A MITEL
PRODUCT
GUIDE

OpenScape Desk Phones

CPx10

Administrator Documentation for Zoom Phone (SIP)

12/2025

A31003-D3000-M104-01-76A9

Mitel

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.

	For safety reasons, the telephone should only be supplied with power: • using the original power supply unit. • over a LAN with PoE (Power over Ethernet), which complies with the IEEE 802.3af standard.
	Never open the telephone. Should you encounter any problems, consult your administrator.
	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.

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 Mitel Doc Center.

Technical notes, current information about firmware updates and Zoom Phone features can be found on the Internet at:

- Unify OpenScape Experts Wiki:

  OpenScape Desk Phone CP in Zoom Phone Environment

- Zoom support: Zoom Phone Features

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 97.

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 34).

MARKS

CONFORMS TO
ANSI/UL STD 62368-1
CERTIFIED TO
CAN/CSA C22.2 No. 62368-1

3187698

Contents

OpenScape Desk Phone in Zoom Phone environment

Starting with SIP software V2 R1, the OpenScape Desk Phone CPx10 series is Zoom-certified and fully supported in Zoom Phone environments. Zoom Phone is a cloud-based VoIP service with enhanced AI capabilities.

The CPx10 series supports a wide range of Zoom Phone features. For the latest list of supported features, refer to the official Zoom support page: Supported desk phone features.

> Any SIP software preinstalled on the CP phone is sufficient to start with Zoom Phone. During the initial provisioning, the phone automatically downloads and installs the appropriate Zoom-approved SIP software version.

Future software updates are automatically provided by Zoom phone. The user interface and feature set are automatically adopted when connected to Zoom Phone. For more information, see the official Zoom support page: Managing phones and devices.

Zoom Provisioning

When connecting a CPx10 phone to Zoom Phone, administrators can connect the phone as a 3rd-party phone, or connect the phone as a certified Zoom Phone.

CONNECTING THE PHONE AS A 3RD-PARTY PHONE

The administrator receives a set of parameters that must be configured via the WBM to connect the phone to the Zoom SIP server.

The **Server Type** parameter now includes a ZOOM value, which adjusts the phone's behavior to comply with Zoom SIP requirements (see "SIP registration" → page 103).

CONNECTING THE PHONE AS A CERTIFIED ZOOM PHONE

The CPx10 line supports Zero Touch Provisioning (ZTP) and assisted provisioning.

- Zero Touch Provisioning (ZTP):
  - Only the phone's serial number (MAC address) is needed to connect to Zoom Phone. The serial number is printed on the back of each CP phone and is also included on the package label with a barcode.
  - Phones with preinstalled SIP software and factory defaults automatically connect to Zoom Phone.
  - Firmware updates, SW deployment, and configuration are fully handled by the Zoom server.
  - No local administration interaction is required.

    > If ZTP is not working, Zoom Phone provides a short description on how to manually configure the phone using the assisted provisioning process.

- Assisted Provisioning:
  - Used if ZTP fails or is unavailable.
  - The admin sets the DMS URL in WBM. All other configuration items are provisioned by Zoom Phone.

The phone is fully configured and administrated by Zoom Phone. Firmware updates are automatically distributed. Custom provisioning templates allow tenant Administrators to customize installation and configuration.

Phones can submit location information for nomadic emergency services if the network supports it.

Security and Audio

- Every connection is secured by **SIP over TLS V1.2** and **AES-256 encryption**.
- **OPUS** is used as high quality audio codec.
- Cloud failover ensures minimal service interrupt by automatic switch over between two Zoom data center.

Firewall Requirements

Please ensure network firewall rules allow connectivity according to the Firewall Rules for Mitel IP Phones:

Service / Device	Domain / Host	IP	Port (TCP)	Description
Redirection and Configuration Server – WebUI access	rcs.mitel.com	No fixed IP	443 (HTTPS)	Mitel RCS WebUI interface for enabling and provisioning Zero Touch Provisioning services
Redirection and Configuration Server – Device Access	rcs.aastra.com	15.156.224.40 / 15.156.224.41	443 (HTTPS)	Mitel RCS interface for physical desktop devices
Redirection and Configuration Server – REST API access	rcs.mitel.com	No fixed IP	443 (HTTPS)	Mitel RCS API access for automated management and provisioning of RCS services

Proper port access is required for **Zero Touch Provisioning (ZTP)**:

Service / Device	Trusted Host	IP	Port / Protocol
Mitel OpenScape Desk Phone CP Series – ZTP	cloud-setup.-com	No fixed IP	18443 (TLS)

See also the OpenScape Experts Wiki page.

OpenScape Desk Phone Basic and Enhanced Features

Basic Call features

All basic call features are supported with Zoom phone:

- Basic call
- Hold
- Transfer
- Three party conference (local)
- Voicemail
- Call Forward (local)
- Multiple Call Handling (up to three call appearances)

Enhanced Call Features

Additionally, the following enhanced call features are supported by the CP410 and CP710 Desktop phones:

- Multiple call handling with three line keys
- Speed Dial Keys
- Busy Lamp Field
- Call Park
- Group Pickup
- Call Delegation
- Shared Line Group
- Privacy Mode
- Call Flip
- Call Monitoring (Barge, Monitor, Whisper, Take over, Listen)
- Multi Party Conference (only beta, on customer request)

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.

See also the OpenScape Experts Wiki page.

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.

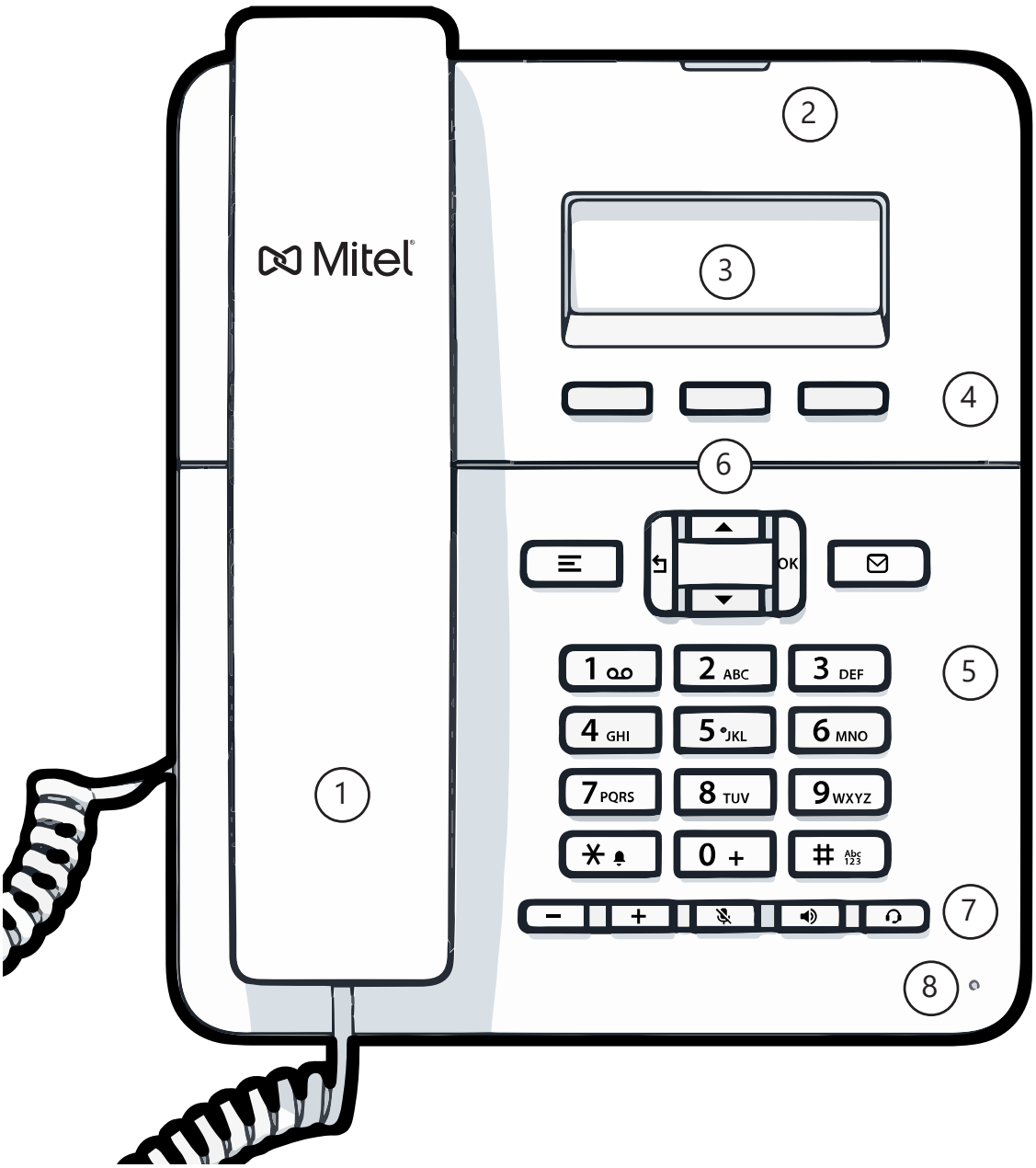
Conventions for this document

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.

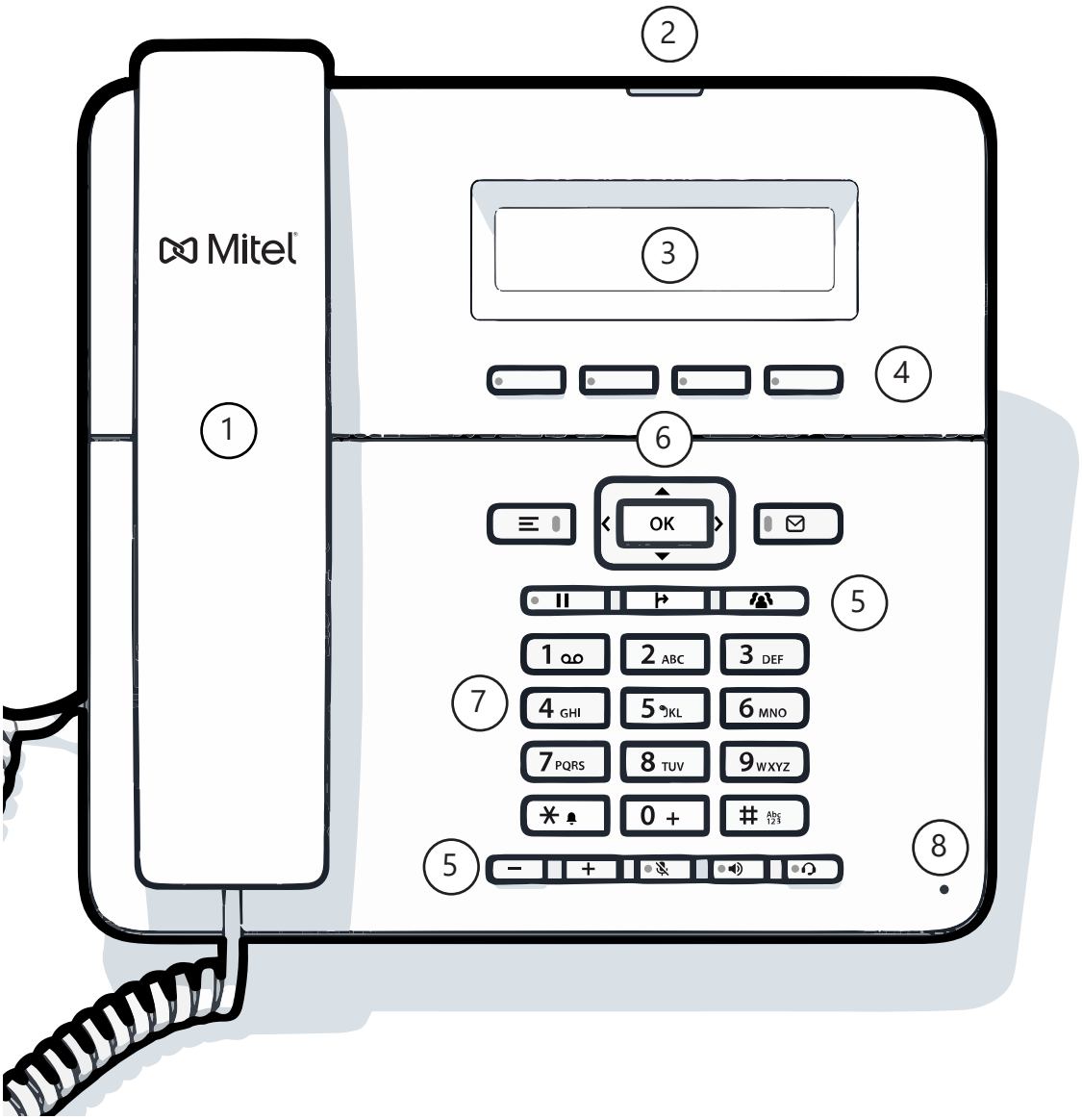
The OpenScape Desk Phone CP G2

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	The **function keys** (non-programmable) are assigned to the following functions during a call:  : Provides access to the user menu for locally controlling the phone settings.  : Allows voicemails to be managed.  : 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**.

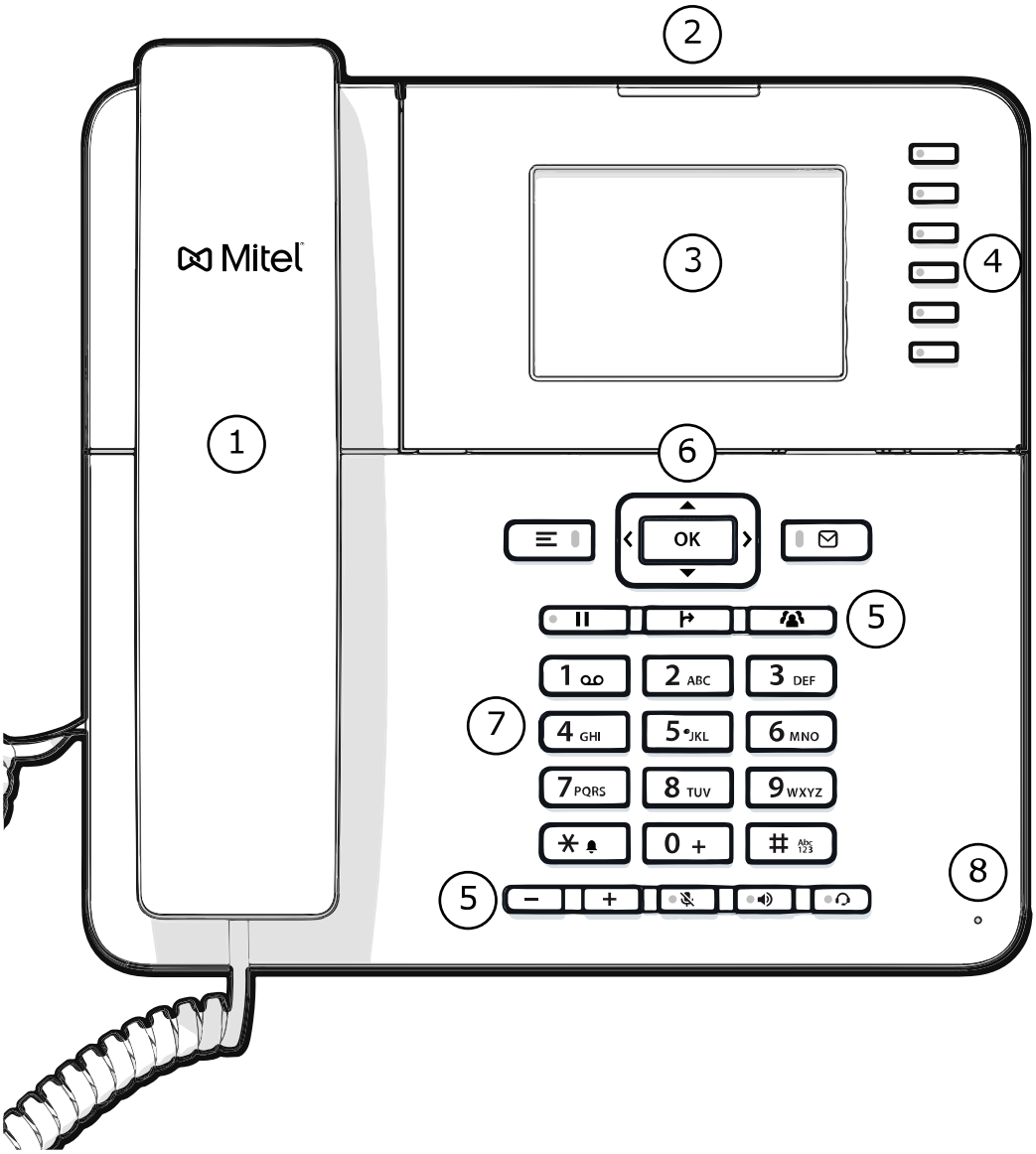
OPENSCAPE DESK PHONE CP210



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.D.
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	The **function keys** (non-programmable) are assigned to the following functions during a call:  : 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**.

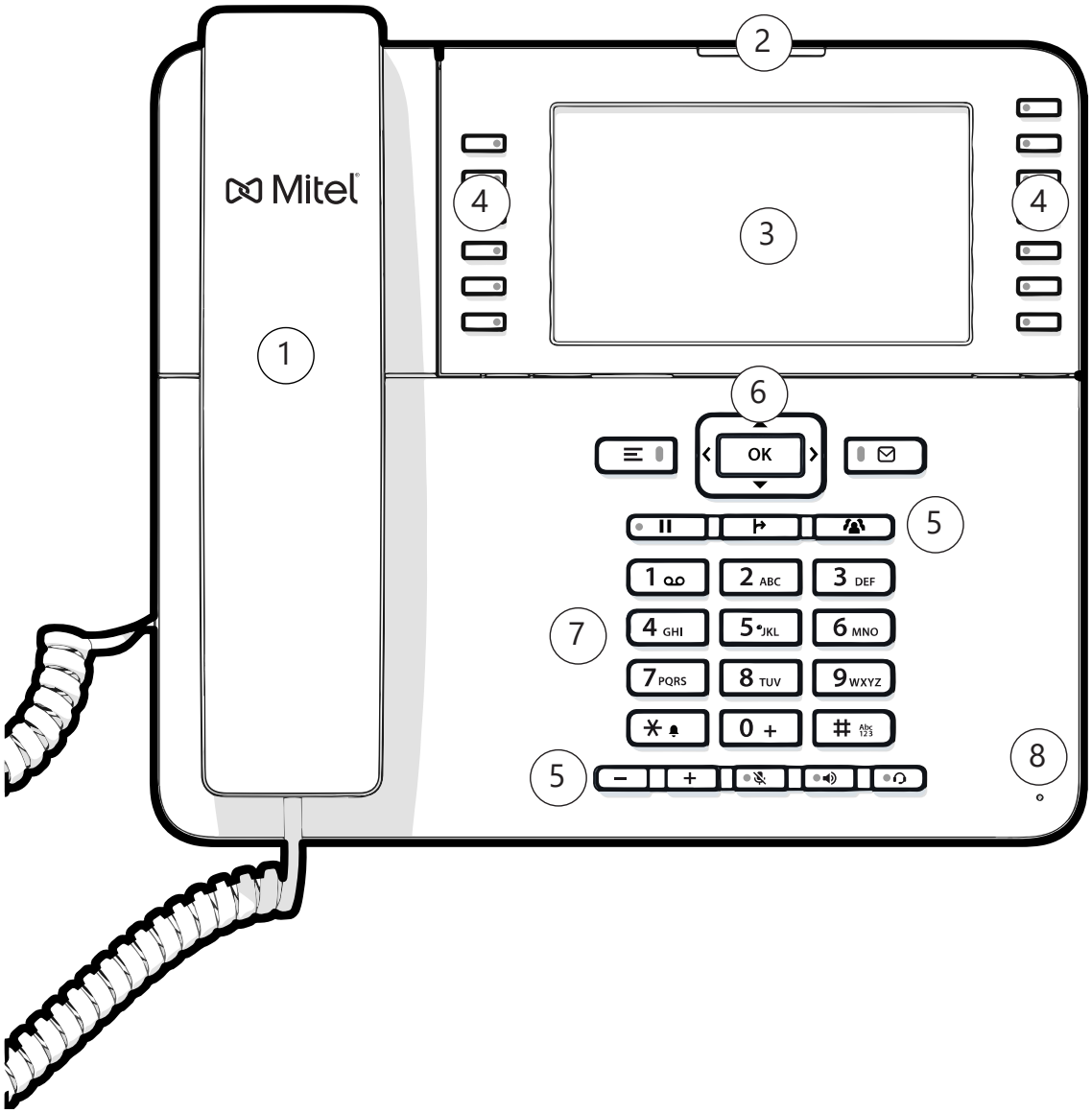
OPENSCAPE DESK PHONE CP410



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	The **function keys** (non-programmable) are assigned to the following functions during a call:  : 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**.

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	The **function keys** (non-programmable) are assigned to the following functions during a call:  : 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 "Using the web interface (WBM)" →1).

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.

OPENSCAPE DEVICE MANAGEMENT SERVICES

The OpenScape Deployment Service (DLS), Broadsoft Device Management Service (DMS) and OSEM (OpenScape Endpoint Management) are management applications for administering phones in both OpenScape and non-OpenScape networks.

In Zoom-connected CP phones, the management role normally performed by DLS/DMS/OSEM is instead performed by the Zoom provisioning and management server. However, within this guide, the term DLS may still appear conceptually to reflect provisioning actions that are now handled by Zoom.

> For detailed configuration information outside of Zoom deployments, refer to the DLS or DMS Administration Guide. and the OSEM Administration Guide on the Mitel Doc Center.

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 SIP clients and 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.

- An FTP server for file transfer, e. g. firmware, configuration data, application software
- An SNTP time server (required if secure interfaces are used)
- A DHCP (Dynamic Host Configuration Protocol) server (recommended).

When deploying OpenScape CPx10 phones with Zoom Phone, ensure that Zoom server provisioning aligns with network requirements, VLAN assignments, and SIP configuration to guarantee full functionality.

Any secure interface, such as IEEE 802.1x, requires a reliable time source. Hence, an SNTP server is essential for these interfaces. For additional information see: https://wiki.unify.com/wiki/IEEE_802.1x

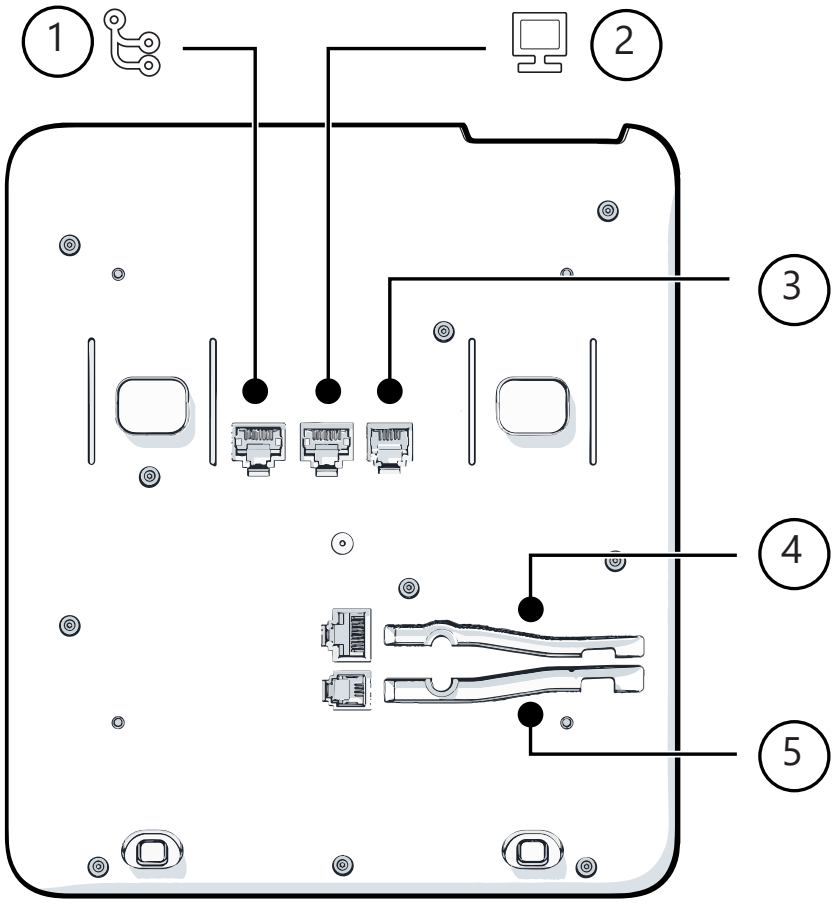
Assembling and installing the phone

SHIPMENT

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

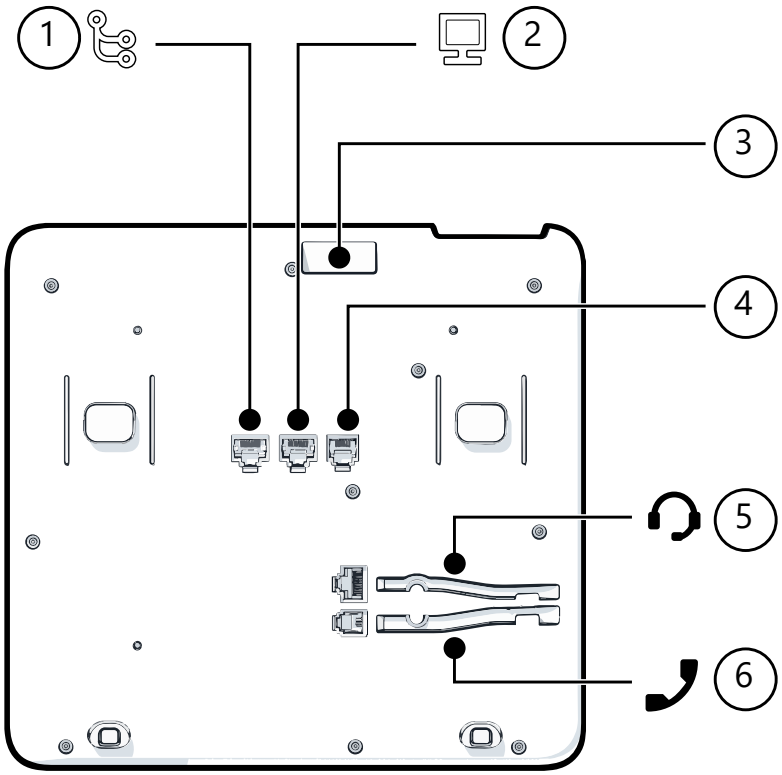
CONNECTORS AT THE BOTTOM SIDE

OpenScape Desk Phone CP110



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

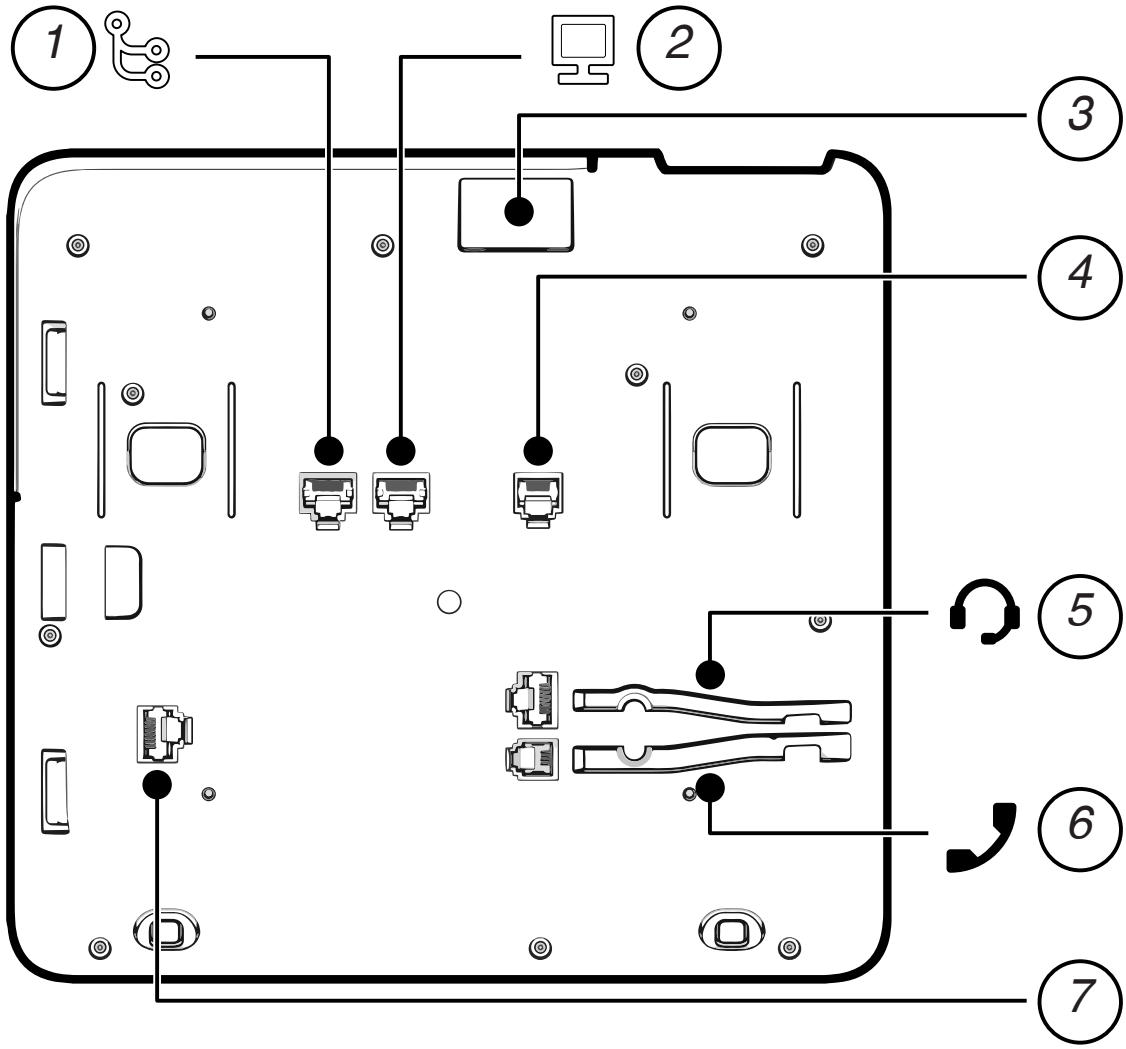
OpenScape Desk Phone CP210



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

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

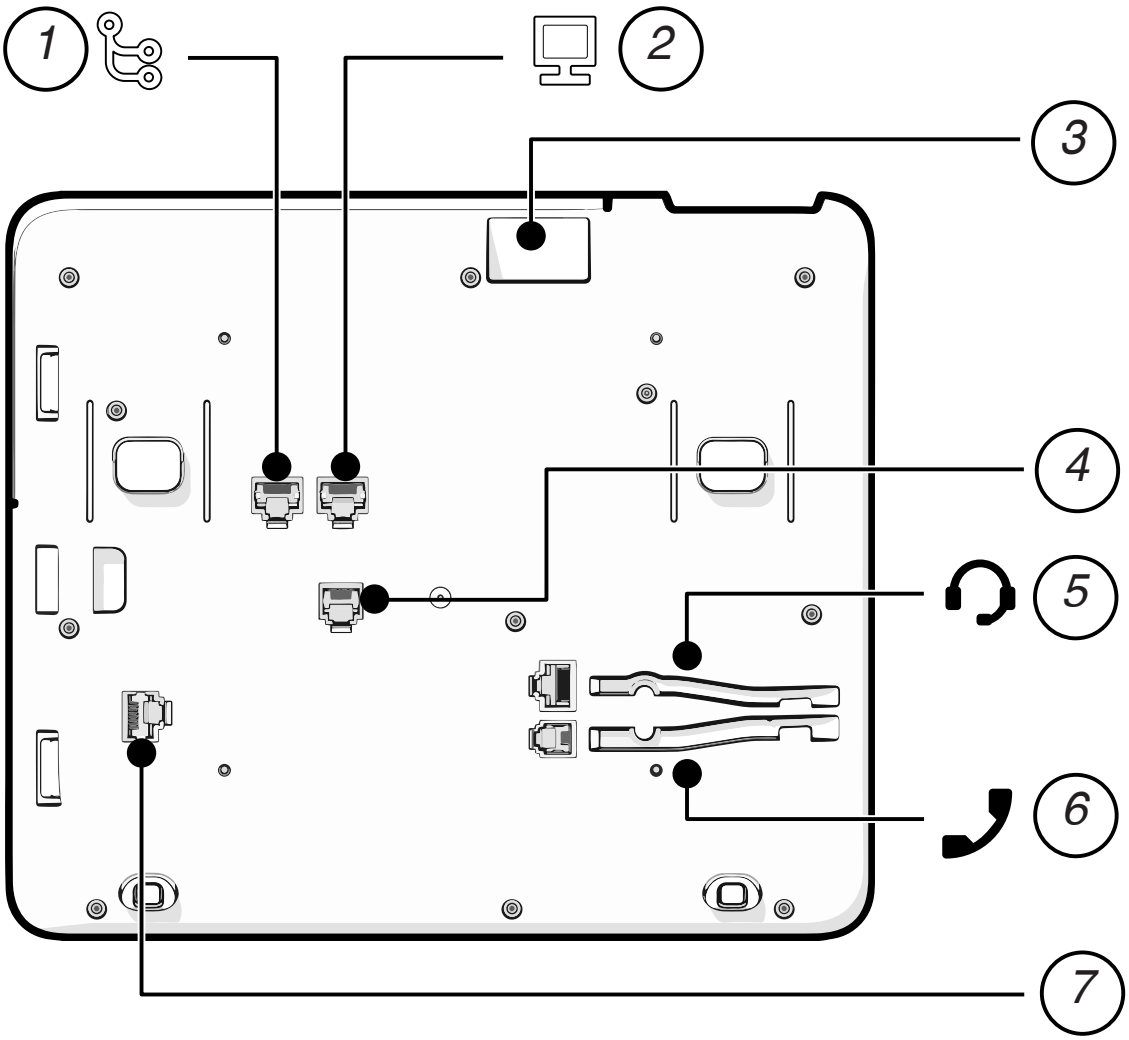
OpenScape Desk Phone CP410



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

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	• PoE (Power Class 1) • Power chord
OpenScape Desk Phone CP210	• PoE (Power Class 2) • Power chord
OpenScape Desk Phone CP410 • Only 1 key module can be connected using PoE	• PoE (Power Class 2) • Power chord
OpenScape Desk Phone CP710 • 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.	• 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 27). 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

Plug-in power supply	Order no.
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 before use. 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 OpenScape Desk Phone CP phones, OpenScape Desk Phone IP phones, or OpenStage phones!

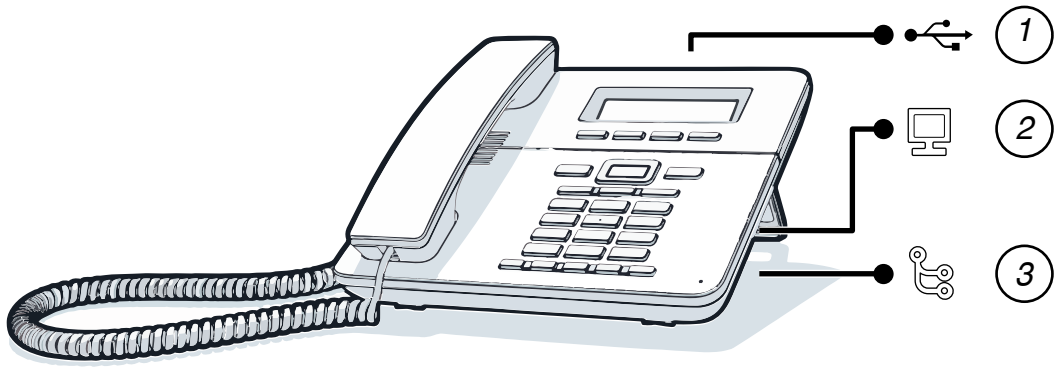


Fig.: 4-1: LAN connections (example)

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 27).

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 G2" → page 17).

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 156).
3. Check that Wi-Fi is enabled (see "Wi-Fi settings" → page 71).
4. If applicable, connect the following optional jacks:
   - Headset (accessory)

   When using a CP10 connector, CP210, CP410, and CP710 phones can be connected to the network via Wi-Fi. They may require a Power-over-Ethernet (PoE) connection to power them if not connected to a power source via the power connection.

KEY MODULES

A key module provides additional programmable keys. The following table shows which key modules are supported per phone model. Key module types cannot be mixed on the same phone. Only one module type may be used per device.

Phone type	Key module (KM)	Number of key modules (max.)[a]	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 standard setup workflow for OpenScape Desk Phone CP endpoints in a Zoom Phone environment. Zero-Touch Provisioning (ZTP) is the default method when a DHCP server is present. If configuration outside ZTP is required, cross-references to the relevant administration sections are provided.

For detailed information, see "OpenScape Desk Phone in Zoom Phone environment" → page 12.

> **Note** Any settings provided by the Zoom provisioning server cannot be overridden by local configuration tools (e.g., web UI or manual provisioning). Local changes are discarded on the next provisioning sync.

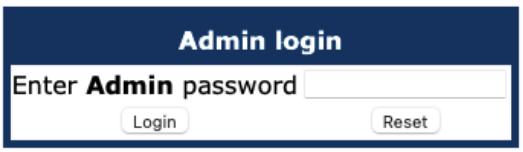
HOW TO ACCESS THE WEB INTERFACE (WBM)

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 35).
   - 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 36).
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 62.
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".



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

- Press **1 3 0** simultaneously. You will be prompted to enter the administrator password.
- Enter the administrator password (default password is **123456**). It is highly recommended to change the password after your first login.
- Confirm with the **OK** key.

OpenScape Desk Phone CP210

- Press **1 3 0** simultaneously. You will be prompted to enter the administrator password.
- Enter the administrator password (default password is **123456**). It is highly recommended to change the password after your first login.
- Confirm with the **OK** key.

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.	• 2 seconds: Ringer off • 3 seconds: Beep sound instead of ringer
# Abc 123	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 56 for IP address and subnet mask, and "Default router / gateway" → page 58 for the default route.

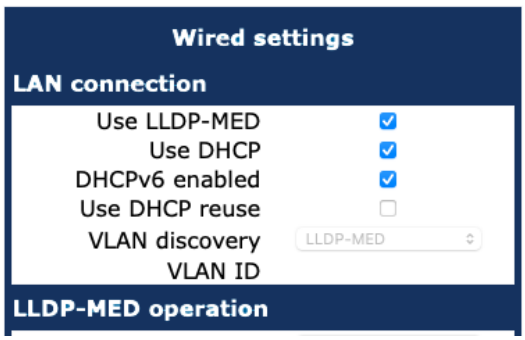
DHCP RESILIENCE

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 100).

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 99.

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.

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	• 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 Mitel redirect server ("cloud-setup.com") from the DNS

Phone contacts the Mitel redirect server using DLS-WPI

Phone displays the Progress prompt

Phone receives configuration items from the Unify Redirect server	• 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.	The stored DLS address is not changed by the result of the DNS look-up. **NOTE:** *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.*

Phone contacts the deployment server using DLS-WPI	

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

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
RS	1	Unable to get the address for the Mitel redirect server DNS lookup failed
RN	3	Unable to establish contact with Mitel redirect server — no reply
RR	2	Unable to establish contact with Mitel 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

(a) The maximum number of key modules supported depends on the available power supply, see **"How to connect the phone via LAN cable" → page 31**.

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 34.

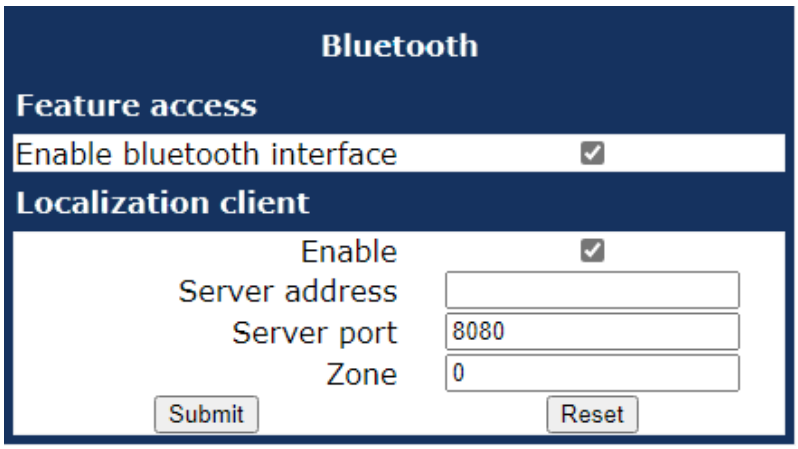
Bluetooth interface

Note This feature is available only on OpenScape Desk Phones CP700 and 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.



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

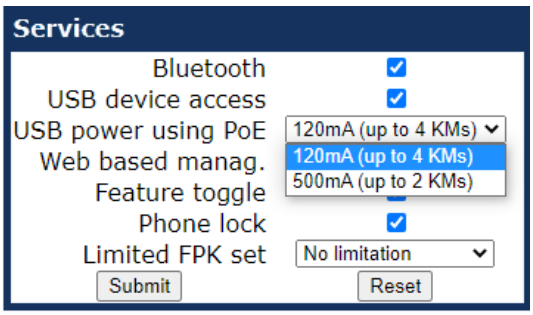
```
|--- Bluetooth
```

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 27).

Administration via WBM

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



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 33).
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 31).
   - 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.

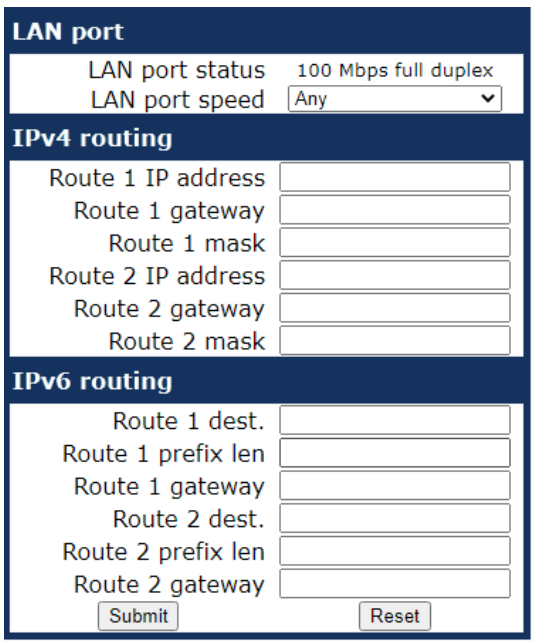
> **Note** Do not use this connection for further phones!

> **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 Management 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 Management 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 Management VLAN ID, as it's not part of that VLAN.
- Packets tagged with the internal Management VLAN ID, become untagged when exiting the LAN port.

There are 3 ways for configuring the VLAN ID:

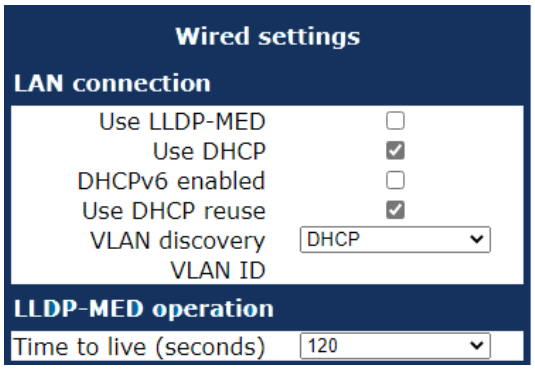
- By LLDP-MED (with fallback to DHCP)
- By DHCP
- Manually

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.



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)
```

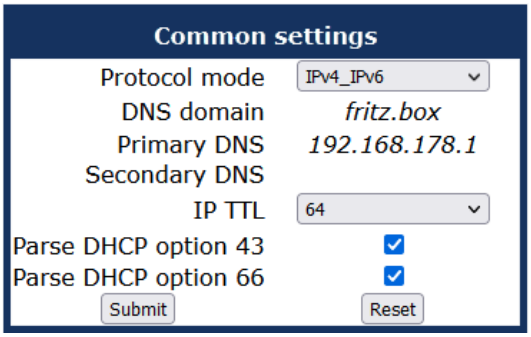
Automatic VLAN discovery using DHCP

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 48).

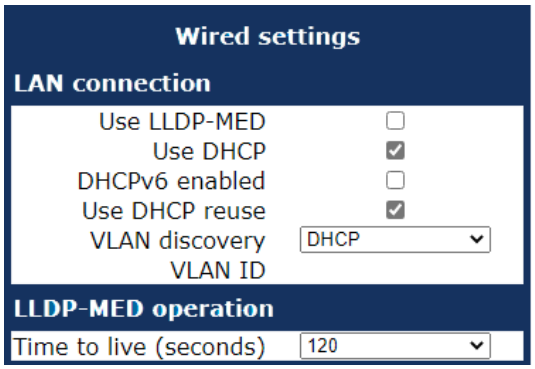
If a phone configured for VLAN discovery by DHCP fails to discover its VLAN, it will proceed to configure itself from the DHCP within the non-tagged LAN. Under these circumstances, network routing may not be correct.

Administration via WBM

1. Open Network > Common settings.



2. To enable VLAN discovery via DHCP, select "IPv4_IPv6" in Protocol mode.
3. Open Network > Wired settings.



4. Deselect "Use LLDP-MED".
5. Select "DHCP" in the VLAN discovery option.
6. 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:

Code	Length	DLS IP address																								
3	25	s	d	l	p	:	/	/	1	9	2	.	1	6	8	.	3	.	3	0	:	1	8	4	4	3
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

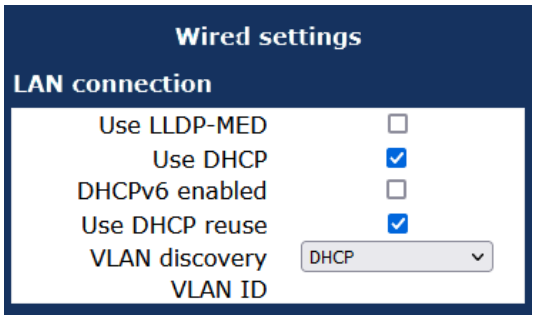
Manual configuration of a VLAN ID

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

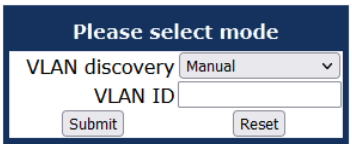
> **Note** If you misconfigure a phone to an incorrect VLAN, the phone will not connect to the network. If in static IP mode, no server connections is possible.

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)

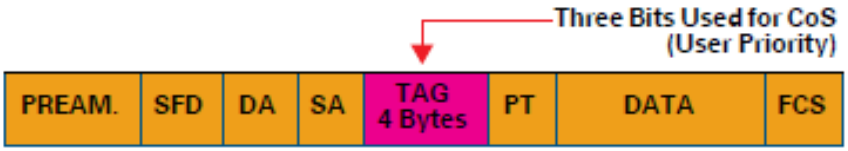
The QoS technology based on layer-2 and the two QoS technologies Diffserv and TOS / IP Precedence based on layer-3 are allowing the VoIP application to request and receive predictable service levels in terms of data throughput capacity (bandwidth), latency variations (jitter), and delay.

> **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 46). The value cannot be changed by another interface.

Layer 2 / 802.1p

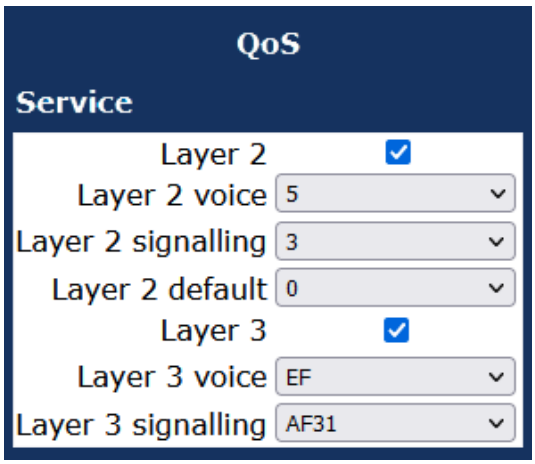
QoS on layer-2 is using 3 Bits in the 802.1q/p 4-Byte VLAN tag which must be added in the Ethernet header.

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

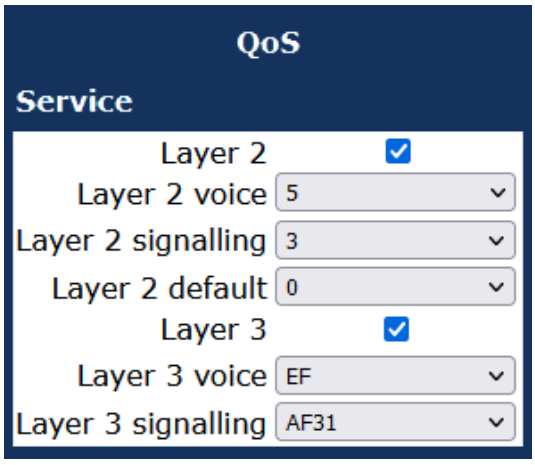
Diffserv assigns a class of service to an IP packet by adding an entry in the IP header.

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 (AFXY), where X is describing the priority class and Y the drop level.
  Four classes X are reserved for AFXY: AF1Y (low priority), AF2Y, AF3Y and AF4Y (high priority).
  Three drop levels Y are reserved for AFXY: AFX1 (low drop probability), AFX2 and AFX3 (High drop probability). In the case of low drop level, packets are buffered over an extended period in the case of high drop level, packets are promptly rejected if they cannot be forwarded.

Administration via WBM

1. Open Network > QoS.



- **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

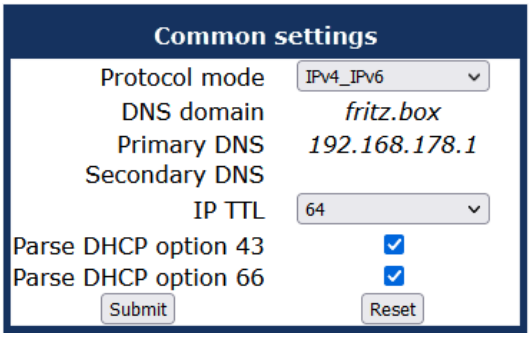
```
|--- Admin
      |--- Network
            |--- QoS
                  |--- Service
                              |---  Layer 3
                              |---  Layer 3 voice
                              |---  Layer 3 signalling
```

PROTOCOL MODE IPV4 / IPV6

- An IPv4 address consists of 4 number blocks, each between 0 and 255, separated by "."
  - Example: 1.222.44.123
- An IPv6 address consists of 8 hexadecimal number blocks, separated by ":" The IPv6 protocol provides a wider range of IP addresses that can be used in a network.
  - Example: 2001:0db8:85a3:08d3:1319:8a2e:0370:7347 or, if not all blocks are used: 2000:1::3

Administration via WBM

1. Open Network > Common settings.



2. For "Protocol mode", select one of the following options:
   - "IPv4_IPv6" uses both protocols
   - "IPv4" uses only the IPv4 protocol
   - "IPv6" uses only the IPv6 protocol
3. Click **Submit**.

Administration via local phone

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

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. For further information, refer to "Resilience and survivability" → page 114.

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

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)

DHCPv6 parameters

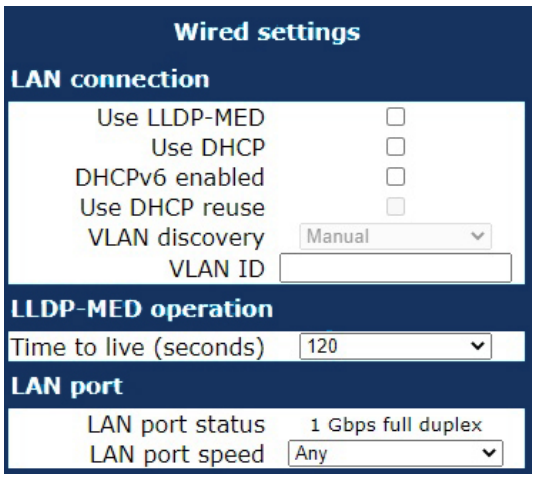
The following parameters can be obtained by DHCPv6, which performs a similar function as Ipv4, but for the IPv6 protocol:

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

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

Administration via WBM - IPv4

1. Open Network > Wired settings.



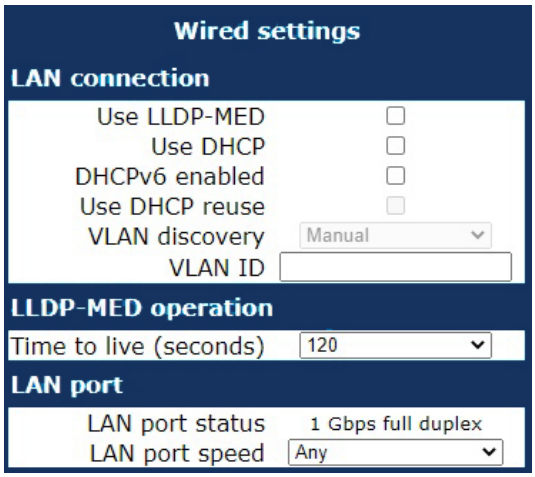
2. Select "Use DHCP".
3. Click **Submit**.

Administration via Local Phone - IPv4

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

Administration via WBM - IPv6

1. Open Network > Wired settings.



2. Select "DHCPv6 Enabled" (default setting is Enabled).
3. Click **Submit**.

Administration via Local Phone - IPv6

```
|--- 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)

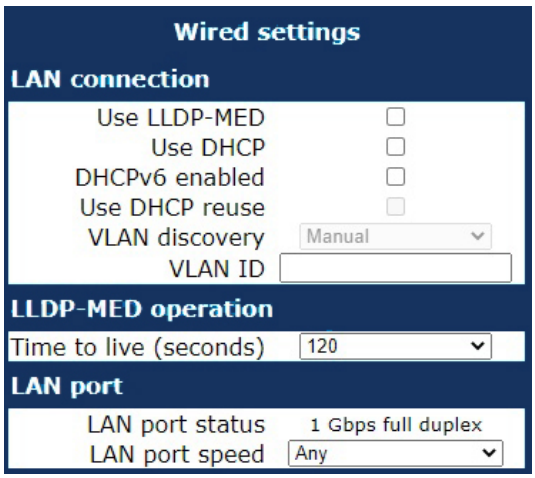
By default, IP configuration by DHCP and LLDP-MED is enabled. For manual IP configuration, proceed as follows:

Data required

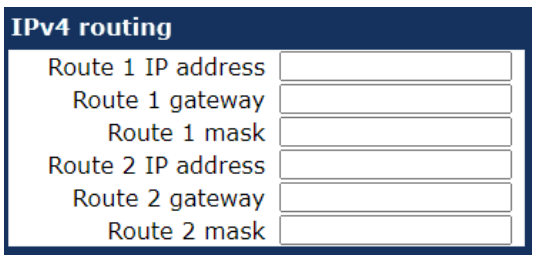
- IP address: used for addressing the phone.
- Subnet mask: subnet mask that is needed for the subnet in use.

Administration via WBM

1. Open Network > Wired settings.



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



3. In the tab "IPv4 routing" or "IPv6 routing" (depending on the settings in Protocol Mode), 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
```

```
|--- Admin
      |--- Network
           |--- Wired settings
                |--- IPv6 routing
                      |--- Route 1 IP
                      |--- Route 1 gateway
```

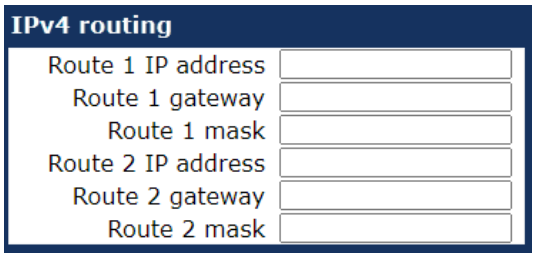
DEFAULT ROUTER / GATEWAY

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.



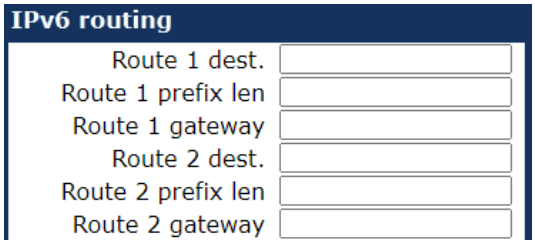
2. Enter the default route, i.e. the IP address of the router that links your IP network to other networks.
3. Click **Submit**.

Administration via local phone - IPv4

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

Administration via WBM - IPv6

1. Open Network > Wired settings.



2. Enter the IP address of the global gateway that links your IP network to other networks.
3. Click **Submit**.

Administration via Local Phone - IPv6

```
|--- Admin
      |--- Network
           |--- Wired settings
                |--- LAN connection
                     |--- IPv6 routing
```

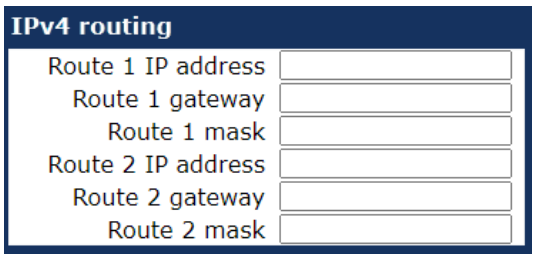
SPECIFIC IP ROUTING

For constant access to network subscribers of other domains, enter a second set of network destinations, in addition to the default route or 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.
- IPv6 route configuration
  - **Route 1/2 destination**: IPv6 address of the selected route.
  - **Route 1/2 prefix len**: Prefix length for the selected route.
  - **Route 1/2 gateway**: IPv6 address of the gateway for the selected route.

Administration via WBM - IPv4

1. Open Network > Wired settings.
2. Go to tab "IPv4 routing".



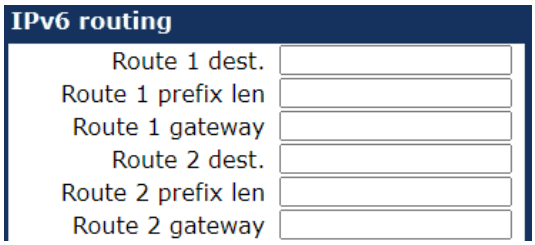
3. Enter the required data:
   - **For Route 1**: Route 1 IP address, Route 1 Gateway, and Route 1 mask.
   - **For Route 2**: Route 2 IP address, Route 2 Gateway, and Route 2 mask.
4. Click **Submit**.

Administration via local phone - IPv4

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

Administration via WBM - IPv6

1. Open Network > IPv6 configuration.
2. Go to tab "IPv6 routing".



3. Enter the required data:
   - **For Route 1**: Route 1 Dest., Route 1 Prefix Len, and Route 1 Gateway.
   - **For Route 2**: Route 2 Dest., Route 2 Prefix Len, and Route 2 Gateway.
4. Click **Submit**.

Administration via local phone - IPv6

```
|--- Admin
      |--- Network
            |--- IPv6 routing
                  |--- Route 1 dest
                  |--- Route 1 prefix len
                  |--- Route 1 gateway
                  |--- Route 2 dest
                  |--- Route 2 prefix len
                  |--- Route 2 gateway
```

DNS

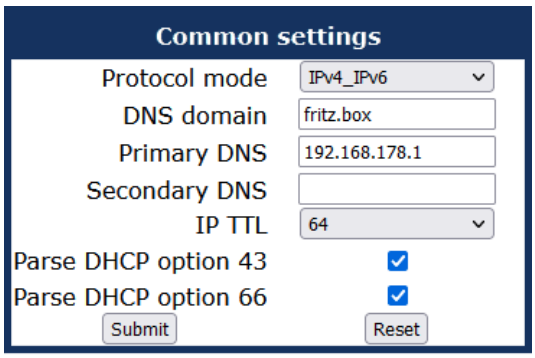
The main task of the domain name system (DNS) is to translate domain names to IP addresses. For some features and functions of the OpenScape Desk Phone CP phone, it is necessary to configure the DNS domain the phone belongs to, as well as the name servers needed for DNS resolving.

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

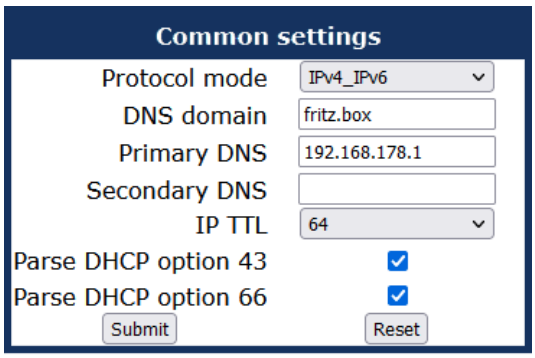
If not provided by DHCP, a primary and a secondary DNS server can be configured.

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" → page 114.

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.

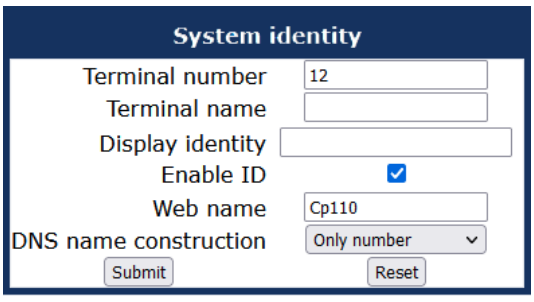
> **Note** DHCP and DNS must be appropriately connected and configured at the customer site.

> **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
```

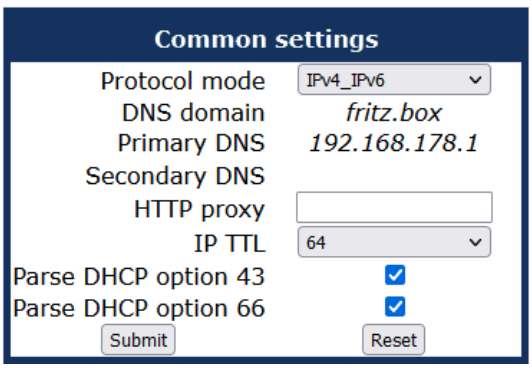
IP TTL

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.



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

Administration via local phone

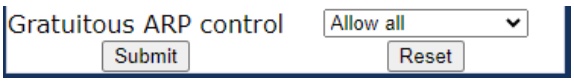
```
|--- Admin
      |--- Network
            |--- Common settings
                  |--- IP Time to live
```

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



1. 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.
2. 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 45.

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 provisioning server, and default mode port, i.e. the port on which the provisioning 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 provisioning server.

It is possible to operate the provisioning server behind a firewall or NAT (Network Address Translation), which prevents the DLS from sending "Contact-Me" messages directly to the phone:

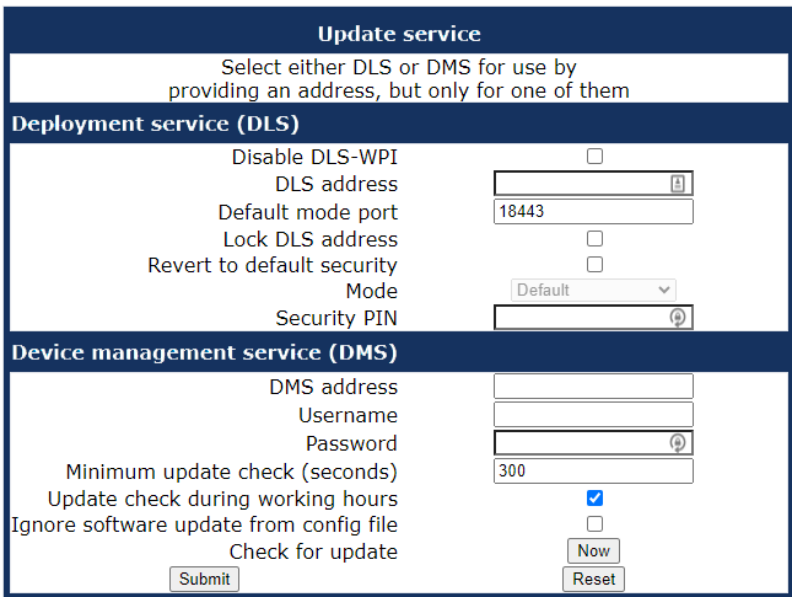
- The provisioning server requests the phone to contact it by sending a HTTP "Contact-Me" request or by leaving a request at the DCMP poll server for the phone to check periodically.
- The phone always establishes the connection to the provisioning server.

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).



Deployment service (DLS)

It is possible to operate the provisioning 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 1).

The DMS is compatible to Zoom 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 (SNMP) is used by Network management systems for monitoring Network-attached devices for conditions that warrant administrative attention. An SNMP manager surveys and, if needed, configures several SNMP elements, e.g. VoIP phones.

> OpenScape Desk Phone CP phones support SNMPv1.

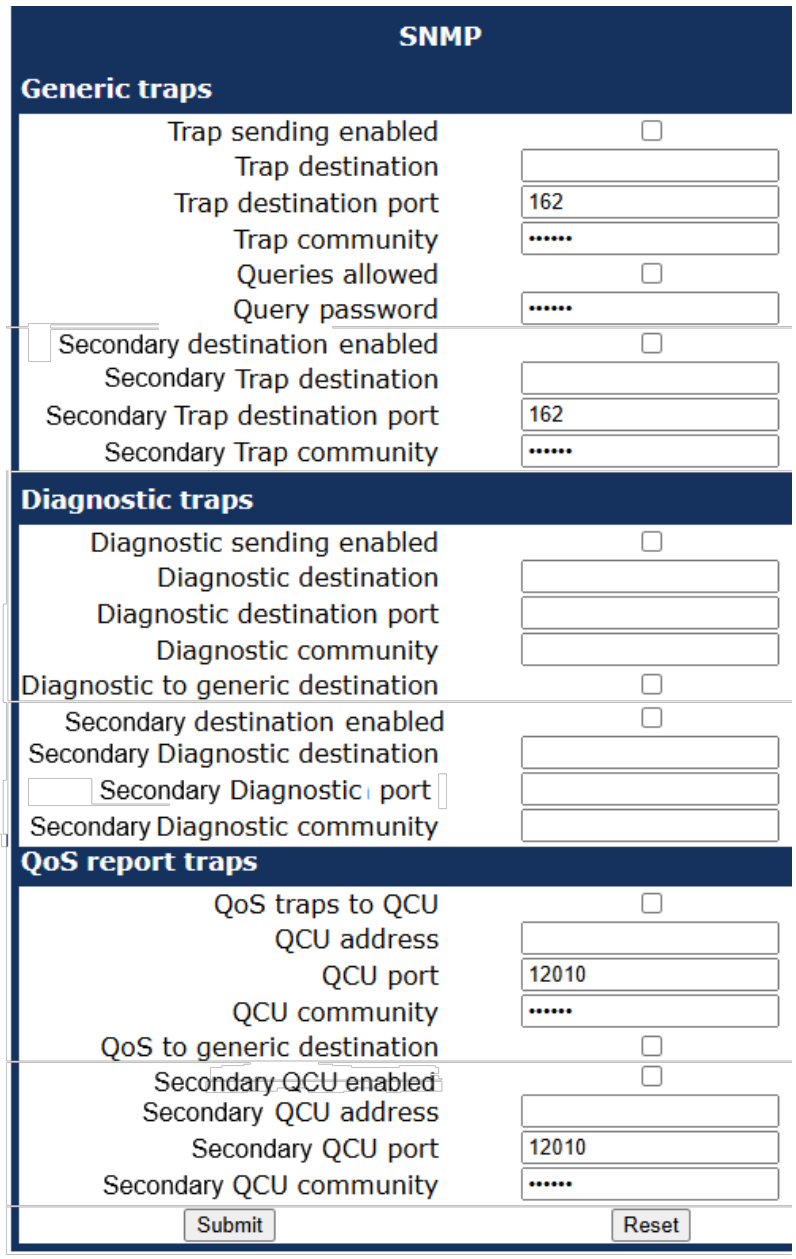
There are currently 4 trap categories that can be sent by the phones:

- **Standard SNMP traps**: OpenScape Desk Phone CP phones support the following types of standard SNMP traps, as defined in RFC 1157:
  - **coldStart**: sent if the phone does a full restart.
  - **warmStart**: sent if only the phone software is restarted.
  - **linkUp**: sent when IP connectivity is restored.
- **QoS Related traps**: These traps are designed specifically for receipt and interpretation by the QDC collection system. The traps are common to SIP phones, HFA phones, Gateways, etc.
- **Traps for important high level SIP related problems**: Currently, these traps are related to problems in registering with a SIP Server and to a failure in remotely logging off a mobile user. These traps are aimed at a non-expert user (e.g. a standard Network Management System) to highlight important telephony related problems.
- **Traps specific to OpenScape Desk Phone CP**: Currently, the following traps are defined:
  - TraceEventFatal: sent if severe trace events occur; aimed at expert users.
  - TraceEventError: sent if severe trace events occur; aimed at expert users.

Note Starting from V2R1, OpenScape CPx10 phones support secondary SNMP server configuration, enabling redundant trap management and improved network monitoring reliability.

Administration via WBM

1. Open System > SNMP.



Generic traps

- **Trap sending enabled**: Enables or disables the sending of a TRAP message to the SNMP manager.

  - Value range: "Yes", "No"
  - Default: "No"
- **Trap destination**: IP address or 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.
- **Secondary destination enabled**: Enables or disables the sending of TRAP messages to the secondary SNMP manager.
- **Secondary Trap destination:** IP address or host name of the secondary SNMP manager that receives traps.
- **Secondary Trap destination port:** Port on which the secondary SNMP manager is receiving TRAP messages.
- **Secondary Trap community:** Secondary SNMP community string for the SNMP manager receiving TRAP messages.

Diagnostic traps

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

QoS report traps

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

Administration via local phone

```
|--- Admin
       |--- System
              |--- SNMP
                     |--- Generic traps
                            |--- Trap sending enabled
                            |--- Trap destination
                            |--- Trap destination port
                            |--- Trap community
                            |--- Queries allowed
                            |--- Query password
                            |--- Secondary destination enabled
                            |--- Secondary Trap destination
                            |--- Secondary Trap destination port
                            |--- Secondary Trap community
                     |--- Diagnostic traps
                            |--- Diagnostic sending enabled
                            |--- Diagnostic destination
                            |--- Diagnostic destination port
                            |--- Diagnostic community
                            |--- Diagnostic to generic destination
                            |--- Secondary destination enabled
                            |--- Secondary Diagnostic destination
                            |--- Secondary Diagnostic port
                            |--- Secondary Diagnostic community
                     |--- QoS report traps
                            |--- QoS traps to QCU
                            |--- QCU address
                            |--- QCU port
                            |--- QCU community
                            |--- QoS to generic destination
                            |--- Secondary QCU enabled
                            |--- Secondary QCU address
                            |--- Secondary QCU port
                            |--- Secondary QCU community
```

Wi-Fi settings

> **Note** Wi-Fi operation requires a CP700X or 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 132).

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.

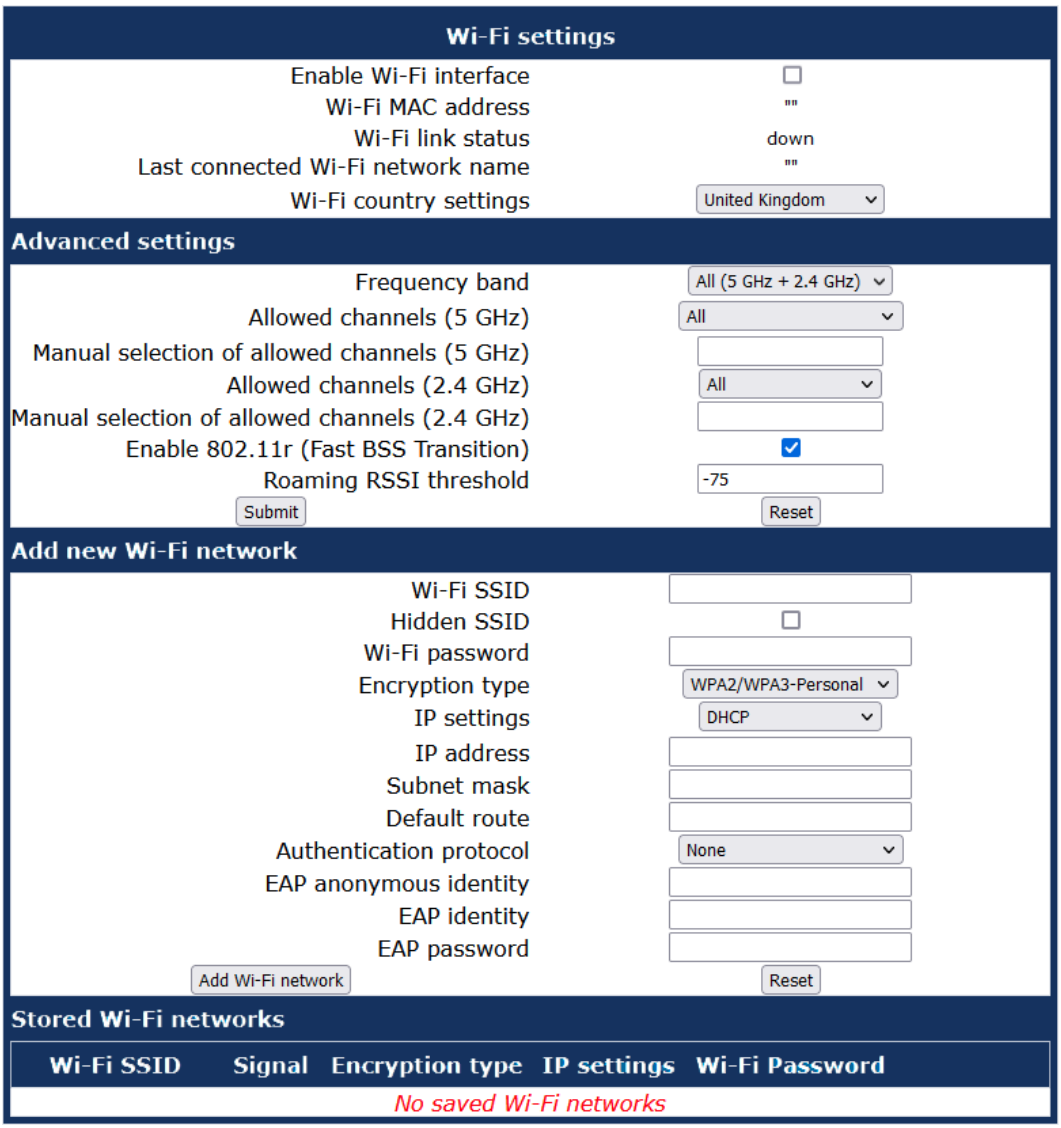
> Wi-Fi connections with no encryption type, WEP or WPA are characterized as non-secure networks.

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.
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 75

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 WI-FI 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 network 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).

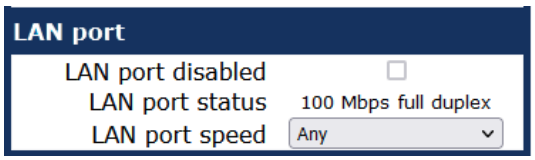
Once the phone has acquired a DLS address, it will open up a secure connection to DLS for downloading configuration parameters using the WPI protocol. Any certificates needed for Wi-Fi authentication or SIP/TLS will also be downloaded as a part of this process. If a DLS address is specified in the downloaded 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, CP700X 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, CP700X 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

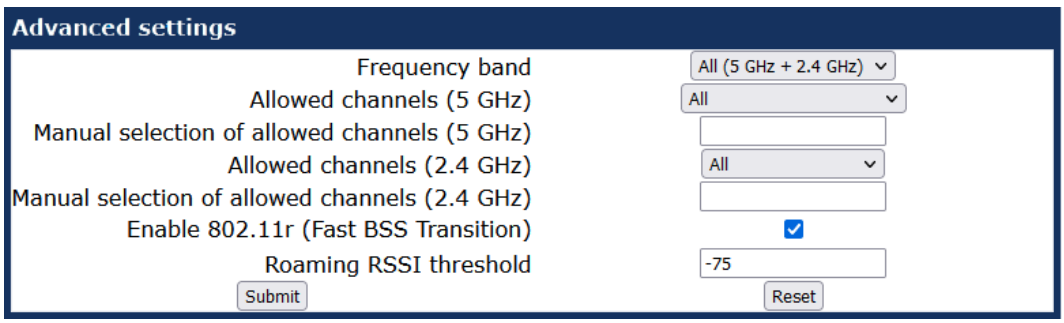
1. Edit the text field to configure the roaming RSSI threshold. Value can be set as a negative integer (RSSI value in dBm).

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.



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
```

Security and policies

Zoom Phone always uses SRTP for media encryption and TLS for signaling. Because secure media is enforced by Zoom, the Zoom phone does not need to verify whether SRTP is being used, and no secure-call icon is displayed on the device.

All calls are encrypted automatically.

Certificate validation settings (SIP server certificate validation and backup SIP server certificate validation) may be enabled depending on Zoom's provisioning requirements, but they are not related to SRTP indication.

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

> For delivering the root certificate, a deployment server is required.

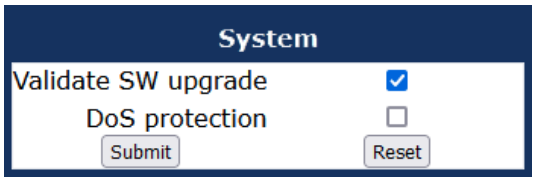
SYSTEM

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

> By default this feature is enabled.

Administration via WBM

1. Open System > Security > System.



2. Enable or disable the validation of the software update or upgrade.
3. Enable the DoS (Denial of Service) protection to help prevent the phone from being used by malicious software.
4. Click **Submit**.

Administration via local phone

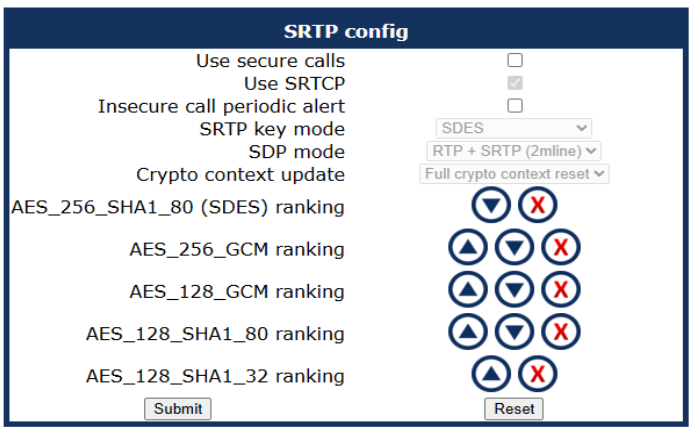
```
|--- Administration
      |--- System
            |--- Security
                  |--- System
                        |--- Validate SW upgrade
                        |--- DoS protection
```

SRTP CONFIGURATION

The SRTP (Secure Real-time Transport Protocol) type sets the key exchange method for SRTP. All calls on Zoom CP phones are encrypted using SRTP and TLS. No additional configuration is required. The phone automatically handles secure call setup.

Administration via WBM

1. Open System > Security > SRTP configuration.



SRTP key mode

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

- DTLS
- SDES
- MIKEY

> **Note** If SRTP is enabled, ANAT interworking is only possible if SDES is configured as the key exchange protocol for SRTP (see "Media / SDP " → page 107).

Insecure call periodic alert

Not used in Zoom-connected CP phones.

SDP mode

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

- 0=RTP + SRTP (2mline)
- 1=SRTP + RTP (2mline)
- 2=SRTP only
- 3= SRTP or RTP (1mline)

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

The following choices are available:

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

Crypto context update

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

- Full crypto context reset (default) - CP phone recreates the locally stored SRTP crypto context whenever it either receives new SRTP key generated by the other party (Rx direction) or when it generates its own new SRTP master key (Tx direction). The "Full crypto context reset" particularly applies to the ROC (Roll Over Counter) that must be in this case reset back to 0.

- Key update (RFC compliant)- Upon refreshing the SRTP keys, CP phone only updates the respective crypto context (Rx or Tx), without recreating it. Therefore, ROC preserves its value throughout the key update.

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

- **AES_128_SHA1_80** - Available for both SDES and DTLS.
- **AES_128_SHA1_32** - Available for both SDES and DTLS.
- **AES_256_SHA1_80** - Available only for SDES.
- **AES_256_GCM** - Available for DTLS, providing authenticated encryption with associated data (AEAD) for enhanced security.
- **AES_128_GCM** - Available for DTLS, providing authenticated encryption with associated data (AEAD) for enhanced security.

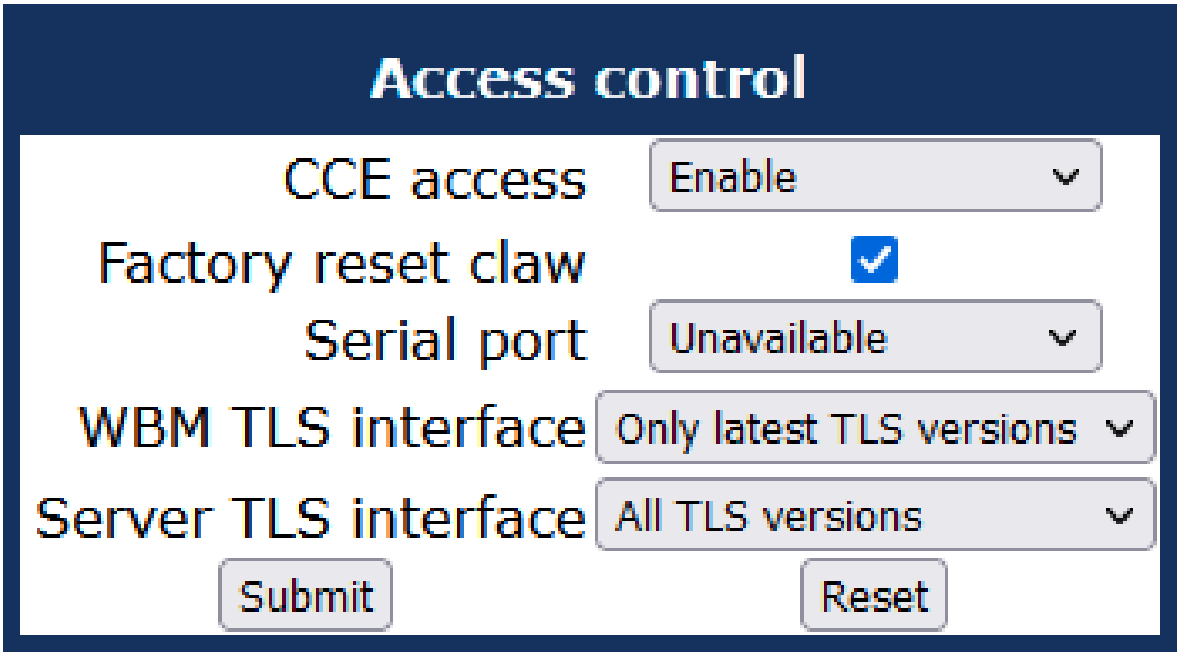
Administration via local phone

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

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 local CTI access and HPT access. When Disable is selected, both TCP and UDP are disabled. With Enable, there are no restrictions.
- With **Factory reset claw**, the 'hooded claw' keypad mechanism to initiate a factory reset without requiring an authenticated access can be enabled or disabled.
- The **Serial port** parameter controls access to the serial port. When set to No password, a terminal connected to the port can interact with the phone's operating system without restrictions. When "Passwd reqd" is selected, the serial port requires a password for access (root user is not available). When Unavailable is chosen, the serial port is not accessible.
- As a prerequisite, the root user needs to create a user and to define a password via Serial Access, so that access can be granted when the Password required prompt is issued.
- **WBM TLS interface** allows the web server to support obsolete TLS versions (TLS 1.0 and TLS 1.1) as well as the latest versions (current latest version is TLS 1.2). By default only the latest TLS version is allowed. Other interfaces (e.g. SIP) are not affected by this setting.
- **Server TLS interface** allows all interfaces, except the web server, to support obsolete TLS versions (TLS 1.0 and TLS 1.1) as well as the latest versions (current latest version is TLS 1.2). By default all TLS versions are allowed. The web server interface is not affected by this setting.

Administration via local phone

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

SECURITY LOG

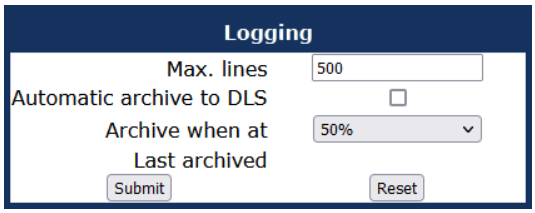
> In Zoom-connected CP phones, the management role normally performed by DLS/DMS/OSEM is instead performed by the Zoom provisioning and management server. However, within this guide, the term DLS may still appear conceptually to reflect provisioning actions that are now handled by Zoom.

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

> **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 deployment server. When activated, the deployment server 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 possible values are "0%, 10%”, ”20%”, ”30%”, ”35%”, ”40%”, ”45%”, ”50%”, ”55%”, ”60%”, ”65%”, ”70%”, ”80%”, ”90%”.
  - The value may be set to 0% by both the phone and the deployment server and this value will prevent the phone from archiving or telling the deployment server that it needs archiving. The security log upload may be accomplished in two ways:
    - If "Automatic archive to deployment server" is enabled, if the security log reaches the threshold % for unarchived entries, the phone will initiate an upload.
    - If "Automatic archive to deployment server" is NOT enabled and the security log reaches the threshold % for unarchived entries, the phone only sets the "archive-me" flag, it does not initiate the archive.

    It is up to the deployment server to recognize the flag and initiate an upload.
- Last archived shows the date when the security log was last archived to the deployment server.

Administration via local phone

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

SECURITY-RELATED FAULTS

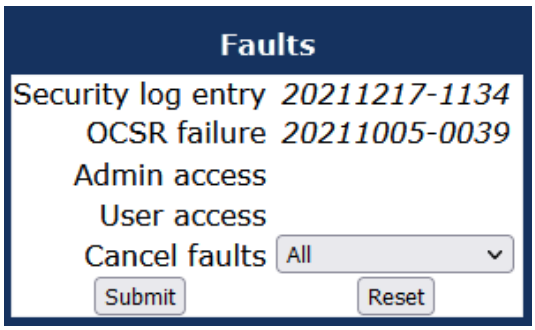
> In Zoom-connected CP phones, the management role normally performed by DLS/DMS/OSEM is instead performed by the Zoom provisioning and management server. However, within this guide, the term DLS may still appear conceptually to reflect provisioning actions that are now handled by Zoom.

The security related faults can be automatically notified to the DLS as a log file. There is also an entry in the faults list to indicate when a security log entry was lost. It should appear the same as the other entries, i.e. "Security log entry" may be shown without a time-stamp (if no log entries have been lost), whereas "by Admin access" may have a time-stamp if there had been too many admin password failures.

> **Note** The entries in this list are only displayed until they are reported to the DLS. After that, the entries are automatically deleted from the phone.

Administration via WBM

1. Open System > Security > Faults.



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

- If the entries are not deleted automatically, they can be deleted manually using the **Cancel faults** parameter.

Administration via local phone

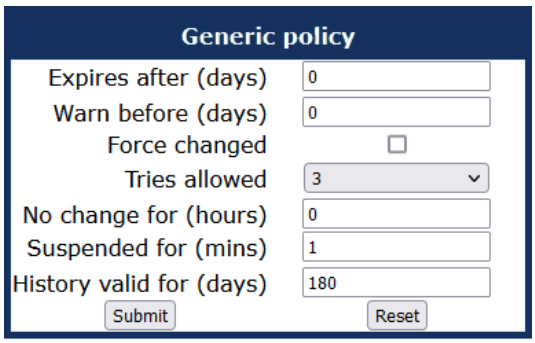
```
|--- Administration
      |--- System
            |--- Security
                  |--- Faults
                        |--- Security log entry
                        |--- OCSR failure
                        |--- Admin access
                        |--- User access
```

PASSWORD POLICY

Generic policy

Administration via WBM

1. Open Security and Policies > Password > Generic Policy.



- **Expires after (days)**: Sets the maximum validity period of a password.
- **Warn before (days)**: Specifies when the user or admin is notified that his password will expire.
- **Force changed**: Only affects the User password. When Force changed is activated, the user is forced to change the password at next login. This only applies to users, not to administrators.
- **Tries allowed**: Specifies the maximum number of password entry trials before the password is suspended.
  - Values: 0 (no limits), 2, 3, 4, 5
- **No change for (hours)**: Specifies a period before a password is allowed to be changed again.
  - Value range: 0 to 99
- **Suspended for (mins)**: Defines how long a password is suspended after the number of failed retries has exceeded.
  - Value range: 0 to 99

- **History valid for (days)**: Defines a period in days during which the history is valid. Passwords no longer used are kept in history lists for the user and admin passwords to prevent reuse of past passwords. This list is organized as FIFO (First In, First Out) so that it always contains the latest passwords.

Display password change prompt

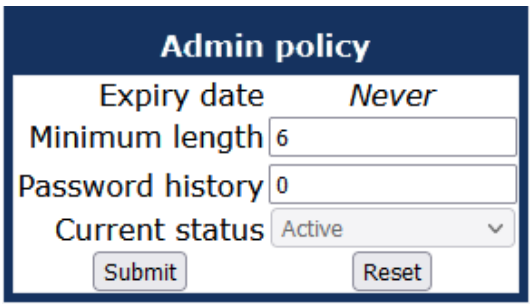
The admin can make the phone prompt the user to change the password immediately. Such a prompt may be triggered by the use of "Force changed" via the WBM in the Administration section or by a similar request by the DLS. It may also be triggered if the user password has expired or otherwise been invalidated. The prompt is shown when the user attempts to use their password.

> If the user ignores the prompt and does not change the password, the prompt is displayed again. This only affects the user password.

Admin policy

Administration via WBM

1. Open Security and Policies > Password > Admin Policy.



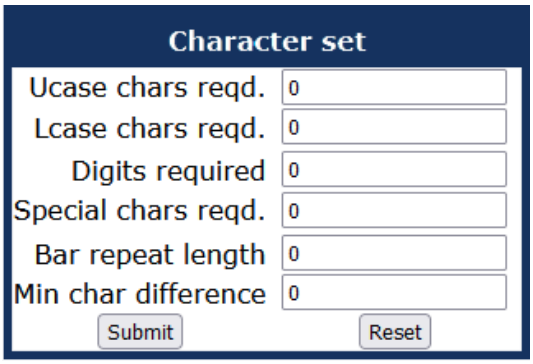
- **Expiry date**: Shows the date and time when the admin password will expire.
- **Minimum length**: Defines the minimum number of characters for the admin password.
- **Password history**: Specifies the number of entries to be kept in the admin password history. New passwords must not match any password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

Character set

The composition of the password can be configured.

Administration via WBM

1. Open Security and Policies > Password > Character set.



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

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 ."*#,?!’+-()@/:_

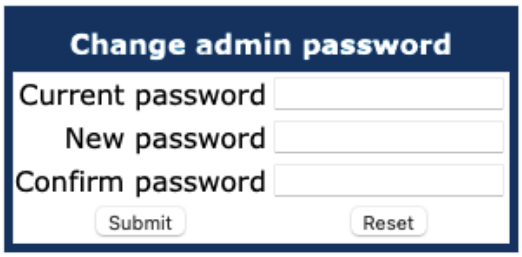
Default passwords

- **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.



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.

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**.

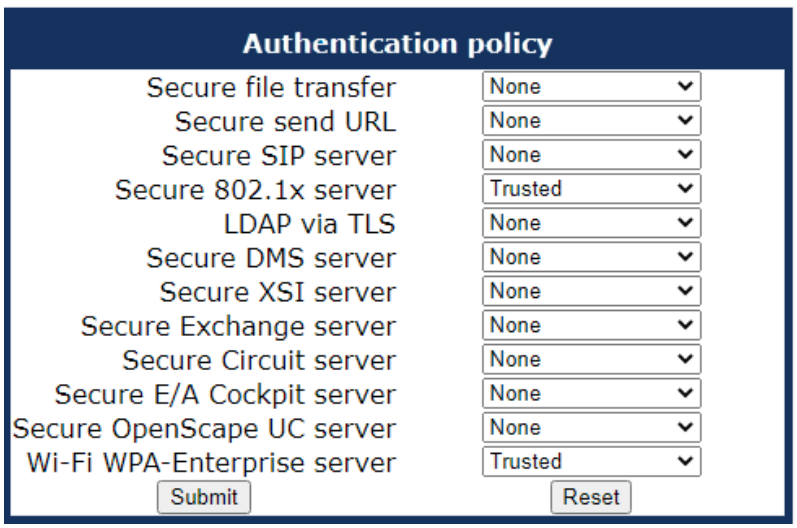
CERTIFICATE POLICY

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.



- Secure file transfer sets the authentication level for the HTTPS server to be used (see "Common FTP / HTTPS settings (defaults)" → page 206).
- Secure HFA gateway sets the authentication level for the HFA gateway connected to the phone (see "HFA gateway settings" →1).
- Secure 802.1x server sets the authentication level for the 802.1x authentication server.

Administration via local phone

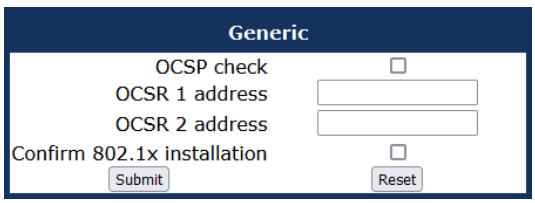
```
|--- Admin

       |--- Security and policies

              |--- Certificates

                     |--- Authentication policy

                            |--- Secure file transfer

                            |--- Secure HFA gateway

                            |--- Secure 802.1x server
```

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).

Administration via WBM

1. Open Security and Policies > Certificates > Generic.



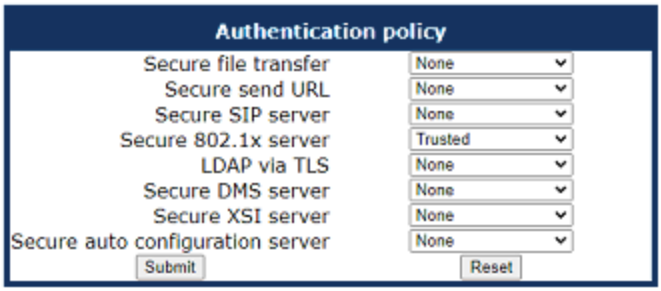
- **OCSP check**: When activated, the configured OCSR is requested to check if the certificate has been revoked.
- **OCSR 1 address**: Specifies the IP address (or FQDN) of a primary OCSP responder.
- **OCSR 2 address**: Specifies the IP address (or FQDN) of a secondary OCSP responder. OCSR 2 is tried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

Server authentication policy

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

Administration via WBM

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



- **Secure file transfer** sets the authentication level for the HTTPS server to be used (see "Common FTP / HTTPS settings (defaults)" → page 206).
- **Secure send URL** sets the authentication level for the server to which special HTTP requests are sent on key press ("Send URL" function, see "Send request via HTTP / HTTPS " → page 174).
- **Secure SIP server** sets the authentication level for the SIP server connected to the phone (see "SIP registration" → page 103).
- **Secure 802.1x server** sets the authentication level for the 802.1x authentication server.
- **LDAP via TLS** sets the authentication level for LDAP access.
- **Secure DMS server** sets the authentication level for a Device Management Server (DMS).
- **Secure XSI server** sets the authentication level for a Broadsoft Extended Server.
- **Secure auto configuration server** sets the authentication level for a TR-069 auto configuration server

Administration via local phone

```
|--- Admin
      |--- Security & policies
            |--- Certificates
                  |--- Authentication policy
                        |--- Secure file transfer
                        |--- Secure send URL
                        |--- Secure SIP server
                        |--- Secure 802.1x
                        |--- LDAP via TLS
                        |--- Secure DMS server
                        |--- Secure XSI server
                        |--- Acs. Authentication
```

SCEP

SCEP (Simple Certificate Enrollment Protocol) allows automatic provisioning and renewal of certificates on the phone. SCEP server supports only one certificate per device. If there is another request, it is rejected or the previous certificate is overwritten, based on server settings.

To set up SCEP, the following parameters must be configured:

SCEP

- **Address**: SIP address configured for SCEP.
- **Url**: Name of the Url, e.g. scep.
- **Port** (optional item): Port configured for SCEP, e.g. 8080.
- **Secret** (optional item): Shared secret is a certificate hash verifying the authenticity of the certificate. CA authenticates the device with shared secret.
- **CA fingerprint (sha1)** (optional item): CA fingerprint is a certificate hash verifying the authenticity of the certificate. Device authenticates the CA with fingerprint. Sha1 encryption is used.
- **Renew before expiry**: The device sends a request for a new certificate a given number of days in advance. Possible options are:
  - 0
  - 10
  - 20
  - 30

Certificate configuration

For certificate generation, **Common (CN)** field is mandatory. The parameters **Country (C)**, **Province (ST)**, **City (L)** and **Orgnaization (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

> **Note** Since HFA V1R6.5.0 and SIP V1R6.5.0, the following are available: DLS client, https client, LDAP client, BWDMS client, Acs client.

> **Note** For the CP700X and CP710 phones the **WLAN client** option is also available.

- **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 a certificate on the following occasions:

- After start-up (if SCEP is configured but no certificate received yet).
- On demand (via the Admin page).
- When the certificate expiration date is within the 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 the server does not support all mandatory capabilities, the phone does not attempt to request any certificates.

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

After the phone sends a SCEP request, the SCEP server returns a CA certificate and the fingerprint. 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 checklist. If the certificate request was the result of immediate action (On demand), an error message "Certificate error" is displayed.

> **Note** For existing certificates, the phone asks the SCEP server for a certificate renewal by updating the existing enrolled certificate with a new one.

Note: In case SCEP returns multiple CA certificates, they all needthe to be stored in proper locaton and used in services they belong to.

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

Handling pending status

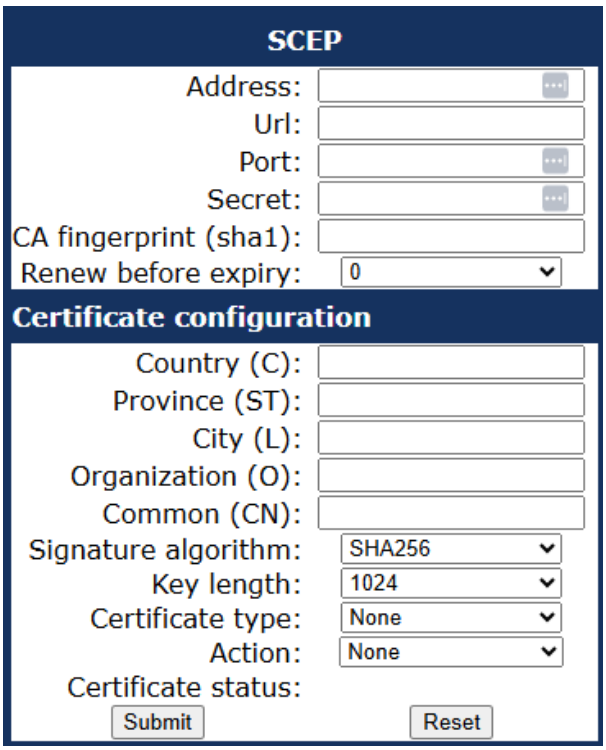
When the phone sends a request to SCEP server, server can reply with status PENDING. This may mean it is waiting for manual approval from administrator or any other action which prevents it to deploy certificate immediatelly.

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

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

Administration via WBM

Security and Policies > Certificates > SCEP



Administration via Local Phone

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

System settings

TERMINAL AND USER IDENTITY

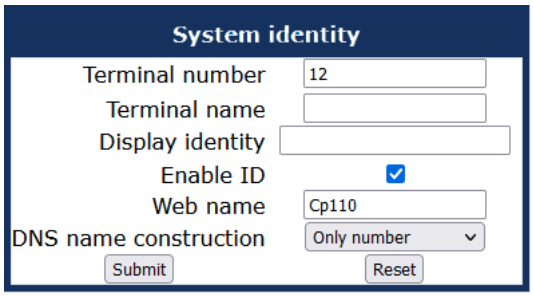
Terminal identity

Within a SIP environment, the "Terminal Number" may serve as a phone number. The "Terminal Name" provides textual name that may be used to identify a call party (as a contact name). The values are used in the user information part of SIP URIs.

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

Administration via WBM

1. Open System > System Identity.



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

Administration via local phone

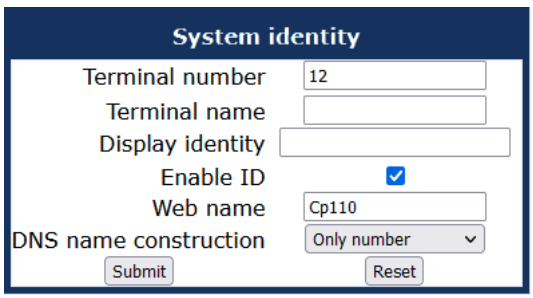
```
|--- Admin
      |--- System
            |--- Identity
                  |--- Terminal number
                  |--- Terminal name
```

Display identity

If an individual name or number is entered as "Display identity" and "Enable ID" is activated, it is displayed in the idle screen as well as the CP710 status bar instead of the Terminal number.

Administration via WBM

1. Open System > System Identity.



Administration via local phone

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

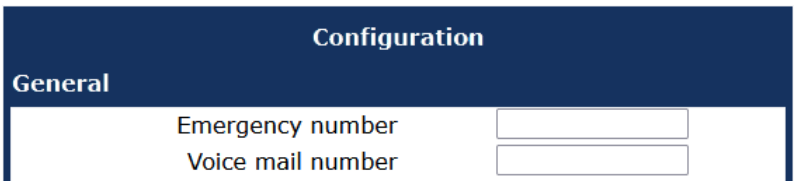
EMERGENCY AND VOICE MAIL

It is important to have an emergency number configured. If the phone is locked, a dialer menu option for making an emergency call is created.

> **Note** If more than one emergency number is needed, additional numbers can be configured in the canonical dial settings ("Canonical dialing configuration" → page 194).

Administration via WBM

1. Open System > Features > Configuration.



2. Enter the emergency number.
3. If a mailbox located at a remote server is used, enter the Voice mail number.

Administration via local phone

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

ENERGY SAVING

Backlight time setting

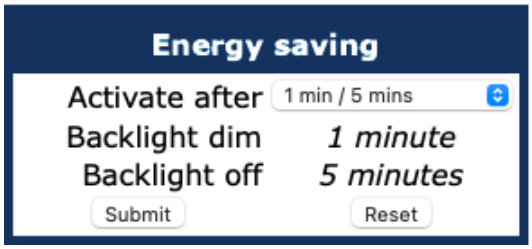
> **Note** This feature is available only on OpenScape Desk Phone CP410 and CP710 phones.

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.

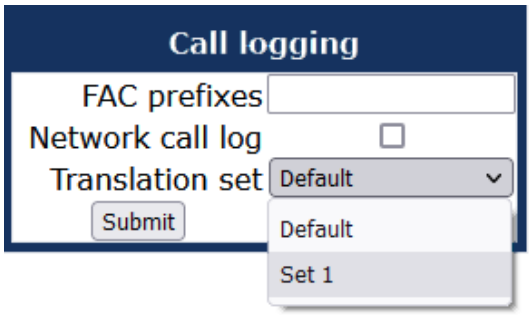
TRANSLATION SET CHANGE

Provides a set of customized translations, e.g. "Call Log" instead of "Conversation" in a specific environment.

The translation set is not customer-specific and available for any customer to configure at admin level.

Administration via WBM

1. Open Local functions > Call logging menu.



2. Select between multiple preset options (0 - "Default", 1 - "Set 1").
   - "Default" means that no dialect is selected and the default translation labels are used.
   - "Set 1" uses special translations to customize the selected screen labels.
3. Click **Submit**.

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.

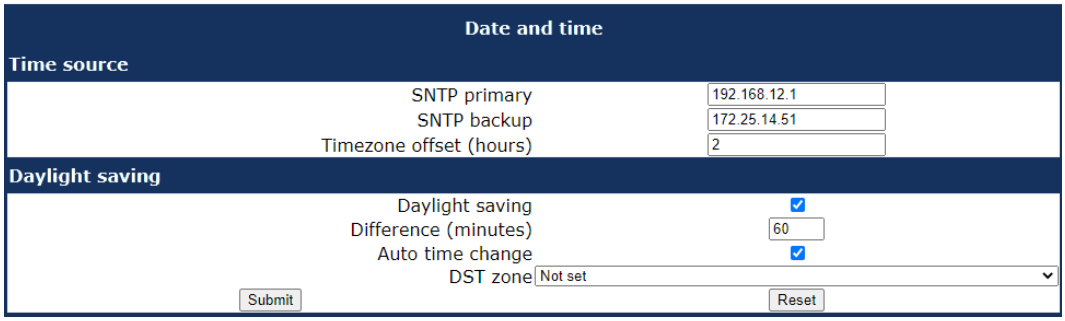
The difference (minutes) parameter defines how many minutes the clock is put forward for DST. In Germany, for instance, the value is +60.

> **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.



- **SNTP primary**: IP address or host name of the SNTP server
- **SNTP backup**: Secondary SNTP server
- **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
```

Setting date and time without the SNTP server

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

> **Note** The manual setting of time and date is described in the user manual, not in the administrator manual.

SIP ADDRESSES AND PORTS

SIP addresses

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

Administration via WBM

1. Open System > Registration.

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

> **Note** Enhanced survivability using DNS SRV is available. To make use of it, a special configuration is required (see "Resilience and survivability" → page 114).

Administration via local phone

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

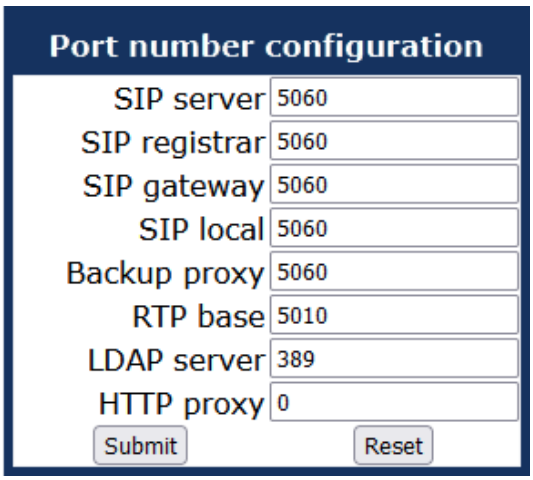
SIP ports

In this group of parameters, the ports for the SIP server, the SIP registrar, and the SIP gateway are defined), as well as the SIP port used by the phone (SIP local) (see "SIP addresses" → page 101).

> The port values are editable unless obtained from the DHCP server.

Administration via WBM

1. Open Network > Port number configuration.



- **SIP server**: Port of the SIP proxy server.
  - Default: 5060.
- **SIP registrar**: Port of the server at which the phone registers.
  - Default: 5060.
- **SIP gateway**: Port of the SIP gateway.
  - Default: 5060.
- **SIP local**: Port used by the phone for sending and receiving SIP messages.
  - Default: 5060.
- **Backup proxy**: Port used for backup of the phone data.
  - Default: 5060
- **RTP base**: Port used for delivering real-time data, e.g. audio.
  - Default 5010

- **LDAP server**: Port used for communicating with the directory server.
  - Default: 389
- **HTTP proxy**: Sits between an HTTP client and server to manage data content (caching, security etc.).

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

Administration via local phone

```
|--- Admin
      |--- Network
            |--- Port Configuration
                  |--- SIP server
                  |--- SIP registrar
                  |--- SIP gateway
                  |--- SIP local
                  |--- Backup proxy
                  |--- RTP base
                  |--- LDAP Server port
                  |--- HTTP proxy
```

SIP REGISTRATION

Registration is the process by which centralized SIP Server / Registrars become aware of the existence and readiness of an endpoint to make and receive calls. The phone supports a number of configuration parameters to allow this to happen. Registration can be authenticated or unauthenticated depending on how the server and phone is configured.

Unauthenticated registration

For unauthenticated registration, the following parameters must be set on the phone:

- Terminal number or Terminal name (see "Terminal identity" → page 95)
- SIP server and SIP registrar address (see "SIP addresses" → page 101).

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

Authenticated registration

The phone supports the digest authentication scheme and requires some parameters to be configured in addition to those for unauthenticated registration. By providing a User ID and a Password which match with a corresponding account on the SIP registrar, the phone authenticates itself. Optionally, a Realm can be added. This parameter specifies the protection domain wherein

the SIP authentication is meaningful. The protection domain is globally unique, so that each protection domain has its own arbitrary user names and passwords.

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

Note If registration has not succeeded at startup or registration fails after having been previously successfully registered the phone will try to re-register every 30 seconds. This is not configurable.

If the registration is not answered at all, the phone will try to re-register every 60 seconds by default. This is configurable (see "Maximum registration backoff timer" → page 119).

Zoom-specific behavior (from V2.R0.18.0)

Set the SIP **Server Type** to **ZOOM** to connect the phone to Zoom Phone. All other server-specific behavior is handled automatically.

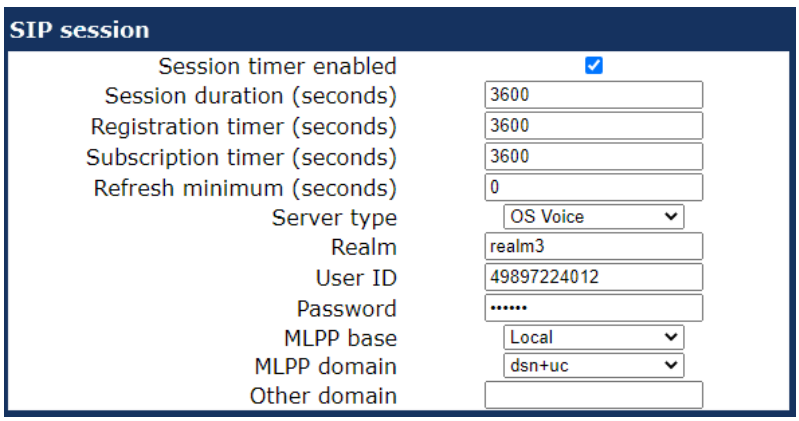
When set to "ZOOM", the phone:

- Processes authentication exchanges according to Zoom SIP requirements.
- Does **not** display the secure call alert icon (Zoom always uses SRTP and TLS and all calls are considered secure).

  Registration timers and other parameters continue to function normally.

Administration via WBM

1. Open System > Registration.



- **Registration timer (seconds)**: Expiry time of the registration in seconds.
  - Default value: 3600.

- **Server type**: Specifies the type of server the phone will register to. When selected, certain features may adjust their behavior to comply with the server's expected operation.

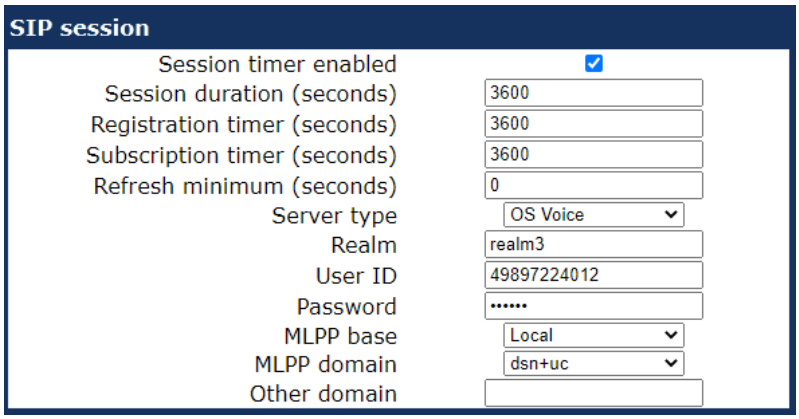
  Set the SIP **Server Type** to **ZOOM** to connect the phone to Zoom Phone.

- **Realm**: Protection domain for authentication.
- **User ID**: User name required for an authenticated registration.
- **Password**: Password required for an authenticated registration.
- **Subscription timer (seconds)**: Expiry time of subscription in seconds.
  - Range: 60-7200
  - Default value: 3600
  - Server type: Available for all server types

Re-registration timer

Administration via WBM

1. Open System > Registration > SIP session.



Note The new data item is controlled by the administrator, and also part of the user profile for mobility. It is not changeable during a call.

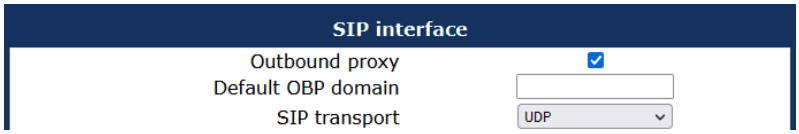
- For REGISTER event, the "expires time" must be configurable by a "guard time". The "expires time" is provided by the SIP server in its response to a REGISTER request by the phone. The SIP standard states that the devices can refresh from half of the expires time to the end. If the answer from SIP server is a refresh time of 600 sec. this means the devices can send the refresh after 300 sec up to 600 sec later.
- "Guard time" can be configured on the phone in order to reduce the refresh time using the "Refresh minimum" setting.
- In the previous case, if the answer from SBC is 600 sec and the guard time is 15 sec, the refresh from device will sent between 585 sec (600-15) and 600 sec after a previous registration.
- In case of SUBSCRIBE for every event or group of events (the same type), the Subscription refresh time is also configured by the guard time.

SIP COMMUNICATION

Outbound proxy

Administration via WBM

1. Open System > SIP interface.



- **Outbound proxy**: Determines whether an outbound proxy is used or not. If this option is set to "Yes", the phone routes outbound requests to the configured proxy. The outbound proxy will fulfill the task of resolving the domain contained in the SIP request. If "No" is set, the phone will attempt to resolve the domain by itself.
  - Value range: "Yes", "No"
  - Default: "Yes"; when System > Registration > Server type is set to "HiQ8000" (firmware version V3 onwards): "Yes"
- **Default OBP domain**: Alternative value for the domain that is given in the outbound request. If a Default OBP (Outbound Proxy check box) domain is set and the number or name dialed by the user does not provide a domain, this value is appended to the name or number. Otherwise, the domain of the outbound proxy is appended.

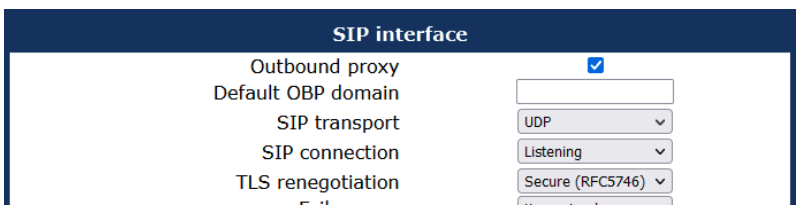
Administration via local phone

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

Selecting the SIP transport protocol

Administration via WBM

1. Open System > SIP interface.



- "SIP transport" selects the transport protocol to be used for SIP messages.
  - Value range: "UDP", "TCP", and "TLS"
  - Default is "UDP"
  - Default when System > Registration > Server type is set to "HiQ8000" (firmware version V3 onwards): "TLS".

Administration via local phone

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

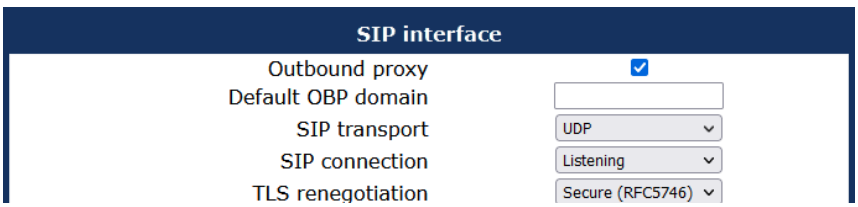
SIP connection

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

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

Administration via WBM

1. Open System > SIP interface.



- Persistent (SB): Persistent connection with Switchback.
  - Value range: "Listening", "Persistent (SB)"
  - Default: "Persistent (SB)"

Administration via local phone

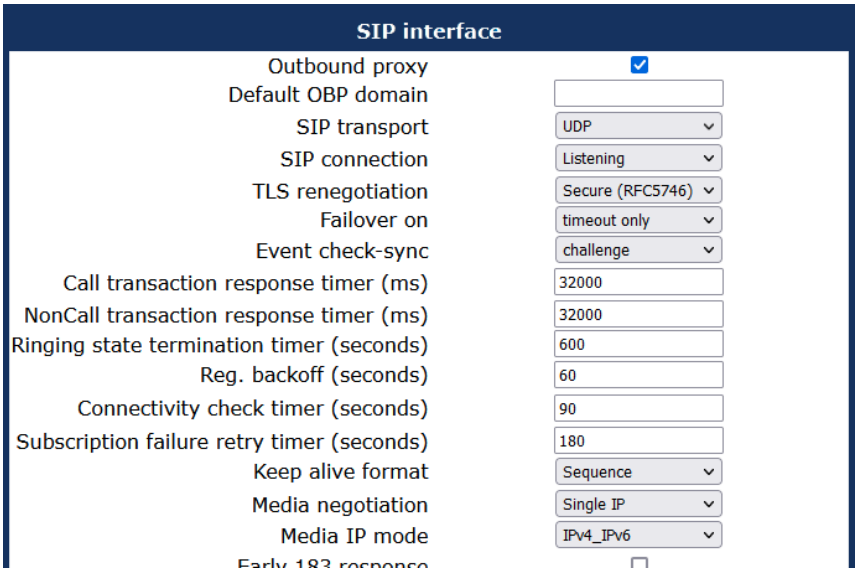
```
|--- Admin
      |--- System
            |--- SIP Interface
                  |--- SIP connection
```

Media / SDP

OpenScape Desk Phone CP phones support IPv4/IPv6 media address negotiation in SDP using ANAT (Alternative Network Address Types). ANAT allows for the expression of alternative network addresses (e. g., different IP versions) for a particular media stream.

Administration via WBM

1. Open System > SIP interface.



- When Media negotation is set to "ANAT", ANAT is supported; the phone will re-register with the SIP server and advertise ANAT support in the SIP header.
- When set to "Single IP" or "ICE", ANAT support is disabled.
- When set to "ICE" the phone will negotiate the best route for the media stream (see "Interactive connectivity establishment (ICE)" → page 121)

Note If SRTP is enabled, ANAT interworking is only possible if SDES is configured as the key exchange protocol for SRTP (see "System" → page 78).

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

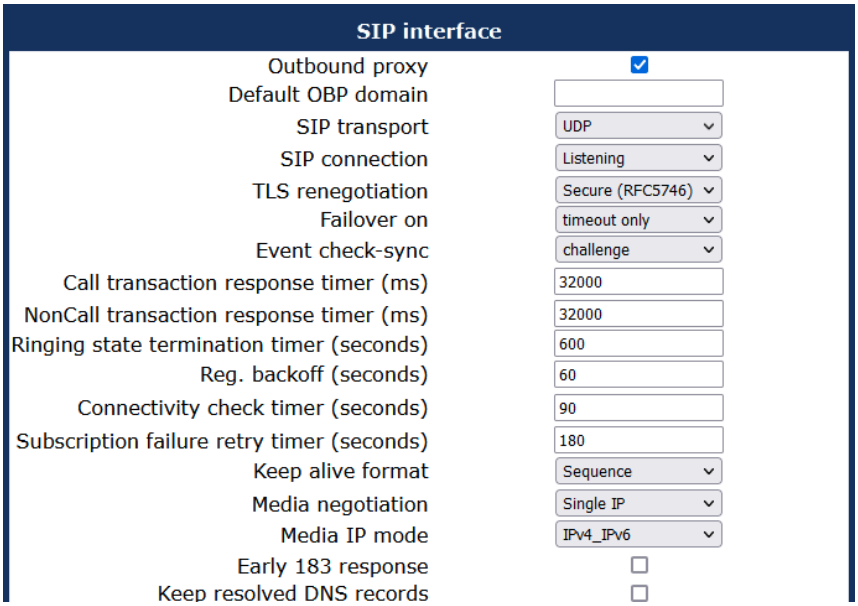
Administration via local phone

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

Early 183 response

Administration via WBM

1. Open System > SIP interface.



- If **True**, in response to an initial SDP offer in a SIP INVITE the phone will generate a SIP 183 response that includes an SDP answer with all the attributes that is provided in a subsequent 200 OK.
- If **False**, the phone will not generate a SIP 183 response, with early SDP answer, to a SIP INVITE.

Administration via local phone

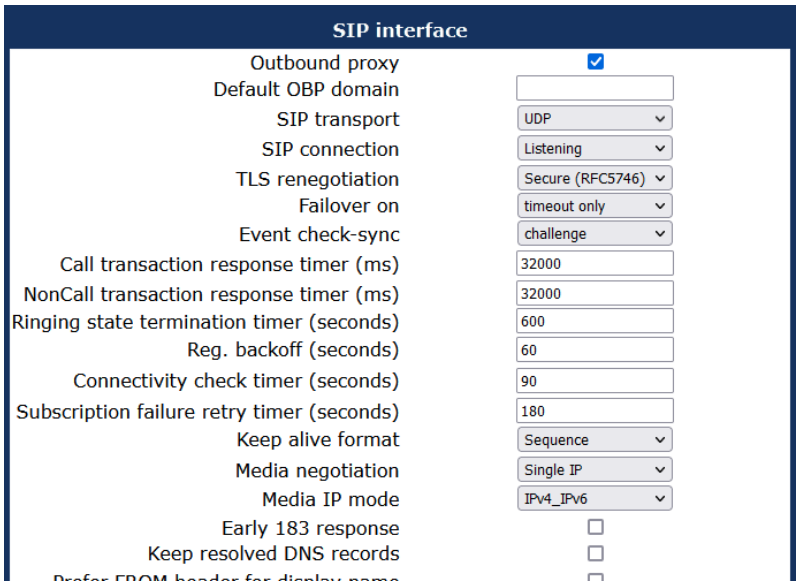
```
|--- Admin
       |--- System
              |--- SIP Interface
                     |--- Early 183 response
```

Keep resolved DNS records

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

Administration via WBM

1. Open System > SIP interface.



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

> **Note** There must be at least one successful DNS look-up where the phone can keep and use the DNS records for the future work. After a device reboot, DNS records are not retained and there is a new look-up.

If this option is disabled, the DNS records will not be retained. Every attempt to resolve an IP address must be successful in order to establish a SIP connection.

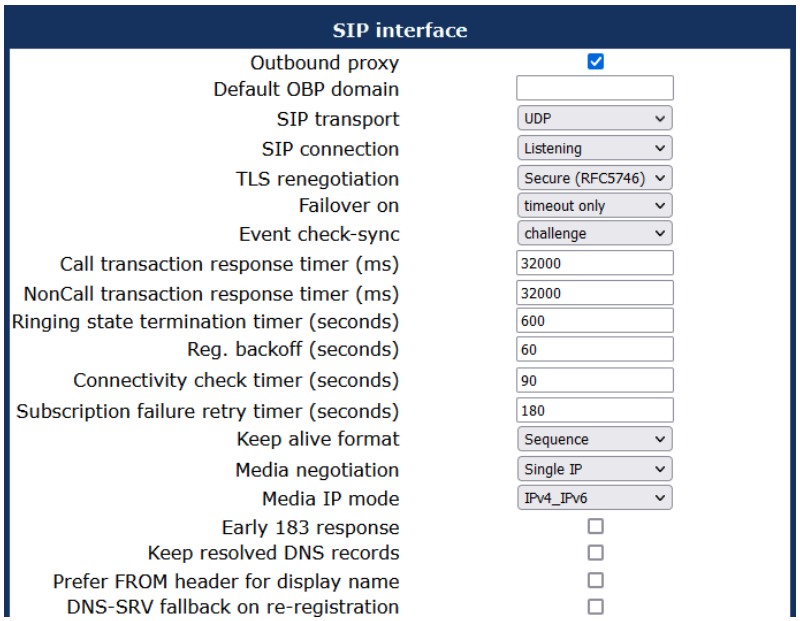
Administration via local phone

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

Prefer FROM header

Administration via WBM

1. Open System > SIP interface.



If "Prefer FROM header for display name" is enabled, the phone display will use the information provided by the "FROM Header" field.

In any other case (not activated) the display information is provided by the "P-Asserted-id Header" (PAI Header). If not provided, the FROM header information is used. The signalled name is only used if the phone does not match the call number to a contact on the phone.

> By default, the feature is disabled.

Administration via local phone

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

DNS-SRV fallback on re-registration

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

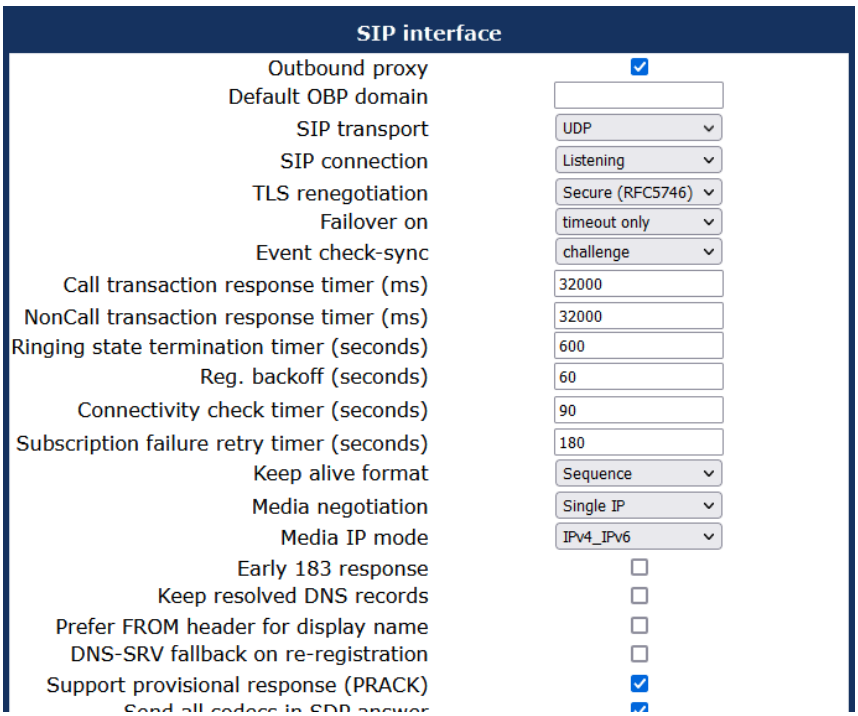
If **False,** the phone will always try to reconnect to the primary SBC when doing re-registration. If the attempt is not successful, the call succeeds through the secondary SBC since the phone has already registered.

Note Blacklisted IPs remains blacklisted, unless there is a re-registration attempt.

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

Administration via WBM

1. Open System > SIP interface.



Administration via local phone

```
|--- Administrator settings
      |--- System
            |--- SIP Interface
                  |--- DNS-SRV fallback on re-registration
```

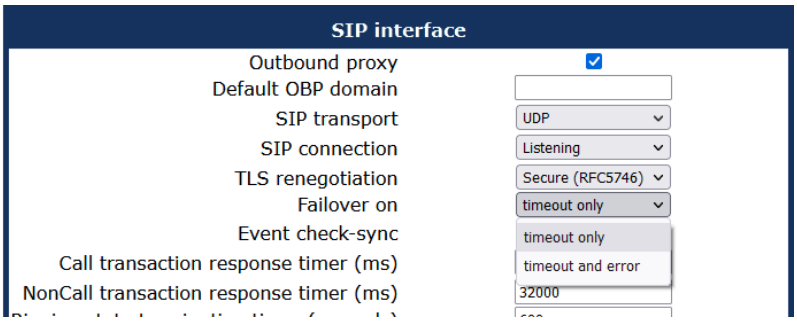
Failover on SIP 5XX server response

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

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

Administration via WBM

1. Open System > SIP interface.



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

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

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

When receiving a 500 or 503 error response on a SIP request (with "Failover on" set to "Timeout and Error"), the phone will failover immediately without taking any timers into account (e.g. transaction timer). When set to "timeout only" the failover will only occur if there is no response.

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

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

SIP SESSION TIMER

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

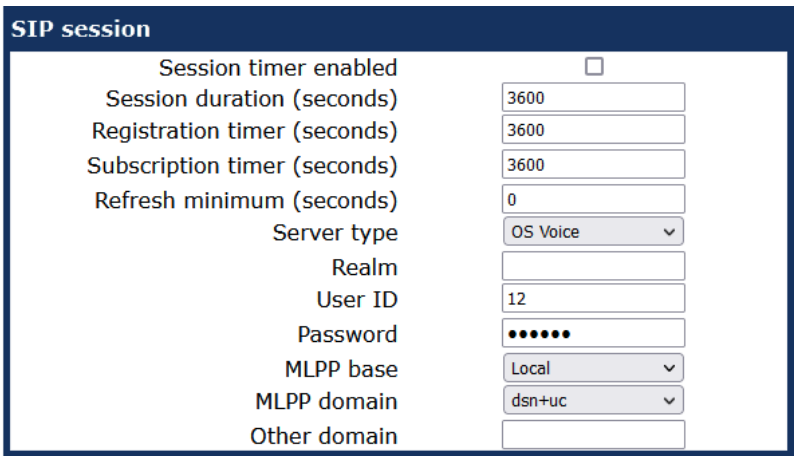
This feature is sufficiently backward compatible such that only one end of a call needs to implement the SIP extension for it to work.

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

> **Note** Some server environments support their own mechanism for auditing the health of a session. In these cases, the Session timer must be deactivated.

Administration via WBM

1. Open System > Registration.



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

Administration via local phone

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

RESILIENCE AND SURVIVABILITY

To allow for stable operation even in case of Network or server failure, OpenScape Desk Phones have the capability of switching to a fallback system. The switchover is controlled by various configurable check and timeout intervals.

DNS SRV can be used for enhanced survivability in two ways:

- In a scenario with a survivability proxy
- In a scenario with multiple primary SIP servers.

The DNS server provides the phone with a prioritized list of SIP servers via DNS SRV. The phone fetches this list periodically from the server, depending on the TTL (time to live) specified for the DNS SRV records.

Enable DNS SRV requests

To enable DNS SRV requests from the phone, make the following settings:

1. For a scenario with multiple "primary" SIP servers enter the corresponding DNS SRV domain name under SIP server and SIP registrar and set the SIP server and SIP registrar ports to 0.
   - The web interface paths are specified in "System > Registration > SIP server address/SIP registrar address" and "Network > Port configuration > SIP server/SIP registrar" (see "SIP addresses" → page 101 and "SIP ports" → page 102).
2. For a scenario with a survivability proxy enable the use of an outbound proxy for routing outbound requests.
   - The web interface path is System > SIP interface > Outbound proxy (see "Outbound proxy" → page 106).
3. Enter the DNS SRV domain name as SIP gateway address and set the SIP gateway port to "0".
   - The web interface paths are "System > Registration > SIP gateway address" and "Network > Port configuration > SIP gateway" (see "SIP addresses" → page 101 and "SIP ports" → page 102).

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

A survivability proxy acts as a relay between the phone and the primary SIP server. Thus, the address of the survivability proxy is specified as gateway or SIP server at the phone (see "SIP registration" → page 103).

When the TCP/TLS connection between the survivability proxy and the SIP server breaks down, e. g. because of server failure, the survivable proxy itself acts as a replacement for the primary SIP server. Vice versa, in case the phone can not reach the survivability proxy itself, it will register directly with the primary SIP server, provided that it is specified in the DNS SRV server list.

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

Survivability with distributed SIP servers

Another way to realize survivability is the use of multiple, geographically separated SIP servers. Normally, the phone is registered with that server that has the highest priority in the DNS SRV server list. If the highest priority server fails to respond to the TCP/TLS connectivity check or SIP messages the phone will register with the server that has the second highest priority (see "TLS connectivity check" → page 116). The availability is verified continuously in the background when

using TLS or TCP as SIP transport protocol via an ongoing connectivity-check (see "TLS connectivity check" → page 116 for TLS connectivity check and "TCP connectivity check" → page 117 for TCP connectivity check).

Survivability with a backup SIP server

Along with the registration at the primary SIP server, the phone is registered with a backup SIP server. In normal operation, the phone uses the primary server for outgoing calls. If the phone detects that the connection to the primary SIP server is lost, it uses the backup server for outgoing calls. This connection check is realized by 2 timers (see "Response timer" → page 117 and "Non-INVITE transaction timer" → page 118).

For configuring the backup server, refer to "Backup SIP server" → page 120.

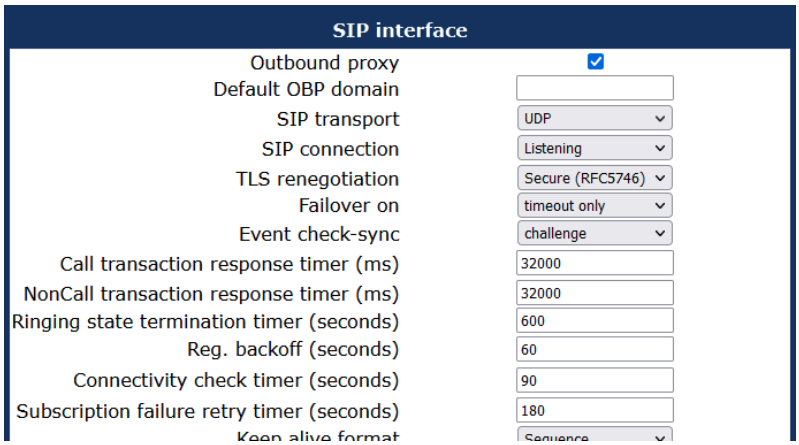
> **Note** In survivability mode, some features will presumably not be available. The user is informed by a message in the Call View display.

TLS connectivity check

A regular check ensures that the TLS link to the main SIP server is active.

Administration via WBM

1. Open System > SIP interface.



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

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

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

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

> If no other primary SIP server is found via DNS SRV, the phone will switch over to a backup server for making receiving calls. For configuring the backup server, refer to "Backup SIP server" → page 120.

TCP connectivity check

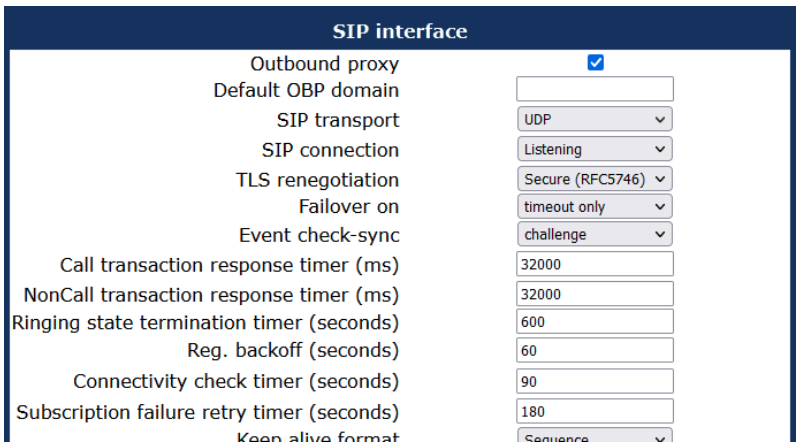
A regular check ensures that the TCP link to the main SIP server is active.

> The same mechanisms as described in "TLS connectivity check" also apply for "TCP connectivity check" (see "TLS connectivity check" → page 116).

If no other primary SIP server is found via DNS SRV, the phone will switch over to a backup server for making receiving calls. For configuring the backup server, refer to "Backup SIP server" → page 120.

Administration via WBM

1. Open System > SIP interface.



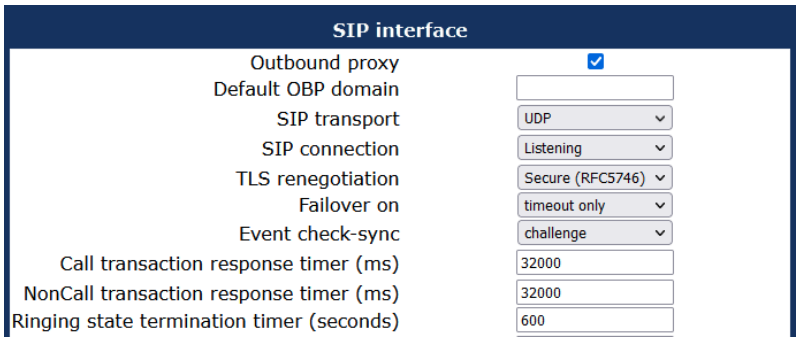
- When the Connectivity check timer is set to a non-zero value, TCP keep live messages is sent at the defined interval. If the link is found to be dead, the phone uses DNS SRV to find another SIP server. For this, the DNS SRV records must be properly configured in the DNS server.
  - Value range: 0 (off),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

Response timer

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

Administration via WBM

1. Open System > SIP interface.



- If the call transaction timer expires before the phone gets a response from the SIP server, the phone assumes that the server had died and then attempts to contact the backup server, if configured. If there is no backup server configured, the phone just tidies up internally.
  - The data is given in milliseconds.
  - The default value is 32 000.

Administration via local phone

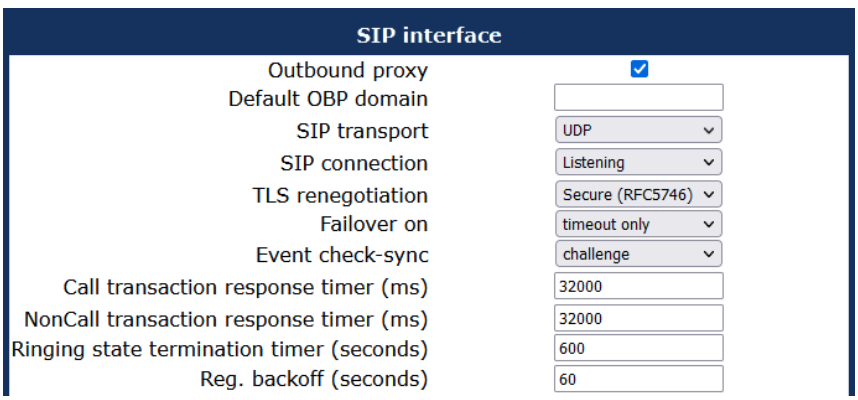
```
|--- Admin
      |--- System
            |--- SIP Interface
                  |--- Call trans. (ms)
```

Non-INVITE transaction timer

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

Administration via WBM

Open System > SIP interface.



- The data is given in milliseconds.
  - The default value is 32 000.

Administration via local phone

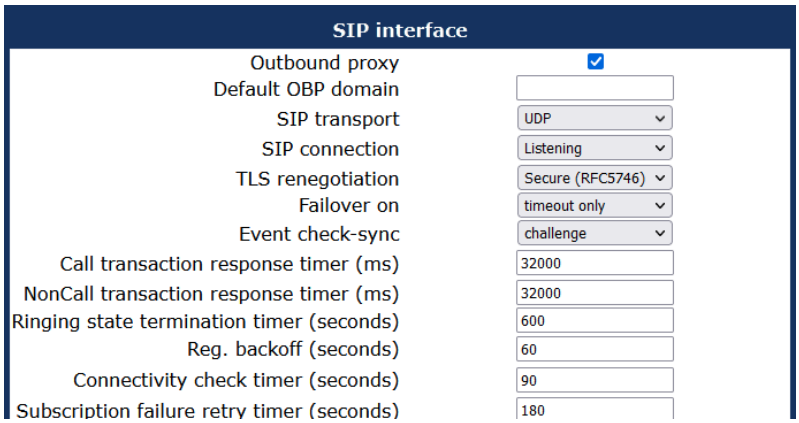
```
|--- Admin
      |--- System
            |--- SIP Interface
                  |--- NonCall transactions (ms)
```

Maximum registration backoff timer

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

Administration via WBM

1. Open System > SIP interface.



2. Set the registration backoff timer.
   - Values: 60 to 600 secs
   - Default: 60s

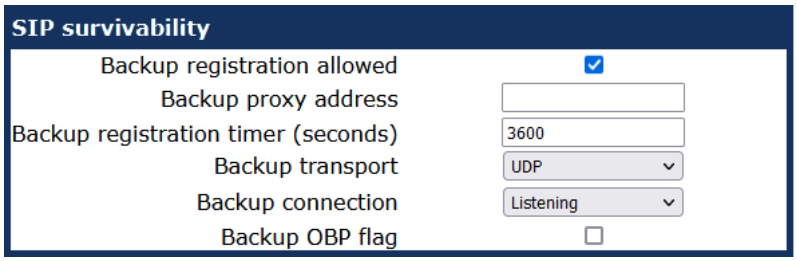
Administration via local phone

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

Backup SIP server

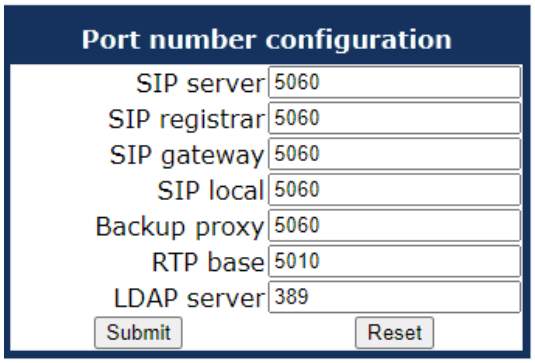
Administration via WBM

1. Open System > Registration.



- **Backup registration allowed / Backup registration flag**: Determines whether or not the backup proxy is used as a SIP Registrar. The Backup registration allowed flag indicates whether or not the phone treats the backup proxy server as a SIP registrar. If set to "Yes", the phone tries to register its SIP address with the server whose IP address or host name is specified by Backup proxy address.
  - Value Range: "Yes", "No"
  - Default: "Yes"
- **Backup proxy address**: IP address or host name of the backup proxy server.
- **Backup registration timer**: Expiry time of the registration in seconds. The Backup registration timer determines the duration of a registration with the backup SIP server.
  - Default: 3600
- **Backup transport**: Transport protocol to be used for messages to the backup proxy. The Backup transport option displays the current transport protocol used to carry SIP messages to the Backup proxy server.
  - Value range: “TLS”, “TCP”, “UDP”
  - Default: "UDP"
- **Backup Connection**: SIP connection type of the Backup Connection (listening or persistent with Switchback) (see "SIP connection" → page 107).
  - Value range: "Listening", "Persistent (SB)"
  - Default: "Persistent (SB)"
- **Backup OBP flag**: Determines whether or not the backup proxy is used as an outbound proxy. The Backup OBP flag indicates whether or not the Backup proxy server is used as an outbound proxy.
  - Value range: "Yes", "No"
  - Default: "No"

2. Open Network > Port configuration.



- **Network > Port Configuration > Backup proxy**: Port of the backup proxy server.
  - Default: 5060

INTERACTIVE CONNECTIVITY ESTABLISHMENT (ICE)

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

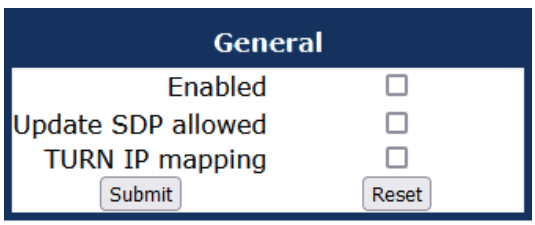
ICE works by adding to the SDP several candidate addresses by which the peer device may contact the phone. It is used to provide a direct media connection between Circuit clients and the phone.

> **Note** ICE Lite is also supported, according to Section 8.2 of RFC 5245. The phone continues to use the full ICE implementation to work with the ICE Lite implementation on Google Voice server.

General

Administration via WBM

1. Open System > ICE > General.



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

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

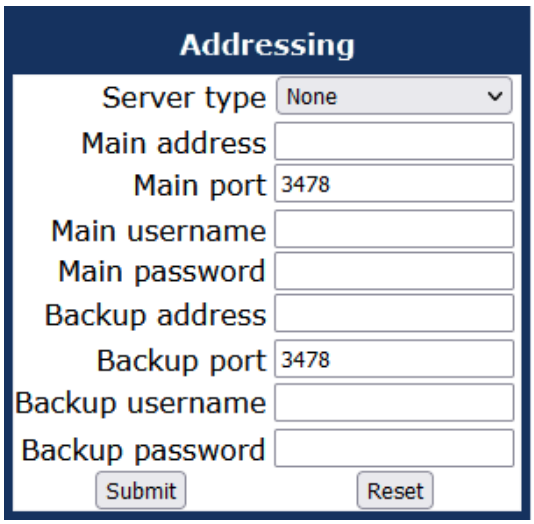
Administration via local phone

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

Addressing

Administration via WBM

1. Open System > ICE > Addressing.



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

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

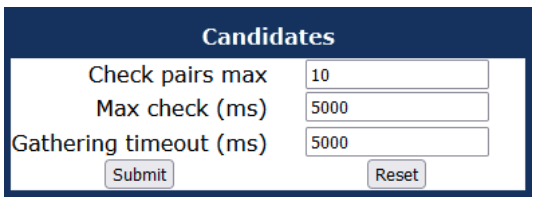
Administration via local phone

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

Candidates

Administration via WBM

1. Open System > ICE > Candidates.



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

Administration via local phone

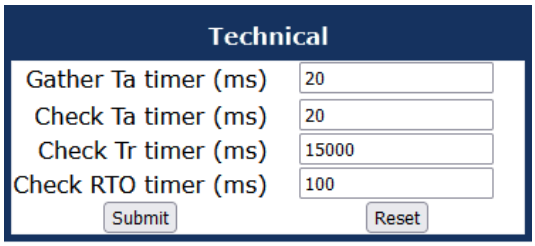
```
|--- Administration
      |--- System
            |--- ICE
                  |--- Candidates
                        |--- Check pairs max
                        |--- Max Check (ms)
                        |--- Gathering timeout (ms)
```

Technical

Warning **This node contains configuration that only experts should change!**

Administration via WBM

1. Open System > ICE > Technical.



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

Administration via local phone

```
|--- Administration
      |--- System
            |--- ICE
                  |--- Technical
                        |--- Gather Ta timer (ms)
                        |--- Gather RTO timer (ms)
                        |--- Check Ta timer (ms)
                        |--- Check RTO timer (ms)
```

FEATURES

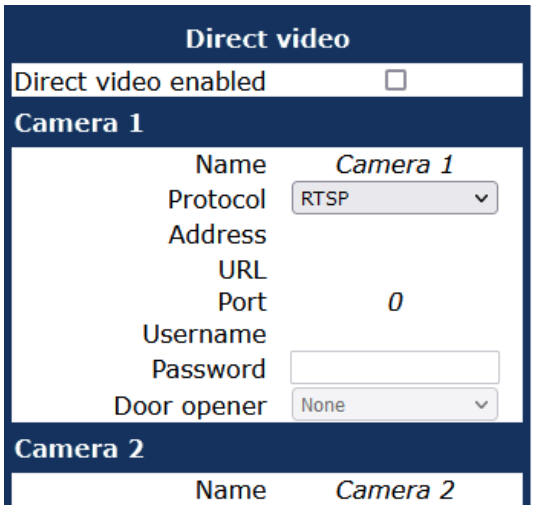
Direct video

On CP710 phones it is possible to stream video content to the phone display by controlling an external supported camera via a URL, triggered by a freely programmable key or menu item. Up to 4 cameras can be configured.

> **Note** Phones fully support RTSP video stream up to 640 x 480 px resolution. If a higher resolution video feed is received, it is displayed in a smaller video window to maintain high-quality performance even under hardware limitations.

Administration via WBM

1. Open System > Features > Direct video.



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

Administration via local phone

```
|--- Admin
    |---System
        |--- Features
             |--- Direct video
                  |--- Feature access
                       |--- Enabled
                  |--- Camera 1
                       |--- Name
                       |--- Protocol
                       |--- Address
                       |--- Port
                       |--- URL
                       |--- Username
                       |--- Password
                       |--- Door opener
                  |--- Camera 2
                       (as Camera 1)
                  |--- Camera 3
                       (as Camera 1)
                  |--- Camera 4
                       (as Camera 1)
```

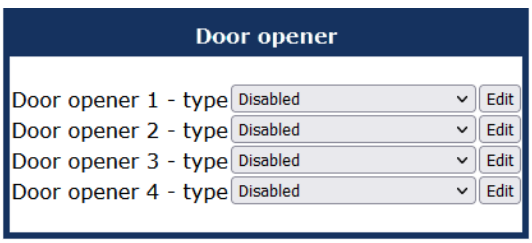
Door opener

> This feature is available only on OpenScape Desk Phones CP410, CP700, CP700X, CP600 and CP710 phones.

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

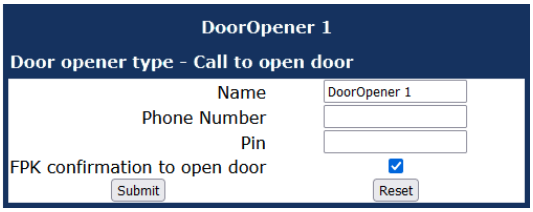
Administration via WBM

1. Open System > Features > Door opener.



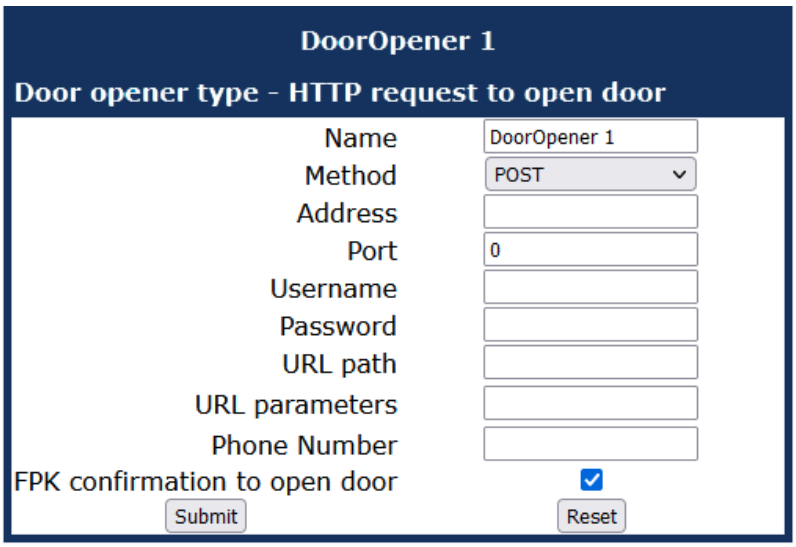
2. Select an option. The available options are:
   - Disabled
   - Call to open door
   - HTTP request to open door
   - HTTPS request to open door
3. Click **Edit** to configure the door opener. The configuration of the door openers depends on the selected control method.

4. If the selected control method is "Call to open door", enter the following fields:



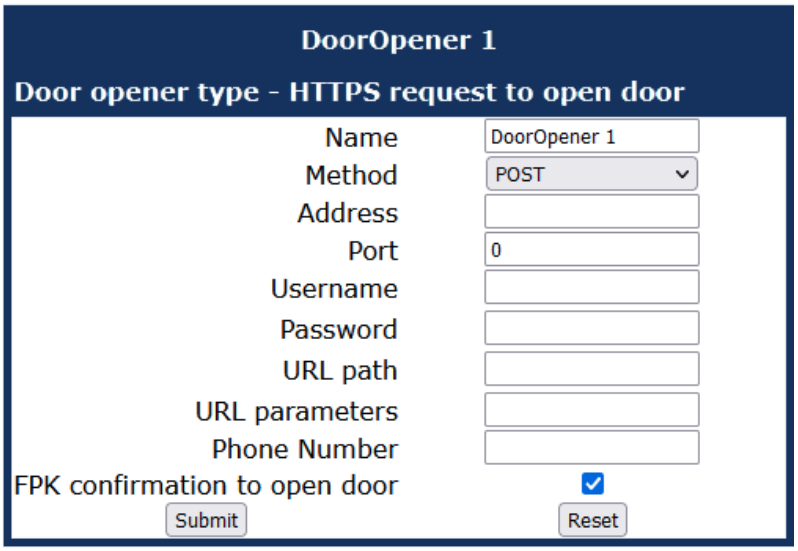
   - Name (mandatory): freely selectable name for the door opener (can be custom name or alphanumeric).
   - Phone Number (mandatory): the phone number controlling the door opener.
   - Pin (mandatory): the PIN to open the door, same PIN as configured at Door opener device.
   - FPK confirmation to open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

5. If the selected control method is HTTP request to open door fill in the following fields:



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

6. If the selected control method is HTTPS request to open door fill in the following fields:



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

Administration via local phone

```
|--- Admin
    |---System
        |--- Features
             |--- Door opener 1
                  |--- Door opener type
                       |--- Disabled
                       |--- Call to open door
                            |--- Name
                            |--- Phone number
                            |--- PIN
                            |--- FPK confirmation to open door
                       |--- HTTP request to open door
                            |--- Name
                            |--- Method
                            |--- Address
                            |--- Port
                            |--- Username
                            |--- Password
                            |--- URL path
                            |--- URL parameters
                            |--- Phone number
                            |--- FPK confirmation to open door
                       |--- HTTPS request to open door
                            (as HTTP request to open door)
             |--- Door opener 2
                  (as Door opener 1)
             |--- Door opener 3
                  (as Door opener 1)
             |--- Door opener 4
                  (as Door opener 1)
```

Note If "Direct video" is enabled, the following lines are added at the bottom of the menu list for each Door opener type.

```
                       |--- Associated Camera
                       |--- Automatic Door Video
```

SYSTEM

OpenScape Desk Phone CP phones support the following security option:

- PKI-based SPE (Signaling and Payload Encryption)

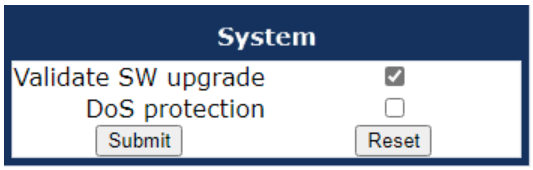
The signalling transport main / standby parameter selects the protocol to use for signalling. TCP and TLS are avaliable.

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 89.

> **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.

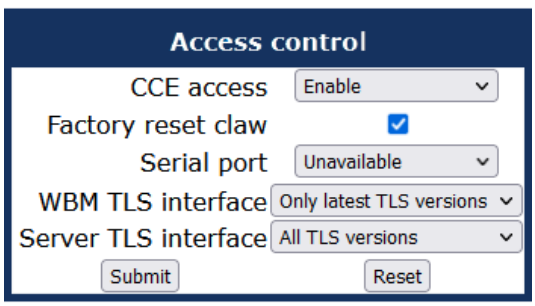
Administration via local phone

```
|--- 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
```

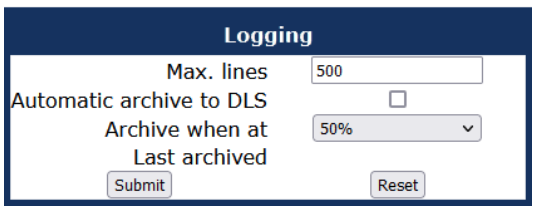
Security log

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
```

Feature access

Administration via WBM

1. Open System > Features > Feature access.
2. Enable or disable the following features and interfaces:

- Blind transfer (see "Blind call transfer" → page 165)
- 3rd call leg (consultation from a second call; see user manual)
- Call establish
  - Callback (see "Callback" → page 1 and "Callback URIs" →1)
  - Call pickup (see "Directed pickup" → page 168)
  - Group pickup (see "Group pickup" → page 168)
  - Call deflection (see "Deflect a call" → page 166)

    - Call forwarding (see "Call forwarding (standard)" → page 162)
    - Caller ID: Enables the user to change the default caller ID when calling via RingCentral API → 1
    - Do not disturb (see "Do not disturb" → page 168)
- Refuse call (see "Allow "Refuse Call"" → page 134)
- Repertory dial key (see "Repertory dial" → page 169)
- Ext / int forwarding (see "Call forwarding by call type" → page 163)
- Phone book lookups (see user manual)
- DSS feature (see "Direct Station Select (DSS)" → page 1)
- BLF feature (see "BLF key" → page 171)
- Agent feature (see "Call center agent" → page 149)
- Video calls (CP710 only, see "Direct video" → page 124)
- CTI control (see "Configuring the uaCSTA interface" → page 1)
- Bluetooth (CP710 only, see "Bluetooth interface" → page 42)
- USB device access (only for phones with a USB port, see "Connectors at the bottom side" → page 27)
- USB power using PoE (CP710 only , see "Configuring the USB access" → page 156)
- Web based manag. (see "Web-based management (WBM)" → page 24)
- Feature toggle (see "Feature toggle" → page 1)
- Phone lock (see user manual)
- Limited FPK set (see "Free programmable keys" → page 157)

Administration via local phone

```
|--- Admin
     |--- System
          |--- Features
               |--- Feature access
                    |--- Call control
                         |--- Blind transfer
                         |--- 3rd call leg
                    |--- Call establish
                         |--- Callback
                         |--- Call pickup
                         |--- Group pickup
                         |--- Call deflection
                         |--- Call forwarding
                         |--- Call establish
                         |--- Do not disturb
                         |--- Refuse call
                         |--- Repertory dial key
                         |--- Ext/int forwarding
                    |--- Call associated
                         |--- Phone book lookups
                         |--- DSS feature
                         |--- BLF feature
                         |--- Agent feature
                         |--- Video calls
                    |--- CTI
                         |--- CTI control
                    |--- Services
                         |--- Bluetooth
                         |--- Web based manag.
                         |--- USB device access
                         |--- USB power using PoE
                         |--- Feature toggle
                         |--- Phone lock
                         |--- Limited FPK set
```

Feature configuration

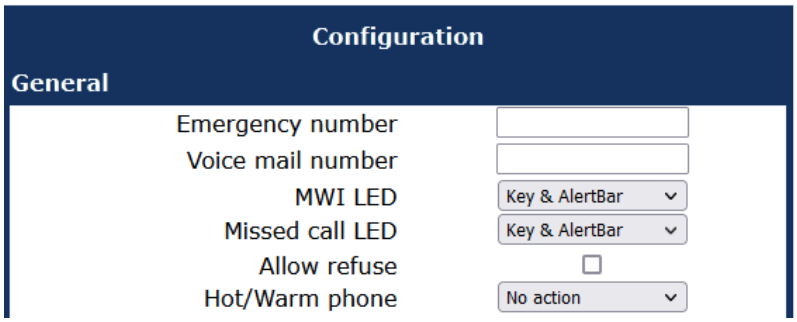
ALLOW "REFUSE CALL"

> This parameter defines whether the "Refuse Call" feature is available on the phone.

Note This parameter can also be configured under System > Features > Feature access (see "Feature access" → page 132).

Administration via WBM

1. Open System > Features > Configuration.



2. Enable or disable "Allow refuse".

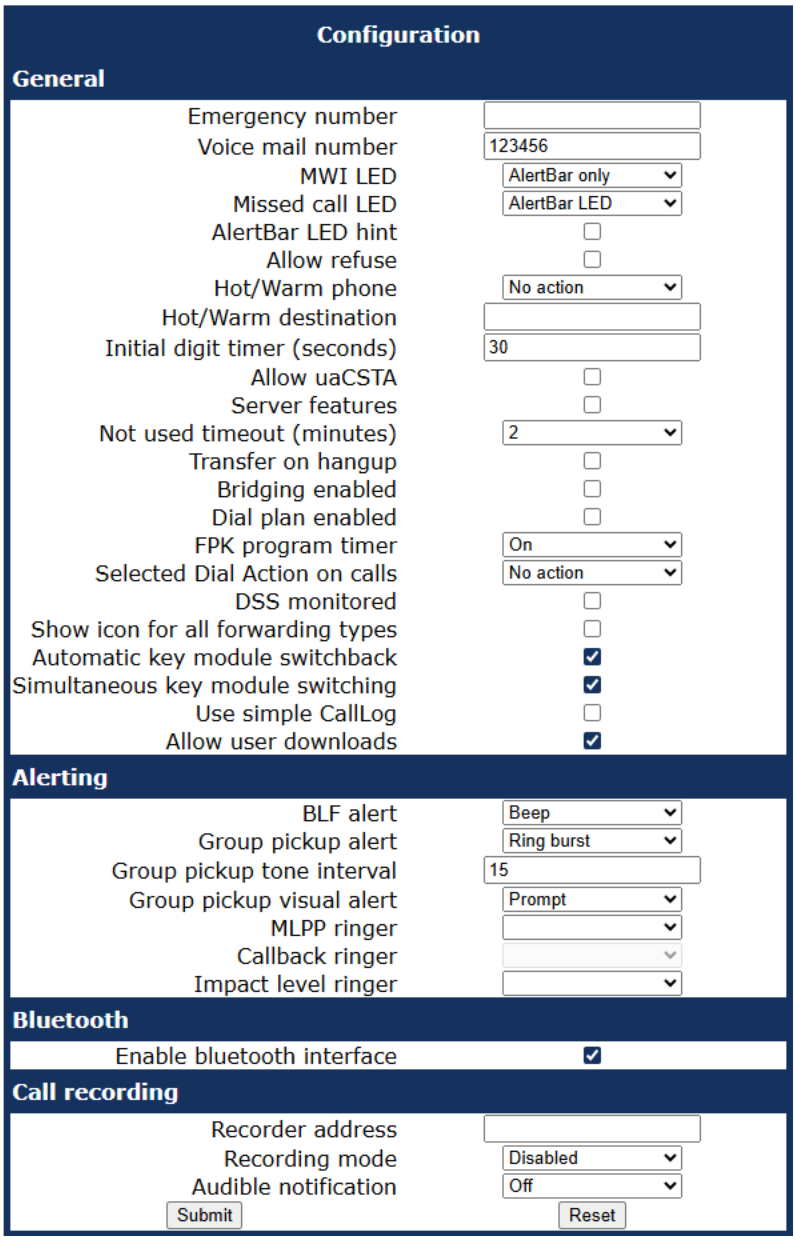
Administration via local phone

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

HOT OR WARM PHONE

Administration via WBM

1. Open System > Features > Configuration.



If the phone is configured as hot phone, the number specified in “Hot warm destination” is dialed immediately when the user goes off-hook. For this purpose, Hot or warm phone must be set to "Hot phone". If set to "Warm phone", the specified destination number is dialed after a delay which is defined in “Initial digit timer (seconds)” (also refer to "Initial digit timer" → page 137).

During the delay period, the user can dial a number which is used instead of the hot / warm destination. In addition, the user is provided with a dial tone during the delay period. With the setting "No action", hot phone or warm phone functionality is disabled.

Administration via local phone

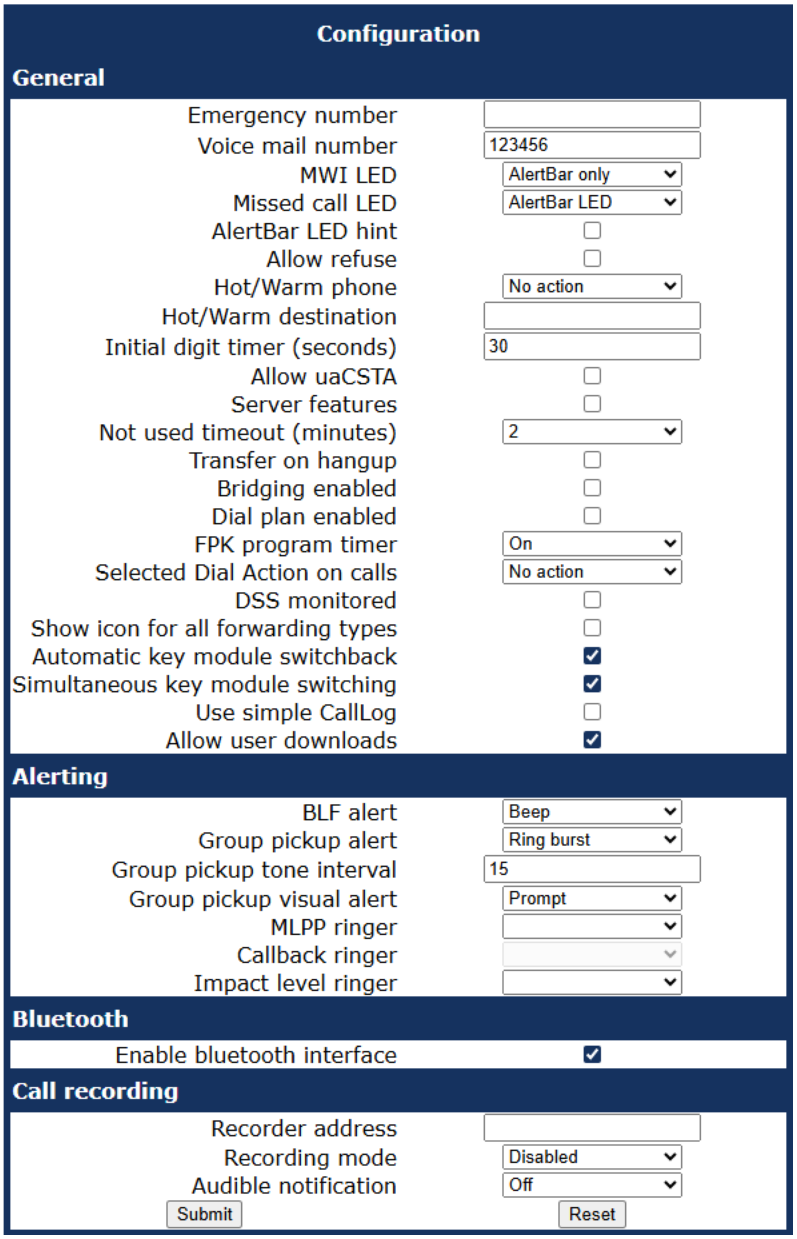
```
|--- Admin
       |--- System
              |--- Features
                     |--- Configuration
                            |--- General
                                   |--- Hot / warm phone
                                   |--- Hot / warm destination
                                   |---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

INITIAL DIGIT TIMER

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

Administration via WBM

1. Open System > Features > Configuration.



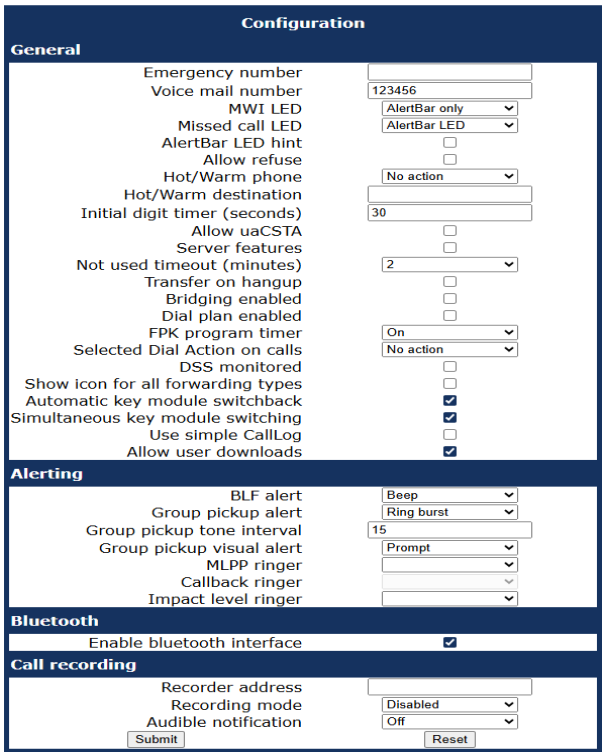
Administration via local phone

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

SHOW FORWARDING ICON

Administration via WBM

1. Open System > Features > Configuration.



The parameter "Show icon for all forwarding types" enables a call forwarding icon on the display for any type of call forwarding. If disabled, only "Forwarding conditional" is indicated by the icon.

- Values: Enabled or disabled
- The default is disabled.

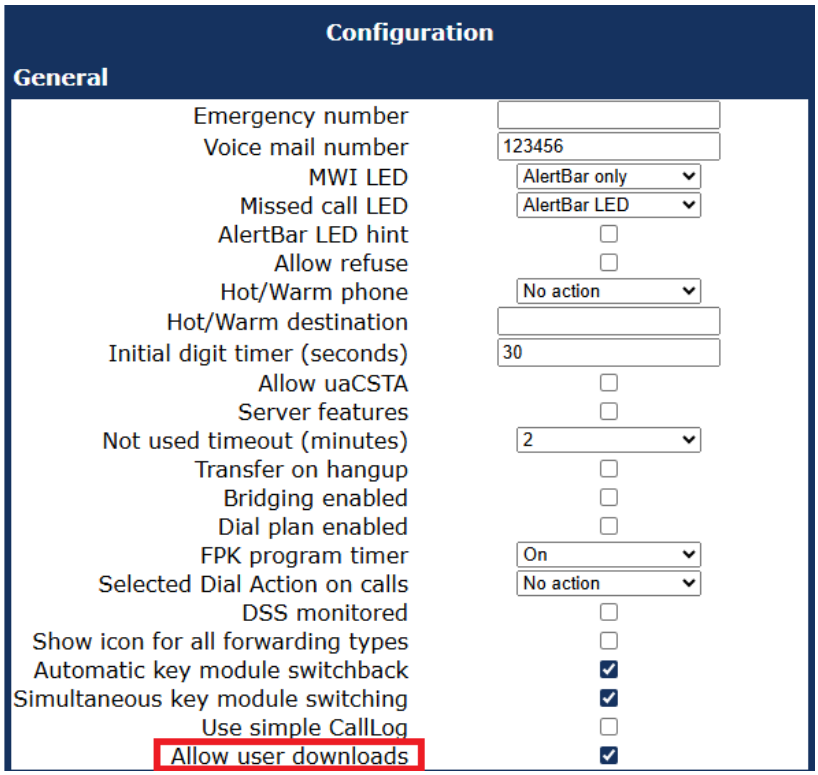
Administration via local phone

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

ALLOW USER DOWNLOADS

Administration via WBM

1. Open System > Features > Configuration.



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

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

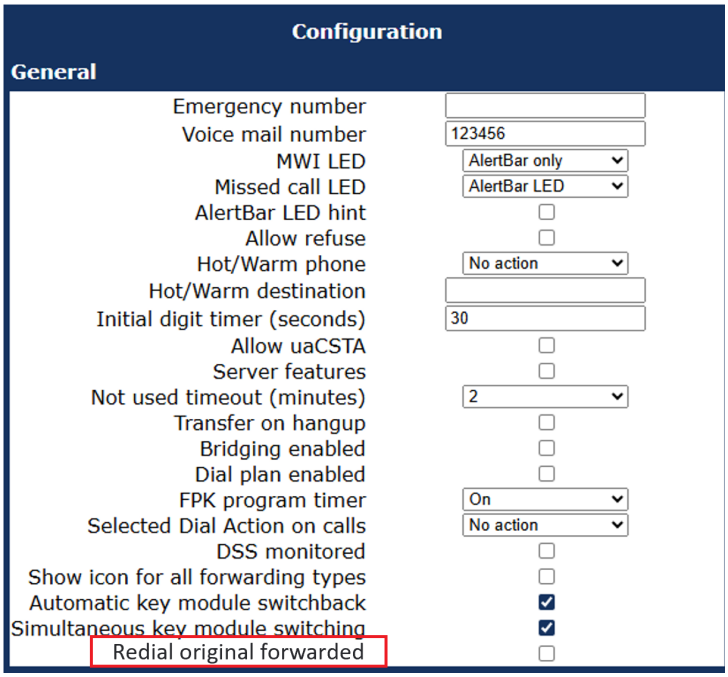
- Values: Enabled or disabled
- The default is enabled.

Administration via local phone

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

REDIAL ORIGINAL FORWARDED

Administration via WBM



The parameter "Redial original forwarded" controls the display order and redial behavior for forwarded outgoing calls. If enabled, it moves the originally called entry above the connected party entry in the **Conversations** list and ensures the Redial function calls the originally dialed number instead of the forwarded destination.

- **Values**: Enabled or disabled
- The default is disabled.

Administration via local phone

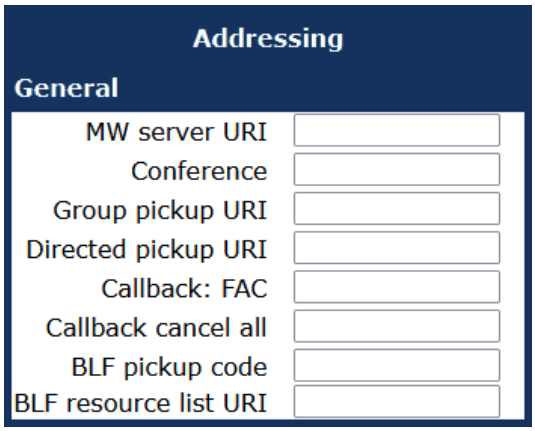
```
|--- Admin
    |--- System
        |--- Features
            |--- Configuration
                |--- General
                    |--- Redial original forwarded
```

MULTIPLE-PARTY CONFERENCE CALL

As an administrator, you must explicitly allow phones to use the Zoom Multi Party Conference (MPC) functionality.

Administration via WBM

1. Open System > Features > Addressing.



2. In the **Conference** field, enter the value `*96` to enable conference functionality on the Zoom phone devices.

> For non-Zoom devices, enter the appropriate value, e.g. *123456780*.

1. Assign an FPK to the **Conference** feature (ID=**22**).

GROUP PICKUP

> **Note** This feature is available only when Group Call Pickup or Directed Pickup is enabled on the Zoom Phone server for the user.

Group Call Pickup is controlled entirely by the Zoom server. The phone must be assigned to a pickup group in Zoom.

Zoom uses a BLF key configured with:

- a **Group Pickup URI**, and
- a **BLF pickup code**

The BLF pickup code determines whether the BLF key performs a **group pickup** or a **directed pickup**, depending on the configuration of the Group Pickup URI.

- **Group Pickup**: Uses a specific Zoom pickup code (e.g., *98) to monitor and pick up calls for the group.
- **Directed Pickup**: Uses a specific Zoom pickup code (e.g., *97) to monitor and pick up calls from specific users.

When a call is ringing for the group, the BLF key flashes.

Pressing the BLF key will:

- send the pickup request defined by the BLF pickup code
- pick up either the group call or a specific user's call (directed), according to the server configuration

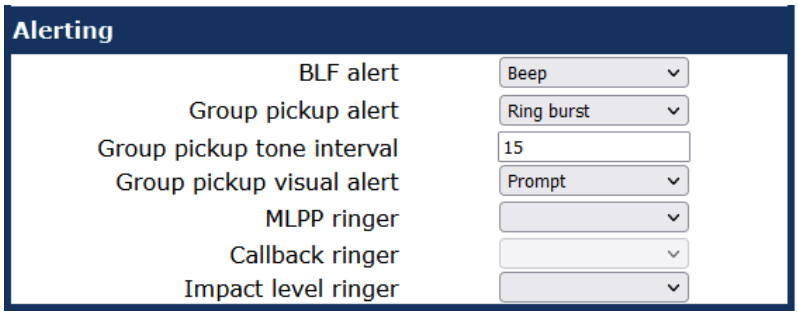
The phone must be displaying a group pickup alert for the call to be answered. If no alert is displayed, pressing the BLF key triggers the pickup request to the server.

Pickup alert

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

Administration via WBM

1. Open System > Features > Configuration.
2. Use the "Group pickup tone allowed" parameter to enable or disable the acoustic alert for pickup group calls.



- The default is active.
- If enabled, "Group pickup alert" selects whether the phone uses the current ringtone or an alert beep.
- If disabled, the phone always uses an alert tone.

Depending on the phone state and the setting for "Group pickup alert", the group pickup tone comes from the loudspeaker, the handset, or the headset. The volumes can be set in the local user menu, in "Audio > Volumes". The following table shows the group pickup alert behavior for each possible scenario:

Phone state			Group pickup as ringer enabled	Group pickup as ringer disabled
Ringer on	Idle		Ring tone speaker	Beep speaker
	In call	Handset	Ring tone speaker	Beep Handset
		Handset open listening	Beep Handset and speaker	Beep Handset and speaker
		Headset	Ring tone speaker	Beep headset
		Headset open listening	Beep headset and speaker	Beep headset and speaker
		Hands-free	Beep speaker	Beep speaker
Ringer off	Idle		Nothing	Nothing
	In call	Handset	Nothing	Beep Handset
		Handset open listening	Beep Handset and speaker	Beep Handset and speaker
		Headset	Nothing	Beep headset
		Headset open listening	Beep headset and speaker	Beep headset and speaker
		Hands-free	Beep speaker	Beep speaker

Group pickup visual alert

This setting defines how the user accepts a pickup call:

- If **Prompt** is selected, an incoming pickup call is signaled by the "Pickup call" prompt on the display and by the flashing pickup key. As soon as the user goes off-hook or presses the speaker key, the pickup call is accepted. Alternatively, the user can press the corresponding function key, if configured.
- If **Notify** is selected, an incoming pickup call is signaled by the "Pickup call" prompt on the display and by the flashing Pick up key. To accept the call, the user must confirm the alert by pressing OK or by pressing the flashing pickup key.

- If **FPK only** (default setting) is selected, an incoming call is signaled only by the flashing pickup key. To accept the call, the user must press the flashing Pick up key. "Pickup call" is shown on the display, and the user can either lift the handset or press the speaker key or the headset key to accept the call.

Administration via local phone

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

CALL TRANSFER

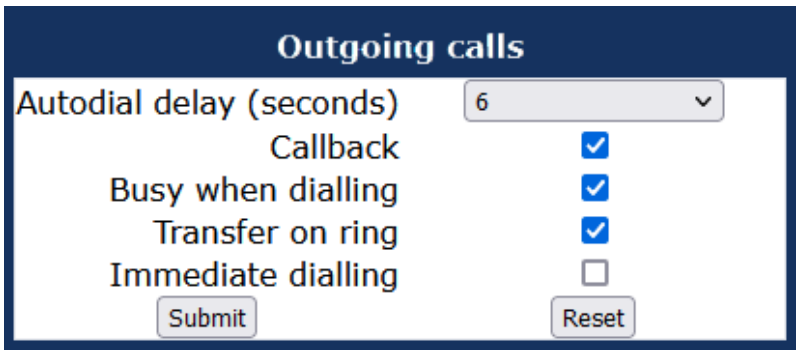
Transfer on ring

If this function is active, a call can be transferred after the user has dialed the third participant's number, but before the third party has answered the call.

Note This feature is enabled or disabled in the User menu.

Administration via WBM

1. Open User > Configuration > Outgoing calls.



- The default is "Yes".

Administration via local phone

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

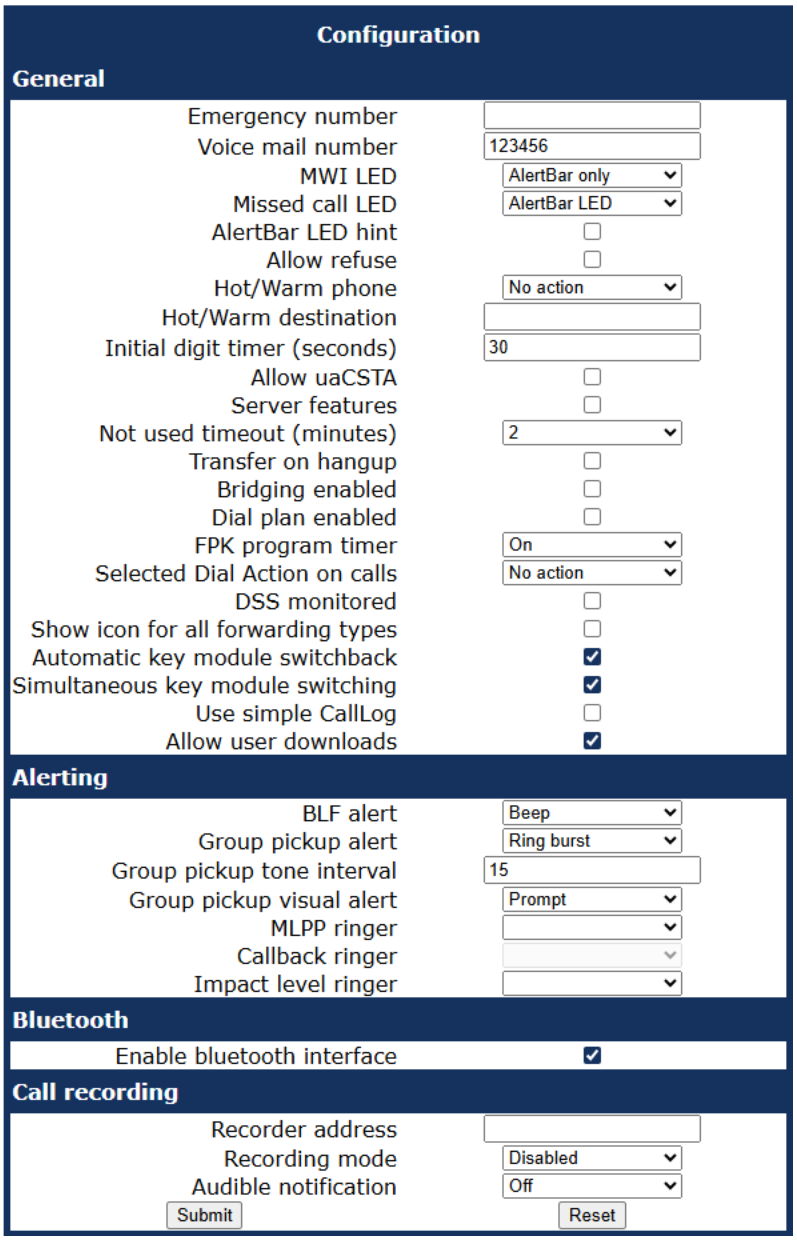
Transfer on hang-up

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

By default, the feature is disabled.

Administration via WBM

1. Open System > Features > Configuration.



2. Enable or disable "Transfer on hangup".

Administration via local phone

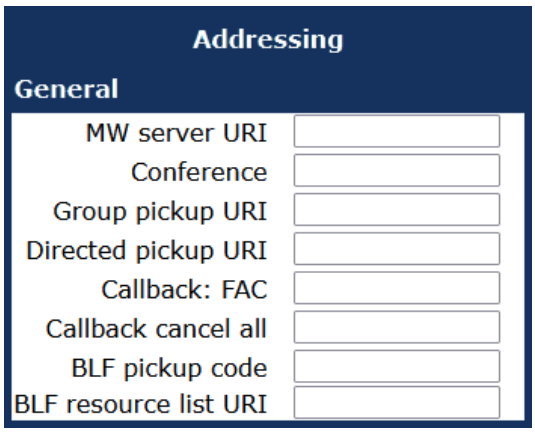
```
|--- Admin
      |--- System
            |--- Features
                  |--- Configuration
                        |--- General
                              |--- Transfer on hangup
```

MESSAGE WAITING ADDRESS

The MWI (Message Waiting Indicator) is an optical signal which indicates that voice mail messages are on the server. Depending on the SIP server / gateway in use, the Message waiting server address, that is the address or host name of the server that sends message waiting notifications to the phone, must be configured.

Administration via WBM

1. Open System > Features > Addressing.



Administration via local phone

```
|--- Admin
      |--- System
            |--- Features
                  |--- Addressing
                        |--- MWI server URI
```

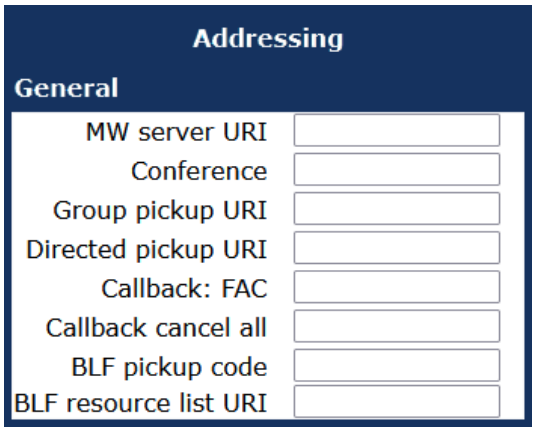
SYSTEM-BASED CONFERENCE CALL

The Conference URI provides the number or URI used for system based conference calls, which can involve 3 to 16 members.

> **Note** This feature is not available on every system.

Administration via WBM

1. Open System > Features > Addressing.



2. Enter the conference URI or number in "Conference".

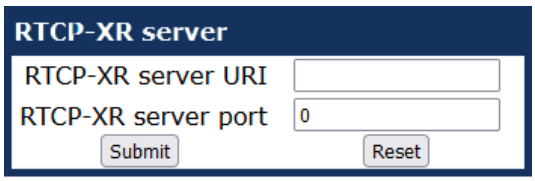
> **Note** It is recommended not to enter the full URI, but only the user part. For example, enter "123", not "123@SIP SERVER ADDRESS". Entering a full address may cause conflicts when OpenScape Desk Phone CP operates across multiple nodes. The default value provisioned by Zoom is "***96**".

RTCP-XR SERVER

The RTCP-XR (Real Time Control Protocol Extended Reports) transmits voice quality reports after the conclusion of a call.

Administration via WBM

1. Open System > Features > Addressing.



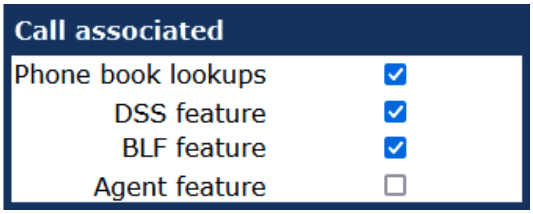
- **RTCP-XR URI:** URI to be used for transmitting voice quality reports after the conclusion of a call.
- **RTCP-XR port:** Port value of RTCP-XR server.

> If RTCP-XR port value is not configured or is empty, the RTCP-XR port value is taken from the SIP server port value.

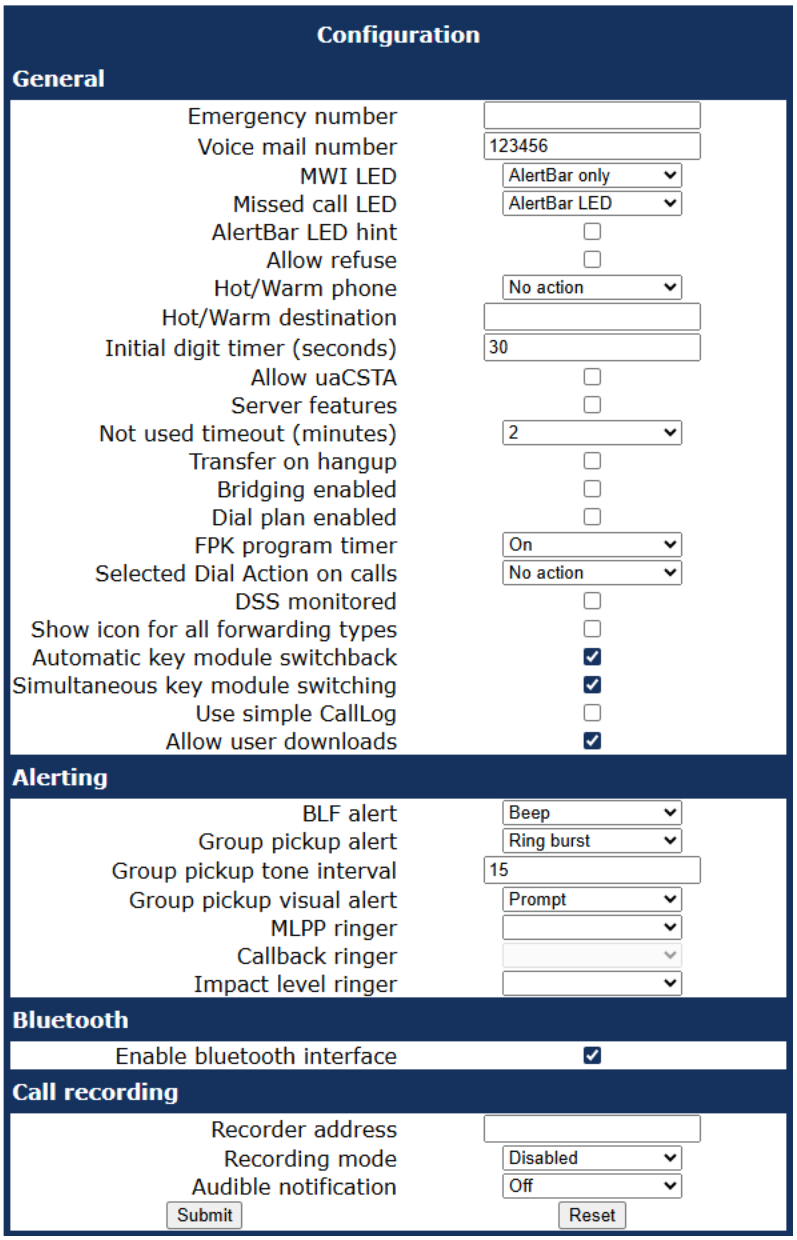
CALL CENTER AGENT

Administration via WBM

1. Open System > Features > Feature access.



2. Enable **Agent Feature**.
3. Click **Submit**.
4. Open System > Features > Configuration.



5. Enable **Server features**.
6. Click **Submit**.

Administration via local phone

```
|--- Admin
     |--- System
          |--- Features
               |--- Feature access
                    |--- Call associated
                         |--- Agent feature
               |--- Configuration
                    |--- General
                         |--- Server features
```

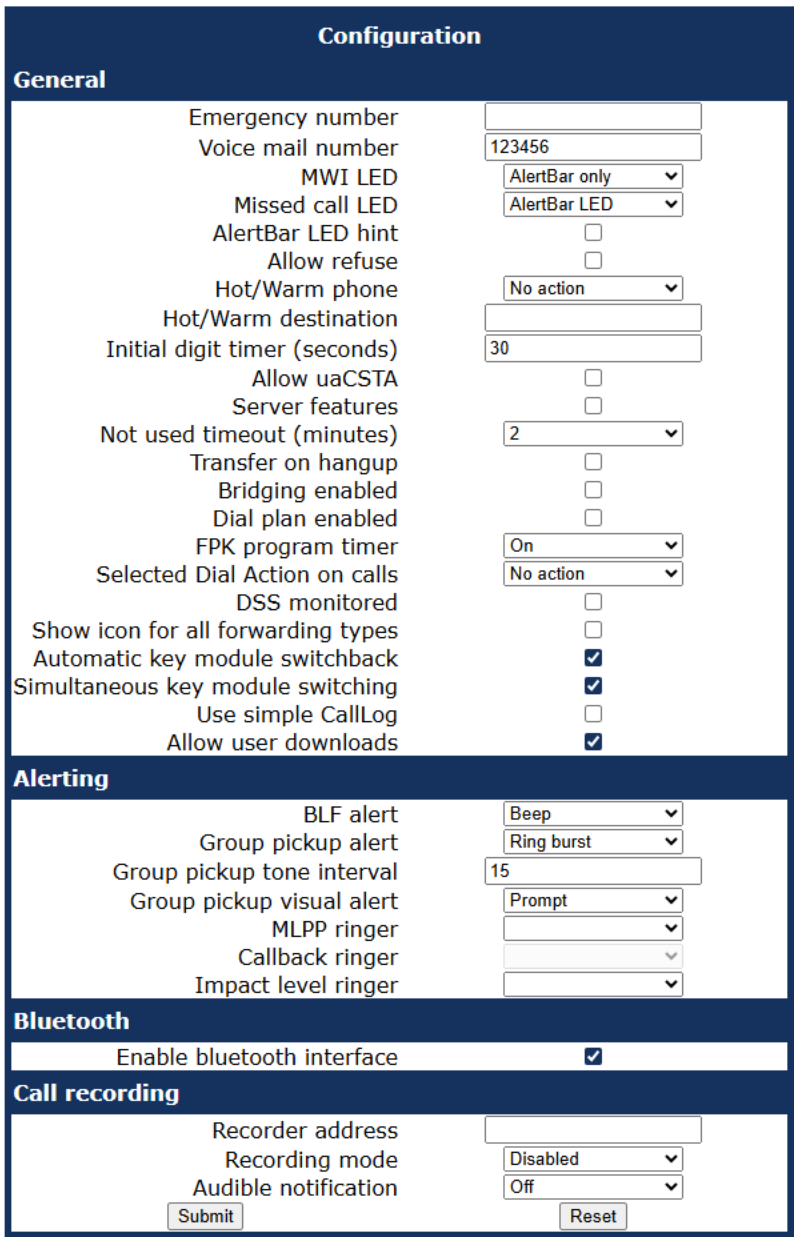
CONFIGURING THE LOCAL MENU TIMEOUT

The timeout for the local user and admin menu is configurable. When the time interval is over, the menu is closed and the administrator or 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.

> **Note** The current position in the user or admin menu is kept in case the user or admin has exited the menu, e.g. for receiving a call. Thus, if the user or admin re-enters the menu before the time-out, he is directed to that submenu, or parameter, which he has been editing before.

Administration via WBM

1. Open System > Features > Configuration.



2. Select the timeout.
   - The timeout ranges from 1 to 5 minutes.
   - The default value is 2 minutes.
3. Click **Submit**.

Administration via local phone

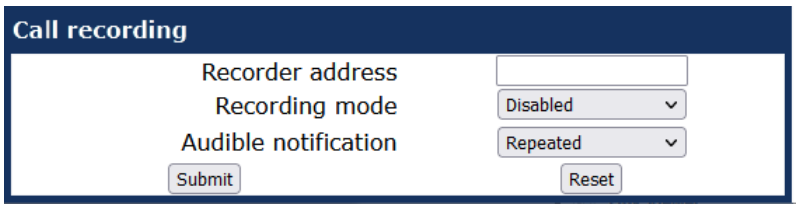
```
|--- Admin
      |--- System
            |--- Features
                  |--- Configuration
                        |--- General
                              |---  Not used timeout
```

CALL RECORDING

Call recording is possible for OpenScape Desk Phone CP using an "ASC Voice Recorder". The implementation is similar to a local conference, with the recording device acting as the third conference member. To start recording, the phone calls the recording device and provides it with the mixed audio data. Unlike a true local conference, the call used for recording can not transport audio from the recording device to the phone.

Administration via WBM

1. Open System > Features > Configuration.



- With the Recorder address / Recorder number parameter, the SIP address of the call recorder is specified.
- With the Call recording mode / Recording Mode parameter, the behavior of the feature is determined:
  - **"Disabled"**: The user cannot turn recording on.
  - **"Manual"**: The user starts and stops recording manually using the menu or a free programmable key. Call recording stays enabled when the phone returns to idle mode.
  - **"Auto-start"**: The recording starts automatically for each call. The user can stop it manually only during a call. When the call ends, call recording is automatically available for the next call.
  - **"All Calls"**: The recording starts automatically for all recordable calls; the user can not stop the recording manually.
  - **"One call"**: The user starts and stops recording manually during a call using the menu or a free programmable key. When the call finishes, call recording is automatically turned off again.
- The Audible indication / Audible Notification parameter determines if and how the parties in a call are informed when a call is being recorded:
  - **"Off"**: No audible indication is given.
  - **"Single-shot"**: A single audible indication is given when recording commences or resumes.

- **"Repeated"**: An audible indication is given when recording commences or resumes, and repeated periodically during the recording.

Administration via local phone

```
|--- Admin
     |--- System
          |--- Features
               |--- Configuration
                    |--- Call Recording
                         |---  Recorder number
                         |---  Recorder mode
                         |---  Audible notification
```

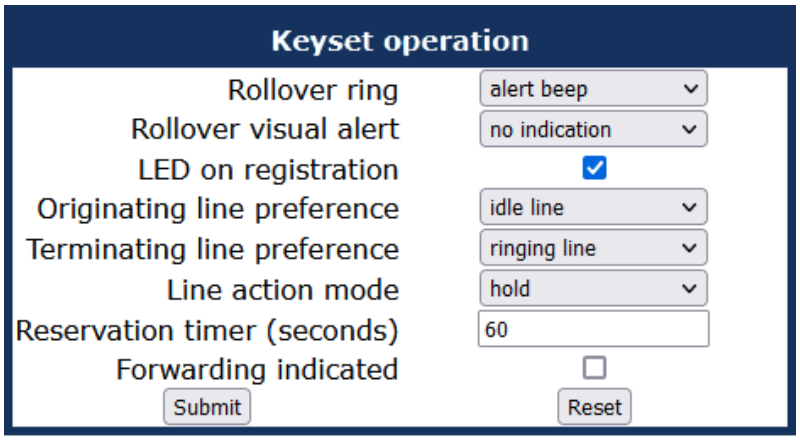
ROLLOVER VISUAL ALERT

> This feature is available only on OpenScape Desk Phones CP410, CP700, CP700X, CP600 and CP710 phones.

This feature allows user to have a visual indication of rollover calls so that the user can directly see the call related information. A rollover call is one that has been received on a phone that is busy with a call on a different line, e.g. the call may have been routed from a busy line to another line on the same phone.

Administration via WBM

1. Open System > Features > Keyset operation.



- **No indication (default)**: when "Rollover visual alert" is set to "no indication", the phone does not provide any visual indication of an incoming rollover call on the main display.
- available for the next call: when "Rollover visual alert" is set to "visual alert", the phone will provide a visual indication in form of a sausage-shaped notification on the bottom of the current screen for an incoming rollover call.

The information provided to the user on a single incoming rollover call:

- Line key label on the left side
- Remote party information on the right side

The information provided on multiple incoming rollover calls:

- The amount of incoming calls

LANDING SCREEN

This feature is available only on OpenScape Desk Phones CP410, CP700, CP700X, CP600 and CP710 phones.

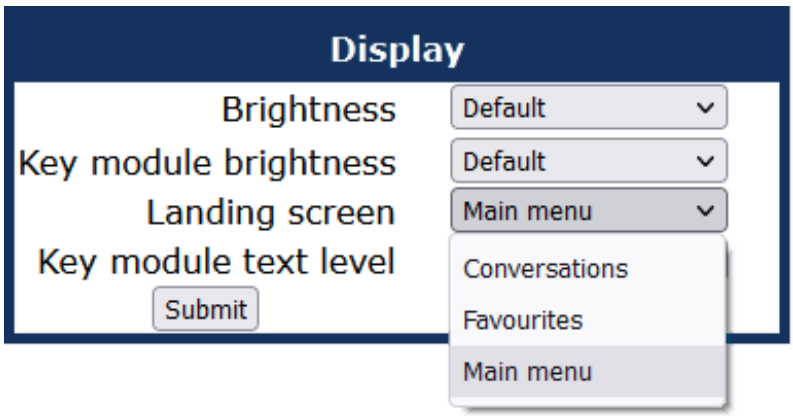
Based on defined trigger conditions the phone may automatically show one of the following screens as the landing screen (i.e. top of the UI stack):

- Conversation list
- Favourites
- Main menu

Note The default landing screen is "Conversations".

Administration via WBM

1. Open User > Phone > Display.



2. Select the landing screen.

ASSOCIATED LINES

This setting is automatically administered by the Zoom server.

Associated lines allow you to use multiple appearances of the line to allow it to handle multiple calls on the same line when connected to a Zoom server.

A phone can be configured with multiple key appearances for the same registered line. Each key appearance can handle one call at a time, while the Zoom line itself can support up to three simultaneous calls.

Associated lines on a Zoom phone allow:

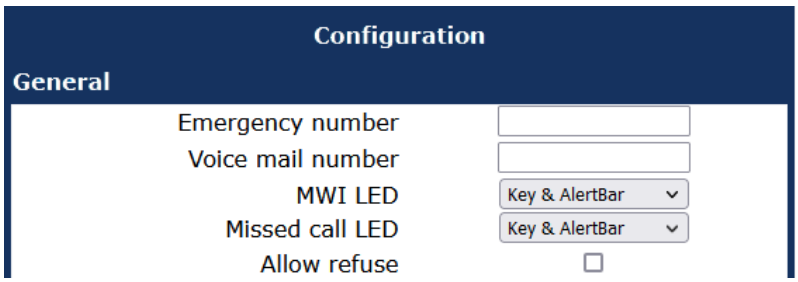
- Multiple key appearances for the same registered line (primary or shared).
- Handling of multiple calls per line using the key appearances.
- Consultation, call waiting, and alternating between calls using the associated key appearances.
- Consistent shared-line behavior across all devices registered to the same line.

MWI LED

This configurable item is added to the administrator settings to allow the administrator to control how new voice mails are indicated to the user: via the LED of the mailbox key only, via the AlertBar LED only, or via both LEDs.

Administration via WBM

1. Open System > Features > Configuration.



2. For MWI LED, select one of the following options:
   - "Key only" (default)
   - "Key & AlertBar"
   - "AlertBar only"

Administration via local phone

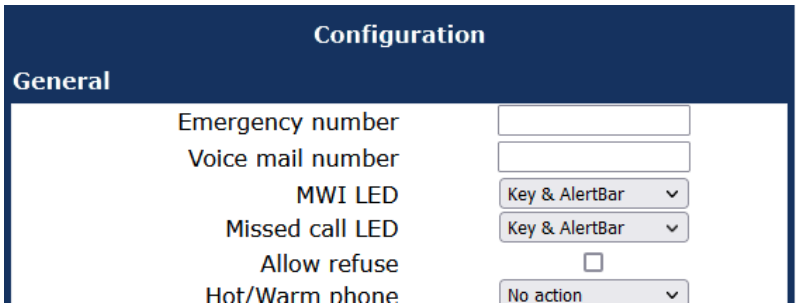
```
|--- Admin
     |--- System
          |--- Features
               |--- Configuration
                    |--- MWI LED
```

MISSED CALL LED

This configurable item is added to the administrator settings to allow the administrator to control how new missed calls are indicated to the user via LEDs on the phone: via the LED of the mailbox key only, via the AlertBar LED only, via both LEDs, or no LED indication.

Administration via WBM

1. Open System > Features > Configuration.



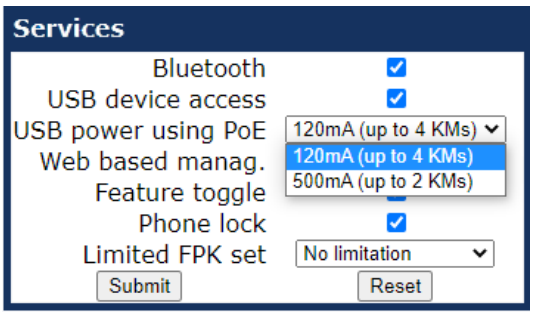
2. For "Missed call LED", select one of the following options:
   - "Key only" (default)
   - "Key & AlertBar"
   - "AlertBar only"
   - "No LED"

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 27).

Administration via WBM

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



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 33).
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 31).

- 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**.

Free programmable keys

The key programming can be accessed via the WBM, 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". CP210 can also support KM710 & KM410.
- The OpenScape Desk Phone **CP110** phone provides three free programmable keys (FPKs). These are called „Phone keys".

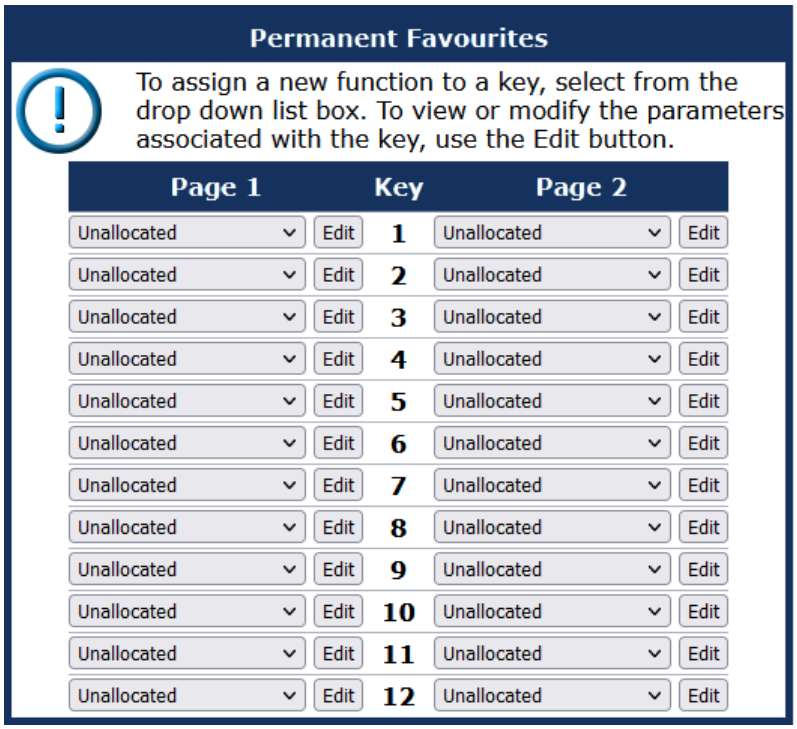
HOW TO CONFIGURE FREE PROGRAMMABLE KEYS

Free programmable keys (FPKs) can be configured via the WBM.

> - The following screen shows the setting on a CP710 phone.
> - The same menu item on CP410 has a different name and allows for 16 keys.
> - The same menu item for CP210 & CP110 is also different and allows up to 4 or 3 keys respectively

Administration via WBM

1. Open System > Features > Permanent Favourites.



2. To assign a new function to a key, select a function from the drop down list.
3. To view or modify the parameters associated with the key, click **Edit**.
4. After editing the selected key, save the changes.

ENABLING "LONG PRESS" FOR FPKS

Note The long press feature is enhanced for the CP210.

Programmable Key Configuration on Zoom Phones:

Long presses on Line keys or Park keys do not open a key programming menu. Instead, a long press displays call information for that key (active or held call) or parked call information, if applicable.

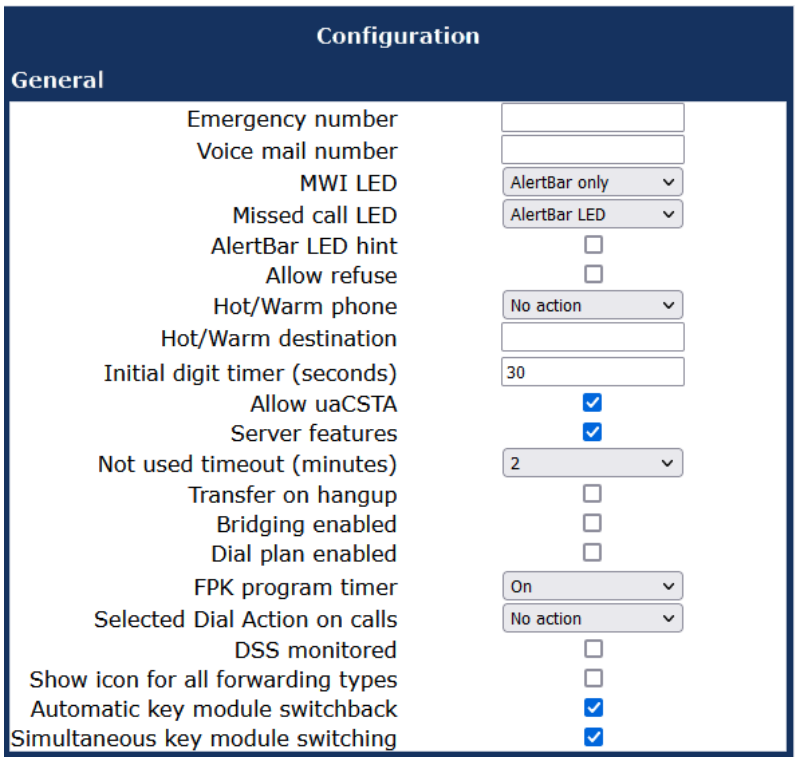
FPKs (Function/Programmable Keys) can still be programmed via the settings menu; long-pressing a key is only for viewing call or parked call details.

For keyset and DSS functionality, refer to "Multi-line appearance " → page 181.

The "long press" feature can be enabled or disabled by setting the FPK program timer parameter.

Administration via WBM

1. Open System > Features > Configuration.



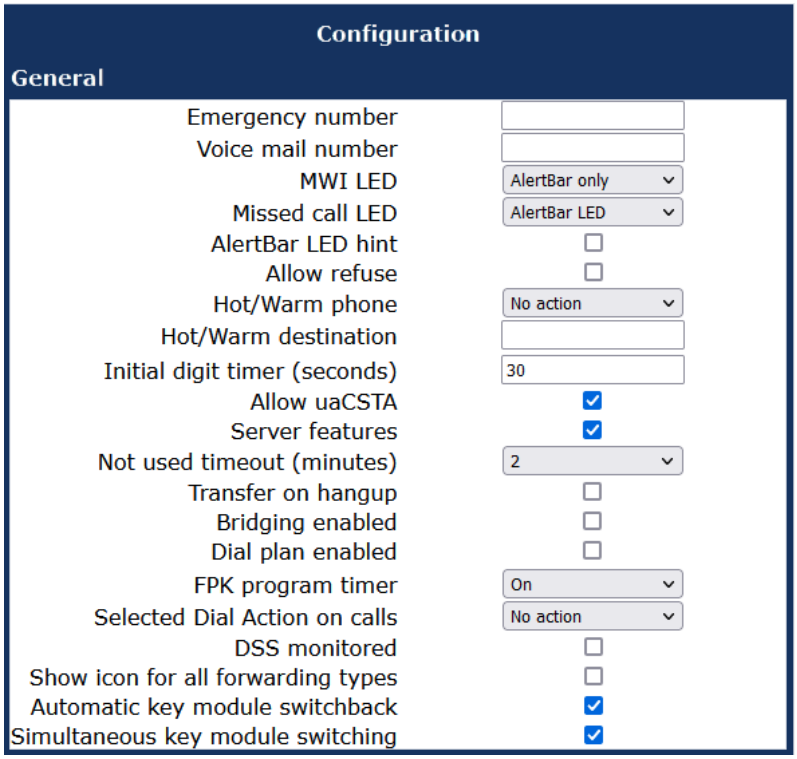
2. Set the FPK program timer to On or Off.
   - **Parameter to On**: long press will access the setting menu to program the pressed key.
   - **Parameter to Off**:
     - CP110 and CP210 - Feature on 2nd level of the FPK is accessed with long press.
     - CP410 and CP710 - Long press is disabled.
3. Click **Submit**.

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 WBM

1. Open System > Features > Configuration.



The available options are:

- **Consult**: the action performed is a consultation transfer to the destination configured in the **Selected Dialing Key** menu which has been pressed.
- **Transfer**: the action performed is a blind transfer to the destination configured in the **Selected Dialing Key** menu which has been pressed.
- **No Action**: no action will take place. The call will continue to be active or held based on what the user has selected.
  - Default value: **No Action**.

Administration via local phone

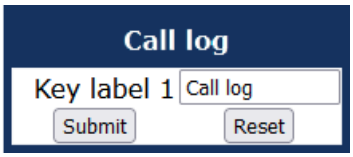
```
|--- Admin
      |--- System
           |--- Features
                |--- Configuration
                     |--- General
                          |--- Selected Dial Action on Calls
```

Renaming or resetting the name of a key

This parameter is available on all program keys.

Administration via WBM

1. Open System > Features > Program keys (or "Key module x").
2. Select the key and click "Edit".



The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

> Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

SELECTED DIALLING

On key press, a predefined call number is called. The call number defined in the "Dial number" parameter is dialled on key press.

1. Open System > Features > Program keys.
2. Select the key assigned to "Selected dialling" and click "Edit".

The label displayed to the right of the key is defined in "Key label".

3. Use the field "Key label" to define or change the name (label) of the key.
4. Enter the phone number.
5. Click **Submit**.

> Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

REPEAT DIALLING ("REDIAL")

On key press, the call number that has been dialed lastly is dialled again.

Administration via WBM

1. Open System > Features > Permanent Favourites.
2. Select the key assigned to "Redial" and click "Edit".

The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

CALL FORWARDING (STANDARD)

This key function controls call forwarding. If forwarding is enabled, incoming calls to the predefined call number are forwarded, depending on the current situation.

Note To use phone based call forwarding, server features must be switched off (see "Call center agent" → page 149). This feature can be enabled or disabled under System > Features > Feature access (see "Feature access" → page 132).

Note If the SIP server type is set as "ZOOM", call forwarding is set for all lines (shared or private).

Administration via WBM

1. Open System > Features > Program keys.
2. Select the forwarding type. The forwarding type parameter determines the forwarding behaviour.
   - If "Unconditional" is selected, any incoming call is forwarded.
   - If "no reply" is set, the call is forwarded when the user has not answered within a specified time span.

     Note The time span is configured in the WBM user pages in User > Configuration > Incoming calls > Forwarding > No reply delay (seconds).

   - If "busy" is selected, incoming calls is forwarded when the phone is busy.
3. Select the key assigned to forwarding and click "Edit".
4. Use the Key label field to define or change the name (label) of the key.
5. Enter the phone number. If a phone number is not entered, the key indicates when the forwarding type is enabled regardless of the destination, and can enable or disable the forwarding type.
6. Click **Submit**.

Call forwarding by call type

This feature enhances the call forwarding (standard) operation by adding support for additional call forwarding settings explicitly for external and internal calls, as well as the existing capability to forward any call, using functional menus that extend the existing "Call Forwarding UI" (see "Call forwarding (standard)" → page 162).

Note To use extended call forwarding, "Server features" and "Allow uaCSTA" must be switched on (see "Call center agent" → page 149).

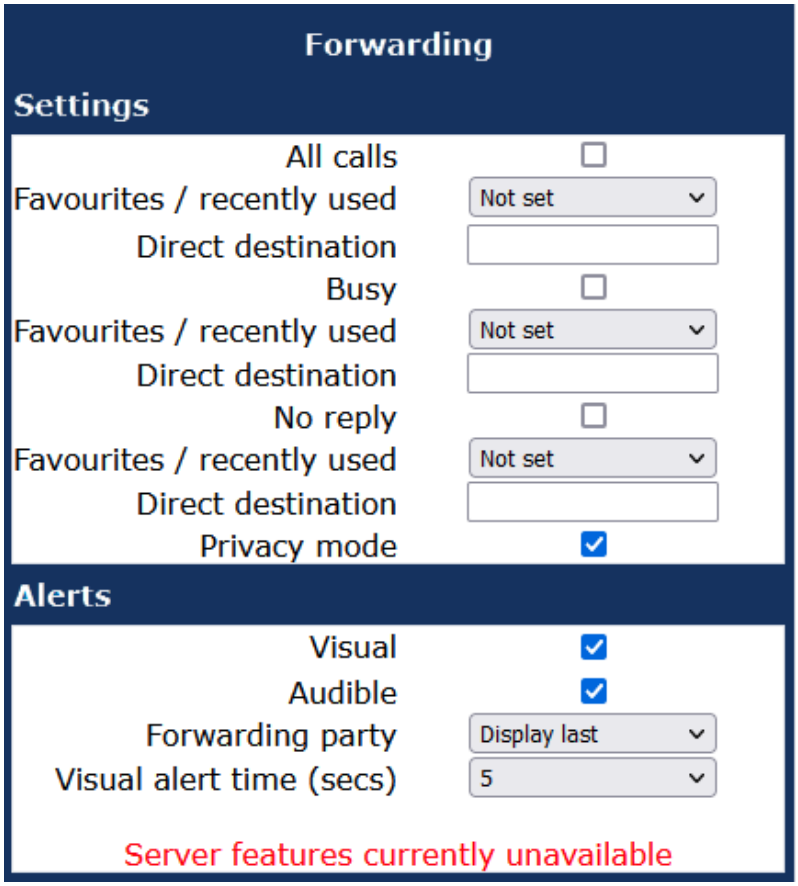
This feature can be enabled or disabled under System > Features > Feature access > Ext/int forwarding (see "Feature access" → page 132).

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to forwarding and click "Edit".
    - **Forwarding type**: Determines forwarding behaviour.
        - Value range: „CF Unconditional any", „CF no reply - any", „CF busy - any", „CF unconditional - ext.", „CF unconditional - int.", „CF no reply - ext.", „CF no reply - int.", „CF busy - ext.", „CF busy - int"
        - Default: „CF Unconditional any"
    - **Destination**: Destination number of call forwarding.

The label displayed to the left of the key is defined in key label. It is possible to have extra keys defined for each call forwarding type.

3. Open Configuration > Incoming calls > Forwarding.



RINGER OFF

Turns off the ring tone. Incoming calls are indicated via LEDs and display only.

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to "Ringer off" and click "Edit".

The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

> Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

HOLD

The call currently selected or active is put on hold. A held call can be retrieved by pressing the key a second time.

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to holding the call and click "Edit".

The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

> Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

ALTERNATE

Toggles between two calls; the currently active call is put on hold.

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to "Alternate" and click "Edit".

The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

BLIND CALL TRANSFER

A call is transferred without consultation, as soon as the phone goes on-hook or the target phone goes off-hook.

> **Note** This feature can be enabled or disabled under System > Features > Feature access (see "Feature access" → page 132).

Administration via WBM

1. System > Features > Program keys.
2. Select the key assigned to "Blind transfer" and click "Edit".

The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

> Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

TRANSFER CALL

Call transfer, applicable when there is one active call and one call on hold. The active call and the held call are connected to each other, while the phone that has initiated the transfer is disconnected.

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to transferring a call and click "Edit".

The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

> Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

DEFLECT A CALL

On key press, an incoming call is deflected to the specified destination.

> This feature can be enabled or disabled under System > Features > Feature access (see "Feature access" → page 132).

The target destination is defined in the Destination parameter.

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to deflecting a call and click "Edit".

The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

SHIFT LEVEL

Shift the level for the programmable keys. When activated, the functions assigned to the shifted level are available on the keys.

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to toggling between the key levels and click "Edit".

The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

> Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

CONFERENCE CALLS

Establishes a multi-party conference call, either as conference call from an active call, from a held call, or by adding a call to a server-based conference call.

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to starting a conference call and click "Edit".

The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

> Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

DO NOT DISTURB

If this feature is activated, incoming calls will not be indicated to the user.

> **Note** This feature can be enabled or disabled in System > Features > Feature access (see "Feature access" → page 132).

> **Note** DND is set for all lines (shared or private).

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to the feature "Do not disturb" and click "Edit".

The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

GROUP PICKUP

On CP phones connected to Zoom, group pickup is performed using BLF keys configured on the Zoom server:

- Group Pickup: *98 (example)
- Directed Pickup: *97 (example)

When a BLF key is pressed, the phone automatically sends the corresponding Zoom pickup code and answers the ringing call in the monitored pickup group.

> No additional local configuration on the phone is required. BLF keys are preconfigured by the administrator with the appropriate pickup codes and monitored extensions.

DIRECTED PICKUP

Directed pickup is performed using a Zoom pickup code (e.g., *97) assigned to a BLF/FPK. When the key is pressed, the phone sends this pickup code to pick up the call ringing at the user's extension being monitored by the BLF key.

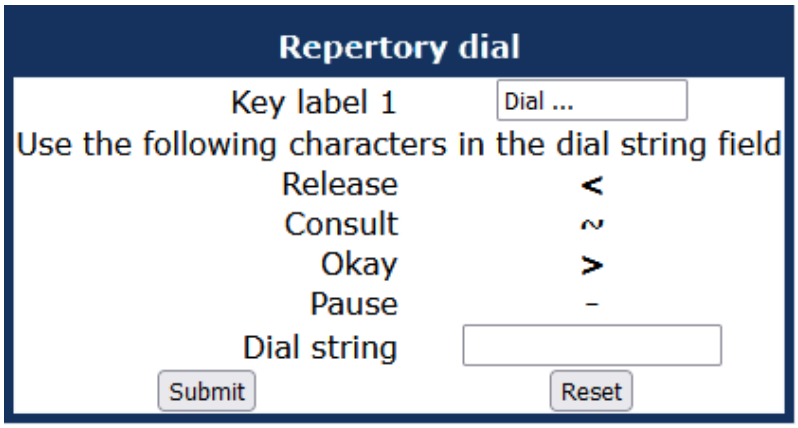
REPERTORY DIAL

This feature is similar to the selected dialing function, but additional special calling functions are possible. The desired number or function is selected via the “Dial string” parameter.

> **Note** This feature can be enabled or disabled under System > Features > Feature access (see "Feature access" → page 132).

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to “Repertory dial” and click “Edit”.



The following call functions are available:

- "<" disconnect a call.
- "~" start a consultation call.
  - Example "~3333>"
- ">" (preceded by a call number) start a call.
  - Example "3333>"
- "-" enter a pause, e. g. for exit-code or international dialing.
  - Example "0-011511234567>"

The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

CONSULTATION

When the phone is engaged in an active call, this function opens a dialing menu to make a consultation call.

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to consultation calls and click "Edit".

The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

> Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

CALL RECORDING

Starts or stops call recording.

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to call recording and click "Edit".

The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

> Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

AUTO ANSWER WITH ZIP TONE

This feature is primarily designed for call centers. If activated and a headset is used, the phone will automatically accept incoming calls without ringing and without the necessity to press a key.

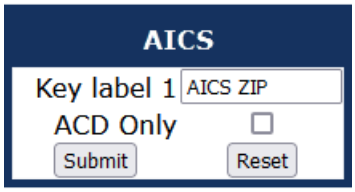
To indicate a new call to the user, a zip tone is played through the headset when the call is accepted.

> **Note** The feature is available for OpenScape Desk Phone CP phones that provide a headset jack; it only operates if the headset is plugged in.

If the key for feature activation has been pressed before the headset is connected, the feature is automatically activated when the headset is plugged in.

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to "AICS ZIP tone" and click "Edit".



3. Select "ACD Only" to automatically answer only calls from ACD systems.

The text field to the right of the key number defines the key label.

4. Define or change the display name (label) of the key.
5. Click **Submit**.

> Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

BLF KEY

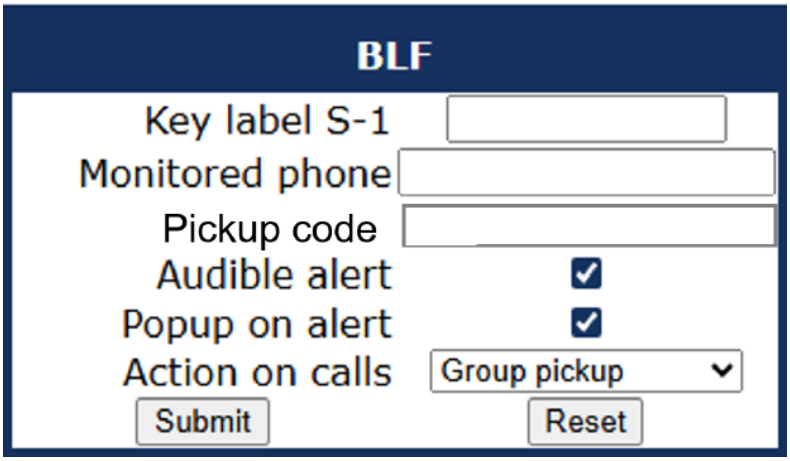
This function offers the possibility to monitor another extension, and to pick up calls for the monitored extension.

> **Note** This feature can be enabled or disabled under System > Features > Feature access (see "Feature access" → page 132).

> This function is intended primarily for operation with an Asterisk and Zoom SIP server. For details, refer to the Administration Manual for OpenScape Desk Phone CP on Asterisk.
> Broadsoft, RingCentral and Zoom are also supported.
> RingCentral supports also Call park keys independent of BLF.

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to "BLF" and click "Edit".



- **Key label**: Label for the key.
- **Monitored phone**: Internal phone number to be monitored for status changes.
- **Pickup code**: Required for **Group Pickup**. The system adds a pickup code prefix to the call pickup URI to enable the function.
  - **Group Pickup**The pickup code (e.g. ***98**) is added as a prefix to the configured Group Pickup URI. This allows the BLF key to monitor and pick up calls for any ringing extension within the group.
  - **Directed Pickup** The pickup code (e.g. ***97**) is added as a prefix to the URI of the target user. This allows the BLF key to monitor and pick up calls for a specific extension.
- **Auditable alert**: Determines whether an audible alert is played to indicate an incoming call for the monitored phone.
- **Popup on alert**: Determines whether an alert pop-up to indicate an incoming call for the monitored phone.
- **Action on calls**: RingCentral feature. The BLF key can be configured to perform a certain action when it is pressed during a call. The available options are:
  - **Transfer**: Configuration with **Transfer** allows the user to pass a call directly to another phone configured in the **BLF** menu (see "Blind call transfer" → page 165).
  - **Consult**: Configuration with **Consult** allows the user to to make a consultation call by pressing the BLF key during the call (see "Consultation" → page 169).
  - **Group Pickup**: When **Group Call Pickup** is used, group members receive an alert when a call is ringing on any other group member's device. Configuration with **Group Pickup** allows a group member to pickup a group call (see "Group pickup" → page 168).
  - **Group pickup ID** is configured as a BLF monitored phone (Group pickup ID - string used by Ring Central to address the appropriate pickup group, used in SIP Header). **Group name** is configured as BLF key label.

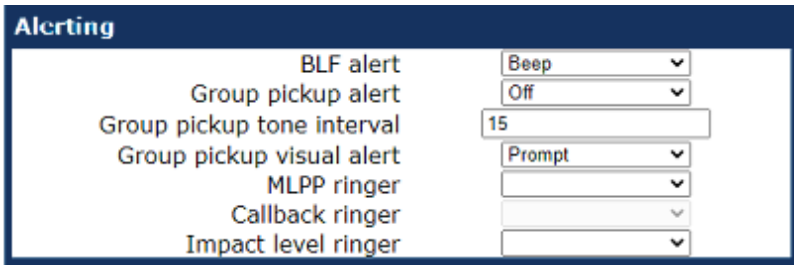
    Note User or extension can be a member of more than one group and each of them can be configured per specific key.

BLF alerting

Administration via WBM for RingCentral

The BLF key can be configured to enable audio notification when any of the monitored phones is ringing.

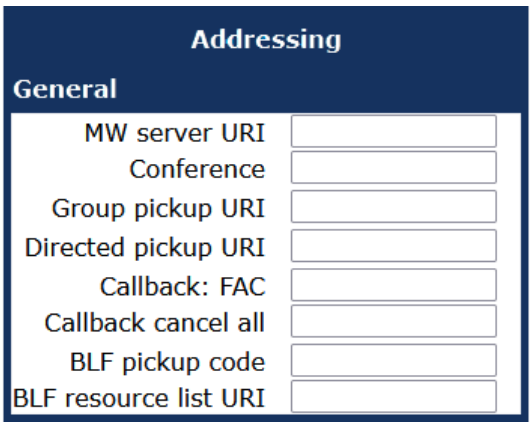
1. Open System > Features > Configuration > Alerting.



- **Beep**: phone plays a beep sound.
- **Ring burst**: phone plays ringer tone for a few seconds.
- **Ring continuous**: phone plays ringer tone whilst any of the monitored phones is ringing.

Administration via WBM

1. Open System > Features > Addressing.



2. Enter the URIs and additional information to add BLF items.

If a resource list URI is given, the phone subscribes to the given URI.

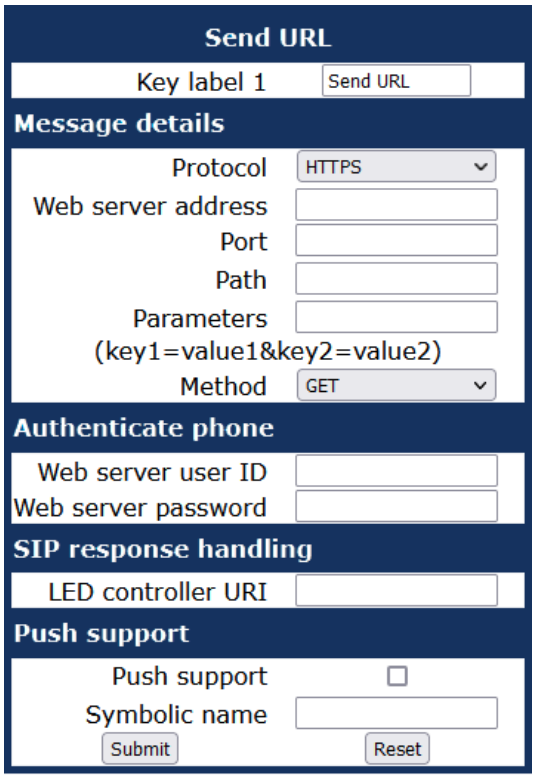
> Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

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 a HTTP or HTTPS request, e. g. login or logout for flexible working hours.

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to sending a URL and click "Edit".



- **Key label**: Label for the key.
- **Protocol**: Transfer protocol to be used. The Protocol parameter defines whether HTTP or HTTPS is used for sending the URL to the server.
  - Value range: "HTTP", "HTTPS"
- **Web server address**: IP address or DNS name of the remote server. The Web server address is the IP address or DNS name of the remote server to which the URL is sent.
- **Port**: Target port at the server. The Port is the target port at the server to which the URL is sent.
- **Path**: Server-side path to the function.The Path is the server-side path to the desired function, i. e. the part of the URL that follows the IP address or DNS name.
  - Example: `webpage/checkin.html`
- **Parameters**: Optional parameters to be sent to the server. 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`

Note 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.

- **Method**: HTTP method used for transfer. The Method parameter determines the HTTP method to be used, which can either be GET or POST. If GET is selected, the additional parameters (Parameters) and the user id/password (Web server user ID/Web server password) are part of the URL. If POST is selected, these data form the body of the message.
  - Value range: "GET", "POST"
- **Web server user ID**: User id for user authentication at the server. 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 server-side path (Path) and the additional parameters (Parameter).
- **Web server password**: Password for user authentication at the server.
- **LED controller URI**: Indicates the state of the call number specified. If the LED controller URI is given, the LED associated with this key indicates the state of the call number or SIP URI specified, provided the SIP server sends a notification:
  - **Busy notification**: LED is glowing.
  - **Ringing notification**: LED is blinking.
  - **Idle notification (state=terminated)**: LED is dark.
- **Push support** : Enables or disables LED control by push requests from the server. If the Push support parameter is activated, the LED is controllable by a combination of an HTTP push request and an XML document.
  For further information, see the XML Applications Developer's Guide.

Note To use the HTTP push solution, ensure that the LED controller URI field is empty. Otherwise, the phone will only use the SIP mechanism for LED control, and ignore the push request.

- **Symbolic name** : Assigns a push request to the appropriate free programmable key or the fixed function key. The Symbolic name is used to assign a push request from the application server to the appropriate free programmable key resp. fixed function key. This value must be unique for all keys involved.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

BUILT-IN FORWARDING

As a programmable key function, this is relevant for OpenScape Desk Phone CP100, CP200/205, CP110 and CP210, which have no fixed forwarding key.

Note On OpenScape Desk Phone CP110 / CP210 this is also available on 2nd level. For more information, see "Enable "Long Press" for FPKs on second level for CP210 Broadsoft " →1.

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to "Built-in forwarding" and click "Edit".

The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

DIRECTORIES

Note This feature is only available for OpenScape Desk Phone CP100, CP200/205, CP110 and CP210.

These key functions opens a menu which enables the user to start the personal or the corporate directory.

- For further information about the personal and corporate directories, refer to the user guides for OpenScape Desk Phone CP family.
- For information about the corporate directory, also refer to "Settings of the corporate directory" → page 224.

Administration via WBM

- For the personal directory, open System > Features > Program keys and select the key assigned to the personal directory.
- Click **Edit** to rename the label.
- For the corporate directory, open System > Features > Program keys and select the key assigned to the corporate directory.
- Click **Edit** to rename the label.

RELEASE

On pressing this key, the current call is disconnected.

Administration via WBM

1. Open System > Features > Program keys.
2. Select the key assigned to "Release" and click **Edit**.

The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

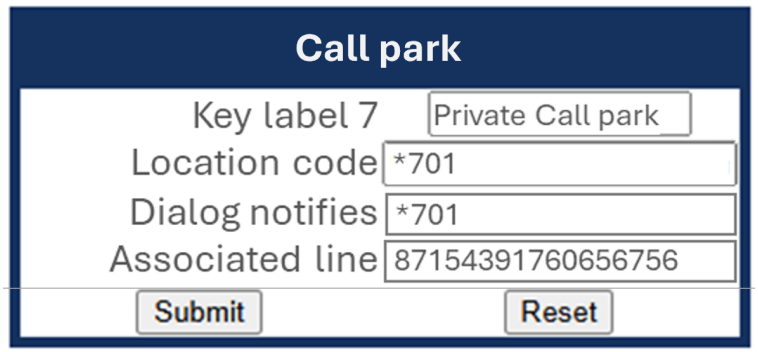
> Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

CALL PARKING

Zoom supports three types of call park: **Public**, **Private**, and **AIM** (Agent-In-Monitoring). Each type determines how calls are parked and retrieved, who can see or retrieve them, and what level of visibility they have.

Administration via WBM

1. Open System > Features > Permanent Favourites (or any **Key module x** page)



- **Location code**: The Zoom call park location, e.g. *844.
- **Dialog notifies**: The phone sends a SIP SUBSCRIBE to this URI for dialog notifications.
- **Associated line**: Identifies the line on this phone to use when retrieving a call parked at this location.

> **Note** The **Associated line** parameter only appears for private call park.

For details about Zoom call parking features and functionality, refer to Zoom's documentation.

Fixed function keys

> This feature is avilable for OpenScape Desk Phone CP100, CP200/205, CP110 and CP210.

The OpenScape Desk Phone CP110 comes with three keys, which can be reprogrammed with specific functions. The preset is:

- Call log
- Directory
- Built-in forwarding

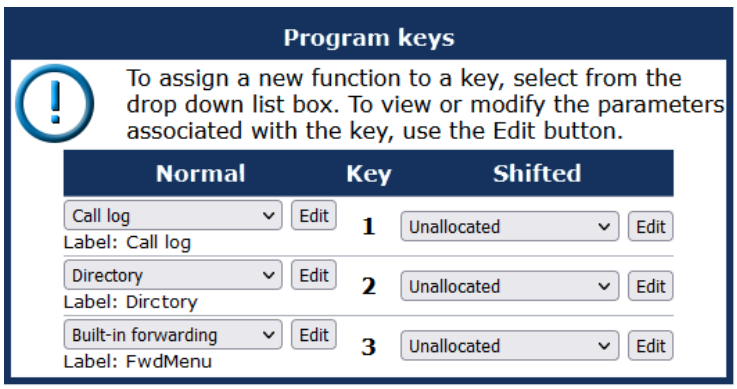
The OpenScape Desk Phone CP210 comes with four keys, which can be reprogrammed with specific functions. The preset is:

- Call log
- Directory
- Built-in forwarding
- Redial

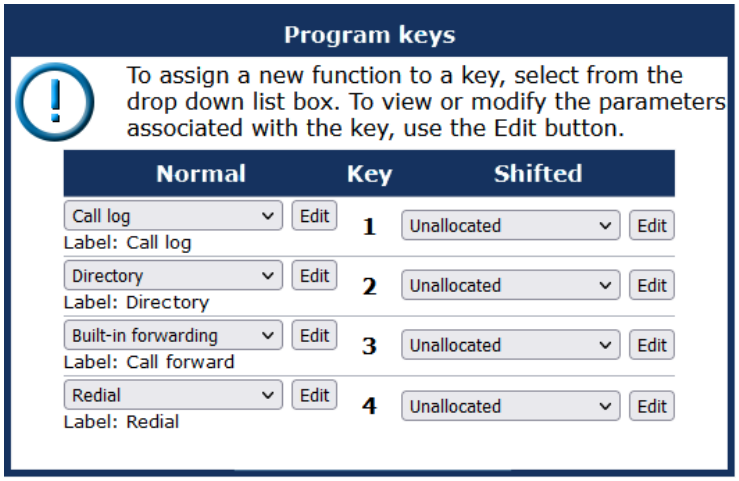
When resetting the phone, these keys are reset to the default factory settings.

Administration via WBM

1. Open System > Features > Program keys.
    - On an OpenScape Desk Phone CP110, three keys can be configured.



- On an OpenScape Desk Phone CP210, four keys can be configured.



2. To assign a new function to a key, select a function from the drop down list.
3. To view or modify the parameters associated with the key, click **Edit**.
4. Click **Submit**.

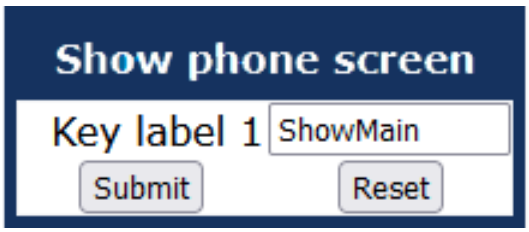
SHOW PHONE SCREEN

> **Note** This feature is only available for OpenScape Desk Phone CP100, CP200/205, CP110 and CP210.

On pressing this key, the phone display switches to call view mode.

Administration via WBM

1. Open System > Features > Program keys.
2. Select Show phone screen and click **Edit**.



The text field to the right of the key number defines the key label.

3. Define or change the display name (label) of the key.
4. Click **Submit**.

> Free Programmable Keys (FPKs) can be configured via the WBM or on the local phone. For details regarding the different ways to configure program keys, refer to "How to configure free programmable keys" → page 157.

Main menu screen options

Note This feature is only available for OpenScape Desk Phone CP700, CP700X, CP600, CP400, CP410 and CP710.

The OpenScape Desk Phone CP410 and CP710 main menu includes fixed functions and additional options depending on the configured server type.

When the phone is connected to a Zoom server, the main menu includes the following fixed options:

- Favourites
- Directory
- Call log
- Voicemail
- Pickup
- Corporate (added by Zoom)

  Users can scroll to Settings and Conversations using the navigation keys.

Note The menu layout is automatically extended based on the Zoom server configuration.

Main menu option configuration

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

On Zoom-connected CPx10 phones, the main menu displays all available menu entries, which can be accessed and scrolled via soft keys. The following entries are available by default:

Standard Menu	Extended Menu
Favourites	Favourites
Conversations	Conversations
Voicemail	Voicemail
Settings	Settings
	Corporate

Note Some menu entries, such as Conversations or Settings, may be hidden depending on administrator configuration. All entries are soft key–accessible and scrollable. There are no fixed-function entries on the main menu.

The Corporate option is added by Zoom and provides access to any corporate-specific features configured via the Zoom server.

Multi-line appearance

Server type must be set to Zoom. The phone automatically registers to the Zoom server.

On Zoom-connected CPx10 phones, each line can have up to three simultaneous appearances. Each appearance represents the same line but allows handling of a separate call at the same time. This setup helps users manage multiple calls efficiently without interfering with ongoing conversations.

- Only one call per line appearance can be active (off-hook) at any given moment.
- Line keys for each appearance are automatically configured by the Zoom server and display the current call status.
- Menu entries and soft keys reflect the status of each line appearance individually.

Multi-line functionality allows shared lines and delegation scenarios (calls may be answered by multiple users or devices).

All behavior for line appearances, including automatic line selection and BLF indicators, is controlled by the Zoom server.

LINE KEY CONFIGURATION

Note It is recommended to configure primary lines only on keys 1 to 6, or 1 to 5, if a shift key is needed. This ensures that the lines are still accessible when the user migrates to a different phone with fewer keys via the mobility feature.

A line corresponds to a SIP address of record (AoR), i.e. a phone number. It is defined by the address parameter. For registration of the line, a corresponding entry must exist on the SIP server, or the SIP registrar server.

A label can be assigned to the line key by setting its key label.

Every keyset must necessarily have an accessible line key for the primary line. To configure the key of the primary line, set Primary line to "true".

If "Ring on" is enabled, the line will ring when an incoming call occurs, and a pop-up window is displayed on the display. If the option is disabled, the incoming call is indicated only by the blinking of the key's LED. If it is desired that the line rings with a delay, the time interval in seconds can be configured by "Ring delay".

When the user lifts the handset to initiate a call, the line to be used is determined by selection rules. For Zoom-connected phones, the next free line appearance is automatically selected. Each line may have up to three appearances on Zoom.

To each line, a priority is assigned by the "Selection order" parameter. A line with the rank 1 is the first line to be considered for use. If more than one line have the same rank, the selection is made according to the key number. Note that "Selection order" is a mandatory setting; it is also relevant to the "Terminating line" setting, as well as to other functions.

Note For the configuration of line keys, the use of the DLS (Deployment Service)/DMS is recommended. For operating the DLS, please refer to the DLS user's guide. For operating DMS, refer to Wiki page http://wiki.unify.com/wiki/Broadsoft_DMS. Alternatively, the web interface or the local menu can be used. Note that the creation of a new line key and the configuration of some parameters can not be accomplished by the phone's local menu.
Generally, it is advisable to restrict the user's possibilities to modify line keys. This can be achieved solely by the DLS. For further instructions, see the DLS Administration Guide.

The Realm, a protection domain used for authenticated access to the SIP server, works as a name space. Any combination of user id and password is meaningful only within the realm it is assigned to. The other parameters necessary for authenticated access are User Identifier and Password. For all three parameters, there must be corresponding entries on the SIP server.

The Shared type parameter determines whether the line is a shared line, i. e. shared with other endpoints, or a private line, i .e. available exclusively for this endpoint. A line that is configured as primary line on one phone can be configured as secondary line on other phones.

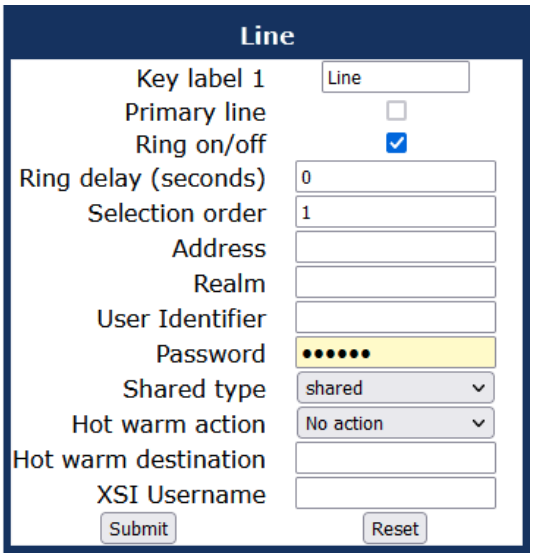
Note Shared lines are not available if System > Registration > Server type is set to "HiQ8000" (see "SIP registration" → page 103).

If a line is configured as hot line, the number indicated in Hot warm destination is dialed immediately when the user goes off-hook for that line. This number is configured in the user menu under **Configuration > Keyset > Lines > Hot/warm destination**. To create a hot line, Hot warm action must be set to "hot line". If set to "Warm phone", the specified destination number is dialed after a delay which is defined in Initial digit timer (seconds) (see "Initial digit timer" → page 137).

During the delay period, it is possible for the user to dial a different number which is used instead of the hot / warm line destination. In addition, the user is provided with a dial tone during the delay period. With the setting "No action", the line key will not have hot line or warm line functionality.

Administration via WBM

1. Open System > Features > Key module x.
2. Select the key assigned to a line and click "Edit".



- **Key label**: Set the label of the line key with the key number "n". Default: "Line"
- **Primary line**: Determines whether the line is the primary line. Value range: "Yes", "No" Default: "No"
- **Ring on/off**: Determines whether the line rings on an incoming call. Value range: "On", "Off" Default: "On"
- **Ring delay (seconds)**: Time interval in seconds after which the line starts ringing on an incoming call. Default: 0
- **Selection order**: Priority assigned to the line for the selection of an outgoing line. Default: 0
- **Address**: Address/phone number which has a corresponding entry on the SIP server-/registrar.
- **Realm**: Domain wherein user id and password are valid.
- **User Identifier**: User name for authentication with the SIP server.
- **Password**: Password for authentication with the SIP server.
- **Shared type**: Determines whether the line is a shared line (shared by multiple endpoints) or a private line (only available for this endpoint). Value range: "shared", "private", "unknown". Default: "shared"
- **Hot warm action** : Determines if the line is a regular line, a hot line, or a warm line. Value range: "No action", "hot line", "warm line"
- **Hot warm destination** : The destination to be dialed from the hot/warm line when the user goes off-hook.
- **XSI Username**: The XSI user name that is related to the configured line key on the tele-phone.

Zoom-specific line settings:

- **Privacy Mode**: Can be enabled to prevent call monitoring on shared lines.
- **Caller ID**: Allows per-line configuration of displayed caller ID for outgoing calls.
- **BLF / Busy Lamp Monitoring (BMW)**: Supports monitoring the status of other extensions or line appearances.
- **Shared Call Appearance (SCA)**: Zoom supports up to 3 simultaneous appearances per line; each appearance can be configured on a key.

For Shared Call Appearance refer to the Shared_call_appearance Wiki page.

> **Note** A new line key can only be added by use of the WBM or the DLS / DMS. Once a line key exists, it can also be configured by the local menu.

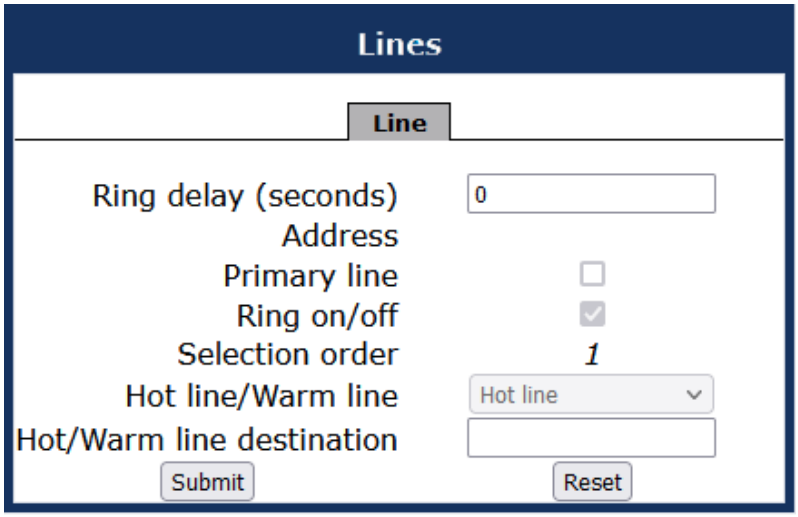
CONFIGURING LINE KEYS FOR KEYSET OPERATION

For Zoom-connected CP phones, additional line-specific features such as Privacy Mode, Caller ID, BLF / Busy Lamp Monitoring (BMW), and Shared Call Appearance (up to 3 simultaneous appearances per line) can also be configured. These settings may be managed via the Zoom web portal, Web interface (WBM), DLS/DMS, or by assigning BLF keys for each line appearance. Local phone configuration is only available if the line key was previously created via WBM or DLS.

Administration via WBM

1. Open System > Features > Configuration > Keyset lines.
2. Select the key assigned to a line and click "Edit".
3. In the Line dialog, set the specific parameters for the line key (see "Line key configuration" → page 181).

4. If hot line / warm line is configured, open User settings > Configuration.



Administration via local phone

> **Note** The configuration of a line via local phone is only possible when the line key has been created via Web interface or DLS before.

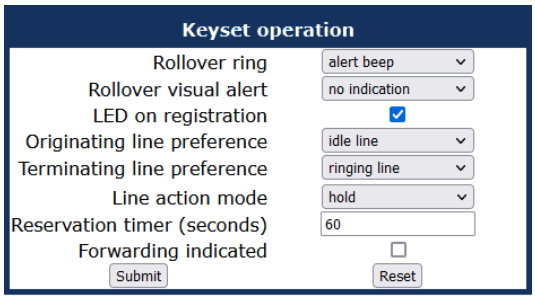
```
|--- Admin
    |--- System
        |--- Features
            |--- Configuration
                |--- Keyset lines
                    |--- Details For Keyset Line xx
                        |--- Address
                        |--- Ring on/off
                        |--- Selection order
                        |--- Hot/warm action
```

CONFIGURE KEYSET OPERATION

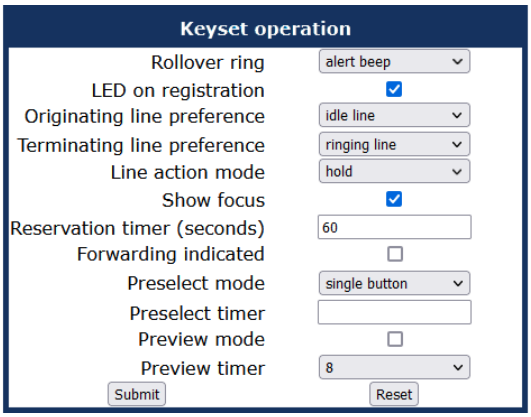
The following parameters provide general settings which are common for all keyset lines.

Administration via WBM

1. Open System > Features > Keyset operation (CP410 / CP710).



2. Open System > Features > Keyset operation (CP110 / CP210).



- **Rollover ring**: Determines if a ring tone will signal an incoming call while a call is active. The setting is used when, during an active call, an incoming call arrives on a different line. If "no ring" is selected, the incoming call will not initiate a ring. If "alert ring" is selected, a 3 seconds burst of the configured ring tone is activated on an incoming call; "alert beep" selects a beep instead of a ring tone. "Standard ring tone" selects the default ringer.
  - Value range: "Standard ring", "No ring", "Alert beep", "Alert ring"
  - Default: "Alert beep"
- **LED on registration**: Determines if line LEDs will signal SIP registration. The parameter determines whether the line LEDs is lit for a few seconds if they have been registered successfully with the SIP server on phone start-up.
  - Value range: "Yes", "No"
  - Default: "Yes"
- **Originating line preference**: Selects the line to be used for outgoing calls. The parameter determines which line is used when the user goes off-hook or starts on-hook dialing. When a terminating call exists, the terminating line preference takes priority over originating line preference.
  - Value range:
    - **"idle line"**: An idle line is selected. The selection is based on the Hunt ranking parameter assigned to each line (see "Line key configuration" → page 181).
    - **"primary"**: The designated Primary Line / Main DN is always selected for originating calls.
    - **"last"**: The line selected for originating calls is the line that has been used for the last call (originating or terminating).

    - **"none"**: The user manually selects a line by pressing its line key before going off-hook or by pressing the speaker key, to originate a call.
  - Default: "Idle line"
- **Terminating line preference**: Determines which line with an incoming call shall be selected for answering.
  - Value range: "Ringing line", "Incoming", "Incoming PLP", "Ringing PLP", "None"
  - Default: "Idle line"
- **Line action mode**: Determines the consequence for an established connection when the line key is pressed. Line action mode determines the consequence for an established connection when the line key is pressed. If "hold" is selected, the call currently active is set to hold as soon as the line key is activated. The user has two options: 1) to reconnect to the remote phone by pressing the line key that corresponds to that call, or 2) to initiate another call from the newly selected line. If "release" is selected, the previously established call is ended.
  - Value range: "Hold", "Release"
  - Default: "Hold"
- **Show focus** (only CP110 / CP210): Determines whether the line key LED blinks or is steady when it is in use. If Show focus is checked, the LED of a line key flutters when the line is in use. If it is not checked, the line key is lit steady when it is in use.
  - Value range: "Yes", "No"
  - Default: "Yes"
- **Reservation timer**: Sets the period in seconds after which a line reservation is cancelled. If set to 0, the reservation timer is deactivated. The Reservation timer sets the period after which the reservation of a line is canceled. A line is automatically reserved for the keyset whenever the user has selected a line for an outgoing call and hears a dial tone. The reservation of a line is accomplished by the OpenScape Desk Phone CP110/210/410 server, which notifies all the endpoints sharing this line.
  - If set to 0, the reservation timer is deactivated.
  - Default: 60
- **Forward indication**: Activates or deactivates the indication of station forwarding. Forward indication activates or deactivates the indication of station forwarding, i. e. the forwarding function of OpenScape Desk Phone CP110 / 210 / 410. If "Forward indication" is activated and station forwarding is active for the corresponding line, the LED of the line key blinks.
  - Value range: "Yes", "No"
  - Default: "No"
- **Preselect mode** (only CP110 / CP210): Determines whether an incoming call is accepted by a single press on the corresponding line key or a double press is needed. Preselect mode determines the phone's behaviour when a call is active, and another call is ringing. If the parameter is set to "Single button", the user can accept the call a single press on the line key. If it is set to "Preselection", the user must first press the line key to select it and then press it a second time to accept the call. In both cases, the options for a ringing call are presented to the user: "Accept", "Reject", "Deflect".
  - Value range: "Single button", "Preselection"
  - Default: "Single button"
- **Preselect timer** (only CP110 / CP210): Sets the timeout in seconds for accepting an incoming call. Preselect timer is relevant if Preselect mode is set to "Preselection". The parameter

sets the timeout in seconds for the second key press that is required to accept the call. After the timeout has expired, the call is no longer available.

Administration via local phone (CP110 / CP210)

```
|--- Admin
     |--- System
          |--- Features
               |--- Keyset operation
                    |--- Rollover rin
                    |--- LED on registration
                    |--- Orig line pref
                    |--- Term line pref
                    |--- Line action mode
                    |--- Show focus
                    |--- Reservation timer
                    |--- Forward
                    |--- Preselect mode
                         |---  Preselect timer
```

Administration via local phone (CP410 / CP710)

```
|--- Admin
     |--- System
          |--- Features
               |--- Keyset operation
                    |--- Rollover ring
                    |--- Rollover visual alert
                    |--- LED on registration
                    |--- Orig line pref
                    |--- Term line pref
                    |--- Line action mode
                    |--- Reservation timer
                    |--- Forward indicated
```

Bridging

> Admins do not need to enable bridging or assign line keys locally. All configuration is handled via Zoom’s portal and provisioning templates.

When the SIP server type is set to ZOOM, the Zoom server manages all line-specific bridging and BLF/BMW behavior. The local admin cannot configure these modes on the phone.

- Each shared line is configured by the Zoom server to define which interaction modes are permitted for users.
- Users may interact with calls on a shared line according to the permissions set by the Zoom administrator:

- Monitor: Silently listen to the call on the shared line.
- Whisper: Speak to the local user on the shared line without the remote party hearing.
- Barge-in: Join the existing call and create a conference.
- Takeover: Replace the current user on the shared line.

- Interaction modes (Monitor, Whisper, Barge-in, Takeover) are automatically enforced by the Zoom server.

DISTINCTIVE RINGERS PER KEYSET LINES

For implicit mapping of line ringer names following format must be used:

"Line-DN of line-Reserved"

Thus for a line with DN=1234 the mapped distinctive ringer name is "Line-1234-Reserved". (The name is case-sensitive, mind the uppercase L and R in name.)

The name needs to be manually constructed and configured by the administrator as a new ringer name and each such name should be manually checked as being unique in the table.

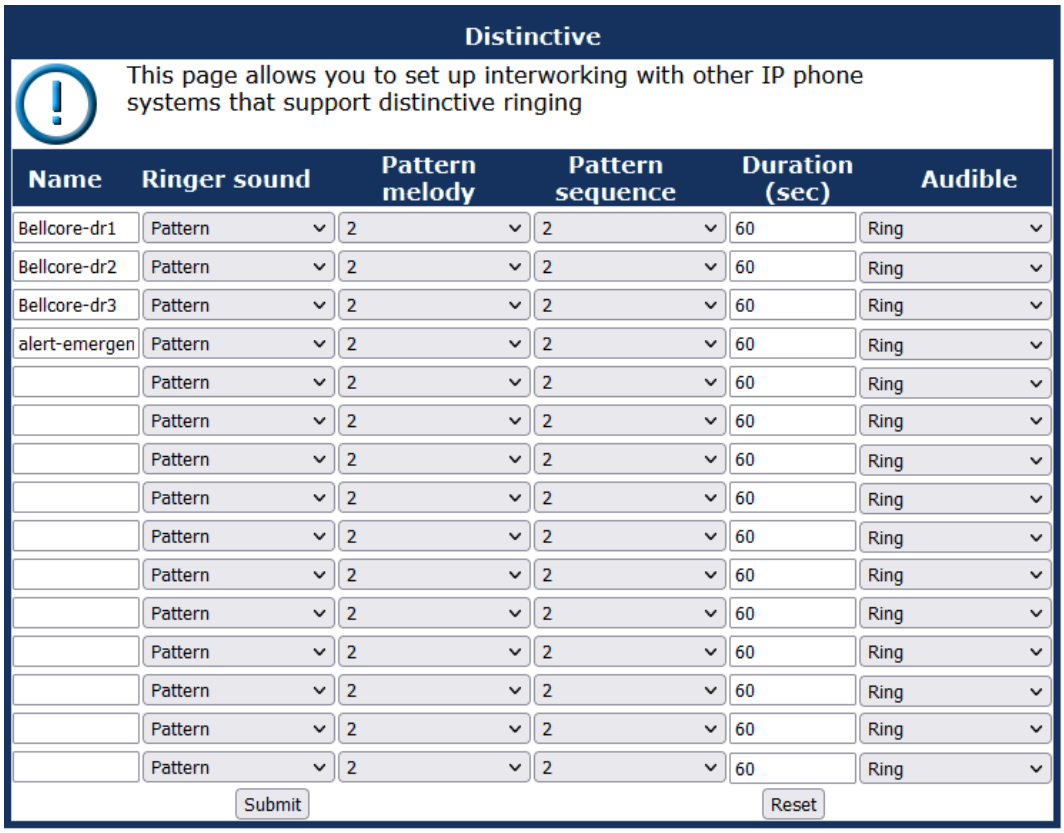
Note When using “Distinctive Ringers per Keyset Lines”, it is not allowed to define “bellcore_dr1”, “bellcore_dr2”, and “bellcore_dr3” in the same distinctive ringer table. Otherwise these settings is used because of higher priority in SIP-INVITE header. MLPP and Lowel Impact Level calls are also with higher priority.

The "User > Configuration > Keyset > Lines" form has the “Destination Number” of the line being configured and this can be used to map directly to distinctive ringer names in the "Admin>Ringer setting" form. If a distinctive ringer with a matching name has not been configured into the table then the ringer related items “Ringer”, “Ringer tone melody”, and “Ringer sequence” in the "User > Configuration > Keyset > Lines" form is absent. If a matching distinctive ringer name is found then the "Ringer" items are editable with the initially shown value being the same as the value in the "Admin>Ringer setting" form. Changes made to the "Ringer" values by the user will also change the matching distinctive ringer values in "Admin>Ringer setting".

Note Destinctive ringers are not applicable for DSS Keys.

Administration via WBM

1. Open Admin > Ringer setting > Distinctive.



- **Name**: Destinctive ringer name .
  - Value Range: "Line-Destination Number of line-Reserved"
- **Ringer sound**: Specifies whether pattern, i. e. melody, or a specific sound file is used as ringer.
  - Default: 'Pattern'
- **Pattern melody**: Determines the melody pattern if Ringer sound is set to 'Pattern'.
  - Value Range: 1,...,8
- **Pattern sequence**: Determines the length and repetitions of pattern.
  - Value Range: "1":1 sec ON, 4 sec OFF, "2": 1 sec ON, 2 sec OFF "3": 0.7 sec ON, 0.7 sec OFF, 0.7 sec ON, 3 sec OFF
  - Default: "1"

Administration via local phone

```
|--- Admin
    |--- Ringer setting
        |--- Distinctive
            |--- 1 .... 15
                |---  Name
                |--- Ringer sound (= Ringer in UserMenu)
                |--- Pattern melody (= Ringer melody in UserMenu)
                |--- Pattern sequence (= Ringer tone sequence in User Menu)
                |--- Duration
                |--- Audible
```

MULTIPLE CALL ARRANGEMENT

Multiple Call Arrangement (MCA) is a BroadWorks feature that allows for multiple calls to be originated concurrently from the same shared line. Hence, a second endpoint may place an outgoing call on the same shared line already in use by another endpoint. To achieve a non-blocking configuration for a group of endpoints sharing a line (meaning that all endpoints in that group can always place an outgoing call) every endpoint in that group must have as many shared line keys provisioned as there are endpoints in the group.

Administration via WBM

Example: Three lines need to be configured for a user. For the first line, use the Key 1 and choose Edit.

> **Note** The primary line should be checked out only for the first line. The selection order must be growing. For all lines, the address must have the same phone number.

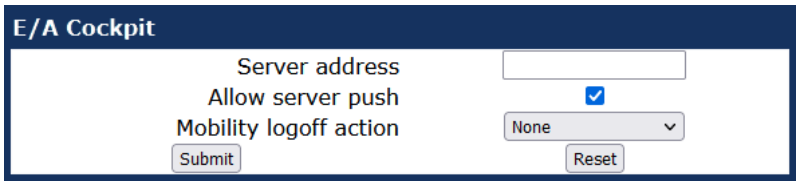
1. Open System > Features > Key module.
2. Select the key assigned to a line and click "Edit".
3. Configure the line key (see "Line key configuration" → page 181).
4. Set up multiple lines accordingly.
5. Click **Submit**.

E/A COCKPIT SETTINGS

To allow access to the integrated E/A cockpit application, the administrator needs to configure the server address and port.

Administration via WBM

1. Open System > Registration > E/A Cockpit.



- The phone will only allow secure connections to the server provided. The default port to access the server is 8443, if no port is configured in the server address field. The phone will try to verify the given data and will allow the access to the integrated E/A cockpit application via the main menu screen if a valid host address (IP or FQDN) is given.
  - **myserver.com** : 8443
- If "Allow server push" is enabled, it allows the E/A Cockpit application to start up on server push requests.

Supported formats:

- Format for HTTP: "http://Server-IP/DN:Server port"
  - IP address or FQDN: e.g. http://172.25.8.67 or fqdn.tld
  - IP address/FQDN + port: e.g. http://172.25.8.67:8443 or fqdn.tld:8443
- • Format for HTTPS: "Server-IP/DN:Server port"
  - IP address or FQDN: e.g. https://172.25.8.67 or fqdn.tld
  - IP address/FQDN + port: e.g. https://172.25.8.67:8443 or fqdn.tld:8443

Note A single E/A cockpit group can consist of a maximum number of four executives and four assistants.

Key modules

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

Note CP410, and CP710 phones can host either the KM710 or the KM410, but not both at the same time.

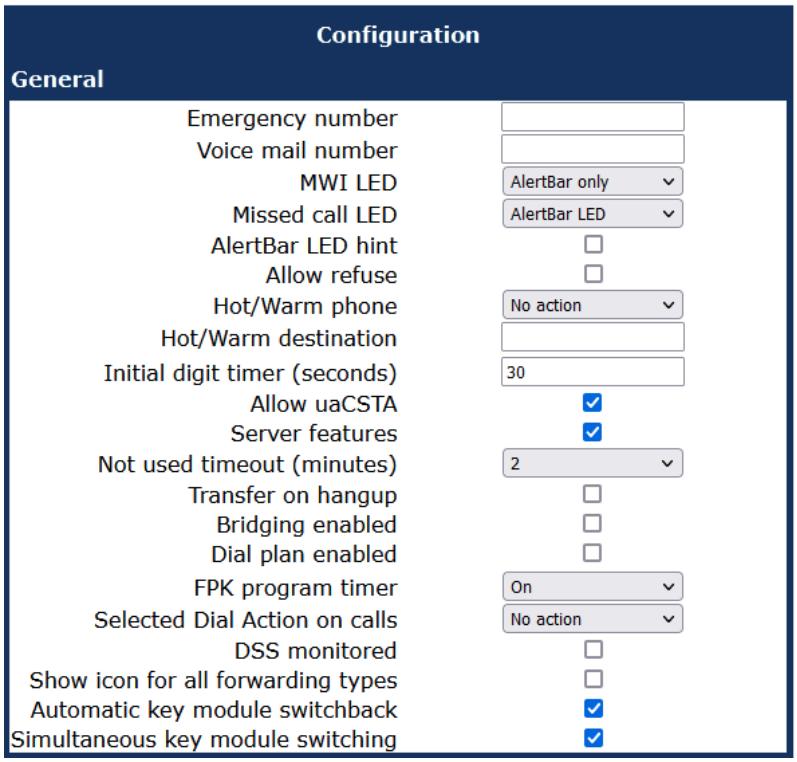
- On an OpenScape Desk Phone CP410 phone the key module KM410 provides 16 additional free programmable keys. The names of the assigned keys can be printed on labels.
- On an OpenScape Desk Phone CP710 the key module KM710 provides 12 additional free programmable keys. The names of the assigned keys are 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.



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**.

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

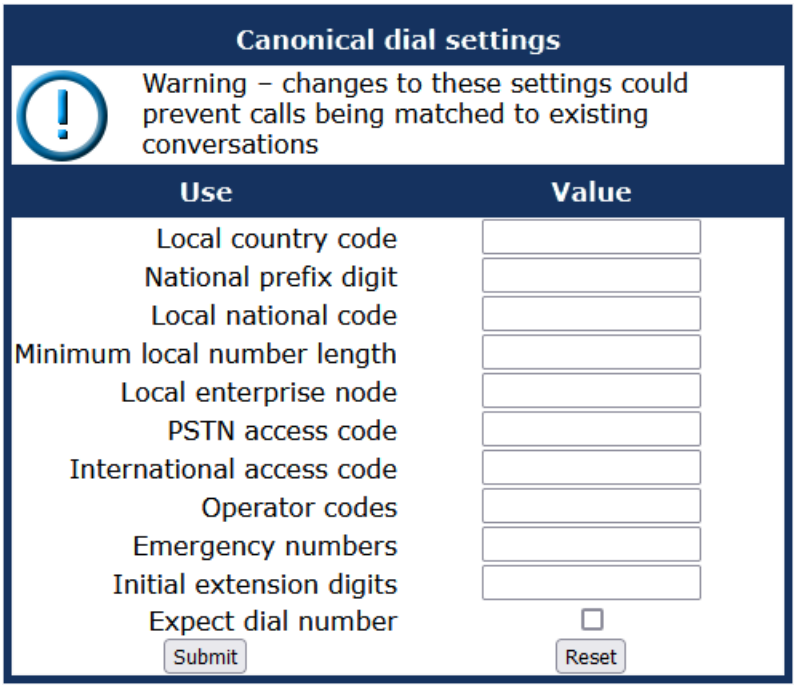
The user enters the extension "1234", the local country code is "49", the local national code is "89", and the local enterprise number is "722". The resulting number in canonical format is "+49897221234".

> **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 260).
> 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**.

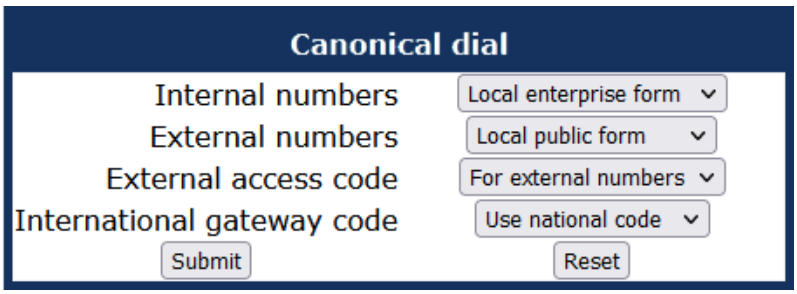


- **Local country code**: E.164-type country code, e.g. "49" for Germany, "44" for United Kingdom
  - Maximum length: 5
- **National prefix digit**: prefix for national connections, e.g. "0" in Germany and United Kingdom
  - Maximum length: 5
- **Local national code**: local area code or city code, e.g. "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 260).

  - **"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(iona)l 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 194). 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.

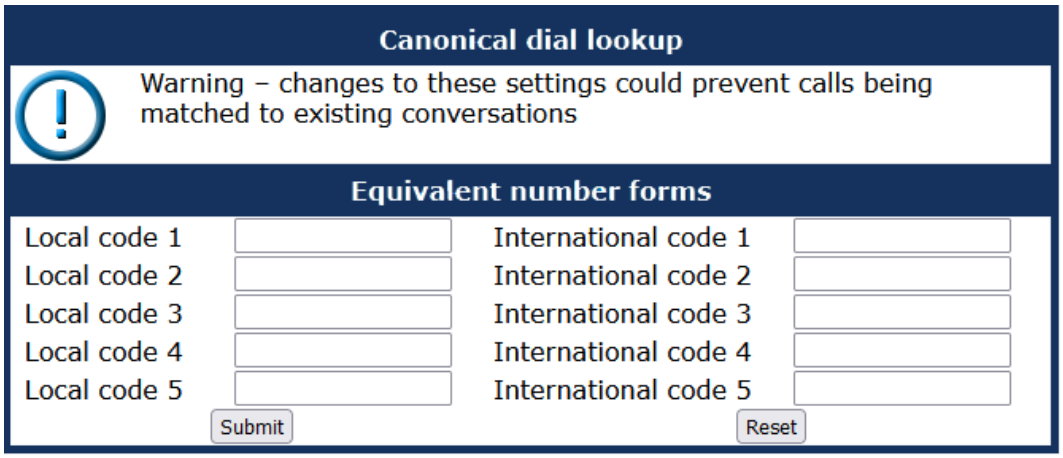
Note To make sure that canonical dial look-up works properly, at least the following parameters of the phone must be provided:

- 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.



- **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
```

CONFIGURING LOCATION DISCOVERY AND EMERGENCY CALLING

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

When connected to Zoom, the CPx10 phone automatically keeps the Zoom server informed of the local network identity. The location discovery process is fully automatic. No additional configuration is required from the administrator.

The location discovery process is automatic. No additional configuration is required from the phone administrator.

The phone automatically:

- Detects and reports network information (SSID for Wi-Fi, LLDP data for Ethernet).
- Sends location data to the Zoom server via SIP REGISTER messages.
- Updates location information when the phone moves to different network locations.

Note Administrators should ensure that LLDP is enabled on network switches if using Ethernet connections for optimal location accuracy.

DIAL PLAN

OpenScape Desk Phone CP phones may optionally use a dial plan residing on the phone. By means of the dial plan, the phone can infer from the digits entered by the user that a complete call number has been entered, or that a particular prefix has been entered. Thus, the dialing process can start without the need to confirm after the last digit has been entered, without delay or with a configurable delay.

> **Note** The standard timer found on the WBM in User menu > Configuration > Outgoing calls > Autodial delay (seconds), is overridden if a dial plan rule is matched.

A dial plan consists of rules defining patterns, timeouts and actions to be performed when a pattern is matched or a timeout has expired. The phone can store one dial plan, which can contain up to 48 different rules.

It is very important that the phone's dial plan does not interfere with the dial plan in the SIP server, PBX, or public network.

The dial plan can be created and uploaded to the phone using the DLS (please refer to the Deployment Service Administration Manual). The DLS can also export and import dial plans as *.csv file. For details about the composition of a dial plan, refer to "Example dial plan" → page 270.

> The current dial plan, along with its status and error status can be displayed on the WBM via Diagnostics > Fault trace configuration > Download dial plan file.

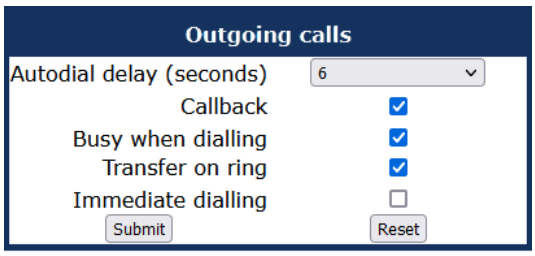
The Dial plan ID and the Dial plan status is displayed in the local menu.

To make use of the dial plan facility, the following requirements must be met:

- A correct dial plan is loaded to the phone.
- In the user menu, Allow immediate dialing is enabled. This condition is only necessary for on-hook dialing, but not for off-hook dialing.
- Dial plan enabled is checked.

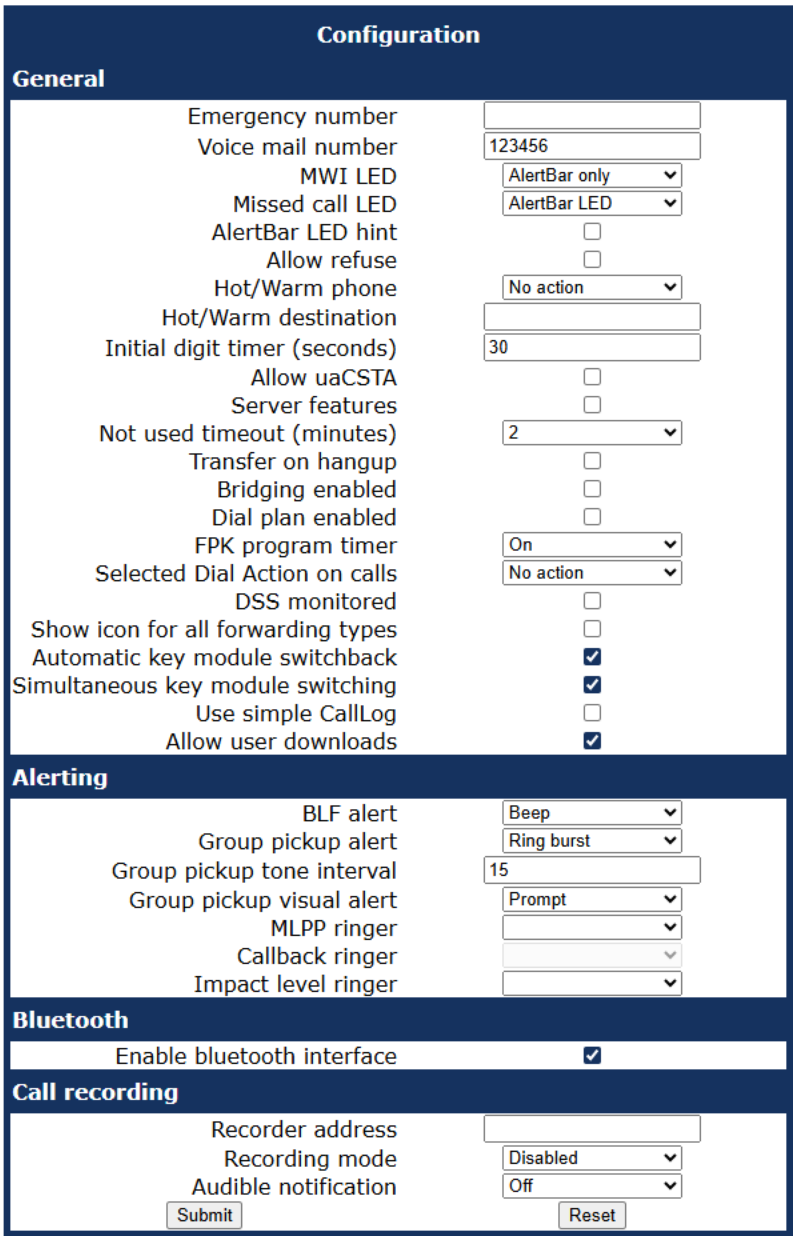
Administration via WBM

1. Open User settings > Configuration > Outgoing calls.



2. Enable "Allow immediate dialing" and click **Submit**.

3. Open Administrator settings > System > Features > Configuration.



4. Activate "Dial plan enabled".

Administration via local phone

```
|--- User
      |--- Configuration
            |--- Outgoing calls
                  |--- Immediate dialing
|--- Admin
      |--- System
            |--- Features
                  |--- Configuration
                        |--- General
                              |--- Dial plan
|--- Admin
      |--- General Information
            |---  Dial plan ID
            |--- Dial plan status
```

Ringer setting

MAP TO SPECIALS

“Map to specials” allows the administrator to create a mapping between predefined special call types and the distinctive ringer name string. Only the special ringers for the default types is shown in the local menu and WBM.

If a default ringer name is not configured in the "Distinctive ringer table" the mapped entry in the "Special ringer table" is greyed and read-only.

“Map to specials” configures the distinctive ringer names for a special ringer type. The user has access to configure a different audio file or pattern for this distinctive ringer via their "Special ringer table". Any change made by the user to this special ringer is reflected in the "Distinctive ringer table" and any change made by the administrator in the "Distinctive ringer table" is reflected in the "Special ringer table".

Administration via WBM

1. Open Ringer setting > Map To Specials.

2. Map the special ringers.
3. Click **Submit**.

SPECIAL RINGERS

The "Special ringers" dialog allows the user to change the ring tones for the special call types listed below, provided that the call type is signaled to the phone. Special ringers can be configured via the user menu for the following call types:

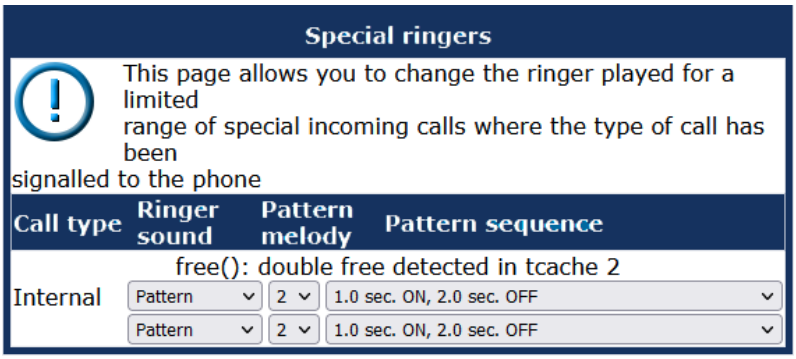
- Internal
- External
- Recall
- Special1
- Special2
- Special3

To make the special ringers available and configurable to the user, the administrator needs to map the call types to specific ringers via the Ringer setting mapping table in "Admin > Ringer setting > Distinctive". Each call type can be mapped to a specific ringer sound, pattern melody, and pattern sequence.

Note The user cannot change the ringer sound, pattern melody and pattern sequence of emergency call types. This can be set only by an administrator. Emergency ringer is always played (regardless of ringer settings) at maximum volume.

Administration via WBM

1. Open User settings > Audio > Special ringers.



For each call type, except emergency calls, the following parameters can be configured:

- The ringer sound parameter determines whether a pattern, i. e. melody, or a specific sound file shall be used as ringer.
- Pattern melody selects the melody pattern that is used if Ringer sound is set to "Pattern".
- Pattern sequence determines the length for the melody pattern, and the interval between the repetitions of the pattern. There are 3 variants:
  - **"1"**: 1 sec ON, 4 sec OFF
  - **"2"**: 1 sec ON, 2 sec OFF
  - **"3"**: 0.7 sec ON, 0.7 sec OFF, 0.7 sec ON, 3 sec OFF

Administration via local phone

```
|--- User
     |--- Audio
          |--- Special Ringers
               |--- Internal
               |--- External
               |--- Recall
               |--- Emergency
               |--- Special 1
               |--- Special 2
               |--- Special 3
```

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 ringers)
- WBM download of binds
- FTP or HTTPS download of files to the phone

When a file is downloaded to the phone, sanity checks are carried out to ensure there are no operational or security impacts on the phone.

WBM checks the 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".

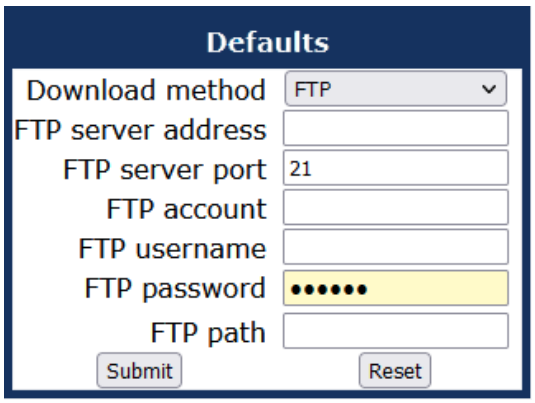
> **Note** If "Use defaults" is activated for a specific file type, any specific settings for this file type are overridden by the defaults.

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.



- **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

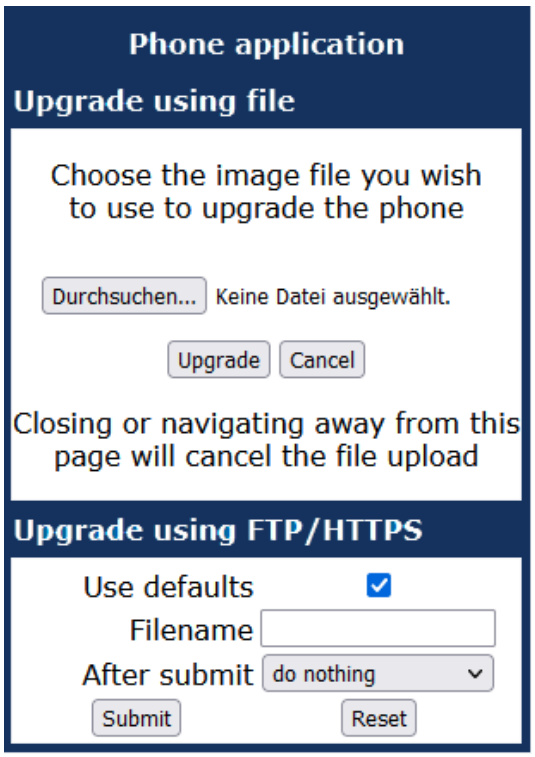
> **Note** Do not disconnect the phone from the LAN or power unit during software update. An active update process is indicated by blinking LEDs and / or in the display.

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.



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

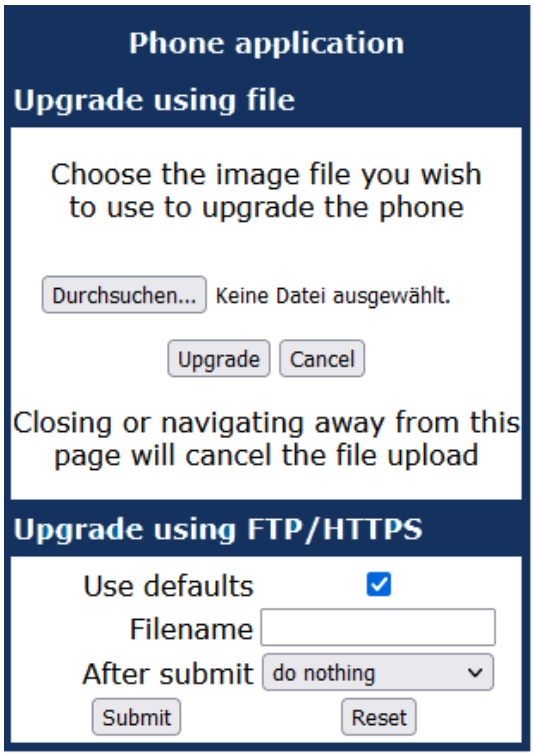
> **Note** The "Cancel" function will not work once the process is in burn state.

Upgrade using FTP / HTTPS

If the default FTP / HTTPS access settings (see "Common FTP / HTTPS settings (defaults)" → page 206) 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.



- **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

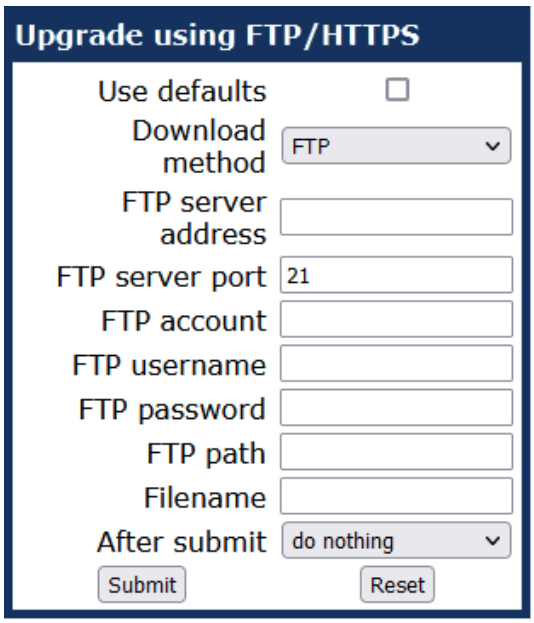
```
|--- Admin
      |--- File Transfer
            |--- Phone application
                  |--- Use default
                  |--- Download method
                  |--- Server
                  |--- Port
                  |--- Account
                  |--- Username
                  |--- Password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

Download / update phone application

If applicable, phone software should be deployed using the Deployment Service (DLS or DMS). 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.



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 (AVATARS)

Note The file size for a picture clip is limited to 300 KB.

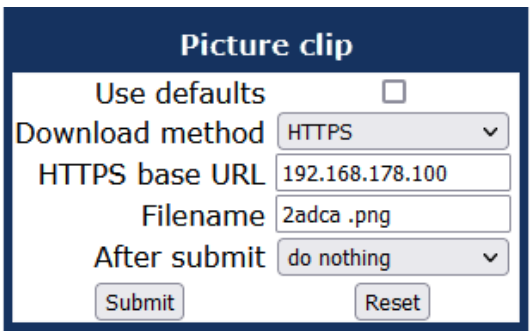
Picture clips are small images used for displaying a picture of a person that is calling on a line. The supported file formats for picture clips are JPEG, BMP and PNG. The file extensions supported for JPEG are "*.jpeg" and "*.jpg".

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 206).

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 211).

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 263).

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 atribute 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 atribute 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

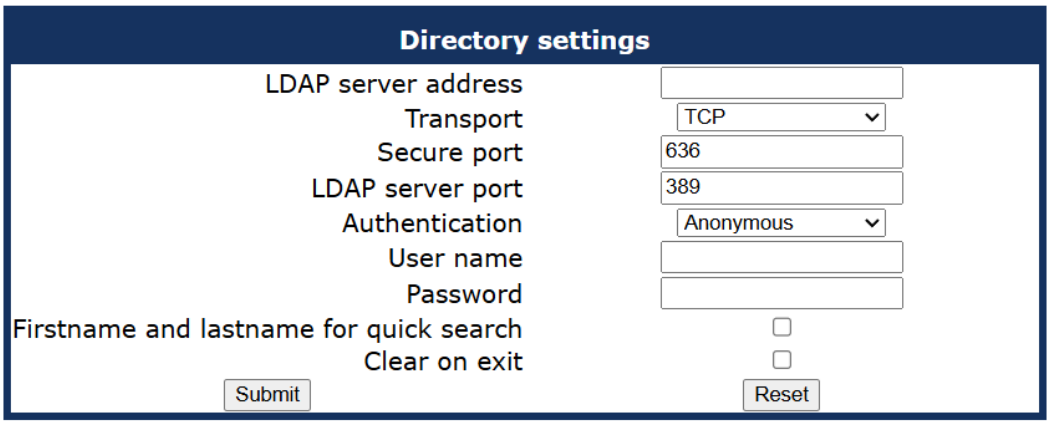
1. Open Settings > Administrator > Local functions > LDAP > Avatar server.

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.



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.

> LDAP template can also be edited via **Admin**>**Local functions**>**LDAP template**.

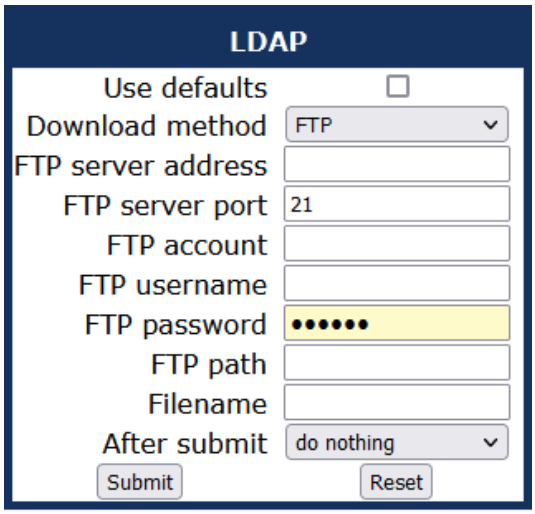
> The OpenScape Desk Phone phones support LDAPv3.

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 206).

Administration via WBM

1. Open File transfer > LDAP.



- **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
```

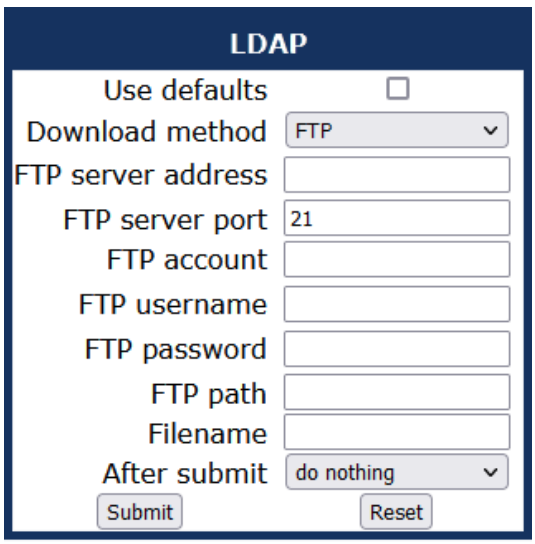
Download LDAP template

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:

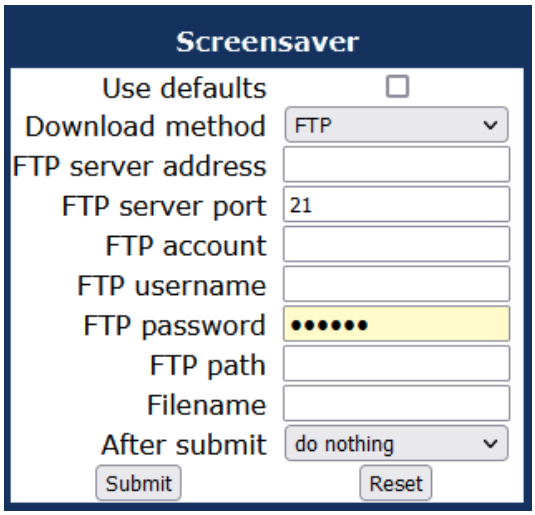
- **Data format**: JPEG, BMP or PNG. JPG is recommended. The file extensions supported for JPEG are jpeg and jpg.
- **Screen format**: 4:3. The images are resized to fit in the screen, so that images with a width / height ratio differing from 4:3 will appear with deviant proportions.
- **Resolution**: 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 specifieds (see "Common FTP / HTTPS settings (defaults)" → page 206).

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

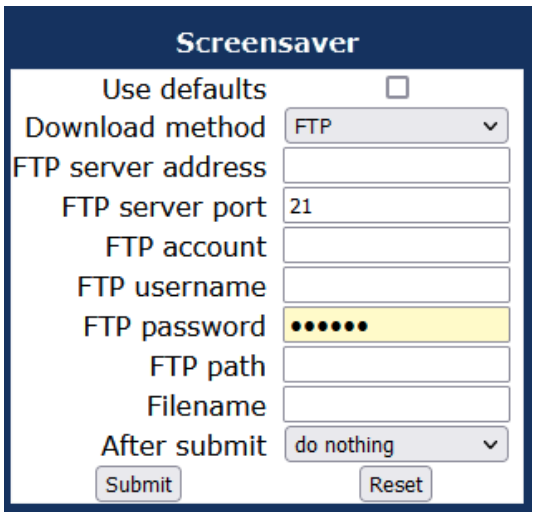
```
|--- Admin
      |--- File Transfer
            |--- ScreenSaver
                  |--- Use default
                  |--- Download method
                  |--- Server
                  |--- Port
                  |--- Account
                  |--- Username
                  |--- Password
                  |--- 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).

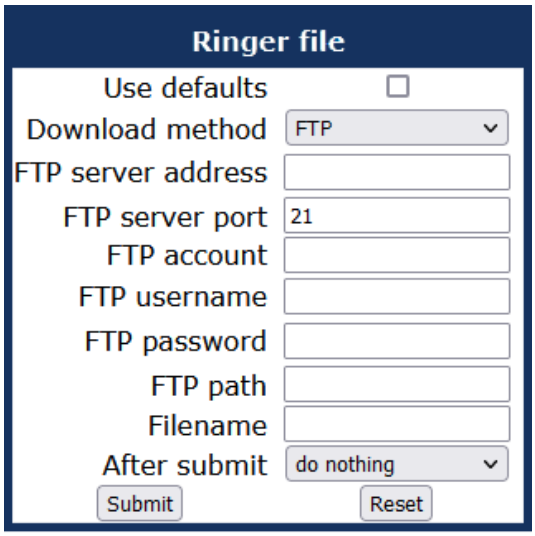
Length	64 kbit/s	80 kbit/s	96 kbit/s	112 kbit/s
0:15 min	0.12 MB	0.15 MB	0.18 MB	0.21 MB
0:30 min	0.23 MB	0.29 MB	0.35 MB	0.41 MB
0:45 min	0.35 MB	0.44 MB	0.53 MB	0.62 MB
1:00 min	0.47 MB	0.59 MB	0.70 MB	0.82 MB

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 206).

Administration via WBM

1. Open File transfer > Ringer file.



- **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

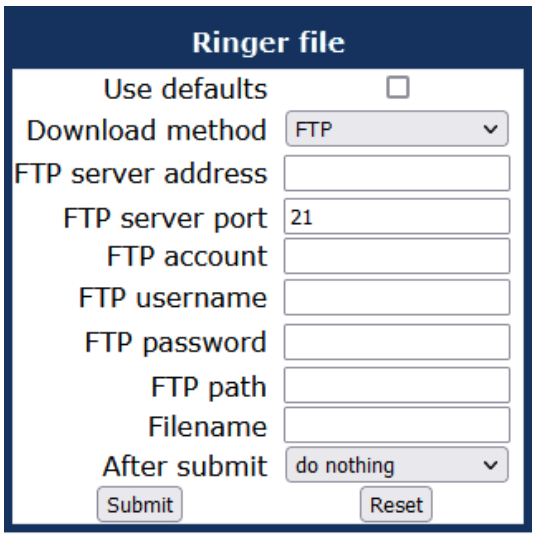
```
|--- Admin
      |--- File Transfer
            |--- Ringer
                  |--- Use default
                  |--- Download method
                  |--- Server
                  |--- Port
                  |--- Account
                  |--- Username
                  |--- Password
                  |--- 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.

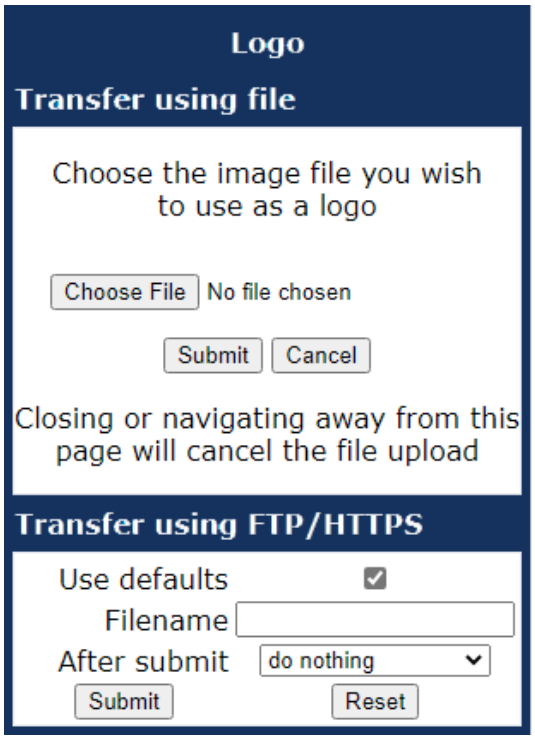
The maximum size of logo image placeholder is as below:

- 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.



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
```

Settings of the corporate directory

LDAP

In Zoom-provisioned environments, CP devices use secure LDAPS queries for Corporate directory search. Users can access contacts either via the Corporate main menu entry or through integrated search (model-dependent). All provisioning, mapping, and certificate handling are managed by the Zoom server, and sub-string matching is enabled across key contact fields.

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 CPx10 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 263.

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.

On Zoom-connected CP phones, there is an additional main menu option, "**Corporate**", which allows users to search the LDAP directory directly from the main menu.

LDAP search (V2.R0.18.0 and on)

Zoom uses LDAPS to access the LDAP Directory server. After V2.R0.18.0, LDAP searches fully support sub-string matching across the listed fields:

- CP HI Models: Lastname, Firstname, Phone Number, Extension Number.

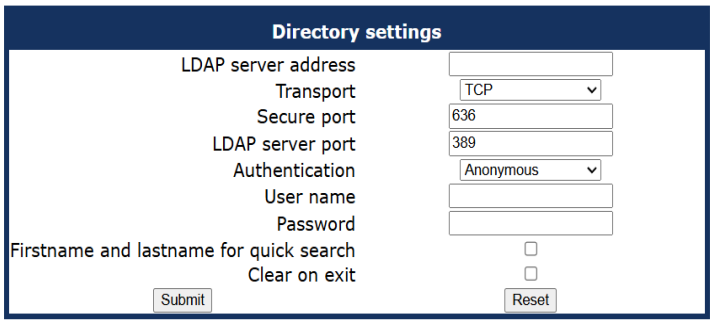
Example: Searching for "zoe" will return LDAP entries where "zoe" appears anywhere in Lastname, Firstname, Phone Number, or Extension Number.

Searches now use a sub-string match (i.e., *<pattern>*).

Double quotes (" ") are NOT used in search queries with Zoom LDAP.

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

Note After V2.R0.18.0, the password length limit has been extended to 255 characters for compatibility with Zoom LDAP requirements.

- **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.

- **LDAP for manual search only**: Allows you to disable the automatic LDAP lookup when an LDAP server is configured. If checked, the user can search LDAP only manually.

  - Value range: "True", "False".
  - Default: "False".

Note This item is available only for CP400/600/700.

- **Firstname and lastname for quick search**: Defines whether the phone searches both Firstname and Lastname or only Lastname.

  Value range: "True", "False". Default: "False".

Note The default value indicates that the search string provided by the user is used to search the Lastname field only on the LDAP server. After V1.11.6.0, it can search both Firstname and Lastname if enabled.

- **Clear on Exit**: When **Clear on Exit** option is enabled, when a CP110 / 210 SIP phone user exits the **Directory** application, any LDAP results on the phone from a previous search are cleared. When re-entering the Corporate option of the Directory feature, the user is prompted to perform a new quick search.

Note The **Clear on Exit** option is available only for the CP110 / 210 SIP phones.

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
               |--- LDAP for manual search only
               |--- Firstname and lastname for quick search
               |--- Clear on Exit
```

CONTACT DETAILS UPDATE

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

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

> Contacts can also be imported via a CSV file or delivered via a Bluetooth Vcard.

- 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)

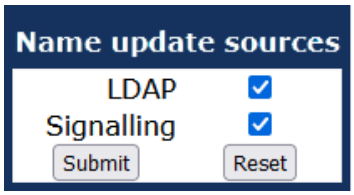
Source of the contact details

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 is 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

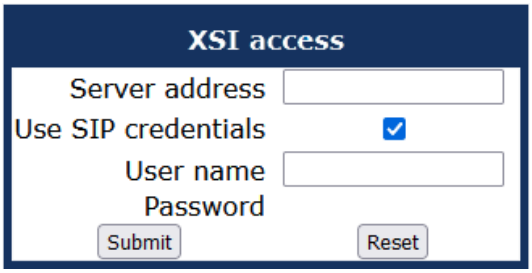
```
|--- Admin
      |--- Local Functions
            |--- LDAP
                  |--- Server address
                  |--- Transport
                  |---  LDAP secure port
                  |---  LDAP server port
                  |--- Authentication
                  |--- User name
            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

XSI access

The BroadSoft Xtended Services Interface (XSI) provides access to various user features like caller lists and directories.

Administration via WBM

1. Open Local functions > XSI access.



2. Enter the XSI server IP address.
3. Enable SIP credentials, if required.
4. Provide the user name and the password.
5. Click **Submit**.

Administration via local phone

```
|--- Admin
      |--- Local Functions
            |--- XSI access
                  |--- Server address
                  |---  Use SIP credentials
                  |--- User name
                  |--- Password
```

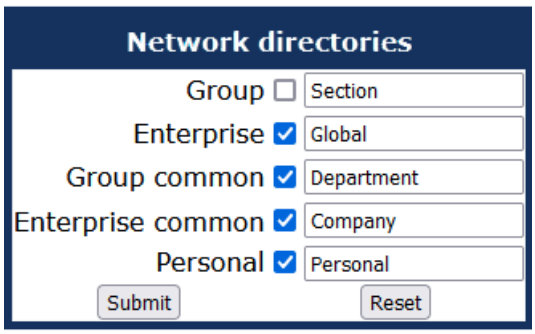
Network directories

Available network directories (accessible by BroadSoft Xtended Services Interface) can be activated or deactivated and supplied with customized names.

> To synchronize network directories, the XSI must be enabled (see "XSI access" → page 229).

Administration via WBM

1. Open Local functions > Network directories.



2. Enable the available directories and provide their names.

Administration via local phone

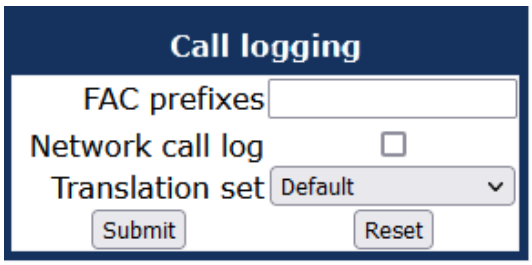
```
|--- Admin
     |--- Local Functions
          |--- Network directories
               |--- Group
               |--- Enterprise
               |--- Group common
               |--- Enterprise common
               |--- Personal
```

Call log

> The network call log and the XSI (for a Broadsoft server) must be enabled (see "XSI access" → page 229).

Administration via WBM

1. Open Local functions > Call logging.



2. Edit the FAC prefixes. A 'FAC prefix' is a Feature Access Code that is inserted at the start of a dialled number to trigger a specific behaviour of the SIP server when dialling the number (e.g. it may hide the callers identity). This setting does not require a Broadsoft server.
3. Enable "Network call log".
4. Select the "Translation set". This setting does not require a Broadsoft server.
5. Click **Submit**.

Speech

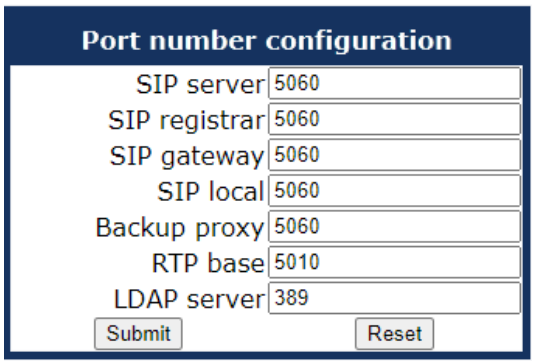
RTP BASE PORT

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.



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 OpenScape Desk Phone CP phone provides the codecs

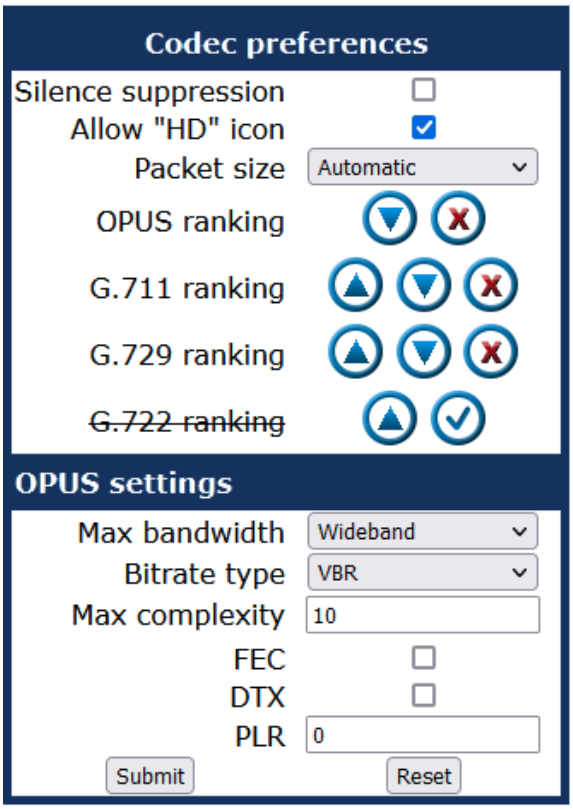
- G.722
- OPUS (only CP210 / CP410 / CP710)
- G.711
- G.729

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.



- **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"
- **OPUS** (only CP210 / CP410 / CP710): Parameters for the OPUS codec.
  - Value Range: "Choice 1", "Choice 2", "Choice 3", "Choice 4", "Disabled", "Enabled"
  - Default: "Choice 1"
- **G.711**: Parameters for the G. 711 codec.
  - Value Range: "Choice 1", "Choice 2", "Choice 3", "Choice 4", "Disabled", "Enabled"
  - Default: "Choice 2"
- **G.729**: Parameters for the G. 729 codec.
  - Value Range: "Choice 1", "Choice 2", "Choice 3", "Choice 4", "Disabled", "Enabled"
  - Default: "Choice 3"

OPUS settings

> OPUS codec is visible in codec table only for systems that support it.

- **Max bandwidth**: Determines the bandwidth that OPUS encoder should operate on. The OPUS codec may decrease the bandwidth from Wideband to Narrowband as it see fit. However if set to Narrowband, it will never increase to Wideband by itself. The bandwidth also determines the optimum bitrate if encoder is in CBR mode (12 kb/s at NB, 20 kb/s at WB).
  - Value Range: "Narrowband" (8kHz), "Wideband" (16kHz)
  - Default: "Wideband"
- **Bitrate type**: Configures if OPUS encoder should work in VBR or CBR modes.
  - Value Range: "CBR", "VBR"
  - Default: "VBR"
- **Max complexity**: Determines the maximum computational complexity of the codec. Lower values indicate worse quality.
  - Value Range: 0 to 10
  - Default: 10
- **FEC**: Forward Error Correction (FEC) is used to include redundant payload data for better quality in lossy networks, but increases computational complexity and bandwidth.
  - Value Range: "On", "Off"
  - Default: "Off"
- **DTX**: Discontinuous Transmission (DTX) determines whether to send empty payload frames during silence periods.
  - Value Range: "On", "Off"
  - Default: "Off"
- **PLR**: Packet loss rate (PLR) provides packet loss percentage of the Network as an input to encoder.
  - Value Range: 0 to 100
  - Default: 0

Administration via local phone

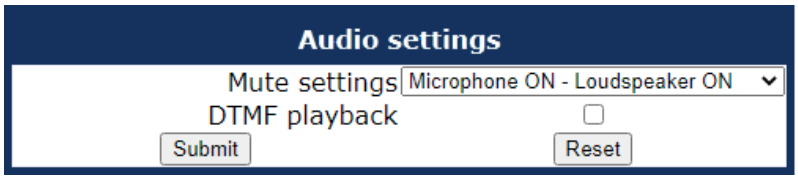
```
|--- Admin
     |--- Speech
          |--- Codec Preferences
               |--- Silence suppression
               |--- Packet size
                    |--- OPUS
                    |--- G.711
                    |--- G.729
                    |--- G.722
               |--- OPUS settings
```

AUDIO SETTINGS

The usage of microphone and speaker for speakerphone mode can be controlled by the administrator. Both microphone and loudspeaker can be switched on or off separately. By default, both microphone and loudspeaker are switched on.

Administration via WBM

1. Open Speech > Audio settings.



2. Select the following options:
   - Both loudspeaker and microphone are turned on.
   - Both loudspeaker and microphone are turned off.
   - The microphone is turned off, but the loudspeaker is turned on.

Administration via local phone

```
|--- Admin
      |--- Speech
            |--- Audio Settings
                  |--- Disable microphone
                     |---  Disable loudspeech
                     |---  DTMF playback
```

> The DTMF playback feature aims at the capability to play DTMF tones for digits received using RFC2833 coding (i.e. Rtp events) in the current active audio device (headset / loudspeaker / handset).

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

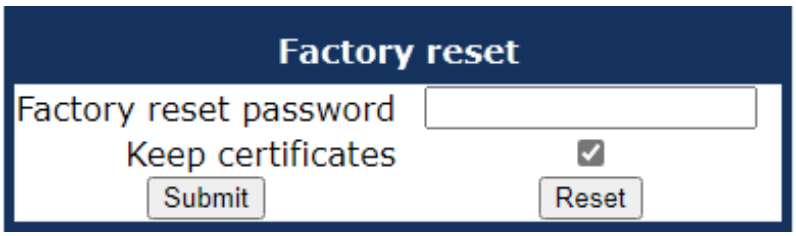
```
|--- Admin
      |--- Maintenance
            |--- Restart
```

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:

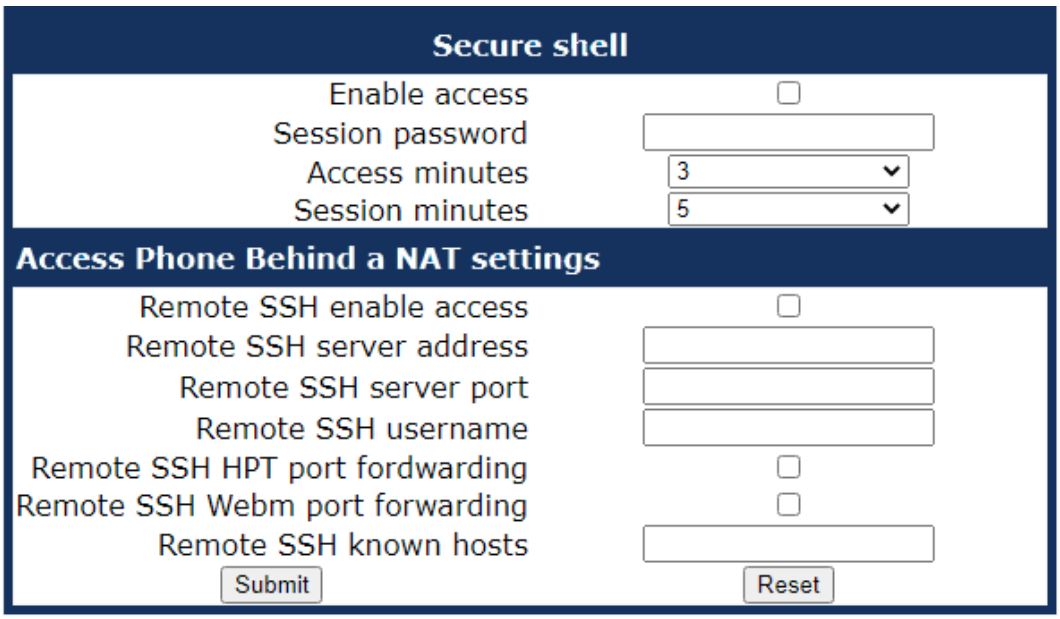
- **Log folder and files**: read only
- **User data folder and files**: read / write access
- **Opera deploy folders and files**: read only
- **Version folder**: read / write access; version files: read only

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.

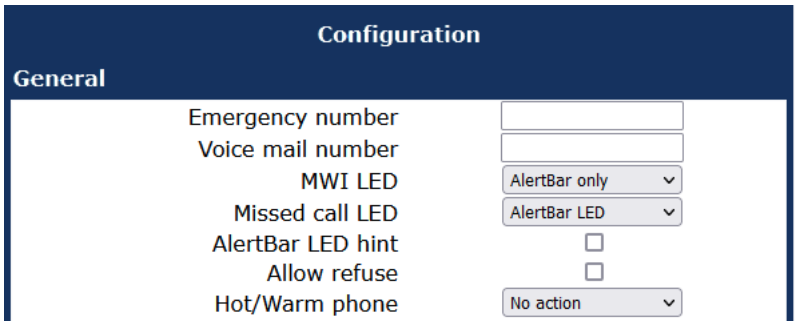
AlertBar LED hint

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.



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.

DISPLAY GENERAL PHONE INFORMATION

General information about the status of the phone can be displayed if desired.

Administration via WBM

1. Open General information.

- **MAC address**: Shows the phone's MAC address.
- **Software version**: Displays the version of the phone's firmware.
- **Last restart**: Shows date and time of the last reboot.
- **UBoot version**: Shows the software version of the UBoot loader.
- **Dial Plan ID**: Displays the identifier of the active dial plan assigned to the phone. A dial plan defines the rules for how dialed numbers are interpreted and routed by the phone system.
- **Dial plan status**: Shows whether the dial plan is active and functioning correctly.

Administration via local phone

```
|--- Admin
     |--- General Information
          |--- MAC address
          |--- Software ver.
          |--- Last restart
          |--- Dial plan ID
          |--- Dial plan status
```

DISPLAY DIAGNOSTIC INFORMATION

In addition to the general phone information, extended data can be displayed (also see "Display general phone information" → page 238).

Administration via WBM

1. Open Diagnostics > Diagnostic information > View.

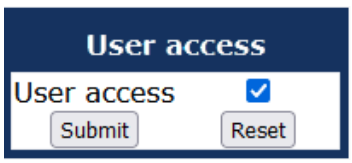
USER ACCESS TO DIAGNOSTIC INFORMATION

If this option is enabled, extended phone data is also displayed to the user. To view the data, the user opens the "Diagnostic information" link in the user menu of the WBM interface.

> **Note** The Diagnostic Information can also be viewed by the user on the local phone by selecting “User > Diagnostic information”.

Administration via WBM

1. Open Diagnostics > Diagnostic information > User access.



2. Enable user access.
3. Click **Submit**.

DIAGNOSTIC CALL

The feature "Rapid Status Diagnostic Call" will provide the possibility to place a diagnostic call, for example by the user, which starts call related tracing on the phone and on involved OpenScape Voice and collect these traces at OpenScape Voice Trace Manager (OSVTM). With all these traces

available, a call can be followed throughout the voice system and a possible problem can be detected faster. As all traces from all involved components are available at the first level support, the analysis of a possible problem can be started immediately.

A so-called diagnostic scenario will enable traces on all involved SIP components of the OSC Voice solution and store all traces at a central server. A tool will help service to follow a call through the traces and determine the point of problem.

If the call is recognized as a diagnostic call, the traces is sent to DLS as a first step and then DLS will forward them to OSVTM. Collected traces will either be sent after a successful end of diagnostic scenario or trace file is full.

A dial-prefix needs to be specified and prefixed to the dialed number (that should be identical to a number which the user identified a possible problem). This prefix is filtered before placing a call, so that the SIP messages is similar to the ones for the problematic destination.

The SIP header "X-Siemens-Trace-ID" has been chosen, as this is a special SIP field created for this feature. Existence of the diagnostic call, start and finish of a diagnostic call can be determined via this field [1].

Trace id is unique throughout the system and the following format is used to generate trace id:

```
TraceId: <UNIX_Timestamp>_<Last 6 bytes of MAC Address>
```

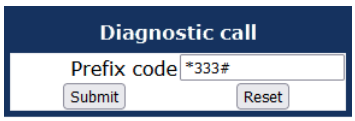
If related calls (diagnostic or not) are established following the start of the diagnostic call, then it turns to be a diagnostic scenario. Related calls become diagnostic (if they are not already) and traces are collected until the last diagnostic call ends plus a predefined timer. This timer guarantees capturing related information regarding to a problematic scenario.

The diagnostic call can only be determined during the call so initial traces might get lost. For this reason, user may need to do additional call. This is completely user related and user should be informed about the process. There will not be any restriction to prevent user to dial the prefix. If the prefix is configured by admin, user can always dial the prefix and start a diagnostic call. The prefix must consist of the leading asterisk followed by three digits and the hash.

Example: *333#.

Administration via WBM

1. Open Maintenance > Diagnostic call.



Administration via local phone

```
|--- Admin
      |--- Maintenance
            |--- Diagnostic Call
```

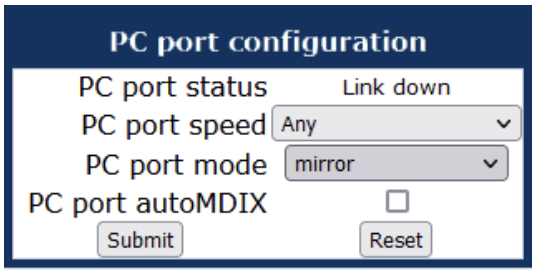
Note If the administrator tries to change trace configuration or delete existing traces this will not be allowed and admin gets the following error:
Change not allowed: Diagnostic tracing is active!

LAN MONITORING

The LAN port mirror facility allows for monitoring all network traffic at the phone's LAN port. Additionally, there is a possibility to monitor LAN traffic and port settings in the Local user menu.

Note For LAN monitoring the PC port mode needs to be set to "Mirror".

1. Open Network > PC port configuration.



2. Set the PC port mode to "mirror".
3. Click **Submit**.

Administration via local phone

```
|--- User
     |--- Network information
          |--- DNS name
          |--- URL
          |--- IPv4 address
          |--- IPv6 Global Addr.
          |--- IPv6 Linklocal Addr.
          |--- LAN RX
          |--- LAN TX
          |--- PC RX
          |--- PC TX
          |--- LAN autonegotiated
          |--- LAN information
          |--- PC autonegotiated
          |--- PC information
```

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

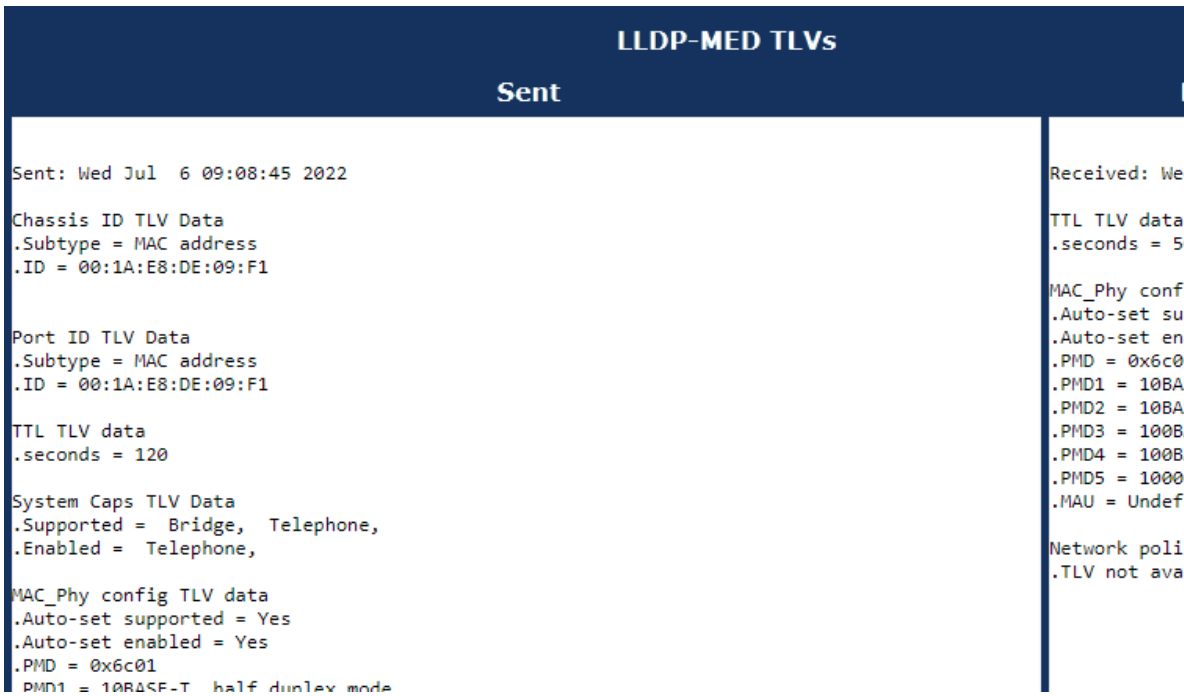
(Type-Length-Value) format.

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 269.

View Data From WBM

1. Open Diagnostics > LLDP-MED TLVs. Example:



- **Chassis ID**
- **Port ID**
- **YYL**
- **System Caps**
- **MAC_Phy config**: Identifies the duplex and bit-rate capability of the sending device, its current settings, and whether they are auto-negotiated or manually configured.
- **LLDP-MED Caps**: The TLVs supported by the phone and the switch as well as the specific device class they belong to.
- **Network policy (Voice)**: VLAN ID and QoS (Quality of Service) parameters for voice traffic.
- **Network policy (Voice signalling)**: VLAN ID and QoS (Quality of Service) parameters for signalling.
- **Network policy (Video conferencing)**: VLAN ID and QoS parameters for video traffic.
- **Extended Power**: Power Consumption; relevant for PoE.
- **Inventory – Hardware Revision**
- **Inventory – Firmware Revision**
- **Inventory – Software Revision**

- **Inventory – Serial Number**
- **Inventory – Manufacturer Name**
- **Inventory – Model Name**
- **Inventory – Asset ID**
- **TTL**: Time To Live. Determines how long the TLVs are valid. When expired, the device will send a new set of TLVs.

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.

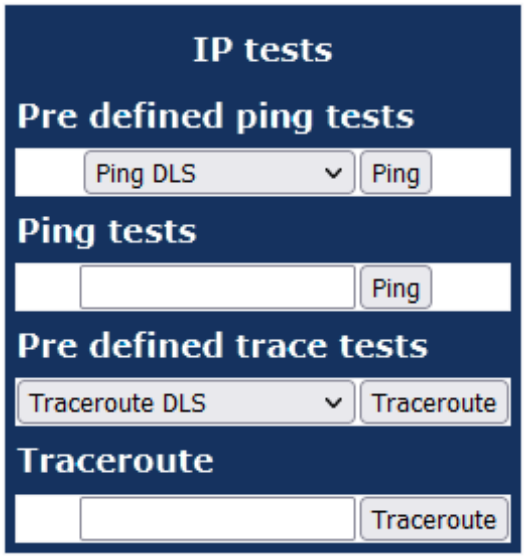
```
|--- Admin
                              |--- Network
                                   |--- Wired settings
                                      |--- LLDP-MED operation
                                             |--- Chassis ID
                                             |--- Port ID
                                             |--- YYL
                                             |--- System cap’s
                                             |--- MAC_Phy config
                                             |--- LLDP-MED cap’s
                                             |--- Network policy (Voice)
                                             |--- Network policy (Voice Signalling)
                                             |--- Network policy (Video conferencing)
                                             |--- Extended Power
                                             |--- Inventory – Hardware Revision
                                             |--- Inventory – Firmware Revision
                                             |--- Inventory – Software Revision
                                             |--- Inventory – Serial Number
                                             |--- Inventory – Manufacturer Name
                                             |--- Inventory – Model Name
                                             |--- Inventory – Asset ID
                                             |--- TTL
```

IP TESTS

For network diagnostics, the OpenScape Desk Phone CP phone can ping any host or network device to determine whether it is reachable. Additionally, the IP route to a host or network device can be traced using the traceroute tool contained in the phone software.

Administration via WBM

1. Open Diagnostics > Miscellaneous > IP tests.



- The **Pre Defined Ping tests** provide pinging for a pre-defined selection of servers: DLS, SIP server, and SIP registrar.
- **Ping tests** enables the pinging of the entered IP address.
- The **Pre Defined Trace tests** provide traceroute tests for a pre-defined selection of servers: DLS, SIP server, and SIP registrar.
- **Traceroute** enables traceroute tests for the entered IP address.

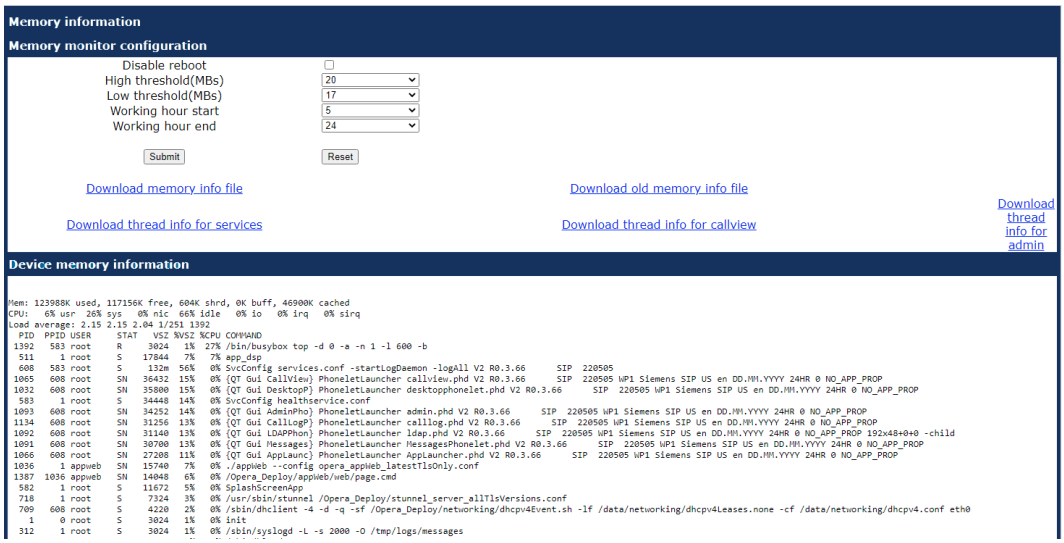
PROCESS AND MEMORY INFORMATION

The processes currently running on the phone’s operating system as well as their CPU and memory usage can be monitored here. 100 processes are monitored on the web page. For further information, refer to the manual of the "top" command for Unix or 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.



- When “Disable reboot” is enabled, 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 and CP210, the default value is 20 MB.
  - For OpenScape Desk Phone CP410 and CP710, it is 30 MB.
- With Low Threshold (MBs), the threshold for off-time is defined.
  - For OpenScape Desk Phone CP110 and CP210, the default value is 17 MB.
  - For OpenScape Desk Phone CP410 and CP710, 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.

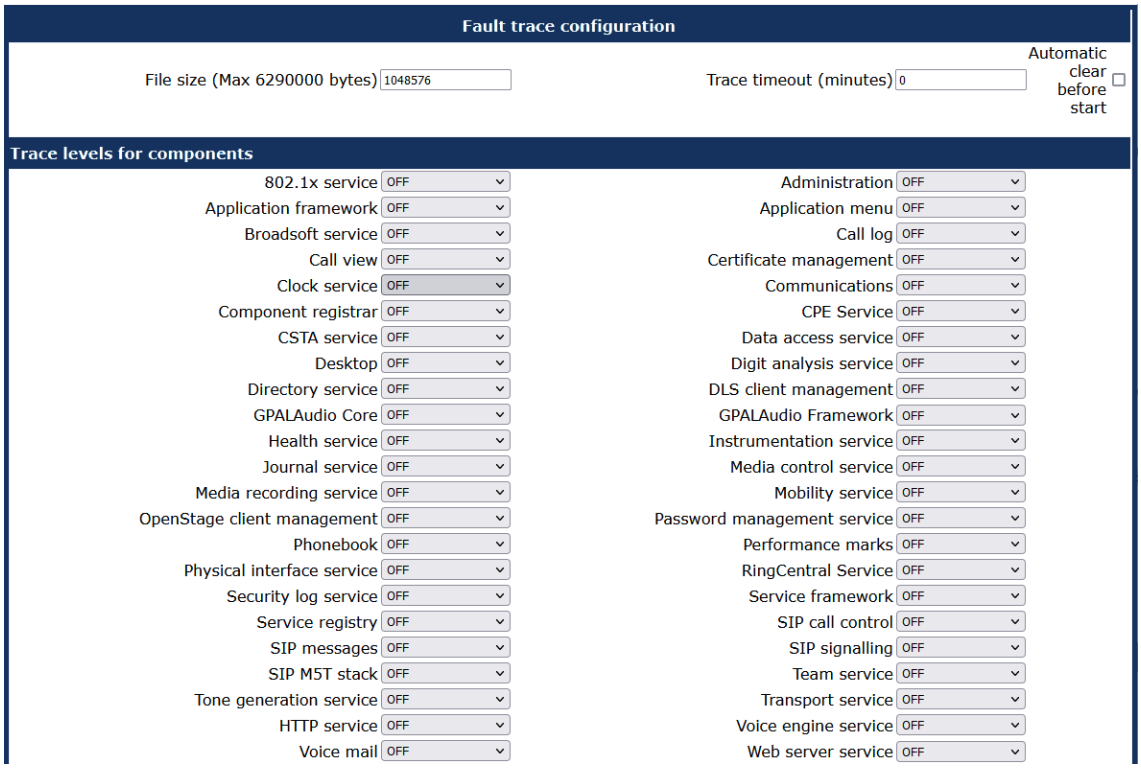
FAULT TRACE CONFIGURATION

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

> **Note** The absolute maximum file size is 6,290,000 bytes. However, on OpenScape 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.



- 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. For details, refer to "Example dial plan" → page 270
- **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** (CP710 only)
- **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

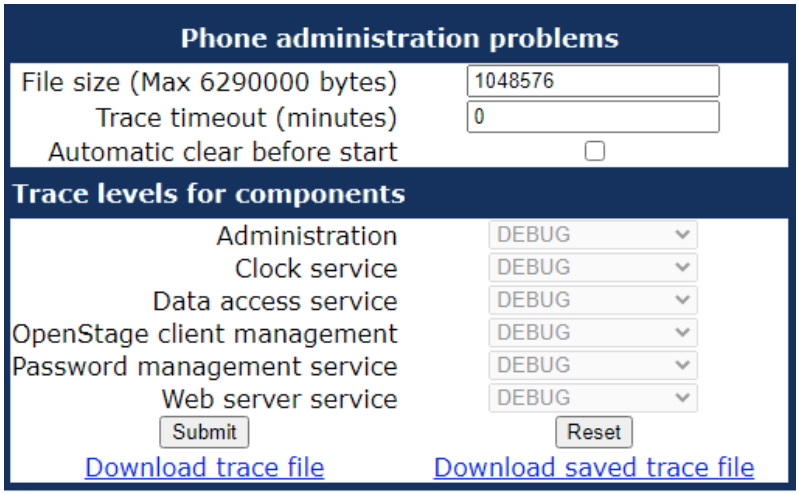
In order to simplify tracing for a specific problem, the tracing levels can be adjusted using predefined settings. The "EasyTrace" profiles provide settings for a specific area, e. g. call connection. On pressing Submit, those predefined settings are sent to the phone. If desired, the settings can be modified anytime using the general mask for trace configuration under Diagnostics > Fault Trace Configuration (see "Fault trace configuration" → page 245).

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

Phone administration problems

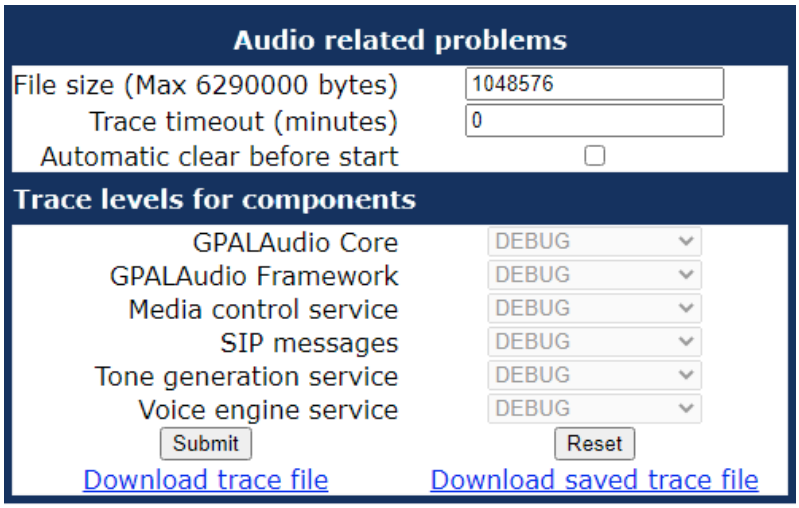
The phone administration problems define a set of trace profiles that will help in investigating problems in a specific area.

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



Audio related problems

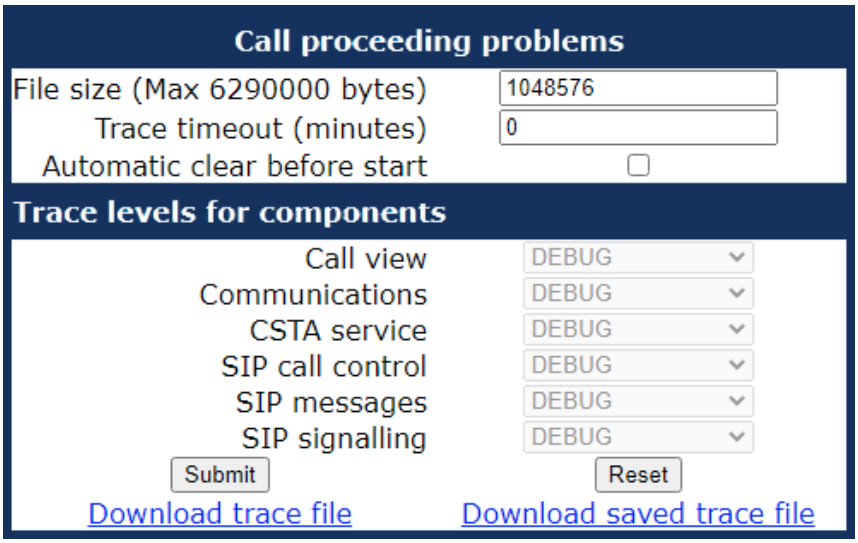
1. Open Diagnostics > EasyTrace Profiles > Audio related problems.



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

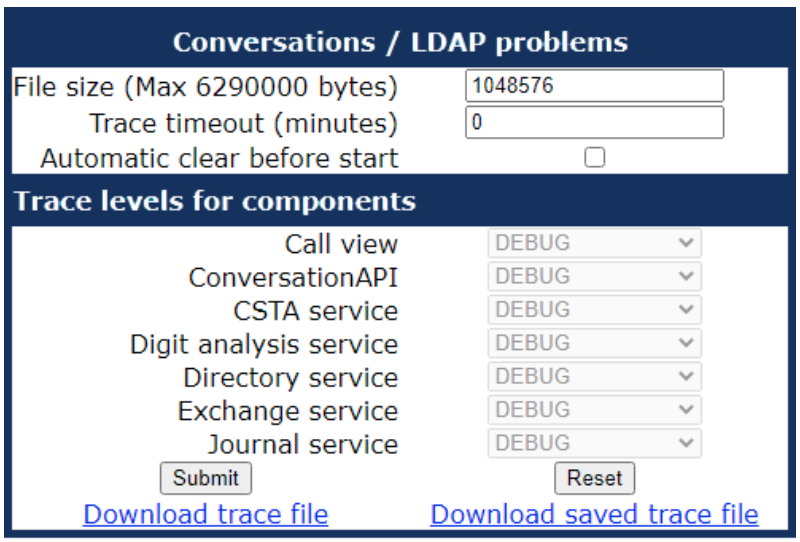
Open Diagnostics > EasyTrace Profiles > Call proceeding problems.



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.

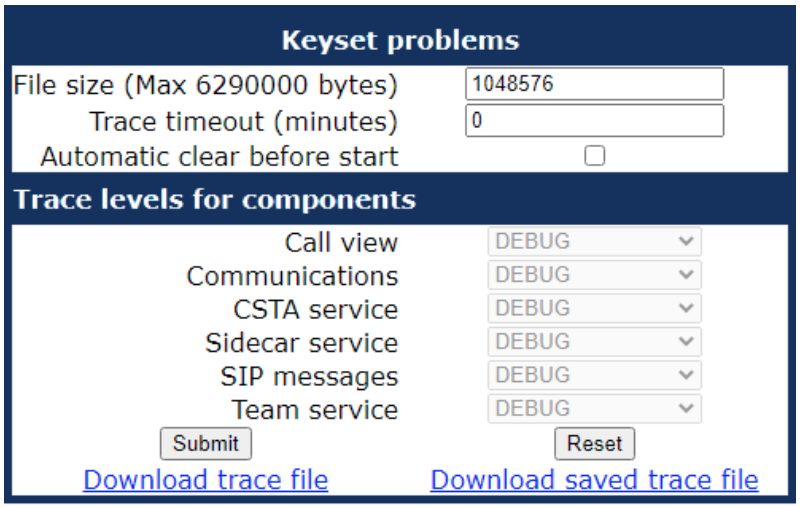
Conversations / LDAP problems

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



Keyset problems

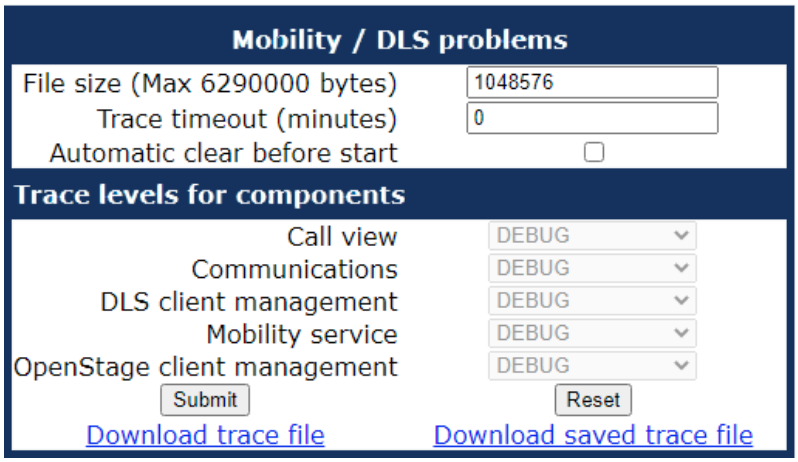
1. Open Diagnostics > EasyTrace Profiles > Keyset problems.



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.

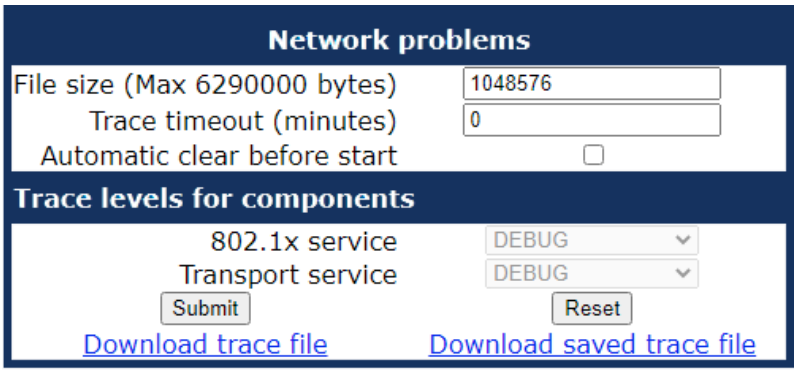
Mobility / DLS problems

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



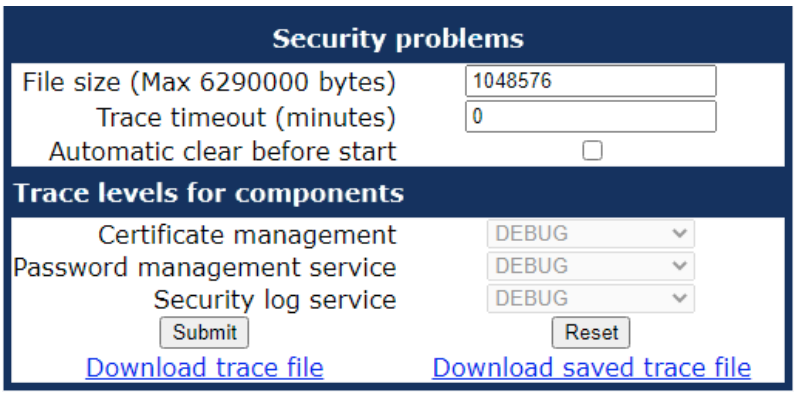
Network problems

1. Open Diagnostics > EasyTrace Profiles > Network problems.



Security problems

1. Open Diagnostics > EasyTrace Profiles > Security problems.

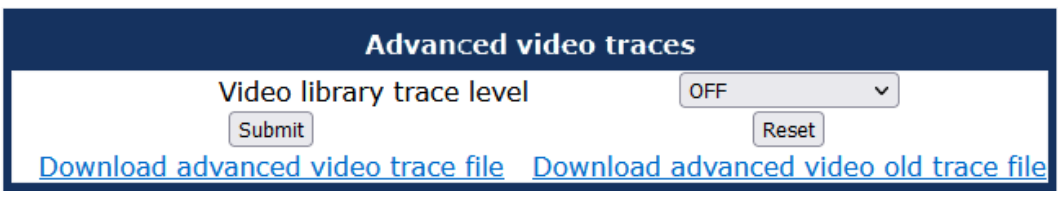


ADVANCED VIDEO TRACES

The trace level specifies the level of information the code will include in the trace file. The set of trace levels is specific to the library.

Note This feature is available only on OpenScape Desk Phones CP700 and CP710.

1. Open Diagnostics > Advanced video traces.

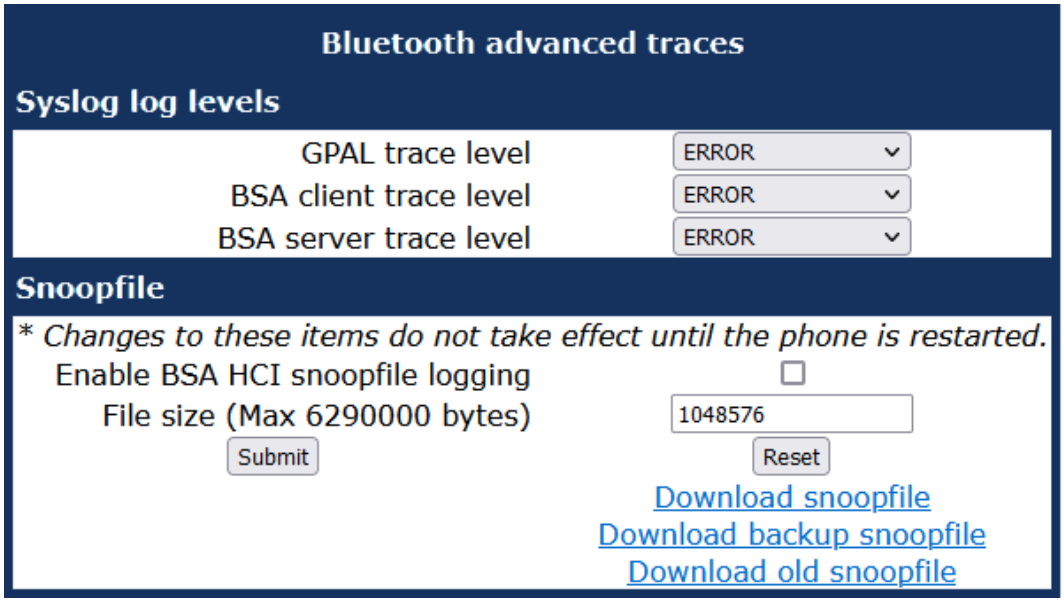


2. Select the trace level and click **Submit**.
3. To archive the file, select **Download**.

BLUETOOTH ADVANCED TRACES

Note This feature is available only on OpenScape Desk Phones CP700 and CP710.

1. Open Diagnostics > Bluetooth advanced traces.



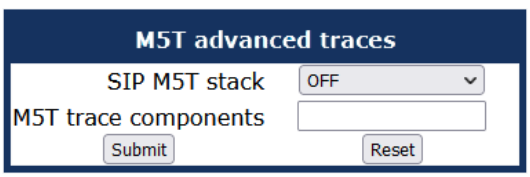
2. Define the trace levels ("NONE", "ERROR", "CUSTOM", "WARNING", "API", "EVENT", "DEBUG". Similar to Video library trace levels it defines the level of information that the code will include in trace files.
3. Select "Enable BSA HCI snoopfile logging". Snoopfile logging is a Boolean that determines if a snoopfile is created and can be downloaded
4. Define the file size (max. 6.3 MB) and click **Submit**.
5. For archiving the file, select **Download**.

M5T ADVANCED TRACES

This is a service item for enhanced SIP traces. The stack provided by M5T allows very deep tracing (not needed during standard operation).

Administration via WBM

1. Open Diagnostics > M5T Advanced Traces.



2. Select the M5T stack to select trace level for the M5T stack tracing.
3. Click **Submit**.

QOS REPORTS

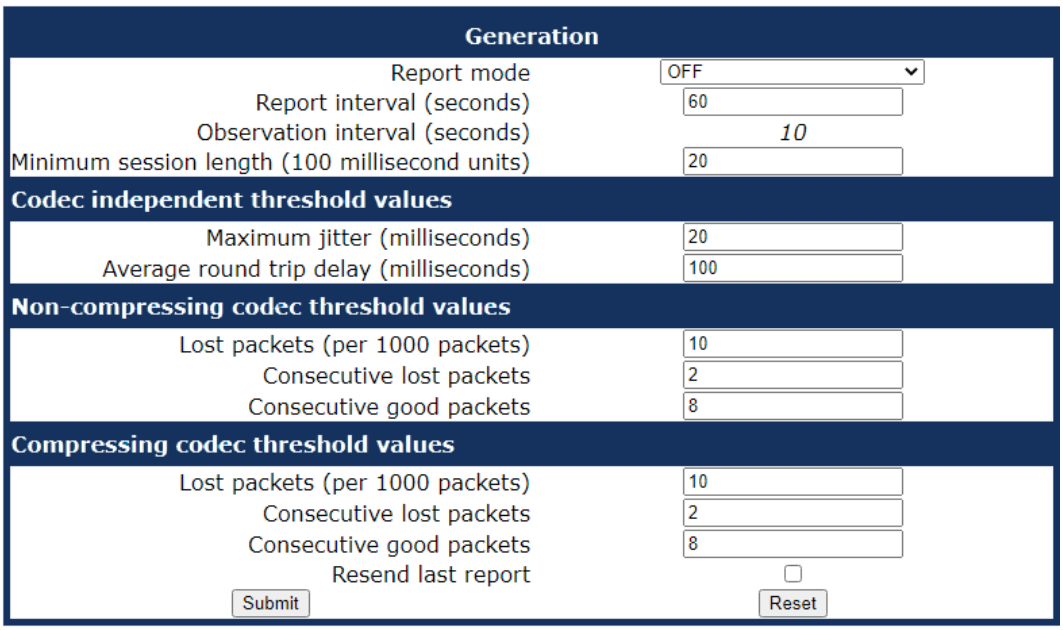
Conditions and thresholds for report generation

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.



- **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.

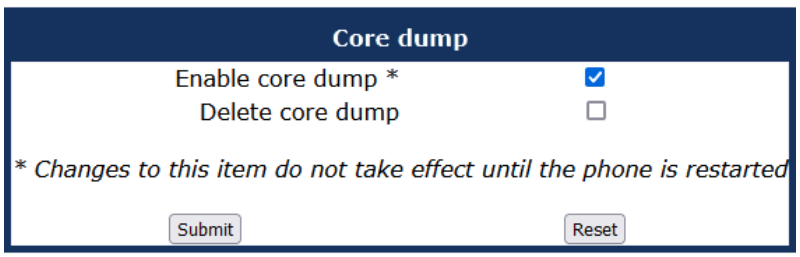
Administration via local phone

```
|--- 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
```

CORE DUMP

Administration via WBM

1. Open Diagnostics > Miscellaneous > Core Dump.



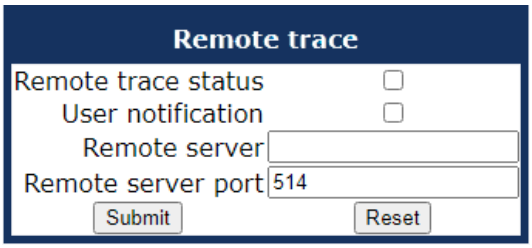
- If "Enable core dump" is enabled, a core dump is initiated in case of a severe error. The core dump is saved to a file. By default, this function is active.
- If "Delete core dump" is activated, the current core dump file is deleted when clicking **Submit**.
  - By default, this feature is not enabled.
- 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.



- 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 "Use 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

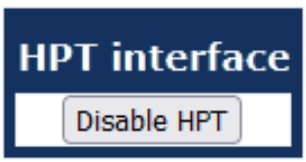
```
|--- Admin
     |--- Maintenance
          |--- Remote trace
               |--- Remote trace status
               |--- User notification
               |--- Remote ip
               |--- Remote port
```

HPT INTERFACE (FOR SERVICE)

For special diagnosis and maintenance tasks, the service staff may employ the HPT tool, which is able to control and observe an OpenScape Desk Phone remotely.

Administration via WBM

1. Open Maintenance > HPT interface.



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 245).

Administration via local phone

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

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	1st 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.

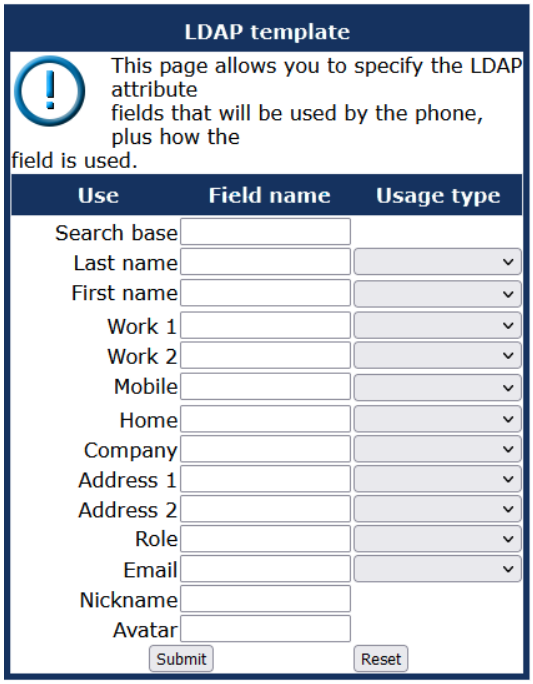
The following examples show the relations between GUI field names, the attribute labels used in the template, and exemplary mappings to LDAP attributes.

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.

Note From V2.R0.18.0 onward, if the SIP server type is set to 'ZOOM', 'Phone number' replaces the 'Work 1' field, and 'Extension' replaces the 'Work 2' field.

Administration via WBM

1. Open Local functions > LDAP template.



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 lables	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

OpenScape Desk Phone CP field	LDAP template lables	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 → 212

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

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

Microsoft Active Directory specific example

OpenScape Desk Phone CP field	LDAP template attribute	LDAP attribute	Example value
Last name	ATTRIB01	sn	Doe
First name	ATTRIB02	givenName	John
Business 1	ATTRIB03	ipPhone	9991234
Business 2	ATTRIB04	otherTelephone	9992345
Mobile	ATTRIB05	mobile	017711223344
Private	ATTRIB06	homePhone	441274333444
Company	ATTRIB07	company	Example Inc.
Address 1	ATTRIB08	department	Administration
Address 2	ATTRIB09	l	
Job function	ATTRIB10	title	Product Manager
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:

```
OpenScape Desk Phone CP LDAP TEMPLATE (v.1)
SEARCHBASE="dc=example,dc=com"
ATTRIB01="sn"
ATTRIB02="givenName"
ATTRIB03="ipPhone"
ATTRIB04="otherTelephone"
ATTRIB05="mobile"
ATTRIB06="homePhone"
ATTRIB07="company"
ATTRIB08="department"
ATTRIB09="l"
ATTRIB10="title"
ATTRIB11="mail"
ATTRIB12=”nickname”
ATTRIB13=””
EOF
```

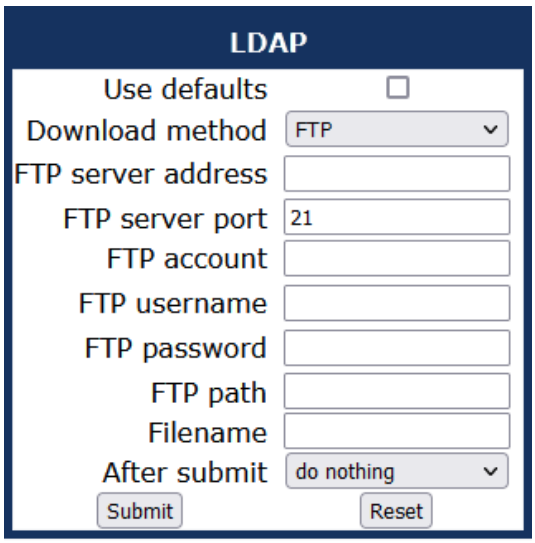
UPLOAD THE LDAP TEMPLATE TO THE PHONE

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 214).
4. Optionally, use the local menu or the DLS (see the Deployment Service Administration Manual).

Administration via WBM

1. Open File transfer > LDAP.



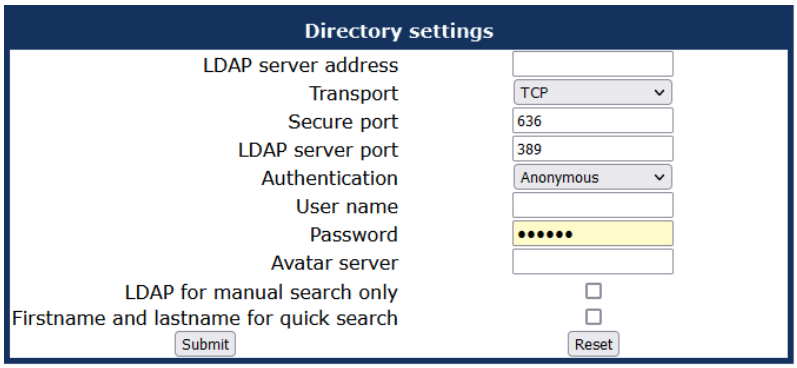
2. Enable “Use defaults” to Save the settings as default values.

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.

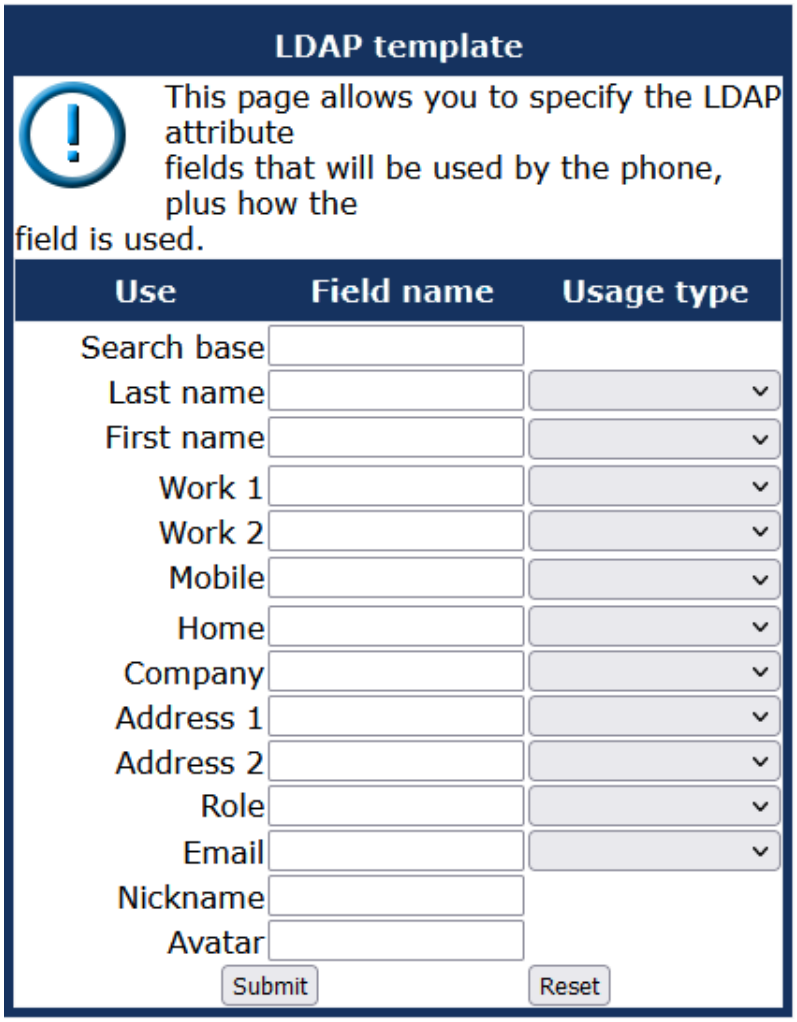


2. Enter the following parameters:
   - **LDAP Server address**: IP address or host name of the LDAP server.
   - **Transport**: Allows the LDAP interface to be encrypted using TLS (via LDAPS) or unencrypted using TCP, typically TCP.
   - **Secure port**: Port used by the LDAP for encrypted (TLS) transport, 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.
   - **Firstname and lastname for quick search**: Defines whether the phone searches both Firstname and Lastname or only Lastname. Value range: "True", "False". Default: "False".
   - **Clear on Exit**: The **Clear on Exit** option is available only for the CP110 / 210 SIP phones. If **Clear on Exit** option is enabled, when a CP110 / 210 SIP phone user exits the **Directory** application, any LDAP results on the phone from a previous search are cleared. When re-entering the Corporate option of the Directory feature, the user is prompted to perform a new quick search.
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.



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

Note From V1.11.6.0 onward, if the SIP server type is set to 'ZOOM', 'Phone number' replaces the 'Work 1' field, and 'Extension' replaces the 'Work 2' field.

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 43). 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

Example dial plan

INTRODUCTION

A dial plan is a set of rules that determine the phone's behaviour on digit entry by the user. Up to 48 rules are possible. With OpenScape Desk Phone CP, a dial plan rule is constructed from 9 parameters. In the following, the setup of a dial plan is explained.

The dial plan entries are preceded by a title line. This is a free format string, e. g. a descriptive name or version number, which can be used by the administrator for version control purposes.

DIAL PLAN SYNTAX

Note The phone will not perform any checking on the title; ensuring that different dial plans are given different titles is part of the administration process.

A dial plan rule is built from the parameters described underneath.

- **Digit string**: A pattern of digits or "*", "#", or "x" characters that is to be matched for starting an action. The maximum length is 24 characters. The "x" character is a wildcard character that represents any of the other digits (it may be upper or lower case).

- **Action** : The action to be taken when the criteria are met. The following options are available:
  - **"S" (Send digits)**: The digits entered are sent to the server when one of the following three conditions is satisfied:

    a) the maximum digits have been received, or

    b) the timer expires after the minimum digits have been received, or

    c) on receipt of the terminator after the minimum digits.

  - **"C" (Check for other actions)**: If the the digit sequence entered by the user matches Digit string, Maximum length, and Minimum length, the timer starts. On timer expiry, the digit string is sent to the server. If further digits are received before timer expiry, further entries is checked. If the timer is set to 0, the dial string is sent immediately. This option is used when there are more than one rules which start with the same digits.
- **Minimum length**: The dial plan rule will not initiate the sending of digits until at least this number of digits have been entered. However, the digits is sent after the delay configured in User menu > Configuration > Outgoing calls > Autodial delay (seconds).
- **Maximum length**: Automatic sending will occur when this number of digits have been dialed. If not specified, then the digits is sent when the timer expires, or a terminating character is entered.
- **Timer**: This indicates the timeout to be used for subsequent digit handling. If not specified, the default timer value is used (User menu > Configuration > Outgoing calls > Autodial delay (seconds)).
- **Terminating character**: A "*" or "#" character which indicates that the preceding digits should be considered complete, even though the maximum length may not be reached. However, the reach the minimum length must be reached by the string built from the digits entered and the terminating characters.
- **Special indication**:
  - **"E" (Emergency)**: If this character is entered here, the digits matching this rule is sent even if the phone is locked. The number is dialed immediately even when immediate dialing is disabled, and the phone is on-hook.
  - **"b" (bypass)**: The phone lock is bypassed. The number is dialed immediately even when immediate dialing is disabled, if the phone is off-hook.
- **Comment**: A remark on this dial plan entry.
- **Terminator sent**: If set to true, the terminating character is sent to the server along with the dial string proper. If set to false, the dial string is sent without the terminating character.

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
Secure communication with the DLS workpoint interface	---	18444	HTTPS / TCP - SSL / TLS

Service	Server Default Port	Client Default Port	Protocol Stack
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 (LP1)".

Text part	Error code	Scenario	Reason
No telephony	LP1	Unable to use LAN	Physical connection missing (Link Protocol)
	LX1	Unable to use LAN	802.1x error
	LI1	Link problem	No Network connection
	RS2	Unable to Register	No server address configured
	RN2	Unable to Register	No number configured
	RI2	Unable to Register	No phone IP address set
	RA2	Unable to Register	Authentication failed
	RF2	Unable to Register	Server failed
Limited keyset	WS	Limited Keyset support	Waiting to subscribe
Limited service	NT	Network Time	No NTP source
	B8	Unable to Register	Backup route active
Limited service	DF	DNS failure	SIP related DNS lookups fail
Exchange: please check username and password	EX	Exchange failure	Wrong username/password
Exchange: untrusted server			Cert validation failure
connection to Exchange server failed			Other failure

- A special "fast-busy" tone (also called congestion tone) is played if a temporary Network problem causes a user-initiated call action to fail.
- Typical call actions: making an outgoing call; picking up a call from Manual Hold; or Group pickup.
- Phone users include keyset users and mobile users logged on to the phone.
- The special tone is triggered if one of the following SIP response codes is received from the server: 606, 408, or 503.

Glossary

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., Wi-Fi 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 accordance with requests from the application program. The OpenScape Desk Phone CP phone allows for the setting of QoS parameters on layer 2 and layer 3 (DiffServ).

RAM
Random Access Memory. Memory with read / write access.

ROM
Read Only Memory. Memory with read only access.

RTCP
Realtime Transport Control Protocol. Controls the → 275 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.

mitel.com