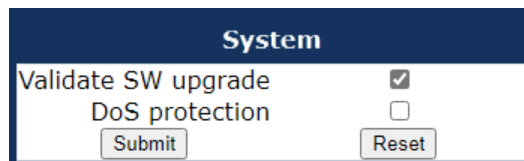
The signalling transport main / standby parameter selects the protocol to use for signalling. TCP and TLS are available.

Certificate validation shows whether the phone certificate used for encrypted logon via TLS is checked against the certificate on the server (and the level of checking). For configuration see “Authentication policy” → [page 138](#).

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

Administration via WBM

1. Open System > Security > System.



- **Validate SW upgrade:** validates if the uploaded Phone software is compatible with the phone.
- **DoS protection:** activates protection against “Denial-of-service” attacks that may cause the network to overload.

Administration via local phone

```
|--- Administration
    |--- System
        |--- Security
            |--- System
```

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 or HFA server.

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

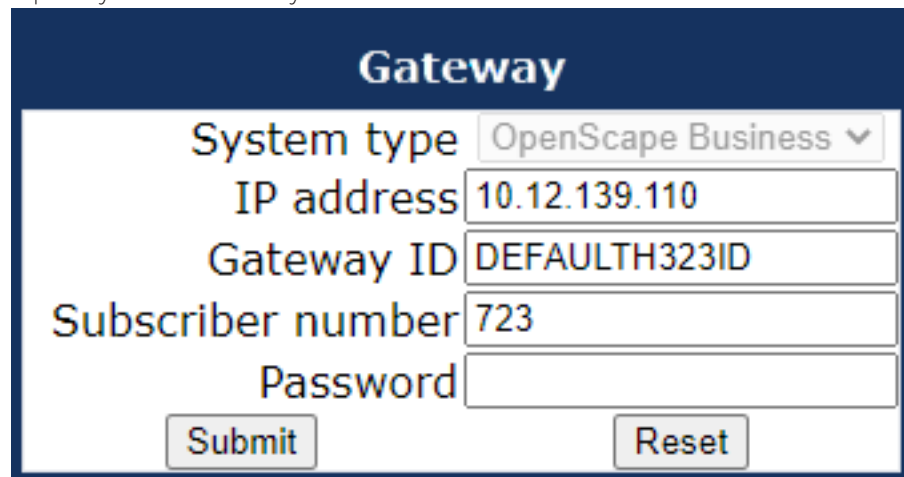
The Subscriber number is used as the internal extension number of the phone. It can be 1 to 24 characters long.

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

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

Administration via WBM

1. Open System > Gateway.



The screenshot shows a web-based configuration interface titled "Gateway". It contains several input fields and two buttons. The "System type" field is a dropdown menu currently showing "OpenScape Business". The "IP address" field contains "10.12.139.110". The "Gateway ID" field contains "DEFAULTH323ID". The "Subscriber number" field contains "723". The "Password" field is empty. At the bottom, there are "Submit" and "Reset" buttons.

Gateway	
System type	OpenScape Business ▼
IP address	10.12.139.110
Gateway ID	DEFAULTH323ID
Subscriber number	723
Password	
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

2. Select the system type and provide the following information:
 - IP address: IP or DNS address of the communication platform or HFA server.
 - Subscriber number: The phone extension.
 - Password: Password for logging on to the HFA server.

3. Click **Submit**.
4. Open Network > Port number configuration.

Port number configuration	
Phone port configuration	
Gateway	4060
Standby gateway	4060
RTP base	29100
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
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

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

Administration via local phone

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

|--- Admin
    |--- Network
        |--- Port configuration
            |--- Gateway
```

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 "HFA gateway settings" → page 78).

Administration via WBM

1. Open System > Standby gateway.

2. Enter the IP address and gateway ID.
3. Enter the subscriber number and password.
4. Click **Submit**.
5. Open Network > Port number configuration.

6. Enter the standby gateway ID.
7. Click **Submit**.

Administration via local phone

| --- Admin

| --- System


```

|--- Standby gateway

|--- System type

|--- IP address

|--- Gateway ID

|--- Subscriber number

|--- Password

|--- Admin

|--- Network

|--- Port configuration

|--- Standby gateway

```

SERVER AND STANDBY SERVER PORTS

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

Administration via WBM

1. Open Network > Port number configuration.
 - 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 local phone

```

|--- Admin

|--- Network

|--- Port configuration

|--- Server port configuration

|   |--- H.225.0 port

|   |--- TC TLS port

|   |--- H.225.0 TLS port

```

```
|--- Standby server port configuration

|--- H.225.0 port

|--- TC TLS port

|--- H.225.0 TLS port
```

REDUNDANCY

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

Administration via WBM

1. Open System > Redundancy.
 - When "Small remote side redundancy" is activated, the phone switches to the standby HFA server if 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" 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.
 - "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" sets the timeout between two "Retry count standby". The default is 30.
 - "Timeout main" sets the timeout between two "Retry count main". The default is 30.
 - "TC test retry" determines the count of how many successful TC tests the main system needs to answer before the phone switches back with Auto switchback 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.
 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 a change of the timing values the SRSR need to be deactivated and re-activated again to take effect.

Administration via local phone

```
|--- Admin

|--- System
```

```

|--- Redundancy

|--- Small remote site

|--- Auto switch back

|--- Retry count main

|--- Timeout main

|--- Retry count stdby

|--- Timeout standby

```

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 "LIN" → page 84) is configured, the user location is communicated to the PSAP. In the US, the number is 911.

Administration via WBM

1. Open System > Features > Configuration.

Configuration

General

Emergency number

LIN

Not used timeout (minutes)

AlertBar LED hint ☐

FPK Name

Bluetooth

Enable bluetooth interface ☒

Enable telephony ☒

Services

Web based manag. ☒

USB device access ☒

USB power using PoE

Telephony settings

Enable telephony settings ☐

2. Enter the emergency number.
3. Click **Submit**.

Administration via local phone

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

LIN

The Location Identification Number (LIN) is a number code that provides detailed geographic information about the phone, including the office room. On issuing an emergency call using the E.911 emergency number (see ["Emergency number" → page 83](#)), 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

1. Open System > Features > Configuration.

Administration via local phone

```
|--- Admin
      |--- System
            |--- Features
                  |--- Configuration
                        |--- General
                              |--- LIN
```

NOT USED TIMEOUT

Note This feature is available only on OpenScape Desk Phone CP410 and CP710 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.

Administration via WBM

1. Open System > Features > Configuration.

Configuration

General

Emergency number

LIN

Not used timeout (minutes)

AlertBar LED hint ☐

FPK Name

Bluetooth

Enable bluetooth interface ☒

Enable telephony ☒

Services

Web based manag. ☒

USB device access ☒

USB power using PoE

Telephony settings

Enable telephony settings ☐

2. Set the interval for the "Not used timeout". The timeout ranges from 1 to 5 minutes.
 - The default value is 2 (minutes).

3. Click **Submit**.

Administration via local phone

| --- Admin

| --- System

| --- Features

```
|--- Configuration
```

```
|--- General
```

```
|--- Not used timeout
```

ENABLE TELEPHONY SETTINGS

Note This feature is available only on OpenScape Desk Phone CP410 and CP710 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

1. Open System > Features > Configuration.

Administration via local phone

```
|--- Admin
```

```
|--- System
```

```
|--- Features
```

```
|--- Configuration
```

```
|--- Telephony settings
```

```
|--- Enable telephony settings
```

ENERGY SAVING

Backlight time setting

Note This feature is available only on OpenScape Desk Phone CP410 and CP710 phones.

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

This parameter can also be configured by the user.

Administration via WBM

1. Open User settings > Phone > Energy saving.



2. Set the backlight time interval.
 - Value range: 1 minute, 5 minutes, 30 minutes, 60 minutes, 2 hours, 4 hours, or 8 hours.
 - Default value: 1 minute.

Administration via local phone

```
|--- User settings
    |--- Phone
        |--- Energy saving
```

Energy efficient Ethernet

The OpenScape Desk Phone CP110 / CP210 / CP410 / CP710 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.

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).

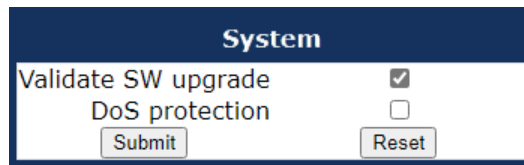
The signalling transport main / standby parameter selects the protocol to use for signalling. TCP and TLS are available.

Certificate validation shows whether the phone certificate used for encrypted logon via TLS is checked against the certificate on the server (and the level of checking). For configuration see "Authentication policy" → page 138.

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

Administration via WBM

1. Open System > Security > System.



- **Validate SW upgrade:** validates if the uploaded Phone software is compatible with the phone.
- **DoS protection:** activates protection against "Denial-of-service" attacks that may cause the network to overload.

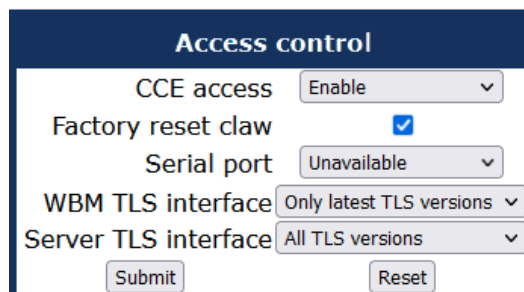
Administration via local phone

```
|--- Administration
      |--- System
            |--- Security
                  |--- System
```

Access control

Administration via WBM

1. Open System > Security > 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 “hooded claw” keypad mechanism to initiate a factory reset without requiring an authenticated access can be enabled or disabled.
- The **Serial port** parameter controls access to the serial port.
 - When set to “No password”, a terminal connected to the port can interact with the phone 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 version is TLS 1.2). By default the latest TLS version is allowed. Other interfaces are not affected by this setting.
- **Server 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 version is TLS 1.2). By default the latest TLS version is allowed.

Administration via local phone

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

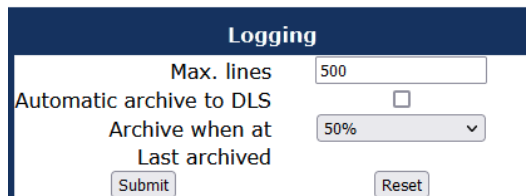
Security log

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.

Note The security log cannot be disabled.

Administration via WBM

1. Open System > Security > Logging.



- 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 is 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 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 local phone

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

Date and time

If the DHCP server in the 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-our 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 is in effect immediately.
- For automatic toggling, enable "Auto time change". 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.

Note The Difference (minutes) must be specified both for manual and automatic DST toggling.

SETTINGS VIA SNTP

Administration via WBM

1. Open Date and time.

Date and time	
SNTP	
SNTP primary	10.12.61.40
SNTP backup	192.168.12.1
Display and Trace time	
Source	System
NOTE: When Display and Trace source is set to System the timezone and daylight savings settings below do not apply	
Timezone and Daylight saving	
Timezone offset (hours)	2
Daylight saving	<input checked="" type="checkbox"/>
Difference (minutes)	60
Auto time change	<input checked="" type="checkbox"/>
DST zone	Not set
Current DISPLAY Time	
Thu Jan 1 00:05:56 1970	
Current UTC Time	
Tue Nov 29 13:15:58 2022	
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

- **SNTP primary**: IP address or host name of the SNTP server
- **SNTP backup**: Secondary SNTP server
- **Source**: The time zone server. The DST settings do not apply when the source is set to local ("System").
- **Timezone offset (hours)**: Shift in hours corresponding to UTC.
- **Daylight saving**: Enables or disables DST in conjunction with "Auto time change".
 - Value range: "Yes", "No".
- **Difference (minutes)**: Time difference when DST 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 is reset to this value.

- **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 is reset to this value.

Administration via Local Phone

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

        |--- Daylight saving
            |--- Daylight saving
            |--- Difference (mins)
            |--- Auto DST
            |--- DST zone
```

Dialing

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).

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 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".

Note

To enable the number conversion, all parameters not marked as optional must be provided, and the canonical look-up settings must be configured (see "Canonical dialing look-up" → page 168).

Changes to these parameters can impact the phone's ability to match calls to contacts.

Administration via WBM

For generating an appropriate dial string, a conversion from canonical format may be required. The following parameters determine the local settings of the phone, like local country code or local national code, and define rules for converting from canonical format to the format required by the PBX.

1. Open **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	<input type="text"/>
National prefix digit	<input type="text"/>
Local national code	<input type="text"/>
Minimum local number length	<input type="text"/>
Local enterprise node	<input type="text"/>
PSTN access code	<input type="text"/>
International access code	<input type="text"/>
Operator codes	<input type="text"/>
Emergency numbers	<input type="text"/>
Initial extension digits	<input type="text"/>
Expect dial number	<input type="checkbox"/>

Submit

Reset

- **Local country code:** E.164-type 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
- **Minimum local number length:** This is considered if the number has not been recognized, nor does it qualify to be an extension number (by its 1st digit).
 - If the number is less than or equal to the Minimum local number length it is canonized as a local number.
 - If the number is greater than the minimum local number length it may be a local number or an international number but the maximum local number length determines how it is canonized.
- **Maximum local number length:** This is considered after the minimum local number length check and applies the following conditions:
 - If the maximum local number length = 0 the number is canonized as a local number by adding the appropriate prefixes.
 - If the number is less than or equal to the maximum local number length the number is canonized as a local number by adding the appropriate prefixes,
 - If the number is greater than the maximum local number length it is considered a complete number and canonized by adding the international prefix character "+".
- **Local enterprise node:** number of the company / PBX wherein the phone is residing
 - Maximum length: 10 (optional)
- **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.

For instance, the extensions 3000-5999 are configured in the OpenScape Desk

Phone, 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

2. Open Local functions > Locality > Canonical dial.

- Internal numbers

Note To enable the phone to discern internal numbers from external numbers, it is crucial that a canonical look-up table is provided ("Canonical dialing look-up" → page 168).

- **"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 dialed as national numbers, thus even local numbers will have a region code prefix (as dialing from a mobile). Numbers for a different country are dialed using the international format.
- **"International form":** All numbers are dialed using their full international number format.

- External access code

- **"Not required":** The access code to allow a public network number to be dialed is not required.
- **"For external numbers":** Default value. All public network numbers is prefixed with the access code that allows a number 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 is dialed explicitly by using the access code for the international gateway to replace the "+" prefix.

- **"Leave as +"**: All international formatted numbers is prefixed with "+".

Administration via local phone

```
|--- Admin
  |--- Local Functions
    |--- Locality
      |--- Canonical settings
        |--- Local country code
        |--- National prefix digit
        |--- Local national code
        |--- Min(imum) local num(ber) length
        |--- Local enterprise node
        |--- PSTN access code
        |--- International access code
        |--- Operator code
        |--- Emergency number
        |--- Initial extension digits
        |--- Expect dial number
  |--- Admin
    |--- Local Functions
      |--- Locality
        |--- Canonical dial
          |--- Internal numbers
          |--- External numbers
          |--- External access code
          |--- Internat(ional) access
```

CANONICAL DIAL LOOK-UP

The parameters given here are important for establishing outgoing calls and for recognizing incoming calls.

In the local phone book, 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, internal numbers must be discerned from external numbers(see ["Canonical dialing configuration" → page 92](#)). The canonical look-up 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.

Note To make sure that canonical dial look-up works properly, at least the following parameters of the phone must be provided:

- Local country code
- Local area code
- Local enterprise code

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.

Administration via WBM

1. Open 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	<input type="text"/>	International code 1	<input type="text"/>
Local code 2	<input type="text"/>	International code 2	<input type="text"/>
Local code 3	<input type="text"/>	International code 3	<input type="text"/>
Local code 4	<input type="text"/>	International code 4	<input type="text"/>
Local code 5	<input type="text"/>	International code 5	<input type="text"/>

- **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
```

Ringer setting

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.

LOCAL RINGERS

Administration via WBM

1. Open Ringer > Local ringers.

Local ringers			
Name	Ringer sound	Pattern melody	Pattern sequence
<i>Internal</i>	Pattern ▼	2 ▼	2 ▼
<i>External</i>	Pattern ▼	2 ▼	2 ▼
<i>Attention</i>	Pattern ▼	2 ▼	2 ▼
<i>Emergency</i>	Pattern ▼	2 ▼	2 ▼
Submit		Reset	

2. Select the ringer sound, pattern melody and sequence for each name.
 - **Name:** Selects the call type to be used.

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".

3. Click **Submit**.

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. It is up to the administrator to configure such that the user hears the required ring tones for the various features or 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
```

RINGER SETTINGS CP100 / CP200

You can select the ringer mode. For CP100 or CP200 phones, any ringer sound may either be one of the following tones

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

Note Once distinctive 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".

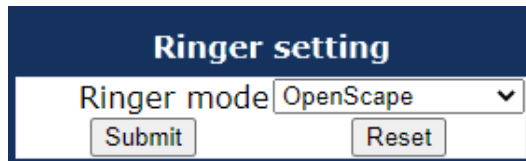
Even though the ringers are configured locally the behaviour of the ringers should be the same as system controlled ones. In particular, cyclic ringers shall be played endlessly until the switch commands to stop playing (and therefore repeated if necessary), whereas single shot ringers should play for 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 WBM

1. Open Ringer > Ringer setting.



2. Select the ringer mode that determines the source of ringer tone.
 - Value range: "OpenScape", "Local ringer"
 - Default: "OpenScape".
3. Click **Submit**.

Administration via local phone

```
|--- Admin
      |--- Settings
            |--- Ringer
```

```
|--- Ringer Setting
      |--- Options
      |--- User changeable
      |--- Ringer mode
      |--- Emergency ringer mode
```

RINGER SETTINGS CP400 / CP600 / CP700

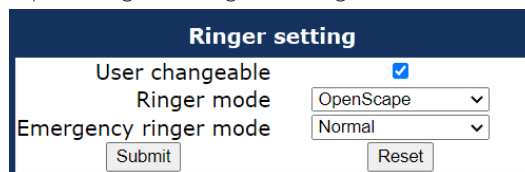
You can allow the user to change ringer settings, select the ringer mode and set an emergency ringer mode.

For CP400, CP600, and CP700 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

1. Open Ringer > Ringer setting.



- **User changeable:** Lets the user change distinctive ringer settings, i.e. change the ringer volume.
 - Value range: Enabled or 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 enabled.
 - Default: "Normal".
2. Click **Submit**.

Administration via local phone

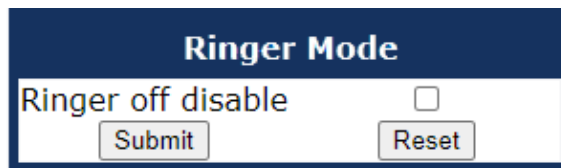
```
|--- Admin
  |--- Ringer
    |--- Options
    |--- User changeable
    |--- Ringer mode
      |--- OpenScape
      |--- Local ringer
    |--- Emergency ringer mode
      |--- Normal
      |--- Always
```

RINGER MODE

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

Administration via WBM

Open 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 ringer by long-pressing the key "*". If pressed, a toast message "Key function unavailable" is displayed for a CP400, CP600, and CP700 phone.

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.

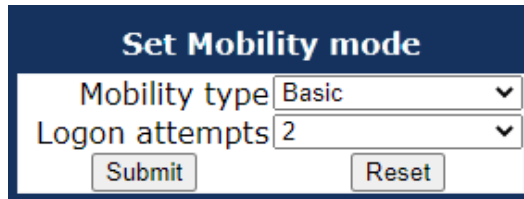
Additionally, the function can no longer be allocated to an FPK (refer to "Free programmable keys" → page 103).

If a CP400, CP600, or CP700 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.

User mobility

The "Set Mobility Mode" parameter controls the behavior of the phone if mobile user logs on to the phone.

1. Open User mobility > Set mobility mode.



2. Select the mobility type:
 - Basic (Default): When a new user logs on at the phone, all user data of the precedent user is shown.
 - Data Privacy: When a new user logs on at the phone, an empty conversation list is 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, is deleted. No synchronization to and from DLS will happen.
3. Select the number of log-on attempts from the drop-down menu.
4. Click **Submit**.

Free programmable keys

The key programming can be accessed via the local phone and via DLS / DMS.

- The OpenScape Desk Phone CP710 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 modules to the phone, with up to four KM710 providing 12 FPKs each or up to four KM410 providing 16 FPKs each.
- The OpenScape Desk Phone CP410 phone provides 16 free programmable keys (FPKs) when a key module is not plugged in, which can be associated with special phone functions. These are called „Phone keys“. Alternatively, the OpenScape Desk Phone CP410 can have up to four key modules KM410 providing 16 FPKs each, or up to four KM710 providing 12 FPKs each.
- The OpenScape Desk Phone CP210 phone provides four free programmable keys (FPKs). This is called „Phone keys“.
- The OpenScape Desk Phone CP110 phone provides three free programmable keys (FPKs). These are called „Phone keys“.

ENABLING "LONG PRESS" FOR FPKS

Note

The long press feature is enhanced for the CP210.

Prerequisites

At the phone, the configuration menu for a specific programmable key is called by a long press on the related key. However, the other methods for key programming remain enabled.

SELECTED DIAL ACTION ON CALLS

This feature allows the user to perform a certain action, while a selected dialing FPK is pressed during an active or held call.

Administration via local phone

```
|--- Admin
    |--- System
        |--- Features
            |--- Configuration
                |--- General
                    |--- Selected Dial Action on Calls
```

Transferring phone software, application, and media files

New software images, hold music, picture clips for phone book entries, LDAP templates, company logos, screen Saver images, and ring tones can be uploaded to the phone via DLS (Deployment Service) or WBM (Web Based Management).

Note

For all user data, which includes files as well as phone book content, the following amounts of storage place are available:

- OpenScape Desk Phone CP710: 100MB
- OpenScape Desk Phone CP410: 100 MB
- OpenScape Desk Phone CP210: 25 MB
- OpenScape Desk Phone CP110: 25MB

LINUX FILE NAME ISSUES

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 file name on the phone could lead to operational or security issues. To protect against this the phone will ensure that the file name for the file to be saved does not contain non-allowed characters. The solution is to replace invalid characters in the names of files to be downloaded onto the phone with a dummy character.

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 file name. Any non-allowed characters are replaced with an "_" (underscore) character. The file name must not start with a "-" (hyphen) character.

This should cover any download mechanism:

- WBM download of user files (such as ringtones)
- 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 file name and file extension entered in any FTP / HTTPS file transfer panel only contains valid characters and that the file extensions (file type) are valid.

- If a file path character or file extension is detected in the file name then an error is displayed and the file transfer is not allowed.

FTP / HTTPS SERVER

There are no specific requirements regarding the FTP server for transferring files to the OpenScape Desk Phone. Any FTP server providing standard functionality will do.

COMMON FTP / HTTPS SETTINGS (DEFAULTS)

For each one of the various file types, e.g. phone application, 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 is used for a specific file type if its Use defaults parameter is set to "Yes".

Note 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 phone application download conditions:

- 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

Administration via WBM

1. Open File transfer > Defaults.

The screenshot shows a 'Defaults' configuration window 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' is an empty text box. The 'FTP username' is an empty text box. The 'FTP password' is a text box filled with dots. The 'FTP path' is an empty text box. At the bottom, there are two buttons: 'Submit' and 'Reset'.

- **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 local phone

```
|--- Admin
  |--- File Transfer
    |--- Defaults
      |--- Download method
      |--- Server
      |--- Port
      |--- Account
      |--- Username
      |--- Password
      |--- FTP path
      |--- HTTPS base URL
```

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 hardware level).

When a new software bind is downloaded to the phone, the following verification is performed:

- 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
- 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

Note

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.

Upgrade using file

You can upgrade the phone application by navigating to a local file. This can be done only by WBM administration.

Administration via WBM

1. Open File transfer > Phone application.

Phone application

Upgrade using file

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

Durchsuchen... Keine Datei ausgewählt.

Upgrade Cancel

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

Upgrade using FTP/HTTPS

Use defaults ☒

Filename

After submit do nothing ▼

Submit Reset

2. Click **Browse...**, and select the file you want to install.
3. Click **Upgrade**.
4. Wait until the upgrade process is finished.

Note The "Cancel" function will not work once the process is in burn state.

Upgrade using FTP / HTTPS

If the default FTP / HTTPS access settings (see "Common FTP / HTTPS settings (defaults)" → [page 105](#)) are used, "Use defaults" must be set to "Yes", and only the file name must be specified.

Administration via WBM

1. Open File transfer > Phone application.

Phone application

Upgrade using file

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

Durchsuchen... Keine Datei ausgewählt.

Upgrade Cancel

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

Upgrade using FTP/HTTPS

Use defaults ☒

Filename

After submit do nothing ▼

Submit Reset

- **Use defaults:** Specifies whether the default FTP / HTTPS access settings shall be used. Value range: "Yes", "No". If enabled, an abbreviated set of options is provided.
- **File name:** 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".
The option "do nothing" allows changes to the set of options and submit the changes to update the page (e.g. select between FTP and HTTPS).

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 host name 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 host name of the HTTPS server in use; only applicable if Download method is switched to "HTTPS".

Administration via local phone

```

|--- Admin
    |--- File Transfer
        |--- Phone application
            |--- Use default
            |--- Download method
            |--- Server
            |--- Port
            |--- Account
            |--- Username
            |--- Password
            |--- FTP path
            |--- HTTPS base URL
            |--- File name

```

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 using the new software.

Updating via FTP or HTTPS

1. Open File transfer > Phone application.

Upgrade using FTP/HTTPS

Use defaults ☐

Download method FTP ▼

FTP server address

FTP server port 21

FTP account

FTP username

FTP password

FTP path

Filename

After submit do nothing ▼

2. Select the transfer protocol.
3. Provide the address and the port number.
4. If required, provide the user name and password.
5. Enter the file name
6. Set "After submit" to "Start download".
7. Click **Submit**.

Start download via local phone

```
|--- Admin
    |--- File Transfer
        |--- Phone app
```

1. Click **OK**.
2. Select **Download**. The download will start immediately.

PICTURE CLIPS

Note 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".

FTP / HTTPS access data

If the default FTP / HTTPS access settings are used, "Use defaults" must be set to "Yes", and only the file name must be specified (see "Common FTP / HTTPS settings (defaults)" → page 105).

Administration via WBM

1. Open File transfer > Picture clip.

- **Use defaults:** Specifies whether the default FTP / HTTPS access settings shall be used.
- **File name:** Specifies the file name of the image file
- **Download method:** Selects the protocol to be used. Value range: "FTP", "HTTPS".
 - Default: "FTP"
- **Server:** IP address or host name 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 host name 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 local phone

```
|--- Admin
    |--- File Transfer
        |--- Picture Clip
            |--- Use default
            |--- Download method
            |--- Server
            |--- Port
            |--- Account
            |--- Username
            |--- Password
            |--- FTP path
            |--- HTTPS base URL
            |--- File name
```

1. On OpenScape Desk Phone CP410 and CP710 select **Download**. The download will start immediately.

Download a picture clip

Note This feature is available for OpenScape Desk Phones CP410 and CP710.

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 (see "FTP / HTTPS access data" → page 111).

Upload picture clips via LDAP

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 px for conversation list and contact details (header)
- 64x64 px 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 must be configured and a suitable LDAP template must be available on the phone. The LDAP template must support a 13th attribute to allow access to a contact's picture (see "Create an LDAP template" → page 171).

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 is 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

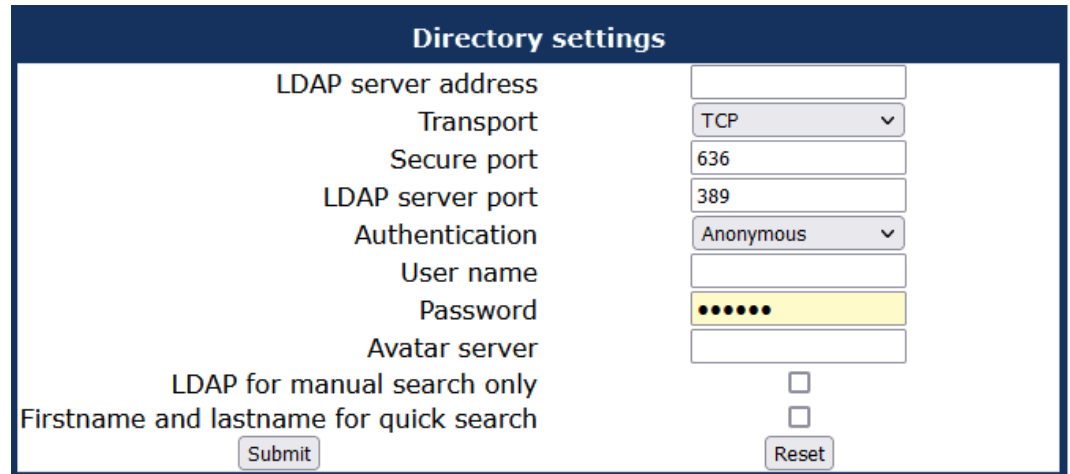
1. Open Settings > Administrator > Local functions > LDAP > Avatar server.

Configuration via DLS

1. Open DeploymentService > IP Devices > IP Phone Configuration > Service Integrations > LDAP Settings > Avatar Server.

Administration via WBM

1. Open Admin > Local functions > Directory settings.



The screenshot shows the 'Directory settings' form. It 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'.
- LDAP server port**: A text input field with '389'.
- Authentication**: A dropdown menu with 'Anonymous' selected.
- User name**: A text input field.
- Password**: A password input field with masked characters (dots).
- Avatar server**: A text input field.
- LDAP for manual search only**: A checkbox.
- Firstname and lastname for quick search**: A checkbox.
- Submit**: A button at the bottom left.
- Reset**: A button at the bottom right.

2. Enter the Avatar server address.
3. Click **Submit**.

LDAP TEMPLATE

The LDAP template is an ASCII text file that allows attributes in an LDAP directory entry to be mapped to the contact fields on the phone. The LDAP template must be modified correctly for successful communication between the directory server and the LDAP client.

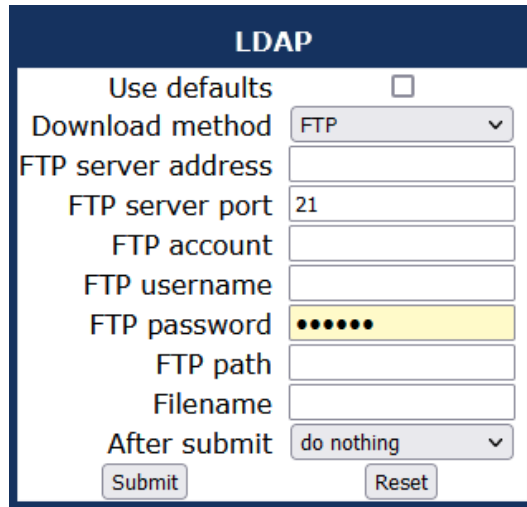
The OpenScape Desk Phone phones support LDAPv3.

FTP / HTTPS access data

If the default FTP / HTTPS access settings are used, "Use default" must be set to "Yes", and only the file name must be specified (see "Common FTP / HTTPS settings (defaults)" → page 105).

Administration via WBM

1. Open File transfer > LDAP.

A screenshot of the LDAP configuration form. The form has a dark blue header with the title 'LDAP' in white. Below the header, there are several fields and controls. At the top, 'Use defaults' is followed by an unchecked checkbox. Below that, 'Download method' is a dropdown menu showing 'FTP'. 'FTP server address' is a text input field. 'FTP server port' is a text input field with '21' entered. 'FTP account' is a text input field. 'FTP username' is a text input field. 'FTP password' is a text input field with masked characters (dots). 'FTP path' is a text input field. 'Filename' is a text input field. 'After submit' is a dropdown menu showing 'do nothing'. At the bottom, there are two buttons: 'Submit' and 'Reset'.

- **Use default:** Specifies whether the default FTP / HTTPS access settings shall be used. Value range: "Yes", "No" Default: "No"
- **File name:** Specifies the file name of the LDAP template file.
- **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 host name 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 host name of the HTTPS server in use; only applicable if Download method is switched to "HTTPS".

Administration via local phone

```

|--- Admin
    |--- File Transfer
        |--- LDAP
            |--- Use default
            |--- Download method
            |--- Server
            |--- Port
            |--- Account
            |--- Username
            |--- Password
            |--- FTP path
            |--- HTTPS base URL
            |--- File name
  
```

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.

The OpenScape Desk Phones support LDAPv3.

Start download via WBM

1. Open File transfer > LDAP.

2. Select the transfer protocol.
3. Provide the address and the port number.
4. If required, provide the user name and password.
5. Enter the file name.
6. Set "After submit" to "start download".
7. Click **Submit**.

Start download via local phone

```
|--- Admin
      |--- File Transfer
            |--- LDAP
```

1. Click **OK**.
2. Select **Download**. The download will start immediately.

SCREEN SAVER

The screen saver can be configured to be displayed when the phone is in idle mode. It performs a slide show consisting of images which can be uploaded using the web interface.

Screen savers are available only on OpenScape Desk Phones CP410 and CP710.

Note The file size for a screen saver 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 screen saver images, the following specifications are valid:

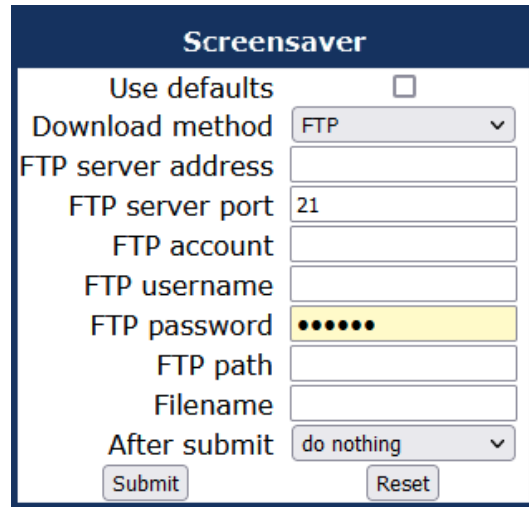
- **Data format:** JPEG, BMP or PNG. JPG is recommended. The file extensions supported for JPEG are jpeg and jpg.
- **Screen format:** 4:3. The images are resized to fit in the screen, so that images with a width / height ratio differing from 4:3 will appear with deviant proportions.
- **Resolution:** The phone's screen resolution is the best choice for image resolution: 320 x 240 px

FTP / HTTPS access data

If the default FTP / HTTPS access setting are used, Use default must be set to "Yes", and only the file name must be specified (see "Common FTP / HTTPS settings (defaults)" → page 105).

Administration via WBM

1. Open File transfer > ScreenSaver.



- **Use defaults:** Specifies whether the default FTP / HTTPS access settings shall be used.
 - Default: disabled
- **Filename:** Specifies the file name of the screensaver image file.
- **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 host name 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 local phone

```
|--- Admin
    |--- File Transfer
        |--- ScreenSaver
            |--- Use default
            |--- Download method
            |--- Server
            |--- Port
            |--- Account
            |--- Username
            |--- Password
            |--- FTP path
            |--- HTTPS base URL
            |--- File name
```

Download screen saver

If applicable, screen savers 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

1. Open File transfer > Screensaver.

2. Set "After submit" to "start download".
3. Click **Submit**.

Start download via local phone

```
|--- Admin
    |--- File Transfer
        |--- Screensaver
```

1. In the administration menu, select "Screensaver".
2. Select **Download**. The download will start immediately.

RINGER FILE

Note 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.

Note 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
 - Bit rate: 16 kB/s
 - Sampling rate: 8 kHz
 - Quantization level: 16 bit
- MIDI format
- MP3 format. The OpenScape Desk Phones CP410 and CP710 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 bit rate of 48 kbit/s 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).

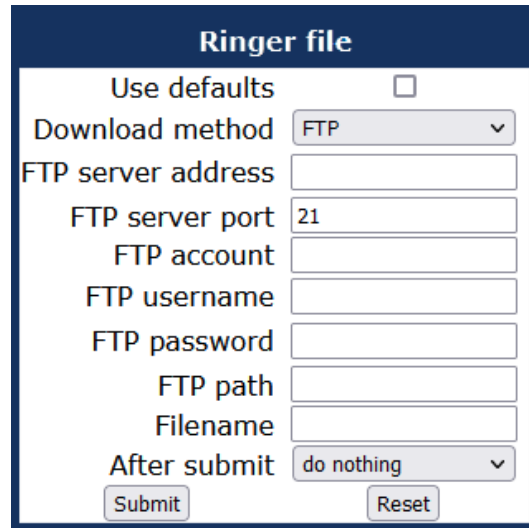
Length	64 kbit/s	80 kbit/s	96 kbit/s	112 kbit/s
0:15 min	0.12 MB	0.15 MB	0.18 MB	0.21 MB
0:30 min	0.23 MB	0.29 MB	0.35 MB	0.41 MB
0:45 min	0.35 MB	0.44 MB	0.53 MB	0.62 MB
1:00 min	0.47 MB	0.59 MB	0.70 MB	0.82 MB

FTP / HTTPS access data

If the default FTP / HTTPS access settings are used, "Use default" must be set to "Yes", and only the file name must be specified (see "Common FTP / HTTPS settings (defaults)" → page 105).

Administration via WBM

1. Open File transfer > Ringer file.



The screenshot shows a web form titled "Ringer file" with a dark blue header. Below the header, there is a "Use defaults" checkbox. The form contains several input fields and dropdown menus: "Download method" (a dropdown menu showing "FTP"), "FTP server address" (a text input field), "FTP server port" (a text input field with "21" entered), "FTP account" (a text input field), "FTP username" (a text input field), "FTP password" (a text input field), "FTP path" (a text input field), "Filename" (a text input field), and "After submit" (a dropdown menu showing "do nothing"). At the bottom of the form are two buttons: "Submit" and "Reset".

- **Use default:** Specifies whether the default FTP / HTTPS access settings shall be used.
 - Value range: "Yes", "No"
 - Default: "No"
- **File name:** Specifies the file name of the ringer file.
- **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 host name 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 local phone

```
|--- Admin
    |--- File Transfer
        |--- Ringer
            |--- Use default
            |--- Download method
            |--- Server
            |--- Port
            |--- Account
            |--- Username
            |--- Password
            |--- FTP path
            |--- HTTPS base URL
            |--- File name
```

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

1. Open File transfer > Ringer file.

2. Set "After submit" to "start download".
3. Click **Submit**.

Start download via local phone

1. In the administration menu, select "Ringer".

```
|--- Admin
    |--- File Transfer
        |--- Ringer
```

1. Press the key labeled **Download**. The download will start immediately.

COMPANY LOGO

Note This feature is available only on OpenScape Desk Phone CP410 and CP710 phones.

Custom company logo can be uploaded to the phone.

Note 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. The administrator 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.

Format of the logo image file

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

- CP710 and CP410: PNG image 24-bit with alpha channel

The 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:

- CP710: 440 x 220 px
- CP410: 216 x 68 px

Resizing is done by keeping the aspect ratio intact.

Administration via WBM

1. Open 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 ☒

Filename

After submit

2. Select a file that conforms to the specifications.
3. Click **Submit**.

If a logo is uploaded, the option "delete logo file" is displayed beneath the option "After submit".

Administration via Local Phone

```
|--- Admin
  |--- File Transfer
    |--- Logo
      |--- Use default
      |--- Download method
      |--- Server
      |--- Port
      |--- Account
      |--- Username
      |--- Password
      |--- FTP path
      |--- HTTPS base URL
      |--- File name
```

UC server

Administration via WBM

1. Open Local functions > Locality > UC Server.
2. Specify the following settings:
 - UC Protocol: selects the protocol to be used.
 - Value range: "HTTP", "HTTPS".
 - UC Server address: IP address or host name 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.
3. Click **Submit**.

Administration via local phone

```
|--- Admin

    |--- Local functions

        |--- UC Server

            |--- UC Protocol

            |--- UC server address

            |--- UC Server port

            |--- User configuration enabled
```

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 or logout for flexible working hours.

- The protocol parameter defines whether HTTP or HTTPS is 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 sent.
- The port is the target port at the server to which the URL is 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

phonenumber=3338&action=huntGroupLogon

The question mark is automatically added between the path and the parameters. If a question mark has been entered at the start of the parameters, it is stripped off automatically.

The method parameter determines the HTTP method used, which can be either GET or POST. If GET is selected, the additional parameters and the user id and password (web server user ID and web server password) are part of the URL. If POST is selected, these data form the body of the message.

If 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).

Administration via WBM

1. Open System > 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

- **Name** defines or changes the name (label) of 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.

Settings of the corporate directory

LDAP

The Lightweight Directory Access Protocol (LDAP) 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.

On an OpenScape Desk Phone CP410 or CP710, the use of the LDAP directory is integrated into the conversations concept.

Example

If a call cannot be mapped to a contact on the phone, the phone can be configured to look up the call contact details from the LDAP directory. In addition, a search for a contact will cover both contacts on the phone and the LDAP directory. The LDAP template maps the LDAP fields to those of the contacts on the phone.

On an OpenScape Desk Phone CP110 or CP210, the LDAP directory can be accessed using the entry Directories > Corporate directory.

The entry is displayed only when a LDAP server is configured.

Note The OpenScape Desk Phone CP phones support LDAPv3.

For connecting the phone 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 must 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 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 guide on setting up LDAP on an OpenScape Desk Phone, refer to "How to set up the "Corporate directory" (LDAP)" → [page 171](#).

On an OpenScape Desk Phone CP110 or CP210, an explicit search field for LDAP requests is supported. The search string is submitted to the LDAP server as soon as **OK** is pressed or when the search trigger timeout expires.

On an OpenScape Desk Phone CP410 or CP710, the search of the LDAP directory is integrated in the conversations search function. The LDAP template allows for a 'nickname' field which allows a search of any text in the field.

Administration via WBM

1. Open Local functions > Directory Settings.

- **LDAP Server address:** IP address or host name 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
- **Contact details update:** The update source for call party names can be set as one or more of the following: Directory, Signaling or Local.
- **Avatar server:** HTTP or HTTPS address, where the pictures are located. The complete HTTP or 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 file name 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.

Administration via local phone

```
|--- Admin
    |--- Local Functions
        |--- LDAP
            |--- Server address
            |--- Transport
            |--- LDAP Secure port
            |--- LDAP Server port
            |--- Authentication
            |--- User name
            |--- Password
            |--- Permanent LDAP Enabled
            |--- Avatar server
```

CONTACT DETAILS UPDATE

Note This option is only available for the OpenScape Desk Phone CP410 and CP710 phones. Not applicable for Broadsoft.

It is possible to update the source used to obtain call party names from one place.

- 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)

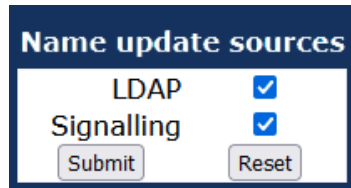
Source of the contact details

When an update source has been specified, the phone will try to match the call party number signaled for a call to an entry in the update source(s). If more than one source is specified then they are used in the following order:

- LDAP
- Signalling

Administration via WBM

1. Open Local functions > Name update sources.



The update source can be set as one or more of the following:

- Directory: LDAP (if an LDAP entry matches the call, the contact is update to match the LDAP entry)
- Signalling: Via SIP (if set then the contact is updated based on the call party name in signaling)

Administration via local phone

```
|--- Admin
    |--- Local Functions
        |--- LDAP
            |--- Server address
            |--- Transport
            |--- LDAP secure port
            |--- LDAP server port
            |--- Authentication
            |--- User name
            |--- Password
            |--- Avatar server
        |--- Name update sources
```

PICTURE VIA LDAP

Note This option is only available for the OpenScape Desk Phone CP410 and CP710 phones.

To display centrally stored contact data the OpenScape Desk Phone CP410 / CP710 will request and retrieve the data from a server.

The OpenScape Desk Phone CP410 / CP710 requests the look-up for all numbers for which the local phone book does not have a picture. In case the phone book 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 phone book is displayed, so the directory server data overrides the local phone book.

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.

Note

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


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 "Canonical dialing settings" → page 168). 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 look-up is unique.

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

Administration via WBM

1. Open 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	<input type="text"/>
National prefix digit	<input type="text"/>
Local national code	<input type="text"/>
Minimum local number length	<input type="text"/>
Local enterprise node	<input type="text"/>
PSTN access code	<input type="text"/>
International access code	<input type="text"/>
Operator codes	<input type="text"/>
Emergency numbers	<input type="text"/>
Initial extension digits	<input type="text"/>
Expect dial number	<input type="checkbox"/>
<input type="button" value="Submit"/>	<input type="button" value="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

```

Speech

RTP BASE PORT

The port used for RTP is negotiated during the establishment of a SIP connection.

The number of the port used for RTCP is the RTP port number increased by 1.

Administration via WBM

1. Open Network > Port number configuration.

Port number configuration	
Phone port configuration	
Gateway	4060
Standby gateway	4060
RTP base	29100
LDAP server	389
HTTP proxy	0

2. Define the RTP base starting point from which the phone will count up when negotiating.
 - Default value is 5010.
3. Click **Submit**.

Administration via local phone

```
|--- Admin
    |--- Network
        |--- Port configuration
            |--- RTP base
```

CODEC PREFERENCES

If "Silence suppression" is activated, the transmission of data packets is suppressed on no conversation, that is, if the user is silent.

The OpenScope Desk Phone CP phone provides the codecs

- G.722
- G.711
- G.729

When a connection is established between two endpoints, the phones negotiate the codec to be used. The result of the negotiation is based on the general availability and ranking assigned to each codec. The administrator can allow or disallow a codec as well as assign a ranking number to it.

The Packet size, i. e. length in milliseconds, of the RTP packets for speech data, can be set to 10 ms, 20 ms, 30 ms, 40 ms, 60 ms or to automatic detection.

Administration via WBM

1. Open Speech > Codec preferences.

Codec preferences

Silence suppression ☐

Packet size Automatic ▼

G.711 ranking ▼ ✗

G.729 ranking ▲ ▼ ✗

G.722 ranking ▲ ✓

Submit Reset

- **Silence suppression:** Suppression of data transmission on no conversation.
 - Value range: "On", "Off"
 - Default: "Off"

- **Allow "HD" icon:** If "On" an additional icon is shown when codec G.722 is used.
 - Value range: "On", "Off"
 - Default: "On"
- **Packet size:** Size of RTP packets in milliseconds.
 - Value range: "10 ms", "20ms", "30ms", "40ms", "60ms", "Automatic"
 - Default: "Automatic"
- **G.722:** Parameters for the G. 722 codec.
 - Value Range: "Choice 1", "Choice 2", "Choice 3", "Choice 4", "Disabled", "Enabled"
 - Default: "Disabled"
- **G.711:** Parameters for the G. 711 codec.
 - Value Range: "Choice 1", "Choice 2", "Choice 3", "Choice 4", "Disabled", "Enabled"
 - Default: "Choice 2"
- **G.729:** Parameters for the G. 729 codec.
 - Value Range: "Choice 1", "Choice 2", "Choice 3", "Choice 4", "Disabled", "Enabled"
 - Default: "Choice 3"

Administration via local phone

```
|--- Admin
    |--- Speech
        |--- Codec Preferences
            |--- Silence suppression
            |--- Packet size
                |--- OPUS
                |--- G.711
                |--- G.729
                |--- G.722
```

Security and policies

CHANGING A PASSWORD

The passwords for user and administrator can be changed.

Note The administrator password should be changed after the first login.

The default password for the user is not set. The default password for the administrator is "123456".

By default, password entry is in numeric mode and a minimum length of 6 characters.

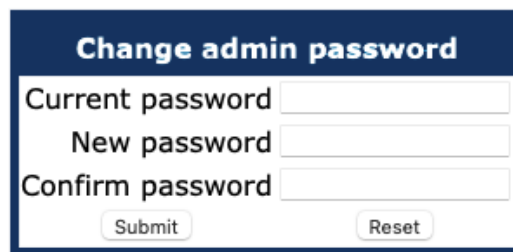
Usable characters are 0-9 A-Z a-z . " * # , ? ! ' + - () @ / : _

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.

Changing the administrator password

1. Open Security and Policies > Password > Change admin password.



A screenshot of a web form titled "Change admin password". The form has a dark blue header with the title in white. Below the header, there are three input fields: "Current password", "New password", and "Confirm password". At the bottom of the form, there are two buttons: "Submit" and "Reset".

2. Enter the current admin password and the new password.
3. Confirm the new admin password and click **Submit**.

Changing the user password

1. Open Security and Policies > Password > Change user password.



A screenshot of a web form titled "Change user password". The form has a dark blue header with the title in white. Below the header, there are three input fields: "Admin password", "New password", and "Confirm password". At the bottom of the form, there are two buttons: "Submit" and "Reset".

2. Enter the admin password and the new user password.
3. Confirm the new user password and click **Submit**.

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
```

RETRIEVE A LOST PASSWORD

Lost user password

If a user password is lost, the administrator may reset the user password.

Lost administrator password

If the administration or user password is lost, and if no DLS is available, new passwords must be provided.

In case of lost administration password, a factory reset is necessary.

1. On the phone, press the number keys 2-8-9 simultaneously. The factory reset menu opens. If not, the key combination is deactivated due to security reason.
2. In the input field, enter the special password for factory reset "124816".
3. Confirm by pressing **OK**.

CERTIFICATES

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).

- When OCSP check is activated, the configured OCSR is requested to check if the certificate has been revoked.

- OCSR 1 address specifies the IP address (or FQDN) of a primary OCSP responder.
- OCSR 2 address specifies the IP address (or FQDN) of a secondary OCSP responder.

Administration via WBM

1. Open Security and Policies > Certificates > Generic.

2. Click **Submit**.

Administration via local phone

```
|--- Admin
      |--- Security and policies
            |--- Certificates
                  |--- Generic
                        |--- Secure file transfer
                        |--- Secure HFA gateway
                        |--- Secure 802.1x server
```

Authentication policy

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

Administration via WBM

1. Open Security and Policies > Certificates > Authentication policy.

Authentication policy	
Secure file transfer	None
Secure send URL	None
Secure SIP server	None
Secure 802.1x server	Trusted
LDAP via TLS	None
Secure DMS server	None
Secure XSI server	None
Secure Exchange server	None
Secure Circuit server	None
Secure E/A Cockpit server	None
Secure OpenScape UC server	None
Wi-Fi WPA-Enterprise server	Trusted

Submit Reset

- Secure file transfer sets the authentication level for the HTTPS server to be used (see "Common FTP / HTTPS settings (defaults)" → page 105).
- Secure HFA gateway sets the authentication level for the HFA gateway connected to the phone (see "HFA gateway settings" → page 78).
- Secure 802.1x server sets the authentication level for the 802.1x authentication server.

Administration via local phone

```
|--- Admin
    |--- Security and policies
        |--- Certificates
            |--- Authentication policy
                |--- Secure file transfer
                |--- Secure HFA gateway
                |--- Secure 802.1x server
```

SCEP

SCEP (Simple Certificate Enrollment Protocol) enables automatic provisioning and certificate renewal on the 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, configure the following parameters:

SCEP

- **Address:** SIP address configured for SCEP.
- **Url:** Name of the address, for example "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

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, Acs client.

For the CP7x 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

The phone contacts the SCEP gateway and asks for the certificate on the following occasions:

- After start-up (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, the phone does not try to request any certificates.

This is logged as ERROR in the trace file and security log. If the certificate request is a result of an immediate action (On demand), the message "SCEP server does not have required capabilities" is displayed.

After the phone sends a SCEP request, the SCEP server returns the CA certificate and fingerprint and the phone checks the validity of the received CA certificate against the fingerprint. If the validity check fails, the phone rejects this certificate and creates an ERROR log in the trace file and security log. If the certificate request is the result of an immediate action (On demand), the message "Certificate error" is displayed.

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

If the SCEP server returns multiple CA certificates, they need to be stored in proper location and used in the services they belong to.

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

Handling pending status

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

In that case, the phone needs to resend an enroll request to check if the status has changed. The phone will resend the request in the following intervals (the interval gets longer every time PENDING is returned) :

- 5 min
- 10 min
- 30 min
- 1 h
- 6 h
- 24 h

If the certificate is not provided at the last attempt (that is after 24 hours), the request is no longer sent and the admin must trigger the action again manually.

If the SCEP server is changed or replaced, the phone certificates deployed by the previous SCEP server must be deleted before deployment from the new SCEP server. If the pending certificate was approved by an SCEP admin, the phone admin should re-request the certificate enrollment to launch the deployment.

Administration via WBM

- Open Security and Policies > Certificates > SCEP

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
```

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

1. Open Maintenance > Restart Phone.
2. Select "Confirm restart".

Administration via Local Phone

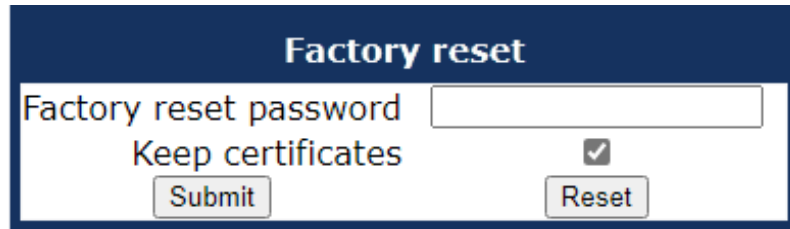
```
|--- Admin
    |--- Maintenance
        |--- Restart
```

Factory reset

This function resets all parameters to their factory settings. A special reset password is required for this operation: "124816".

Administration via WBM

1. Open Maintenance > Factory reset.



2. Enter the factory reset password.
3. If the certificates should be kept on the phone, enable "Keep certificates".
4. Click "Reset".

Administration via local phone

```
|--- Admin
      |--- Maintenance
            |--- Factory reset
```

SSH — secure shell access

The phone 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 time span. When this time span 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

Note It is not possible to log-on as "root" via SSH.

By default, SSH access is disabled.

Administration via WBM

1. Open Maintenance > Secure shell.

- When "Enable access" is active, and the parameters are specified, SSH access is activated.
- With the "Session password" parameter, a required password for the "admin" user is created. It is valid for the time span specified in the parameters.
- Access minutes defines the time span in minutes within which the SSH connection must be established. After it has expired, a log-on via SSH is not possible.
 - Value range: 1...10.
- Session minutes defines the maximum length in minutes for an SSH connection. After it has expired, the "admin" user is logged out.
 - Values: 5, 10, 20, 30, 60.

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 with the user login if logging on as administrator is not permitted.

Administration via local phone

```
|--- Admin
```

```
|--- Licence information
```

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 OpenScape Desk Phone CP110 / CP210 / CP410 phones 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"](#) → page 149).

Administration via WBM

1. Open Maintenance > HPT interface.
2. Click **Disable HPT** to deactivate.

Administration via local phone

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

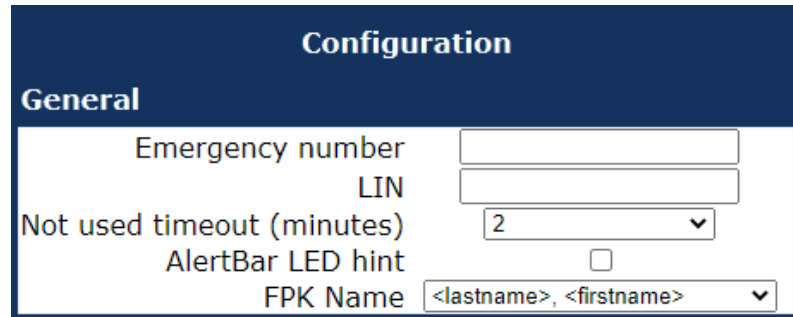
AlertBar LED hint

Note This option is only available for the OpenScape Desk Phone CP410 and CP710 phones.

The administrator can control how the AlertBar LED is automatically turned off when it has been used to indicate a missed call.

Administration via WBM

1. Open System > Features > Configuration.



The screenshot shows the 'Configuration' page with a 'General' tab selected. The page has a dark blue header with the title 'Configuration'. Below the header, the 'General' tab is active. The configuration fields are as follows:

Field	Value
Emergency number	
LIN	
Not used timeout (minutes)	2
AlertBar LED hint	<input type="checkbox"/>
FPK Name	<lastname>, <firstname>

2. Enable "AlertBar LED hint" to turn off the LED as soon as the user enters "Conversations" or "Call log". The conversations screen and the main menu screen will continue to indicate the existence of a new missed call. This function is disabled by default.
3. Click **Submit**.

Diagnostics

Note 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 executed.

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.

Note For details on LLDP-MED, refer to the ANSI/TIA-1057 standard.
For a network configuration example that shows LLDP-MED in operation, refer to "LLDP-Med example" → page 177.

View Data From WBM

1. Open Diagnostics > LLDP-MED TLVs.

LLDP-MED TLVs	
Sent	Received
<p>Sent: Wed Jul 6 09:08:45 2022</p> <p>Chassis ID TLV Data .Subtype = MAC address .ID = 00:1A:E8:DE:09:F1</p> <p>Port ID TLV Data .Subtype = MAC address .ID = 00:1A:E8:DE:09:F1</p> <p>TTL TLV data .seconds = 120</p> <p>System Caps TLV Data .Supported = Bridge, Telephone, .Enabled = Telephone,</p> <p>MAC_Phy config TLV data .Auto-set supported = Yes .Auto-set enabled = Yes .PMD = 0x6c01 .PMD1 = 10BASE-T half duplex mode</p>	<p>Received: Wed Jul 6 09:08:45 2022</p> <p>TTL TLV data .seconds = 5065816</p> <p>MAC_Phy config TLV data .Auto-set supported = Yes .Auto-set enabled = Yes .PMD = 0x6c01 .PMD1 = 10BASE-T half duplex mode .PMD2 = 10BASE-T full duplex mode .PMD3 = 100BASE-TX half duplex mode .PMD4 = 100BASE-TX full duplex mode .PMD5 = 1000BASE-T full duplex mode .MAU = Undefined : 0x0</p> <p>Network policy .TLV not available</p>

- **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 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
                |--- Extended Power
                |--- Network policy (voice)
                |--- Network policy (signalling)
                |--- LLDP-MED cap's
                |--- MAC_Phy config
                |--- System cap's
                |--- TTL

```

FAULT TRACE CONFIGURATION

Error tracing and logging can be configured separately for all components, i. e. the services and applications running on the OpenScope Desk Phone CP. The resulting files can be viewed in the WBM web pages over the download links.

Note The absolute maximum file size is 6,290,000 bytes. However, on OpenScope Desk Phone CP phones, a maximum size not greater than 1,000,000 bytes is recommended due to the amount of available memory.

Administration via WBM

1. Open Diagnostics > Fault trace configuration.

Fault trace configuration			
File size (Max 6290000 bytes) <input type="text" value="1048576"/>		Trace timeout (minutes) <input type="text" value="0"/>	Automatic clear before start <input type="checkbox"/>
Trace levels for components			
802.1x service	OFF	Administration	OFF
Application framework	OFF	Application menu	OFF
Broadsoft service	OFF	Call log	OFF
Call view	OFF	Certificate management	OFF
Clock service	OFF	Communications	OFF
Component registrar	OFF	CPE Service	OFF
CSTA service	OFF	Data access service	OFF
Desktop	OFF	Digit analysis service	OFF
Directory service	OFF	DLS client management	OFF
GPALAudio Core	OFF	GPALAudio Framework	OFF
Health service	OFF	Instrumentation service	OFF
Journal service	OFF	Media control service	OFF
Media recording service	OFF	Mobility service	OFF
OpenStage client management	OFF	Password management service	OFF
Phonebook	OFF	Performance marks	OFF
Physical interface service	OFF	RingCentral Service	OFF
Security log service	OFF	Service framework	OFF
Service registry	OFF	SIP call control	OFF
SIP messages	OFF	SIP signalling	OFF
SIP MST stack	OFF	Team service	OFF
Tone generation service	OFF	Transport service	OFF
HTTP service	OFF	Voice engine service	OFF
Voice mail	OFF	Web server service	OFF

- 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".
- 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 infinitely. 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 is written without time limit.
- If "Automatic clear before start" is enabled, the existing trace file is deleted on clicking **Submit**, and a new, empty trace file is generated. By default, it is unchecked.

Log files

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 is 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 is 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.
- **Download old exception file:** The exception file is stored permanent memory. When the file has reached its size limit, it is 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.
- **Download dial plan file:** If a dial plan has been uploaded to the phone, it is displayed here, along with its status (enabled or disabled) and error status.
- **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.

Components / Services

- Bluetooth service (CP710 only)
- Broadsoft service
- ConversationAPI (CP710 and CP410 only)
- CPE Service
- Exchange service (CP710 and CP410 only)
- GPALAudio Core
- GPALAudio Framework
- OBEX service (CP710 only)
- OpenScape UC service (CP710 and CP410 only)
- RingCentral service
- SIP M5T stack
- vCard parser service
- **Administration:** Deals with the changing and setting of parameters within the phone database, from both the user and the admin menus.
- **Application framework:** All applications within the phone, e.g. Call view, Call log, or directory, are run within the application framework. It is responsible for the switching between different applications and bringing them into and out of focus as appropriate.
- **Application menu:** This is where applications to be run on the phone can be started and stopped.
- **Call Log** (CP110 / CP210): 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.
- **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** (CP110 / CP210): 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:** Analyzes 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 phone book, trying to match incoming and outgoing numbers with entries in the phone book.
- **DLS client management:** Handles interactions with the DLS (Deployment Service).
- **Health service:** Monitors other components of the phone for diagnostic purposes and provides a logging interface for the services in the phone.

- **HTTP Service:** Handles the HTTP service messages.
- **Instrumentation service:** Used by the HPT phone tester to exchange data with the phone for remote control, testing and monitoring purposes.
- **Journal service:** Responsible for saving and retrieving call history information, which is used by the Call log application.
- **Media control service:** Provides the control of media streams (voice, tones, ringing etc.) within the phone.
- **Media recording service:** Logs the data flow generated with call recording.
- **Mobility service:** Handles the mobility feature whereby users can log onto different phones and have them configured to their own profile.
- **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.
- **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.

Note 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, click wheel 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** (CP710 and CP410 only): Handles interactions between the phone and any attached sidecars.
- **SIP call control:** Contains the call model for the phone and is associated with telephony and call handling.
- **SIP messages:** Traces the SIP messages exchanged by the phone.

Note After changing the level for the tracing of SIP messages, the phone must be rebooted. Otherwise the changes would have no effect.

- **SIP signaling:** Involved in the creation and parsing of SIP messages. This service communicates directly with the SIP stack.
- **Team service:** Primarily concerned with keyset operation.
- **Tone generation service:** Handles the generation of the tones and ringers on the phone.
- **Transport service:** Provides the IP (LAN) interface between the phone and the outside world.
- **Video service engine** (CP710 only): 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** (CP110 / CP210): Handles the voice mail functionality.
- **Web server service:** Provides access to the phone via web browser.

- **802.1x service:** Provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. The service is used for certain closed wireless access points.

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 predefined 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" → page 149).

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

Phone administration problems

The phone administration problems define a set of trace profiles that will help in investigating problems in a specific area.

1. Open Diagnostics > EasyTrace Profiles > Phone administration problems.

Phone administration problems	
File size (Max 6290000 bytes)	<input type="text" value="1048576"/>
Trace timeout (minutes)	<input type="text" value="0"/>
Automatic clear before start	<input type="checkbox"/>
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 ▼
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>
Download trace file	Download saved trace file

Audio related problems

1. Open Diagnostics > EasyTrace Profiles > Audio related problems.

Audio related problems

File size (Max 6290000 bytes)	<input type="text" value="1048576"/>
Trace timeout (minutes)	<input type="text" value="0"/>
Automatic clear before start	<input type="checkbox"/>

Trace levels for components

GPALAudio Core	<input type="text" value="DEBUG"/>
GPALAudio Framework	<input type="text" value="DEBUG"/>
Media control service	<input type="text" value="DEBUG"/>
SIP messages	<input type="text" value="DEBUG"/>
Tone generation service	<input type="text" value="DEBUG"/>
Voice engine service	<input type="text" value="DEBUG"/>

[Download trace file](#)[Download saved trace file](#)

Note This EasyTrace profile contains the tracing of SIP messages. After changing the level for the tracing of SIP messages, the phone must be rebooted.

Call proceeding problems

- Open Diagnostics > EasyTrace Profiles > Call proceeding problems.

Call proceeding problems

File size (Max 6290000 bytes)	<input type="text" value="1048576"/>
Trace timeout (minutes)	<input type="text" value="0"/>
Automatic clear before start	<input type="checkbox"/>

Trace levels for components

Call view	<input type="text" value="DEBUG"/>
Communications	<input type="text" value="DEBUG"/>
CSTA service	<input type="text" value="DEBUG"/>
SIP call control	<input type="text" value="DEBUG"/>
SIP messages	<input type="text" value="DEBUG"/>
SIP signalling	<input type="text" value="DEBUG"/>

[Download trace file](#)[Download saved trace file](#)

Note This EasyTrace profile contains the tracing of SIP messages. After changing the level for the tracing of SIP messages, the phone must be rebooted.

Conversations / LDAP problems

1. Open Diagnostics > EasyTrace Profiles > Conversations / LDAP problems.

Conversations / LDAP problems

File size (Max 6290000 bytes)	<input type="text" value="1048576"/>
Trace timeout (minutes)	<input type="text" value="0"/>
Automatic clear before start	<input type="checkbox"/>

Trace levels for components

Call view	<input type="text" value="DEBUG"/>
ConversationAPI	<input type="text" value="DEBUG"/>
CSTA service	<input type="text" value="DEBUG"/>
Digit analysis service	<input type="text" value="DEBUG"/>
Directory service	<input type="text" value="DEBUG"/>
Exchange service	<input type="text" value="DEBUG"/>
Journal service	<input type="text" value="DEBUG"/>

[Download trace file](#)[Download saved trace file](#)

Keyset problems

1. Open Diagnostics > EasyTrace Profiles > Keyset problems.

Keyset problems

File size (Max 6290000 bytes)	<input type="text" value="1048576"/>
Trace timeout (minutes)	<input type="text" value="0"/>
Automatic clear before start	<input type="checkbox"/>

Trace levels for components

Call view	<input type="text" value="DEBUG"/>
Communications	<input type="text" value="DEBUG"/>
CSTA service	<input type="text" value="DEBUG"/>
Sidecar service	<input type="text" value="DEBUG"/>
SIP messages	<input type="text" value="DEBUG"/>
Team service	<input type="text" value="DEBUG"/>

[Download trace file](#)[Download saved trace file](#)

Note

This EasyTrace profile contains the tracing of SIP messages. After changing the level for the tracing of SIP messages, the phone must be rebooted.

Mobility / DLS problems

1. Open Diagnostics > EasyTrace Profiles > Mobility / DLS problems.

Mobility / DLS problems	
File size (Max 6290000 bytes)	<input type="text" value="1048576"/>
Trace timeout (minutes)	<input type="text" value="0"/>
Automatic clear before start	<input type="checkbox"/>
Trace levels for components	
Call view	<input type="text" value="DEBUG"/>
Communications	<input type="text" value="DEBUG"/>
DLS client management	<input type="text" value="DEBUG"/>
Mobility service	<input type="text" value="DEBUG"/>
OpenStage client management	<input type="text" value="DEBUG"/>
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>
Download trace file	Download saved trace file

Network problems

1. Open Diagnostics > EasyTrace Profiles > Network problems.

Network problems	
File size (Max 6290000 bytes)	<input type="text" value="1048576"/>
Trace timeout (minutes)	<input type="text" value="0"/>
Automatic clear before start	<input type="checkbox"/>
Trace levels for components	
802.1x service	<input type="text" value="DEBUG"/>
Transport service	<input type="text" value="DEBUG"/>
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>
Download trace file	Download saved trace file

Security problems

1. Open Diagnostics > EasyTrace Profiles > Security problems.

Security problems	
File size (Max 6290000 bytes)	<input type="text" value="1048576"/>
Trace timeout (minutes)	<input type="text" value="0"/>
Automatic clear before start	<input type="checkbox"/>
Trace levels for components	
Certificate management	<input type="text" value="DEBUG"/>
Password management service	<input type="text" value="DEBUG"/>
Security log service	<input type="text" value="DEBUG"/>
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>
Download trace file	Download saved trace file

Bluetooth problems

Note This option is only available for the OpenScape Desk Phone CP710.

1. Open Diagnostics > EasyTrace Profiles > Bluetooth problems.

Bluetooth problems

File size (Max 6290000 bytes)

Trace timeout (minutes)

Automatic clear before start ☐

Trace levels for components

Bluetooth service	DEBUG ▼
CSTA service	DEBUG ▼
OBEX service	DEBUG ▼
vCard parser service	DEBUG ▼

[Download trace file](#) [Download saved trace file](#)

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

Administration via WBM

1. Open Diagnostics > Advanced audio traces.
 - **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 is cleared after pressing the Submit button.
 - **Capture and stop:**
 - 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):** 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. 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.

QOS REPORTS

Conditions and thresholds for report generation

Note For details about the functionality, refer to the Release Notes.

The generation of QoS (Quality of Service) reports which are sent to a QCU server is configured here.

Administration via WBM

1. Open Diagnostics > QoS Reports > Generation.

Generation	
Report mode	OFF <input type="button" value="v"/>
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	<input type="checkbox"/>
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

- **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 local phone

```
|--- Admin
    |--- Network
        |--- QoS
            |--- Reports
                |--- Generation
                    |      |--- Mode
                    |      |--- Report interval
                    |      |--- Observe interval
                    |      |--- Minimum session length
                |--- Send now
                    |--- Thresholds
                        |--- Maximum jitter
                        |--- Round-trip delay
                    |--- Non-compressing:
                    |--- ...Lost packets (K)
                    |--- ...Lost consecutive
                    |--- ...Good consecutive
                    |--- Compressing:
                    |--- ...Lost packets (K)
                    |--- ...Lost consecutive
                    |--- ...Good consecutive
```

View report

OpenScope 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.

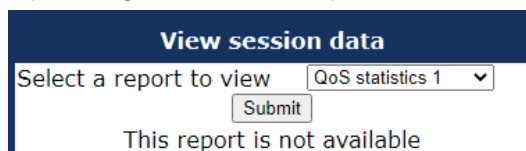
To enable the generation of reports, ensure that:

- The switch QoS traps to QCU (System > SNMP) is activated (see "SNMP" → page 68);
- The conditions for the generation of reports are set adequately.

For details about QoS reports on OpenScope Desk Phone CP devices, see the HiPath QoS Data Collection V 1.0 Service Manual.

Data viewing via WBM

1. Open Diagnostics > QoS reports > View Session Data.



2. Click **Submit**.

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.
- **HiPath Switch ID:** Unique number identifying the HiPath switch to which the endpoints are assigned.
- **LTU number:** In HiPath 4000 only, the shelf identification is taken from the shelf containing a gateway.
- **Slot number:** The slot number where the phone is connected in the shelf.
- **Endpoint type :** Type of the local phone.
- **Version:** Software version of the local phone.
- **Subscriber number type:** Type of subscriber number assigned to the local phone. The possible types are:
 - 1: local number, extension only
 - 2: called number, network call
 - 3: E.164 number of the local phone
- **Subscriber number:** Subscriber number of the local phone.
- **Call ID:** SIP call id.
- **MAC address:** MAC address of the local phone.

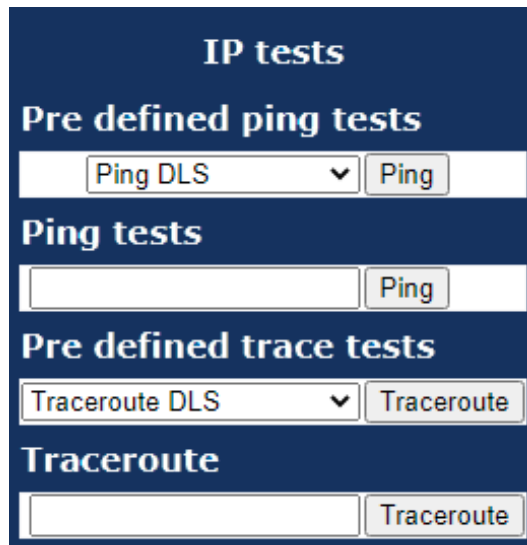
MISCELLANEOUS

IP tests

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

Administration via WBM

1. Open Diagnostics > Miscellaneous > IP tests.



IP tests

Pre defined ping tests

Ping DLS ▼ Ping

Ping tests

Ping

Pre defined trace tests

Traceroute DLS ▼ Traceroute

Traceroute

Traceroute

- **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 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 IP address or hostname.

Memory status information

The processes currently running on the phone 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, 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.

Administration via WBM

1. Open Diagnostics > Miscellaneous > Memory information.

Memory information

Memory monitor configuration

Disable reboot

☐

High threshold(MBs)

Low threshold(MBs)

Working hour start

Working hour end

Submit

Reset

[Download memory info file](#)
[Download old memory info file](#)

[Download thread info for services](#)
[Download thread info for callview](#)
[Download thread info for admin](#)

Device memory information

```

Mem: 123988K used, 117156K free, 604K shrd, 0K buff, 46900K cached
CPU:  0% usr 26% sys  0% nic 66% idle  0% io  0% irq  0% sirq
Load average: 2.15 2.15 2.04 1/251 1392
PID  PPID  USER   STAT  VSZ %VSZ KCPU COWWAND
1392  583  root    R      3024 1% 27% /bin/busybox top -d 0 -a -n 1 -l 600 -b
511   1  root    S      17844 7% 7% app_dsp
608   583  root    S      1326 56% 0% SvcConfig services.conf -startlogDaemon -logAll V2 R0.3.66
1065  608  root    SN     36432 15% 0% (QT Gui CallView) PhoneletLauncher callview.phd V2 R0.3.66
1032  608  root    SN     35800 15% 0% (QT Gui DesktopP) PhoneletLauncher desktopphonelet.phd V2 R0.3.66
583   1  root    S      34446 14% 0% SvcConfig HealthService.conf
1093  608  root    SN     34252 14% 0% (QT Gui AdminPho) PhoneletLauncher admin.phd V2 R0.3.66
1134  608  root    SN     31256 13% 0% (QT Gui CalllogP) PhoneletLauncher calllog.phd V2 R0.3.66
1092  608  root    SN     31140 13% 0% (QT Gui LDAppPhon) PhoneletLauncher ldap.phd V2 R0.3.66
1091  608  root    SN     30700 13% 0% (QT Gui Messages) PhoneletLauncher MessagesPhonelet.phd V2 R0.3.66
1066  608  root    SN     27208 11% 0% (QT Gui Applaunch) PhoneletLauncher Applauncher.phd V2 R0.3.66
1036  1  appweb  SN     15740 7% 0% ./appweb --config opera_appweb_latestTlsOnly.conf
1397  1036  appweb  SN     14046 6% 0% /Opera_Deploy/appweb/web/page.cnd
582   1  root    S      11672 5% 0% SplashScreenApp
718   1  root    S      7324 3% 0% /usr/sbin/stunnel /Opera_Deploy/stunnel_server_allTlsVersions.conf
709  608  root    S      4220 2% 0% /sbin/dhclient -4 -d -q -sf /Opera_Deploy/networking/dhcpv4Event.sh -lf /data/networking/dhcpv4Leases.none -cf /data/networking/dhcpv4.conf eth0
1    0  root    S      3024 1% 0% init
312   1  root    S      3024 1% 0% /sbin/syslogd -L -s 2000 -O /tmp/logs/messages

```

- When "Disable reboot" is checked, no reboot will take place when a memory problem has been found. However, recovery requires a reboot. The recovery process is triggered when the available main memory (RAM) falls below a given threshold value. As memory consumption is assumed to be higher during working hours, two thresholds are configurable.
- The High Threshold (MBs) parameter defines the threshold for off-time:
 - For OpenScape Desk Phone CP110/210, the default value is 10 MB.
 - For OpenScape Desk Phone CP410/710, it is 30 MB.
- With Low Threshold (MBs), the threshold for off-time is defined:
 - For OpenScape Desk Phone CP110/210, the default value is 8 MB.
 - For OpenScape Desk Phone CP410/710, it 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).

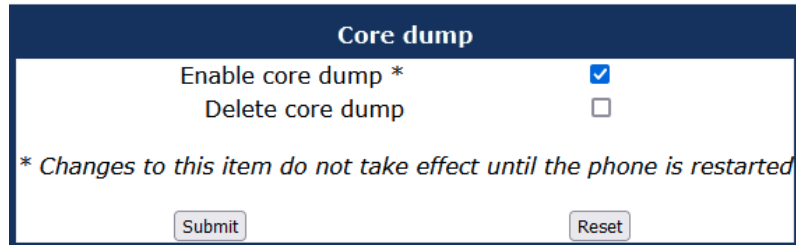
When memory shortage has occurred, information about the incident is written to a log file which can be viewed via the "Download memory info" file link.

If there has been a previous case of memory shortage, the corresponding log file can be viewed via "Download memory info" file.

Core dump

Administration via WBM

1. Open Diagnostics > Miscellaneous > Core Dump.



Core dump

Enable core dump * ☒

Delete core dump ☐

** Changes to this item do not take effect until the phone is restarted*

Submit Reset

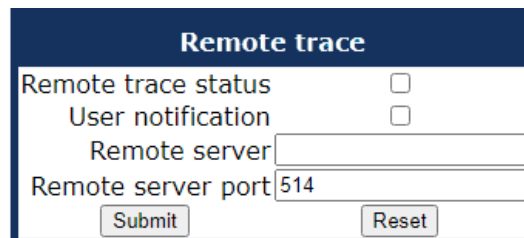
- If "Enable core dump" is enabled, a core dump is initiated in case of a severe error. The core dump is saved to a file. By default, this function is active.
- If "Delete core dump" is activated, the current core dump file is deleted when clicking **Submit**.
 - By default, this feature is not enabled.
- If one or more core dump file exist, hyperlinks for downloading are created automatically.

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.

Administration via WBM

1. Open Diagnostics > Remote trace.



Remote trace

Remote trace status ☐

User notification ☐

Remote server

Remote server port

Submit Reset


- To enable remote tracing, "Remote trace status" must be enabled. Furthermore, the IP address of the server receiving the syslog messages must be entered as remote server, 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 icon will inform the user when remote tracing is active, i.e. when "Remote trace status" is enabled.

Administration via local phone

```
|--- Admin
    |--- Maintenance
        |--- Remote trace
            |--- Remote trace status
            |--- User notification
            |--- Remote ip
            |--- Remote port
```

Key modules

Note On an OpenScape Desk Phone CP110 / CP210 phone no key modules can be connected.

- On an OpenScape Desk Phone CP410 phone the key module KM410 provides 16 additional free programmable keys. The names of the assigned keys can be printed on labels.
- On an OpenScape Desk Phone CP710 the key module KM710 provides 12 additional free programmable keys. The names of the assigned keys are displayed digitally and can have multiple functions ("shifted") invoked by pressing the key .
- The maximum number of key modules that can be attached depends on the phone model, the key module type and whether Power over Ethernet (PoE) is used to power the phone. However, up to 4 key modules can be attached if the phone is not powered by PoE.

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

Administration via WBM

1. Open System > Features > Key module X.
 - The configured keys can be either be in "Normal" or "Shifted" level.
 - When switching to the "Shifted" level, the phone switches automatically back to the "Normal" level, unless configured otherwise.

2. Open System > Features > Configuration.

Configuration

General

Emergency number	<input type="text"/>
LIN	<input type="text"/>
Not used timeout (minutes)	<input type="text" value="2"/>
AlertBar LED hint	<input type="checkbox"/>
FPK Name	<input type="text" value="<lastname>, <firstname>"/>

Bluetooth

Enable bluetooth interface	<input checked="" type="checkbox"/>
Enable telephony	<input checked="" type="checkbox"/>

Services

Web based manag.	<input checked="" type="checkbox"/>
USB device access	<input checked="" type="checkbox"/>
USB power using PoE	<input type="text" value="120mA (up to 4 KMs)"/>

Telephony settings

Enable telephony settings	<input type="checkbox"/>
---------------------------	--------------------------

3. To configure the phone to automatically switch back to the normal level, enable **Automatic key module switchback**. The phone will start a 15 seconds timer and then switch to the non-shifted level on all the attached key modules.
4. Click **Submit**.

Examples and how-tos

Canonical dialing

CANONICAL DIALING SETTINGS

The following example shows settings suitable for the conversion of given dial strings to canonical format.

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 dialed without international prefix.
Local national code	115	Area code within the UK (here: Nottingham).
Minimum local number length	7	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 company 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.
Emergency numbers	999, 555	Set of numbers to access emergency services.
Initial extension digits	2, 3, 4, 5, 6, 8	1 st digits of numbers that are used for extension numbers on the local node.

CANONICAL DIALING LOOK-UP

The following example shows settings suitable for recognizing incoming numbers and assigning them to entries in the local phone-book, 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.

CONVERSION EXAMPLES

In the following examples, numbers entered into the local Directory 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 Directory		+441159432345
Dial string sent when dialing from the Directory	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
External access code		Not required
International gateway code		Use national code
Number stored in the Directory		+498970072345
Dial string sent when dialing from the Directory	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 Directory		+4411511234567
Dial string sent when dialing from the Directory	External numbers = Local public form	234567
	External numbers = National public form	011511234567
	External numbers = International form	004411511234567

How to set up the “Corporate directory” (LDAP)

The “Corporate directory” 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.

PREREQUISITES

- 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.
- 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 and password for all OpenScape Desk Phone CP phones.

CREATE AN LDAP TEMPLATE

The task of an LDAP template is to map the phone’s contact 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.

Note

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.

Administration via WBM

1. Open Local functions > LDAP template.

Use	Field name	Usage type
Search base	<input type="text"/>	
Last name	<input type="text"/>	<input type="text"/>
First name	<input type="text"/>	<input type="text"/>
Work 1	<input type="text"/>	<input type="text"/>
Work 2	<input type="text"/>	<input type="text"/>
Mobile	<input type="text"/>	<input type="text"/>
Home	<input type="text"/>	<input type="text"/>
Company	<input type="text"/>	<input type="text"/>
Address 1	<input type="text"/>	<input type="text"/>
Address 2	<input type="text"/>	<input type="text"/>
Role	<input type="text"/>	<input type="text"/>
Email	<input type="text"/>	<input type="text"/>
Nickname	<input type="text"/>	
Avatar	<input type="text"/>	

Submit Reset

2. Enter the field names and specify the usage type "read-only").
 - "Nickname" does not correspond to a contact field but instead relates to a special attribute that may be defined for LDAP entries. The attribute represents a free format field which may be searched for sub-strings. It is only used for search actions by the phone, not number lookups. If the Nickname attribute is defined in the LDAP template, a phone search action will look for the search string as a sub-string in this field and will ignore the other field attributes.

Generic example (standard attributes)

OpenScape Desk Phone CP field	LDAP template labels	LDAP attribute	Example value
Last name	ATTRIB01	surnameNational	Doe
First name	ATTRIB02	givenNameNational	John
Work 1	ATTRIB03	telephoneNumber	9991234
Work 2	ATTRIB04	AlternatePhone	9992345
Mobile	ATTRIB05	mobile	017711223344

OpenScope Desk Phone CP field	LDAP template labels	LDAP attribute	Example value
Home	ATTRIB06	otherTelephone	441274333444
Company	ATTRIB07	ou	Example Inc.
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 → 112

Using the example above as the LDAP subtree to be searched, the LDAP template file looks like this:

```

OpenScope Desk Phone CP LDAP TEMPLATE (v.1)
SEARCHBASE="O=SIEMENS COMM, C=GB"
ATTRIB01="surnameNational"
ATTRIB02="givenNameNational"
ATTRIB03="telephonenumber"
ATTRIB04="AlternatePhone"
ATTRIB05="mobile"
ATTRIB06="otherTelephone"
ATTRIB07="ou", READONLY
ATTRIB08="departmentText", READONLY
ATTRIB09=""
ATTRIB10="mainFunction"
ATTRIB11="mail"
ATTRIB12="nickname"
ATTRIB13=""
EOF

```

Microsoft Active Directory specific example

OpenScape Desk Phone CP field	LDAP template attribute	LDAP attribute	Example value
Last name	ATTRIB01	sn	Doe
First name	ATTRIB02	givenName	John
Business 1	ATTRIB03	ipPhone	9991234
Business 2	ATTRIB04	otherTelephone	9992345
Mobile	ATTRIB05	mobile	017711223344
Private	ATTRIB06	homePhone	441274333444
Company	ATTRIB07	company	Example Inc.
Address 1	ATTRIB08	department	Administration
Address 2	ATTRIB09	l	
Job function	ATTRIB10	title	Product Manager
Email	ATTRIB11	mail	doe@example.com
Nickname	ATTRIB12	nickname	
Avatar	ATTRIB13		jpeg image

Using the example above as the LDAP subtree to be searched, the LDAP template file looks like this:

```
OpenScope 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
```

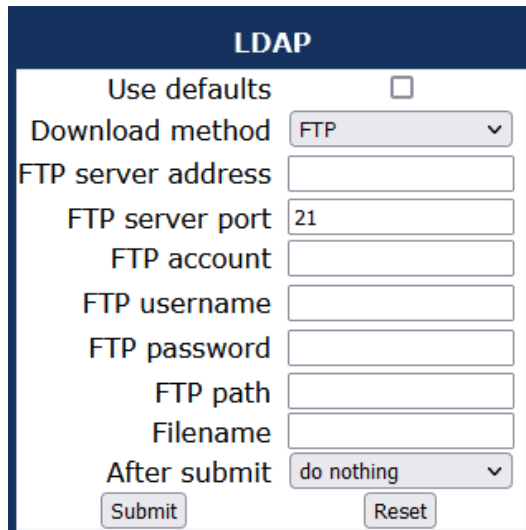
UPLOAD THE LDAP TEMPLATE TO THE PHONE

The administrator may edit the LDAP template on the phone via WBM, or via the DLS. After configuring the LDAP template, it is uploaded to the phone:

1. Save the template under a suitable name, e.g. `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" → page 114).
4. Optionally, use the local menu or the DLS (see the Deployment Service Administration Manual).

Administration via WBM

1. Open File transfer > LDAP.



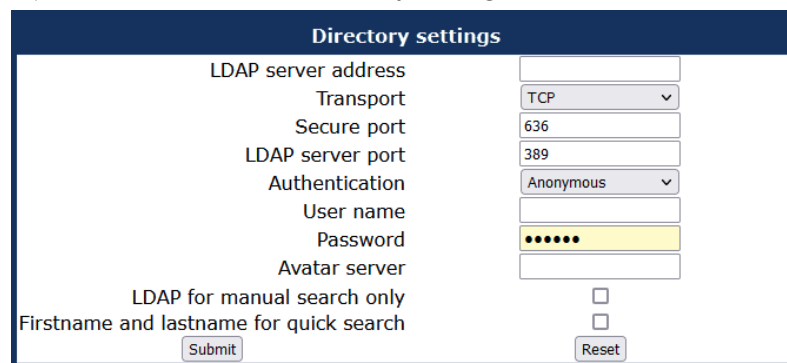
2. Enable "Use defaults" to Save the settings as default values.

3. Select the download method.
4. Enter the server information and user credentials.
5. Specify the file name.
6. Select the action after submitting the information ("do nothing", "start download").
7. Click **Submit**.

CONFIGURE LDAP ACCESS

Administration via WBM

1. Open Local Functions > Directory Settings.



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 with masked characters (dots).
- Avatar server:** A text input field.
- LDAP for manual search only:** A checkbox.
- Firstname and lastname for quick search:** A checkbox.
- Submit:** A button at the bottom left.
- Reset:** A button at the bottom right.


2. Enter the following parameters:
 - **LDAP Server address:** IP address or host name 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:** corresponding to the user name
 - **Permanent LDAP enabled**
3. Click **Submit**.

MAPPING THE LDAP FIELDS

The downloaded LDAP template can be edited on the phone via WBM.

1. Open Local functions > LDAP template.

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	<input type="text"/>	
Last name	<input type="text"/>	<input type="button" value="v"/>
First name	<input type="text"/>	<input type="button" value="v"/>
Work 1	<input type="text"/>	<input type="button" value="v"/>
Work 2	<input type="text"/>	<input type="button" value="v"/>
Mobile	<input type="text"/>	<input type="button" value="v"/>
Home	<input type="text"/>	<input type="button" value="v"/>
Company	<input type="text"/>	<input type="button" value="v"/>
Address 1	<input type="text"/>	<input type="button" value="v"/>
Address 2	<input type="text"/>	<input type="button" value="v"/>
Role	<input type="text"/>	<input type="button" value="v"/>
Email	<input type="text"/>	<input type="button" value="v"/>
Nickname	<input type="text"/>	
Avatar	<input type="text"/>	

2. Map the field names to the usage types.
3. Click **Submit**.

LLDP-MED EXAMPLE

The following example illustrates the mode of operation of LLDP-MED. To evoke a reaction from LLDP-MED, the LAN switch has been set to auto-negotiation, whereas the phone's LAN port is set to 100 Mbit/s, hence a fixed value (see "LAN port settings" → page 47). This configuration error is discovered by LLDP-MED. The following screenshots from the phone local menu show the error messages.

The WBM provides a list of the LLDP-MED TLV messages rather than the more limited LLDP-MED operation menu in local settings. The TLV list is comprehensive whereas the local settings indicate problems with the TLVs.

Note 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, open Network > LLDP-MED Operation.
3. Press **OK**.
4. In the LLDP-MED operation submenu, navigate to MAC_Phy config.
5. Note the status displayed.
6. Select the MAC_Phy config submenu by pressing **OK**.
7. 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

Technical reference

Default port list

The following table contains all default ports, resp. port ranges, and protocols used by the services running on OpenScape Desk Phone CP110/210/410/710 phones.

Service	Server Default Port	Client Default Port	Protocol Stack
Payload transport (VoIP)	5010 - 5059	5010 - 5059	RTP - RTCP
Payload transport (VoIP)	5010 - 5059	5010 - 5059	SRTP - SRTCP
SIP subscriber - TCP is used	5060	32786 - 61000	SIP / TCP
SIP subscriber - TLS is used	5061	32786 - 61000	SIP / TLS
SIP subscriber - UDP is used	5060	5060	SIP / UDP
Directory access via LDAP	---	32786 - 61000	TCP
Directory access via LDAP	---	32786 - 61000	TCP-SSL/TLS
DHCP Client	---	68	DHCP / UDP
DNS Client	---	1024 - 65535	DNS / TCP_ UDP
DLS contact me service - workpoint side	8085	---	HTTP / TCP
Default communication with the DLS workpoint interface	---	18443	HTTPS / TCP - SSL / TLS

Service	Server Default Port	Client Default Port	Protocol Stack
Secure communication with the DLS work-point 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
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

Troubleshooting error codes

For a set of error cases, specific error codes are defined. These error codes are shown in brackets on the display, following a general error note.

Example

"No Telephony possible (LP)"

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
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

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

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
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

Error code	Priority	Problem	Description
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

Error code	Priority	Problem	Description
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	<ul style="list-style-type: none"> • Exchange: check username and password • Exchange: untrusted server • connection to Exchange server failed
CI	16	Circuit failure	<ul style="list-style-type: none"> • Circuit: check username and password • Circuit: untrusted server • connection to Circuit server failed
NT	17	SNTP server unavailable	No SNTP connection

Glossary

Address of Record (AoR)

A SIP URI that represents the "public address" of a SIP user resp. a phone or line. The format is similar to an E-mail address: "username@hostname".

ADPCM

Adaptive Differential Pulse Code Modulation. A compressed encoding method for audio signals which are transmitted by a low bandwidth. 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.

BLE

Bluetooth Low Energy

CSTA

Computer Supported Telecommunications Applications. An abstraction layer for telecommunications applications allowing for the interaction of 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 guarantees on 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 host-names.

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 e.g. ISDN. It requires a 64 kBit/s bandwidth.

G.722

ITU-T standard for audio encoding using split band Network. 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 bit rate is 8 kBit/s. Music or tones such as ring tones or fax tones cannot be transported reliably with this codec.

Gateway

Mediation components between two different Network types, e. g., WiFi Network and ISDN Network.

HTTP

Hypertext Transfer Protocol. A standard protocol for data transfer in internet networks.

IP

Internet Protocol. A data-oriented Network layer protocol used for transferring data across a packet-switched Network. 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 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 accord-

ance 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 → 185 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.

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, 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 switches: 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 Network address that 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 Network

WBM

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

