



Unify OpenScape
Desk Phone CP

Atos Unify
OpenScape Desk Phone
CP110 / CP210

**Atos Unify OpenScape Business
Administrator Documentation HFA**

A31003-C1100-M102-13-76A9

Atos

Important information

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

Trademarks

	<p>The device conforms to the EU Directive as attested by the CE marking. The CE Declaration of Conformity and, where applicable, other existing declarations of conformity as well as further information on regulations that restrict the usage of substances in products or affect the declaration of substances used in products can be found in the Unify Expert WIKI at http://wiki.unify.com/ http://wiki.unify.com in the section "Declarations of Conformity".</p>
	<p>The adjacent symbol indicates that any electrical and electronic products installed and sold in countries of the European Union to which the WEEE2 Directive 2012/19/EU applies should be disposed of separately from the municipal waste stream in appropriate collection systems.</p> <p>Information concerning the proper disposal of your Unify product in the business-to-business market segment is available from your local sales representative in Unify or partner sales.</p>

Software update

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

Online documentation

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

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

Location of the telephone

- The telephone may only be operated using the LAN cabling internally in the building. The device should be connected to the IP infrastructure using a shielded LAN cable: Cat-5 for 100 Mbps or Cat-6 for 1000 Mbps. Make sure in the building installation that this cable shielding is earthed.
- When using an additional Wi-Fi dongle 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 79.

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 24).

Contents

Important information	2
Trademarks.....	2
Software update.....	2
Online documentation.....	3
Location of the telephone.....	3
Product-oriented environmental protection.....	3
License information.....	4
Overview	10
About this manual.....	10
Maintenance notes.....	10
Conventions for this document.....	10
The OpenScape Desk Phone CP family.....	11
OpenScape Desk Phone CP110.....	11
OpenScape Desk Phone CP210.....	13
OpenScape Desk Phone CP710.....	15
Administration interfaces.....	16
Web-based management (WBM).....	16
Local phone menu.....	17
DLS/DMS (OpenScape Deployment Service / Device Management Service).....	17
Startup	18
Prerequisites.....	18
Assembling and installing the phone.....	18
Shipment.....	18
Connectors at the bottom side.....	19
Assembly.....	21
How to connect the phone via LAN cable.....	22
How to use LAN connections.....	23
How to connect the phone via USB Wi-Fi dongle.....	23
Key modules.....	23
Quick start.....	24
How to access the web interface (WBM).....	24
Access via local phone.....	25

How to configure the Terminal number.....	26
Basic Network configuration.....	27
DHCP resilience.....	27
Date and time / SNTP.....	28
Extended Network configuration.....	28
Vendor-specific VLAN discovery and DLS address.....	28
HFA gateway settings.....	38
Manual registration.....	39
Using the local menu.....	39
Setting the DMS address via DHCP.....	40
Administration.....	42
Bluetooth interface.....	42
LAN settings.....	43
LAN port settings.....	43
VLAN.....	45
IP Network parameters.....	49
Quality of Service (QoS).....	49
Use DHCP.....	52
Manual configuration of the IP address.....	54
Default router / gateway.....	55
Specific IP routing.....	56
DNS.....	57
IP TTL.....	59
Configuration & update service.....	60
SNMP.....	63
OpenScape service menu.....	65
Wi-Fi settings.....	65
Setting up a WiFi connection.....	67
Disable LAN port.....	68
Advanced Wi-Fi settings.....	69
System settings.....	71
HFA gateway settings.....	71
HFA emergency gateway settings.....	72
Server and standby server ports.....	73
Redundancy.....	74
Emergency number.....	75

LIN.....	76
Not used timeout.....	77
Enable telephony settings.....	78
Energy saving.....	79
System.....	80
Date and time.....	83
Settings via SNTP.....	84
Dialing.....	85
Canonical dialing configuration.....	85
Canonical dial look-up.....	88
Ringer setting.....	90
Distinctive ringing.....	90
Map to specials.....	92
Special ringers.....	93
Mobility.....	95
Bluetooth mobility.....	96
Free programmable keys.....	96
Feature key for CP710.....	97
Transferring phone software, application, and media files.....	97
Linux file name issues.....	98
FTP / HTTPS server.....	98
Common FTP / HTTPS settings (defaults).....	99
Phone application.....	100
Picture clips.....	104
LDAP template.....	108
Screen saver.....	111
Ringer file.....	114
UC server.....	117
Send request via HTTP / HTTPS.....	117
Settings of the corporate directory.....	120
LDAP.....	120
Contact details update.....	122
System phone book.....	123
Picture via LDAP.....	123
Canonical dial settings.....	124
Speech.....	126
RTP base port.....	126

Codec preferences.....	126
Audio settings.....	129
Security and policies.....	130
Changing a password.....	130
Retrieve a lost password.....	131
Certificates.....	132
Restart phone.....	134
Factory reset.....	134
SSH — secure shell access.....	135
Display license information.....	136
Web Services Interface (WSI).....	136
HPT interface (for service staff).....	136
AlertBar LED hint.....	137
Diagnostics.....	138
LLDP-MED.....	138
Fault trace configuration.....	140
EasyTrace profiles.....	144
Advanced audio traces.....	148
QoS reports.....	149
Miscellaneous.....	154
Remote tracing — syslog.....	156
Key modules.....	157
Examples and how-tos.....	159
Canonical dialing.....	159
Canonical dialing settings.....	159
Canonical dialing look-up.....	159
Conversion examples.....	160
How to set up the “Corporate directory” (LDAP).....	162
Prerequisites.....	162
Create an LDAP template.....	162
Upload the LDAP template to the phone.....	165
Configure LDAP access.....	166
LLDP-Med example.....	167
Technical reference.....	168

Default port list.....	168
Troubleshooting error codes.....	170
Glossary.....	174

Overview

About this manual

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

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

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

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

Maintenance notes

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

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

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

Conventions for this document

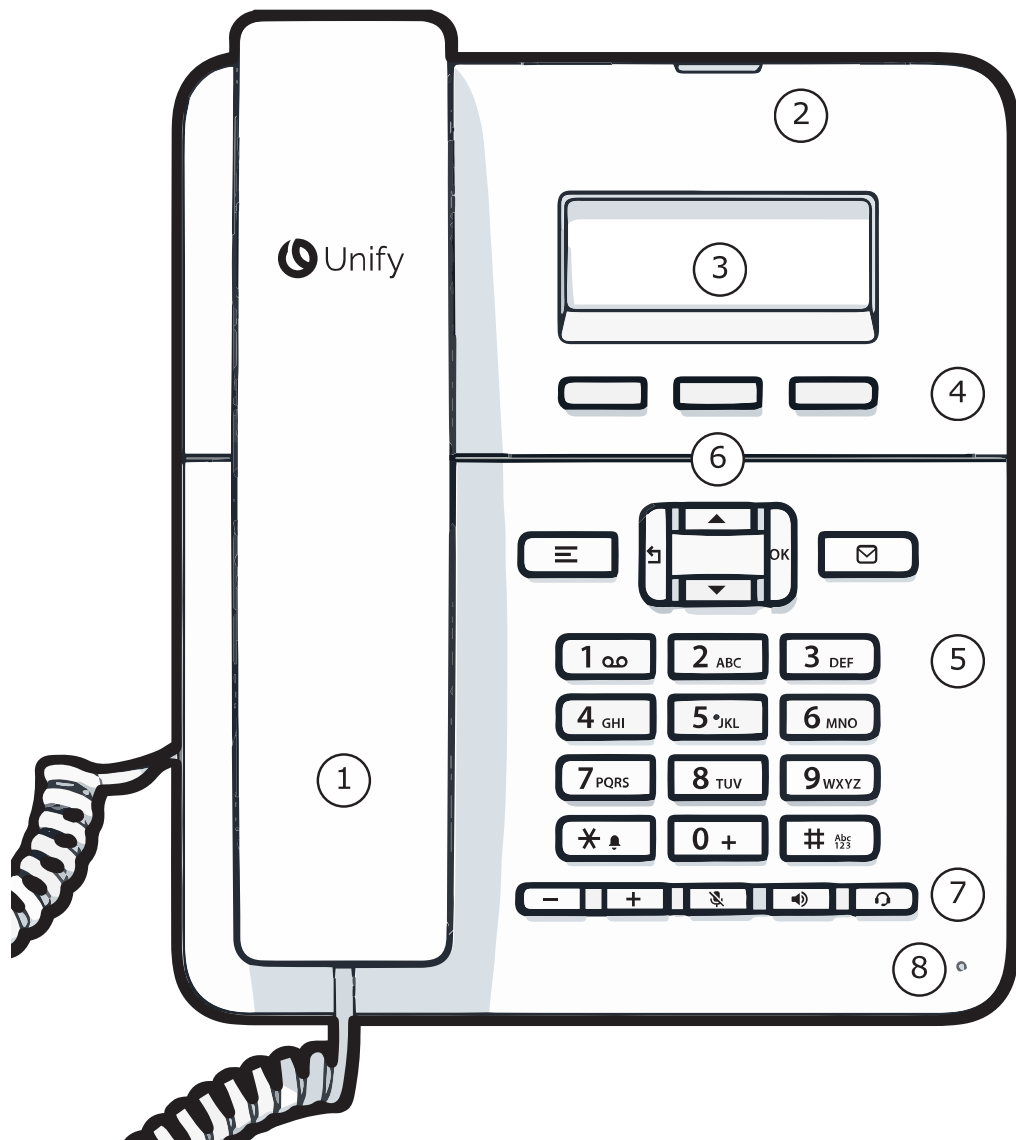
The terms for parameters and functions used in this document are derived from the web interface (WBM). In some cases, the phone's local menu uses shorter, less specific terms and abbreviations. In a few cases the terminologies differ in wording. If so, the local menu term is added with a preceding "/".

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







This document describes the software version 2.0.

The OpenScape Desk Phone CP family

OpenScape Desk Phone CP110

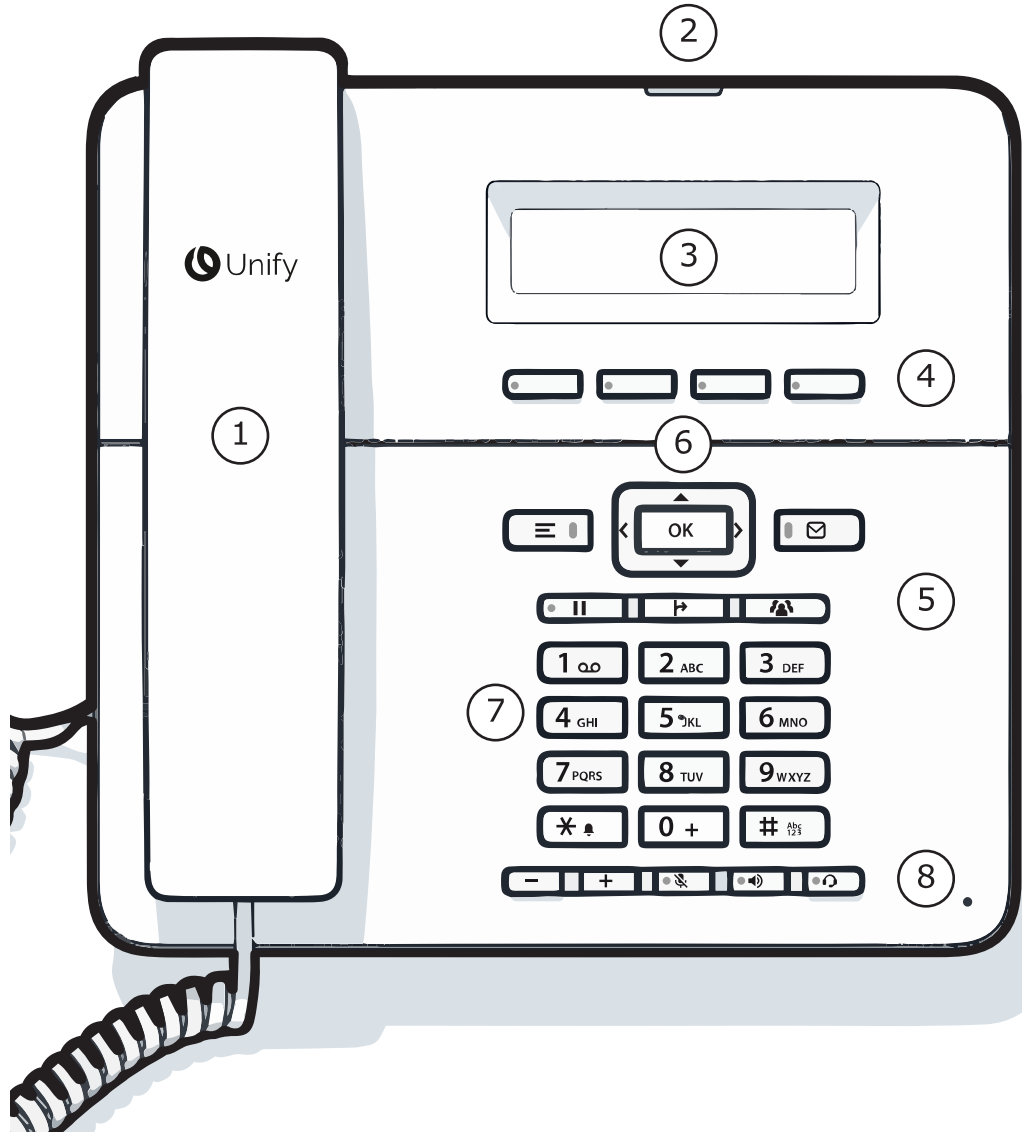


- 1 You can make and receive calls as normal using the **handset**.
- 2 The **status LED** displays the phone connection status. Incoming calls and new voice mails are visually signaled via the Notification LED.

3	The display shows information during telephone operation (three lines with up to 32 characters each).
4	The programmable function keys can be set to various functions.
5	<p>The function keys (non-programmable) are assigned to the following functions during a call:</p> <p>: Provides access to the user menu for locally controlling the phone settings.</p> <p>: Allows voicemails to be managed.</p> <p>: Increases or decreases the speaker or headset volume.</p> <p>: Activates or deactivates the microphone. This prevents the other party from listening in, e.g. when consulting with someone else in the room or in case of background noise.</p> <p>: Activate or deactivates the speakerphone during an active call.</p> <p>: Activates or deactivates the headset.</p>
6	The navigation keys help you navigating through the various phone functions, applications and configuration menus.
7	The dialpad can be used to enter phone numbers and write text.
8	You can listen to calls with the microphone even when the handset is hung up.


The depiction of keys in this manual reflects the keys of the OpenScape Desk Phone CP210 / CP410 / CP710.

OpenScape Desk Phone CP210




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

: Hold or retrieve the active call.


: Transfer a call to another contact.

: Enable access to the conference functions.

: Activate or deactivates the speakerphone during an active call.

: Activates or deactivates the headset.

: Increases or decreases the speaker or headset volume.

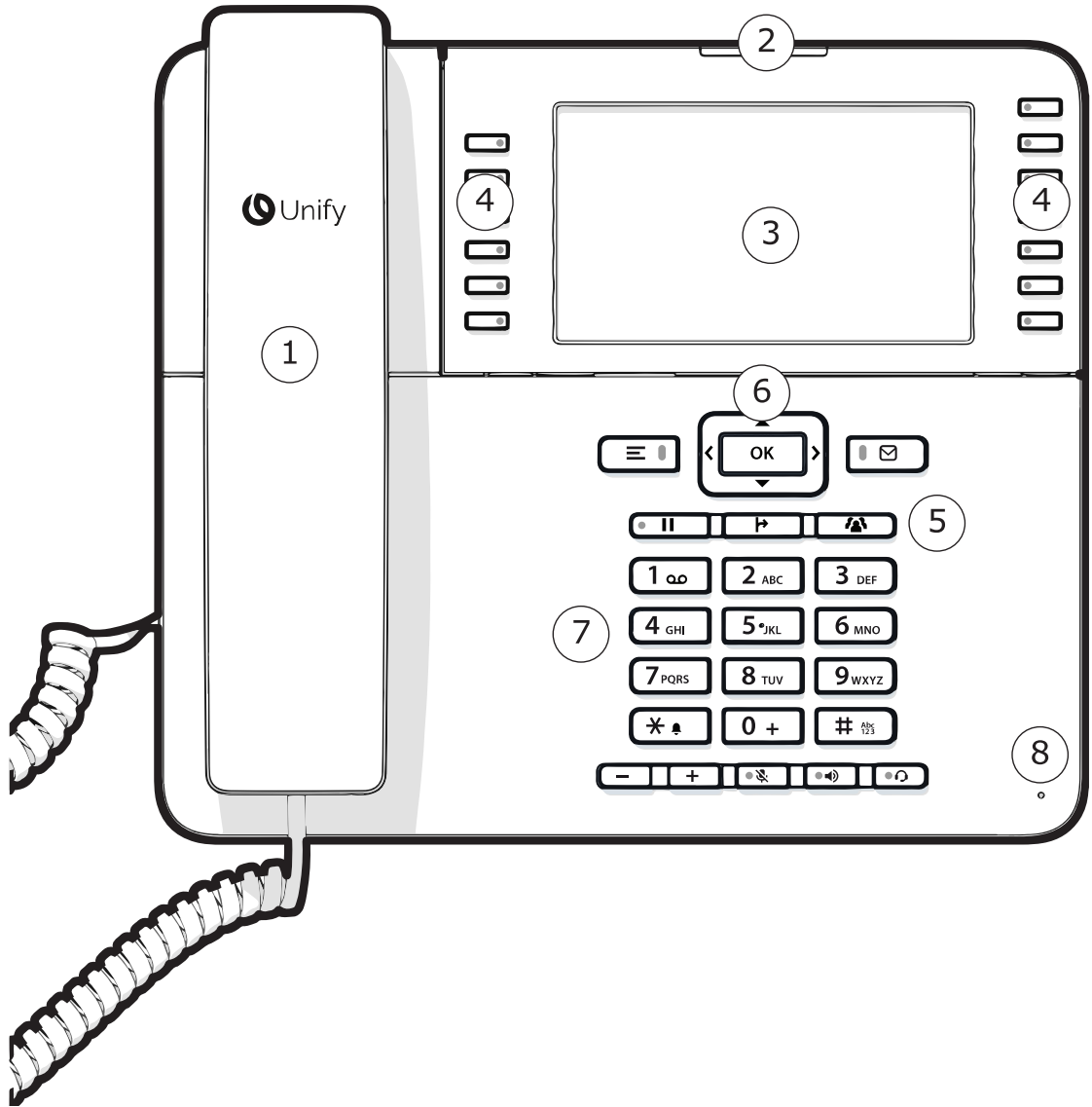
: Activates or deactivates the microphone. This prevents the other party from listening in, e.g. when consulting with someone else in the room or in case of background noise.

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 listen to calls with the **microphone** even when the handset is hung up.

OpenScape Desk Phone CP710




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

: Hold or retrieve the active call.


: Transfer a call to another contact.

: Enable access to the conference functions.

: Activate or deactivates the speakerphone during an active call.

: Activates or deactivates the headset.

: Increases or decreases the speaker or headset volume.

: Activates or deactivates the microphone. This prevents the other party from listening in, e.g. when consulting with someone else in the room or in case of background noise.

- 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 listen to calls with the **microphone** even when the handset is hung up.

Administration interfaces

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

Web-based management (WBM)

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

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

Licenses

This area provides the user with the information about EULA (End User License Agreement) and Open Source licenses. This section is on the main area within WBM, which is not password protected to allow access for the user (see "[Manual registration](#)" → [page 39](#)).

Local phone menu

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

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

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

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

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

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

Startup

Prerequisites

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

- An Ethernet connection to a Network with communication servers.

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

- OpenScape 4000, OpenScape Business, OpenScape Voice, or other SIP server.
- An FTP Server for file transfer, e. g. firmware, configuration data, application software
- A DHCP (Dynamic Host Configuration Protocol) server (recommended).
- DLS (OpenScape Deployment Service) for advanced configuration and software deployment (recommended).

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

https://wiki.unify.com/wiki/IEEE_802.1x

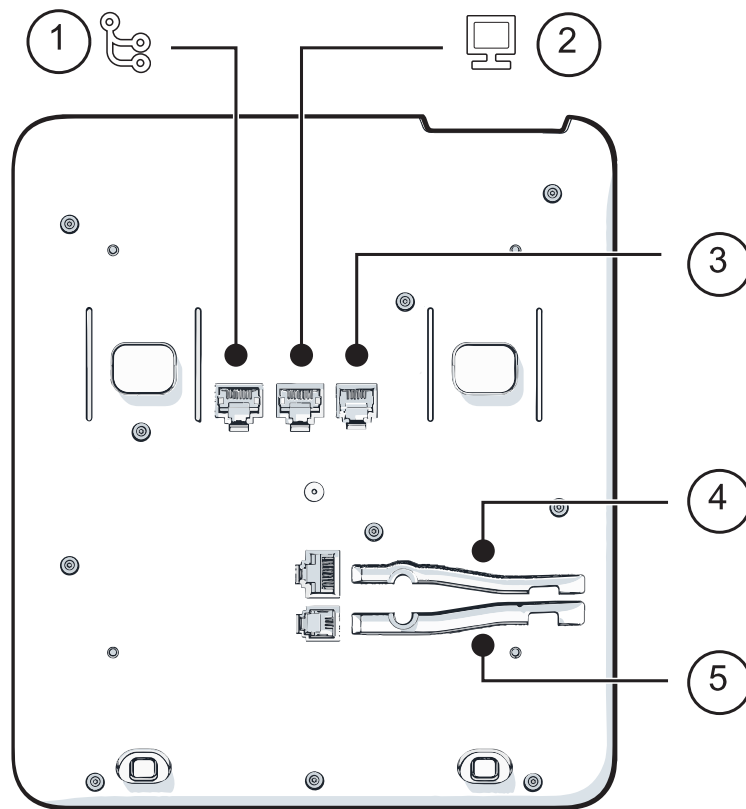
Assembling and installing the phone

Shipment

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

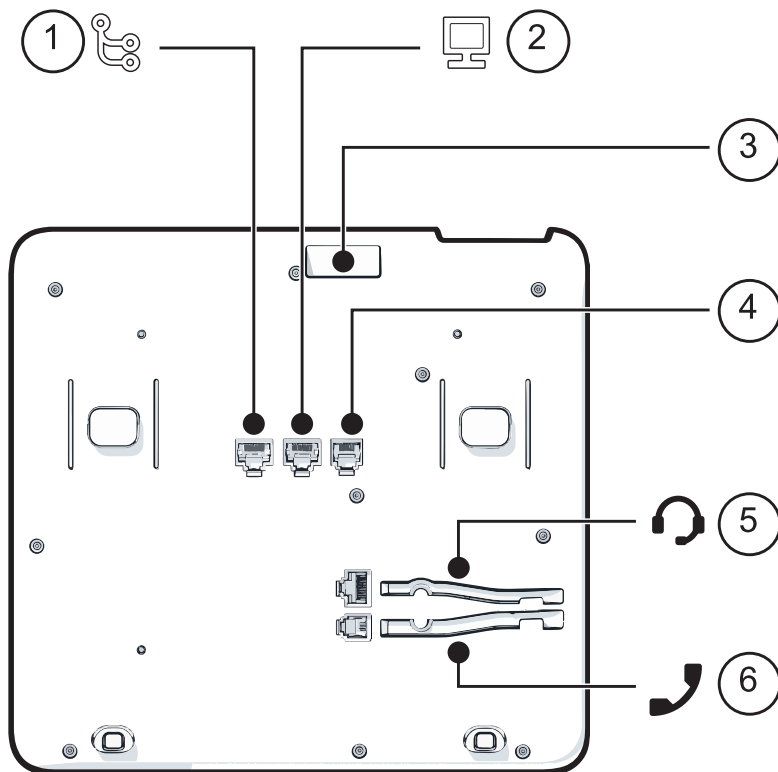
Connectors at the bottom side

OpenScape Desk Phone CP110



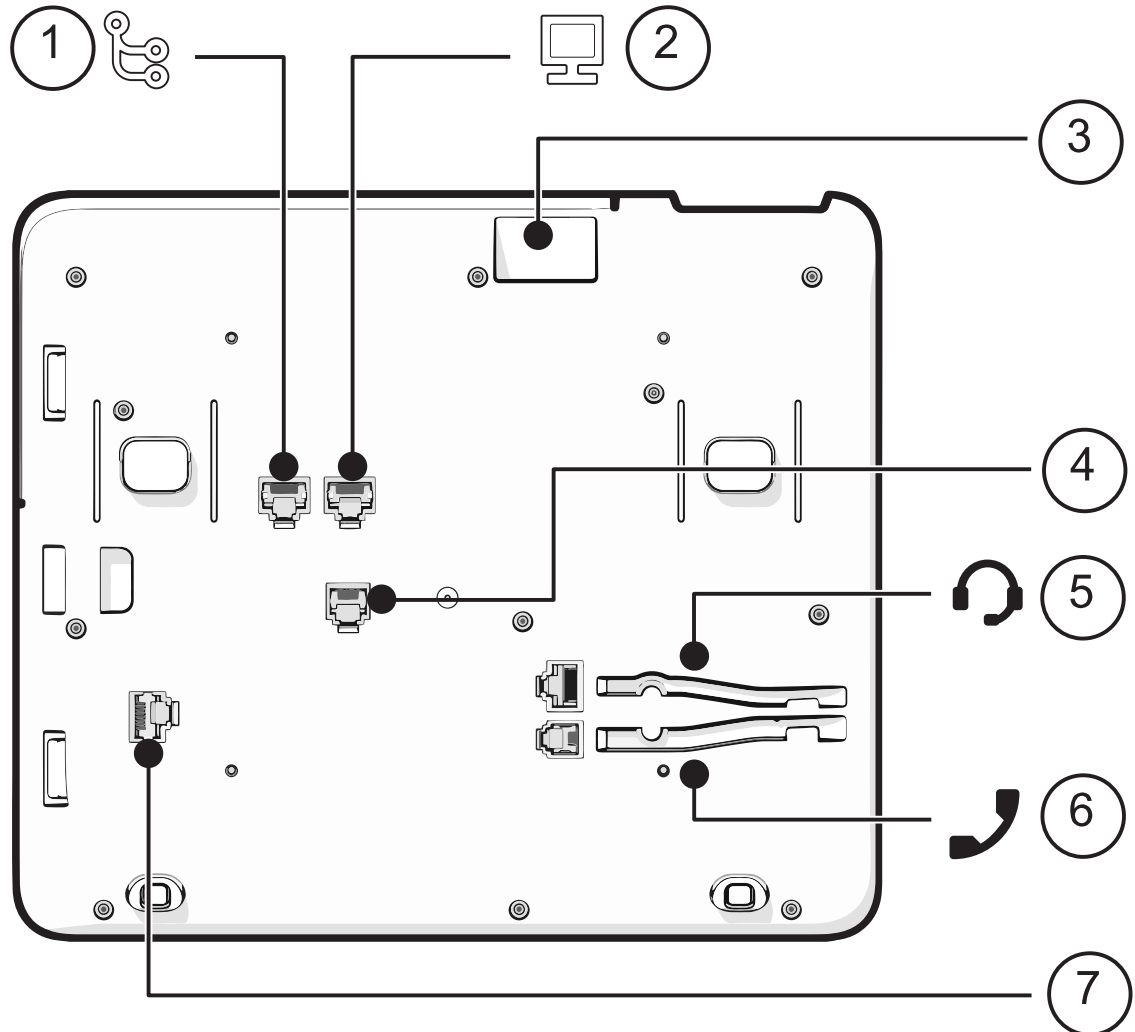
1	Network LAN port	2	PC LAN port
3	Optional power supply	4	Headset port
5	Handset port		

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
7	Key module port		

OpenScope 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		

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 consumption
OpenScape Desk Phone CP110	PoE (Power Class x)
OpenScape Desk Phone CP210	PoE (Power Class x)
OpenScape Desk Phone CP710 (Up to 4 key modules can be connected using PoE)	PoE (Power Class x)

2. If Power over Ethernet (PoE) is **not** supported or the CP410 / CP710 phone has more than four key module connected, plug the power supply unit into the mains.
3. Connect the plug-in power supply unit to the power connector  at the bottom of the phone.

Plug-in power supply	Order no.
Power supply, power cable and plug (Type E+F) for EU	L30250-F600-C141
Power supply, power cable and plug for Great Britain	L30250-F600-C142
Power supply, power cable and plug for USA	L30250-F600-C143
Power supply, power cable and plug for Switzerland	L30250-F600-C182
Power supply, power cable and plug for Italy	L30250-F600-C183
Power supply, power cable and plug for Australia	L30250-F600-C184
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

The OpenScope Desk Phones provide a 1 Gb/s Ethernet switch.

This allows you to connect one additional network device (e. g. a PC) directly via the telephone to the LAN. The direct connection functionality from phone to PC needs to be activated first. This type of connection allows you to save one network connection per switch with the advantage of less network cables and shorter connection distances.

Note Do not use this connection for further OpenScope Desk Phone CP phones, OpenScope Desk Phone IP phones, or OpenStage phones!

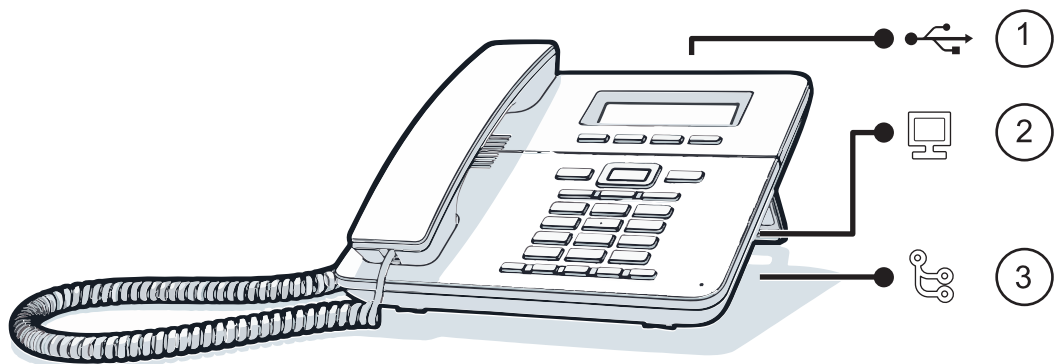


Fig.: 4-1: LAN connections (example)

How to connect the phone via USB Wi-Fi dongle

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



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

1. Insert the USB Wi-Fi dongle into the USB port.
2. Check that Wi-Fi is enabled (see "[Wi-Fi settings](#)" → page 65).
3. If applicable, connect the following optional jacks:
 - Headset (accessory)

Key modules

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

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

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

Quick start

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

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

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

How to access the web interface (WBM)

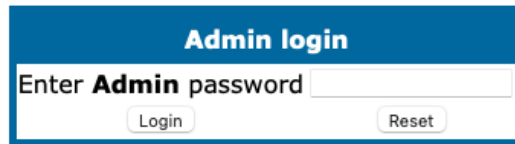
Prerequisites

- The phone IP address or URL is required for accessing the phone web interface via a web browser. By default, the phone will automatically search for a DHCP server on start-up and try to obtain IP data and further configuration parameters from that central server.
- If no DHCP server is available in the IP network or if the DHCP parameter is disabled, the IP address, subnet mask and default gateway /router must be defined manually.

Procedure

1. Access the local phone admin menu (see "[Access via local phone](#)" → page 25).
 - 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 27](#)).
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 58](#)).
 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

1. Press the key for "Settings" .
2. Enter the administrator password (default password is "123456"). It is highly recommended to change the password after your first login (see section ["Changing a password" → page 130](#)).
3. Confirm with **OK** .


OpenScape Desk Phone CP210

1. Press the key for "Settings" .
2. Enter the administrator password (default password is "123456"). It is highly recommended to change the password after your first login (see section ["Changing a password" → page 130](#)).
3. Confirm with **OK** .

OpenScape Desk Phones CP410 / CP710

1. Access the administration menu:
 - Press "1 3 0" simultaneously.
 - Press the "OR" key and use the Up Arrow, Down Arrow and OK keys consecutively to select the administration menu.

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

Key	Key function during text input	Key function when held down
	Enter special characters.	<ul style="list-style-type: none"> • 2 seconds: Ringer off • 3 seconds: Beep sound instead of ringer
	Toggle between lowercase characters, uppercase characters, and digits in the following order: (Abc) -> (abc) -> (123) -> (ABC) -> back to start.	Phone lock on / off.

1. With the OpenScope Desk Phone IP use the keypad for entering parameter values. Use the navigation keys or navigation block to navigate and execute administrative actions in the administration menu.
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, i. e. the SIP name or phone 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 54 for IP address and subnet mask, and "[Default router / gateway](#)" → page 55 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.

Wired settings	
LAN connection	
Use LLDP-MED	<input checked="" type="checkbox"/>
Use DHCP	<input checked="" type="checkbox"/>
DHCPv6 enabled	<input checked="" type="checkbox"/>
Use DHCP reuse	<input type="checkbox"/>
VLAN discovery	LLDP-MED
VLAN ID	
LLDP-MED operation	

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.

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 83](#).

Extended Network configuration

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

- **Static Routing Table** (Option #33): For manual configuration of specific/static routing, see ["Specific IP routing" → page 56](#).

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

- **Domain Name** (Option #15): For manual configuration of the DNS domain name, see ["DNS domain name" → page 57](#).

Vendor-specific VLAN discovery and DLS address

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

If the phone is located in a VLAN (Virtual LAN), a VLAN ID must be assigned. If the VLAN shall be provided by DHCP, VLAN Discovery must be set to "DHCP" (see ["Automatic VLAN discovery using LLDP-MED" → page 29](#)). The corresponding DHCP option is vendor-specific, thus a specific procedure is necessary.

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

- For manual configuration of the DLS server address see ["Configuration & update service" → page 60](#).
- For the configuration of vendor-specific settings by DHCP, there are two alternative methods:
 - Using a vendor class (see ["Using vendor class" → page 33](#))
 - Using the DHCP option #43 (see ["Using option #43 "Vendor Specific" → page 31](#))
- For DMS follow the instructions in ["Setting the DMS address via DHCP" → page 40](#).

VLAN discovery

If the phone is located in a VLAN (Virtual LAN), a VLAN ID must be assigned. If the VLAN is provided by DHCP, VLAN Discovery must be set to "DHCP" (see ["Automatic VLAN discovery using LLDP-MED" → page 46](#)). The corresponding DHCP option is vendor-specific, thus a specific procedure is necessary.

For information on how to use a vendor class, refer to ["Using vendor class" → page 33](#)

Automatic VLAN discovery using LLDP-MED

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

Administration via WBM

1. Open Network > Wired settings.

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

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

Administration via local phone

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

Manual configuration of a VLAN ID

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

Administration via WBM

1. Open Network > Wired settings.

Wired settings

LAN connection

Use LLDP-MED	<input type="checkbox"/>
Use DHCP	<input checked="" type="checkbox"/>
DHCPv6 enabled	<input checked="" type="checkbox"/>
Use DHCP reuse	<input type="checkbox"/>
VLAN discovery	DHCP
VLAN ID	

LLDP-MED operation

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

Please select mode

VLAN discovery: Manual

VLAN ID:

Submit Reset

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

Administration via local phone

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

Using option #43 "Vendor Specific"

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

- **Tag 001:** Vendor name
- **Tag 002:** VLAN ID

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

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

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

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

DLS server address

This setting only applies if a DLS / DMS server is in use.

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

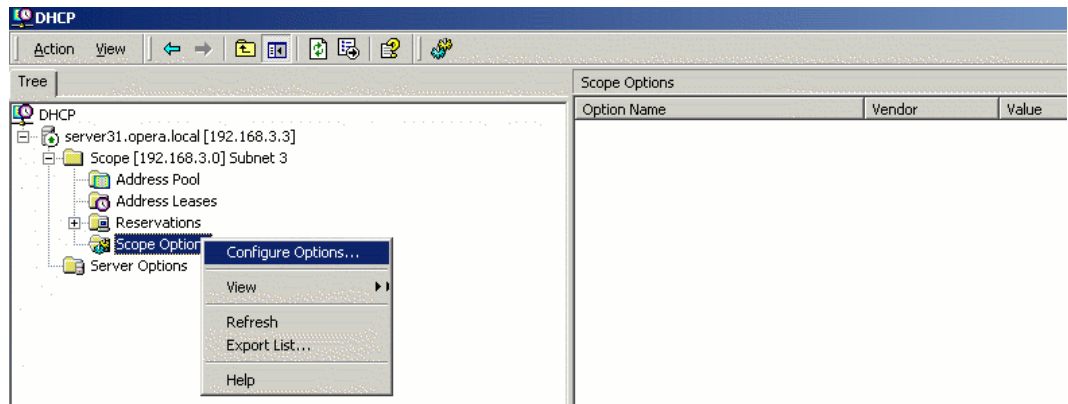
- For manual configuration of the DLS server address see ["Configuration & update service" → page 60](#).
- For configuration of the DMS, see ["Setting the DMS address via DHCP" → page 40](#).
- For the configuration of vendor-specific settings by DHCP, there are two alternative methods:
 - the use of DHCP option #43
 - the use of a vendor class

For information on how to use a vendor class, refer to ["Using vendor class" → page 33](#)

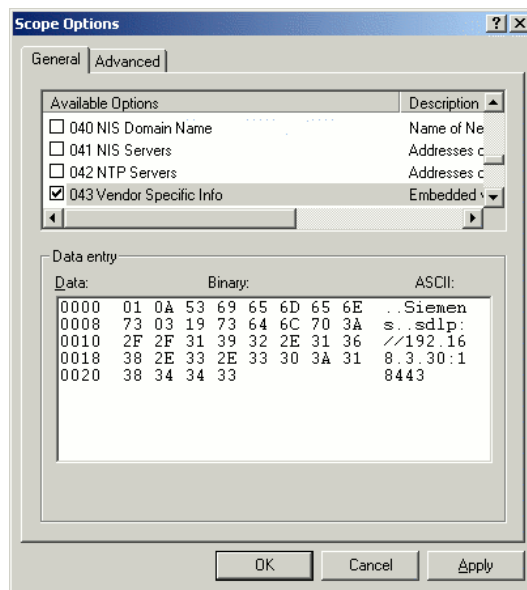
Setting up the DLS Server

1. In the Windows Start menu, select Start > Programs > Administrative Tools > DHCP.

2. Select the DHCP server and the scope.
3. Select "Configure Options" in the context menu using the right mouse button.



4. Enter the IP address and port number of the DLS server.



5. Click **Apply**.
6. Click **OK**.

Using option #43 "Vendor Specific"

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

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

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

- **Tag 004:** DLS hostname

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

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

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

The DLS IP address tag consists of the protocol prefix "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	.	2	.	1	9	:	1	8	4	4	3	
03	19	7-3	6-4	6-C	7-0	3-A	2-F	2-F	3-1	3-9	3-2	3-3	3-3	2-E	3-1	3-6	3-8	2-E	3-2	3-1	3-9	3-A	3-1	3-8	3-4	3-4	3-3

Using vendor class

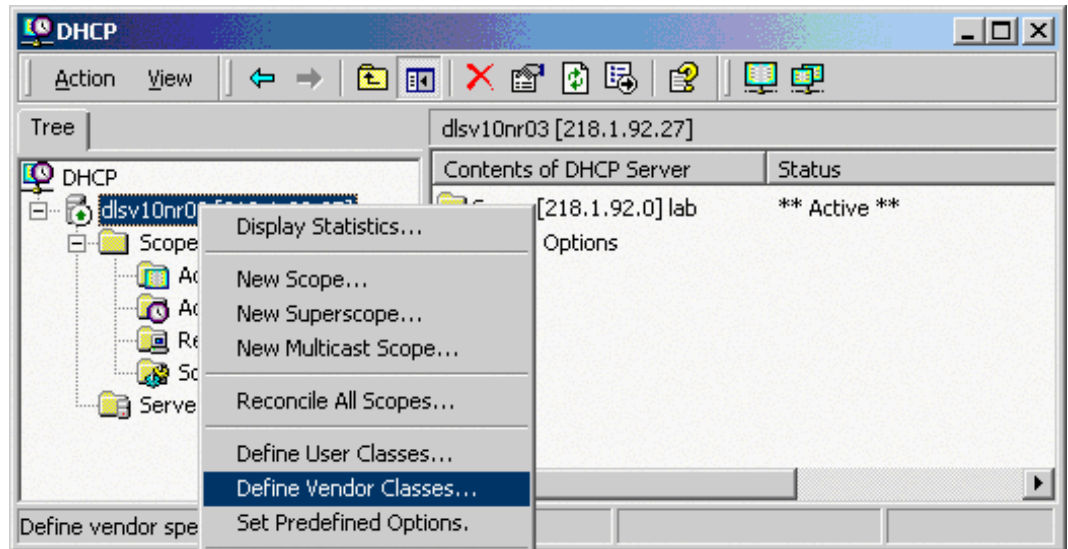
It is recommended to define a vendor class on the DHCP server, thus enabling server and phone to exchange vendor-specific data exclusively. The data is disclosed from other clients. If not done already, create a vendor class by the name of "OptiIpPhone".

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

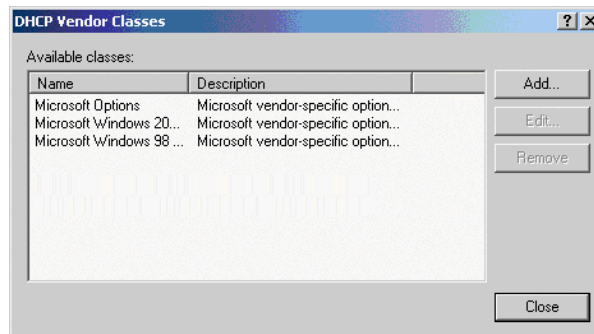
Setup using the Windows DHCP Server

1. In the Windows Start menu, select Start > Programs > Administrative Tools > DHCP.

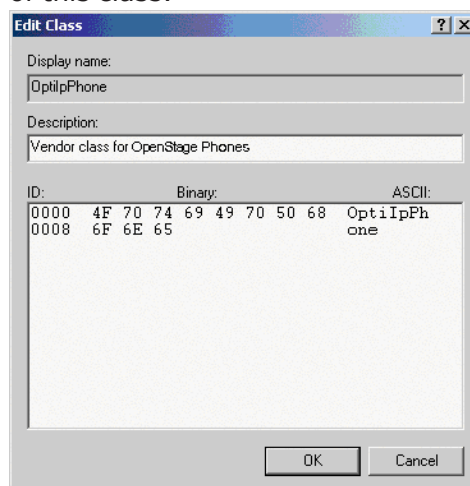
- In the DHCP console menu, right-click the required DHCP server and select **Define Vendor Classes...** in the context menu.



- Click **Add**.



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



- Click **OK**. The new vendor class now appears in the list.
- Close the window.

Add options to the new vendor class

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

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

Note For DHCP servers on a Windows 2003 Server (pre-SP2):
Windows 2003 Server contains a bug that prevents you from using the DHCP console to create an option with the ID 1 for a user-defined vendor class. Instead, this entry must be created with the netsh tool in the command line (DOS shell).

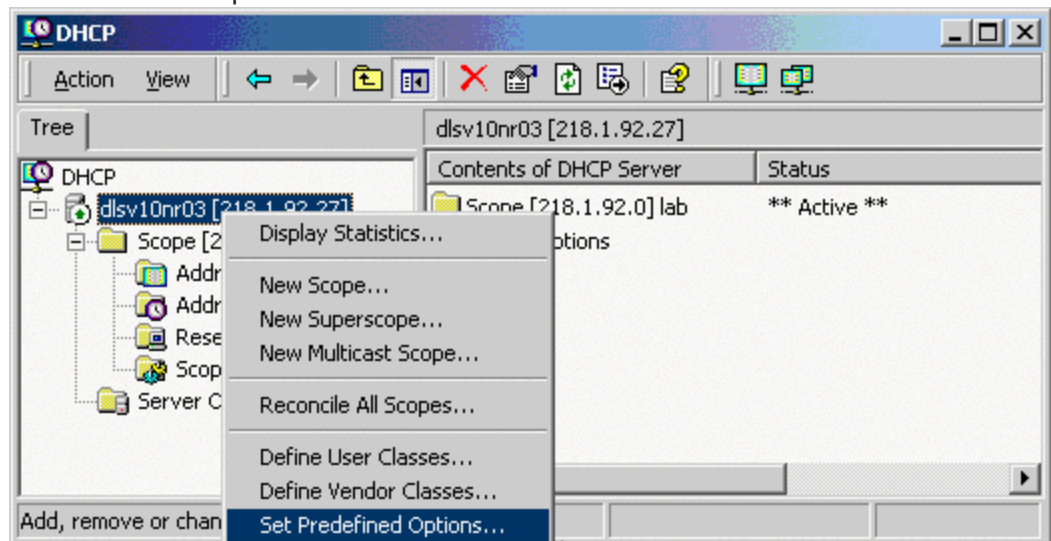
You can use the following command to configure the required option (without error message) so that it also appears later in the DHCP console:

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

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

This error was corrected in Windows 2003 Server SP2.

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



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

Predefined Options and Values [?] [X]

Option class: OptIpPhone

Option name: 001 OptIpPhone element 01

Add... Edit... Delete

Description: tag 1 for OptIpPhone class

Value

String: Siemens

OK Cancel

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

Change Option Type [?] [X]

Class: OptIpPhone

Name: OptIpPhone element 01

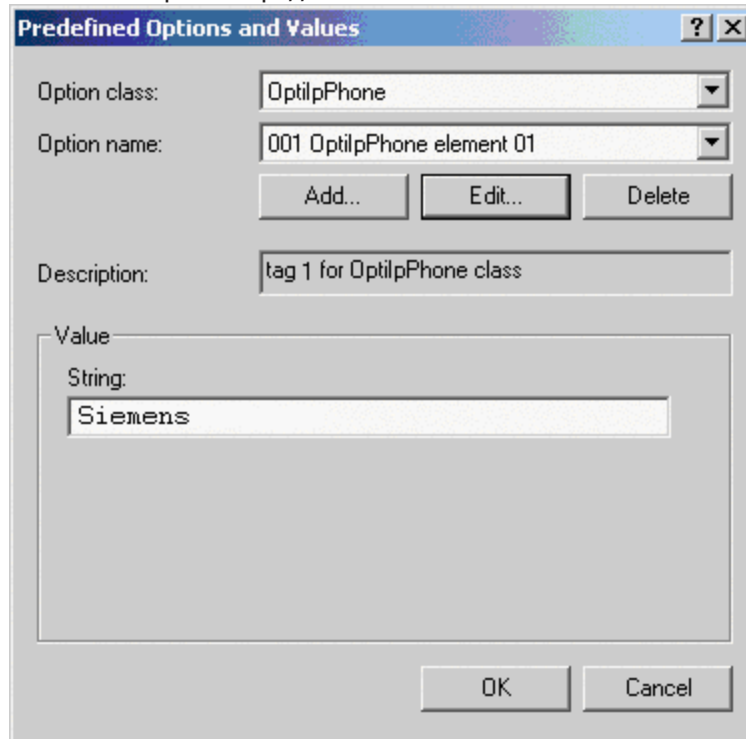
Data type: String Array

Code: 1

Description: tag 1 for OptIpPhone class

OK Cancel

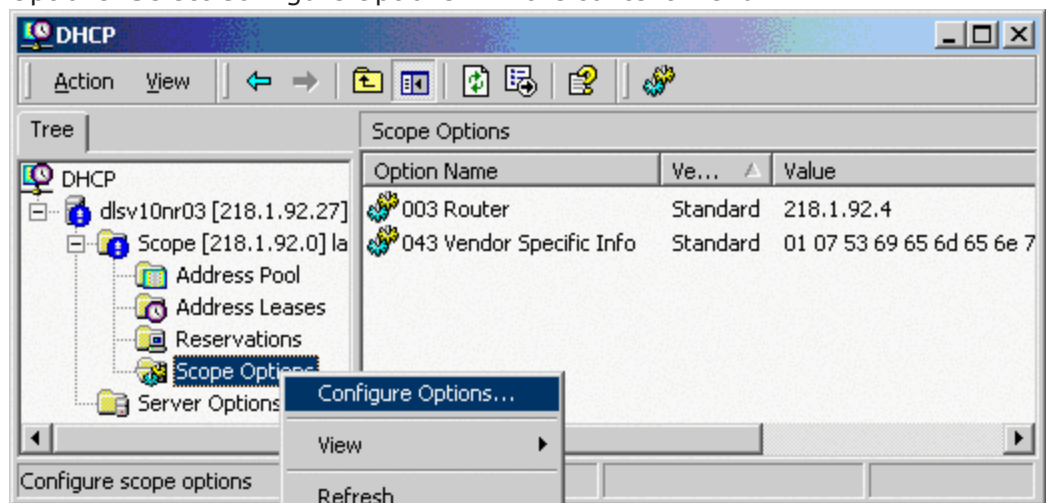
4. Enter the value for this option.
 - **First Pass:** "Siemens"
 - **Second Pass:** DLS address The DLS address has the following format:
<PROTOCOL>:://<IP ADDRESS OF DLS SERVER>:<PORT NUMBER>
Example: sdIp://192.168.3.30:18443



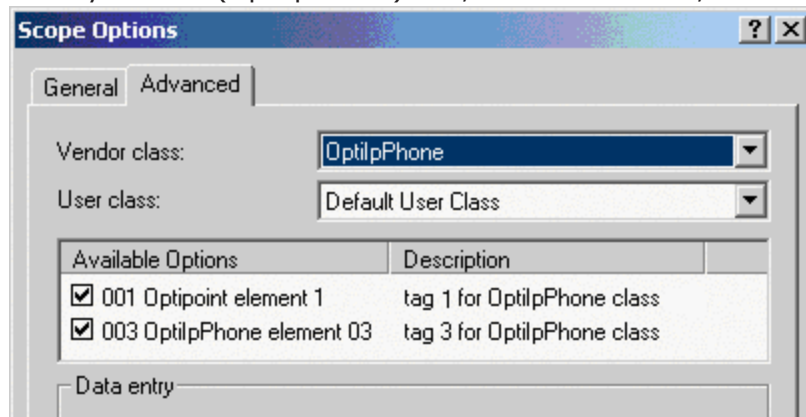
5. Click **OK**.
6. Repeat steps 2 to 5 for the second pass.

Defining the scope for the new vendor class

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



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



3. Activate the options that you want to assign to the scope (in this example, 001 and 003).
4. The DHCP console shows the information that is transmitted for the corresponding workpoints. Information from the Standard vendor is transmitted to all clients, whereas information from the OptiIpPhone vendor is transmitted only to the clients (workpoints) in this vendor class.

Setup using a DHCP server on Unix/Linux

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

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

HFA gateway settings

To connect the OpenScope Desk Phone CP phone to the OpenScope Business or OpenScope 4000 Communication System, the IP or DNS address of the gateway, a subscriber number and the corresponding password is needed.

The subscriber number can be 1 to 24 characters long, and is used as the internal telephone number.

Manual registration

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

Registration	
SIP addresses	
SIP server address	192.168.20.9
SIP registrar address	192.168.20.9
SIP gateway address	
SIP session	
Session timer enabled	<input type="checkbox"/>
Session duration (seconds)	3600
Registration timer (seconds)	3600
Subscription timer (seconds)	3600
Refresh minimum (seconds)	0
Server type	OS Voice
Realm	
User ID	12
Password	•••••

4. Enter the following data:
 - SIP server address
 - SIP registrar address
 - SIP gateway address
5. In the field "User ID", enter the internal extension number of the phone. It can be 1 to 24 characters long.
6. Enter the user password of the subscriber.
7. Click **Submit**.

Using the local menu

1. In the administration menu, go to System > Gateway. For further instructions on entering data using the Local menu see "[Access via local phone](#)" → page 25.

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

2. Enter the IP or DNS address of the HFA gateway provided by the OpenScape Communication System.

3. Enter the phone's Gateway Id, which will also serve as internal phone number.
4. Enter the password associated with the Gateway ID.
5. Select **Save & exit** and click **OK**.

Setting the DMS address via DHCP

When an IP phone is booting, it first obtains an IP address via DHCP. The DHCP server can provide the DMS address to the phone via Option #43 or Option #66.

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

Using option #43

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

Example

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

Each tag has an explicit length value and is closed by the ending "ff".

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

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

Using option #66

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

Option	Length	Content (Example)
42	1d	68747470733a2f2f39332e3132322e3131342e39363a343433-2f646d73

Option #66 does not have specific tags, only a length and content field. The above example provides the following URL in the content field.

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

Administration

This chapter describes the configuration of every parameter available on the OpenScope 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 24.

Bluetooth interface

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

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

Administration via WBM

1. Open Bluetooth.

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

Administration via local phone

|--- Bluetooth

LAN settings

LAN port settings

The OpenScope 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	
LAN port status	100 Mbps full duplex
LAN port speed	Any
IPv4 routing	
Route 1 IP address	<input type="text"/>
Route 1 gateway	<input type="text"/>
Route 1 mask	<input type="text"/>
Route 2 IP address	<input type="text"/>
Route 2 gateway	<input type="text"/>
Route 2 mask	<input type="text"/>
IPv6 routing	
Route 1 dest.	<input type="text"/>
Route 1 prefix len	<input type="text"/>
Route 1 gateway	<input type="text"/>
Route 2 dest.	<input type="text"/>
Route 2 prefix len	<input type="text"/>
Route 2 gateway	<input type="text"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

- **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" (OpenScape Desk Phone CP210 / CP410 / CP710 only).
 - Default: "Any"
- **PC port status:** Represents the connected (i.e. negotiated) speed (or "Link down" if not connected). This is read-only item.
- **PC port speed:** Settings for the Ethernet port connected to a PC.
 - Value range: "Any," "10 Mbps half duplex", "10 Mbps full duplex", "100 Mbps half duplex", "100 Mbps full duplex", "Gbps full duplex" (OpenScape Desk Phone CP210 / CP410 / CP710 only).
 - Default: "Any"
- **PC port mode:** Controls the PC port.
 - Value range: "disabled", "enabled", "mirror".
 - Default: "disabled"
- **PC port autoMDIX:** Switches between MDI and MDI-X automatically.
 - Value range: "On", "Off"
 - Default: "Off"
- **LAN port disabled (CP710 only):** 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
      |--- Number
        |--- LAN port speed
        |--- LAN port status
        |--- PC port speed
        |--- PC port status
        |--- PC port mode
        |--- PC port autoMDIX
```

VLAN

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

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

Note The implementation of a voice Network based on VLANs requires the Network infrastructure (the switch fabric) to support VLANs.

- In a layer-1 VLAN, the ports of a VLAN aware switch are assigned to a VLAN statically. The switch only forwards traffic to a particular port if that port is a member of the VLAN that the traffic is allocated to. Any device connected to a VLAN assigned port is automatically a member of this VLAN, without being a VLAN aware device itself. If two or more Network clients are connected to one port, they cannot be assigned to different VLANs. When a Network client is moving from one switch to another, the switches' ports have to be updated accordingly by hand.
- With a layer-2 VLAN, the assignment of VLANs to Network clients is realized by the MAC addresses of the Network devices. In some environments, the mapping of VLANs and MAC addresses can be stored and managed by a central database. Alternatively, the VLAN ID, which defines the VLAN whereof the device is a member, can be assigned directly to the device, e. g. by DHCP. The task of determining the VLAN for which an Ethernet packet is destined is carried out by VLAN tags within each Ethernet frame. As the MAC addresses are (more or less) wired to the devices, mobility does not require any administrator action, as opposed to layer 1 VLAN.

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

There are 3 ways for configuring the VLAN ID:

- By LLDP-MED
- By DHCP
- Manually

Automatic VLAN discovery using LLDP-MED

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

Administration via WBM

1. Open Network > Wired settings.

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

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

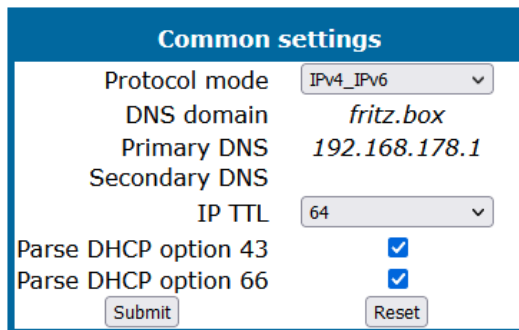
```
|--- Administration
  |--- Network
    |--- Wired settings
      |--- LAN connection
      |--- LLDP-MED operation
      |--- LAN port configuration
      |--- IPv4 routing
      |--- IPv6 routing
```

Automatic VLAN discovery using DHCP

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

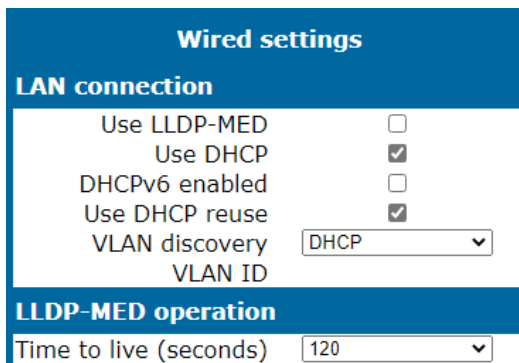
Administration via WBM

1. Open Network > Common settings.



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

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



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

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
      |--- LLDP-MED operation
      |--- LAN port configuration
      |--- IPv4 routing
      |--- IPv6 routing
```

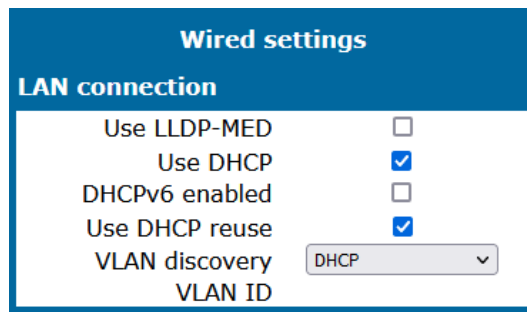
Manual configuration of a VLAN ID

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

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

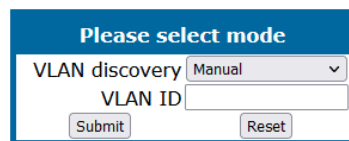
Administration via WBM

1. Open Network > Wired settings.



Wired settings	
LAN connection	
Use LLDP-MED	<input type="checkbox"/>
Use DHCP	<input checked="" type="checkbox"/>
DHCPv6 enabled	<input type="checkbox"/>
Use DHCP reuse	<input checked="" type="checkbox"/>
VLAN discovery	DHCP
VLAN ID	

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



Please select mode	
VLAN discovery	Manual
VLAN ID	
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

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

Administration via local phone

```
|--- Administration
  |--- Network
    |--- Wired settings
      |--- LAN connection
      |--- LLDP-MED operation
      |--- LAN port configuration
      |--- IPv4 routing
      |--- IPv6 routing
```

IP Network parameters

Quality of Service (QoS)

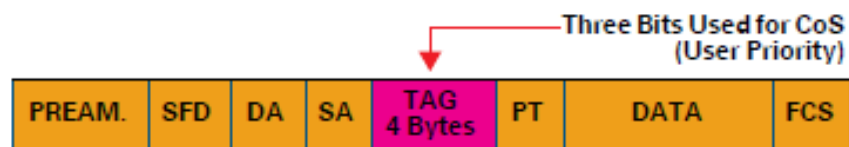
The QoS technology based on layer-2 and the two QoS technologies Diffserv and TOS / IP Precedence based on layer-3 are allowing the VoIP application to request and receive predictable service levels in terms of data throughput capacity (bandwidth), latency variations (jitter), and delay.

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

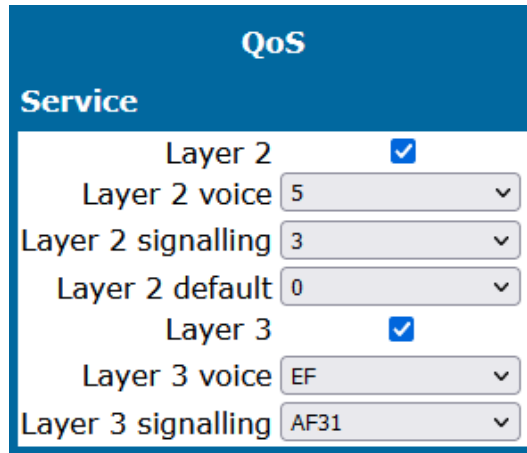
QoS on layer-2 is using 3 Bits in the 802.1q/p 4-Byte VLAN tag which must be added in the Ethernet header.

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.



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

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

Administration via local phone

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

Layer-3 / Diffserv

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

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

- Default: Any traffic that does not meet the requirements of any of the other defined classes is placed in the default per-hop behaviour group. Typically, the forwarding has best-effort forwarding characteristics. The DSCP (Diffserv Codepoint) value for Default is "0 0 0 0 0 0".
- Expedited Forwarding (EF referred to RFC 3246): Expedited Forwarding is used for voice (RTP streams) by default. It effectively creates a special low-latency path in the Network. The DSCP (Diffserv Codepoint) value for EF is "1 0 1 1 1 0".
- Assured Forwarding (AF referred to RFC 2597): Assured forwarding is used for signaling messages by default (AF31). It is less stringent than EF in a multiple dropping system. The AF values are containing two digits X and Y (AFX Y), where X is describing the priority class and Y the drop level. Four classes X are reserved for AFX Y: AF1 Y (low priority), AF2 Y, AF3 Y and AF4 Y (high priority). Three drop levels Y are reserved for AFX Y: 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.

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

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

Administration via local phone

```

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

Use DHCP

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

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

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

Note The change will only have effect if you restart the phone. The phone is able to maintain its IP connection even in case of DHCP server failure.

DHCP parameters

The following parameters can be obtained by DHCP:

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

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.

Wired settings	
LAN connection	
Use LLDP-MED	<input type="checkbox"/>
Use DHCP	<input type="checkbox"/>
DHCPv6 enabled	<input type="checkbox"/>
Use DHCP reuse	<input type="checkbox"/>
VLAN discovery	Manual <input type="button" value="v"/>
VLAN ID	<input type="text"/>
LLDP-MED operation	
Time to live (seconds)	120 <input type="button" value="v"/>
LAN port	
LAN port status	1 Gbps full duplex
LAN port speed	Any <input type="button" value="v"/>

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.

Wired settings	
LAN connection	
Use LLDP-MED	<input type="checkbox"/>
Use DHCP	<input type="checkbox"/>
DHCPv6 enabled	<input type="checkbox"/>
Use DHCP reuse	<input type="checkbox"/>
VLAN discovery	Manual
VLAN ID	<input type="text"/>
LLDP-MED operation	
Time to live (seconds)	120
LAN port	
LAN port status	1 Gbps full duplex
LAN port speed	Any

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

Administration via local phone

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

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

Default router / gateway

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

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

Administration via WBM - IPv4 Configuration

1. Open Network > Wired settings.

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

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

Administration via local phone - IPv4 configuration

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

Specific IP routing

To have constant access to network subscribers of other domains, you can enter a total of two more network destinations, in addition to the default route/gateway. This is useful if the LAN has more than one router or if the LAN is divided into subnets.

IPv4 route configuration

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

Administration via WBM - IPv4 configuration

1. Open Network > IPv4 configuration.

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

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

Administration via local phone

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

DNS

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

DNS domain name

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

Administration via WBM

1. Open Network > Common settings.

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

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

Administration via local phone

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

DNS servers

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

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

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

Administration via WBM

1. Open Network > Common settings.

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

2. 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 > Wired settings.
2. Go to tab "LLDP-MED operation".

Wired settings	
LAN connection	
Use LLDP-MED	<input type="checkbox"/>
Use DHCP	<input type="checkbox"/>
DHCPv6 enabled	<input type="checkbox"/>
Use DHCP reuse	<input type="checkbox"/>
VLAN discovery	Manual <input type="text"/>
VLAN ID	<input type="text"/>
LLDP-MED operation	
Time to live (seconds)	120 <input type="text"/>
LAN port	
LAN port status	1 Gbps full duplex
LAN port speed	Any <input type="text"/>

3. Select the desired value for "Time to live (seconds)".
4. Click **Submit**.

Administration via local phone

```
|--- Admin
  |--- Network
    |--- Wired settings
      |--- LLDP-MED operation
        |--- TTL
```

Configuration & update **service**

The OpenScape Deployment Service (DLS) is a OpenScape management application for administering workpoints in both HiPath and non-HiPath 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.

DLS address, i.e. the IP address or host name of the DLS server, and default mode port, i.e. the port on which the DLS server is listening, are required to enable proper communication between phone and DLS.

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

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

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

Only outbound connections from the phone are allowed. To overcome this restriction, a DLS "Contact-Me" proxy (DCMP) can be deployed. The phone periodically polls the DCMP, which is placed outside of the phone Network, for pending contact requests from the DLS. If there are contact requests, the phone will send a request to the DLS in order to obtain the update, just as with a regular DLS connection.

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

A security PIN can be provided which is used for decrypting data provided by the DLS during bootstrap. For further information, refer to the DLS documentation.

Administration via WBM

1. Open Network > Update Service (**DLS**).

Update service	
Select either DLS or DMS for use by providing an address, but only for one of them	
Deployment service (DLS)	
DLS address	<input type="text"/>
Default mode port	<input type="text" value="18443"/>
Revert to default security	<input type="checkbox"/>
Mode	Default <input type="text"/>
Security PIN	<input type="text"/>
Device management service (DMS)	
DMS address	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Minimum update check (seconds)	<input type="text" value="300"/>
Update check during working hours	<input checked="" type="checkbox"/>
Ignore software update from config file	<input type="checkbox"/>
Check for update	<input type="button" value="Now"/> <input type="button" value="Reset"/>
<input type="button" value="Submit"/>	

- **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.
- **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.

Administration via local phone

```
|--- Admin
  |--- Network
    |--- Update Service
      |--- DLS address
        |--- Default mode port
      |--- Revert to default security
        |--- Mode
      |--- Security PIN
```

SNMP

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

Note OpenScape Desk Phone CP phones support SNMPv1.

Trap categories

There are currently 3 trap categories that can be sent by the phones:

- Standard SNMP traps: OpenScape Desk Phone CP phones support the following types of standard SNMP traps, as defined in RFC 1157:
 - **coldStart**: sent if the phone does a full restart.
 - **warmStart**: sent if only the phone software is restarted.
 - **linkUp**: sent when IP connectivity is restored.
- QoS Related traps: These traps are designed specifically for receipt and interpretation by the QDC collection system. The traps are common to SIP phones, HFA phones, Gateways, etc.
- Traps specific to OpenScape Desk Phone CP phones. Currently, the following traps are defined:
 - **TraceEventFatal**: sent if severe trace events occur; aimed at expert users.
 - **TraceEventError**: sent if severe trace events occur; aimed at expert users.

Administration via WBM

1. Open System > SNMP.

SNMP

Generic traps

Trap sending enabled	<input type="checkbox"/>
Trap destination	<input type="text"/>
Trap destination port	<input type="text" value="162"/>
Trap community	<input type="text" value="*****"/>
Queries allowed	<input type="checkbox"/>
Query password	<input type="text"/>

Diagnostic traps

Diagnostic sending enabled	<input type="checkbox"/>
Diagnostic destination	<input type="text"/>
Diagnostic destination port	<input type="text"/>
Diagnostic community	<input type="text"/>
Diagnostic to generic destination	<input type="checkbox"/>

QoS report traps

QoS traps to QCU	<input type="checkbox"/>
QCU address	<input type="text"/>
QCU port	<input type="text" value="12010"/>
QCU community	<input type="text" value="*****"/>
QoS to generic destination	<input type="checkbox"/>

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

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

Administration via local phone

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

OpenScape service menu

The phone local menu allows for controlling functions provided the OpenScape system. For this purpose, the phone must be logged on at the system.

For information on the available functions, see the phone's user manual.

Administration via local phone

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

Wi-Fi settings

Note This option is only available for the OpenScape Desk Phone CP710, and the OpenScape Desk Phones CP210 and CP410 with an attached Wi-Fi USB dongle.

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. The supported authentication protocols are the following:

- EAP-TLS
- EAP-LEAP
- FAST

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

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

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

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

Administration via WBM

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

Wi-Fi settings

Enable Wi-Fi interface	<input type="checkbox"/>
Wi-Fi MAC address	""
Wi-Fi link status	down
Last connected Wi-Fi network name	""
Wi-Fi country settings	United Kingdom ▾

Advanced settings

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

Add new Wi-Fi network

Wi-Fi SSID	<input type="text"/>
Hidden SSID	<input type="checkbox"/>
Wi-Fi password	<input type="text"/>
Encryption type	WPA2/WPA3-Personal ▾
IP settings	DHCP ▾
IP address	<input type="text"/>
Subnet mask	<input type="text"/>
Default route	<input type="text"/>
Authentication protocol	None ▾
EAP anonymous identity	<input type="text"/>
EAP identity	<input type="text"/>
EAP password	<input type="text"/>

Stored Wi-Fi networks

Wi-Fi SSID	Signal	Encryption type	IP settings	Wi-Fi Password
<i>No saved Wi-Fi networks</i>				

2. Enable the Wi-Fi interface. If disabled, the phone can only connect via Ethernet cable.

Administration via local phone

```

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

Setting up a WiFi connection

When a WiFi-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 WiFi 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).

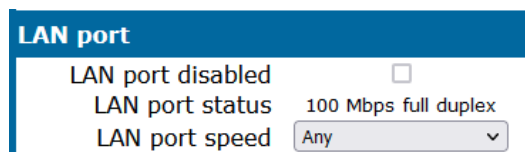
Once the phone has acquired a DLS address, it will open up a secure connection to DLS for downloading configuration parameters using the WPI protocol. Any certificates needed for Wi-Fi authentication or SIP/TLS will also be downloaded as a part of this process. If a DLS address is specified in the downloaded 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 OpenScope Desk Phone CP710 provides 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
        |--- Port configuration
```

Advanced Wi-Fi settings

The OpenScope Desk Phone CP710 provides advanced Wi-Fi options to reduce down-time 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 LocalAdmin, except:

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

Administration via local phone

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

System settings

HFA gateway settings

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

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

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

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

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

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

Administration via WBM

1. Open System > **Gateway**.
 - IP address: IP or DNS address of the communication platform or HFA server.
 - Subscriber number: The phone extension.
 - Password: Password for logging on to the HFA server.
2. Open Network > Port number **configuration**.

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

Administration via local phone

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

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

HFA emergency gateway settings

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

The settings are analog to those for the main system (see "HFA gateway settings" → page 71).

Administration via WBM

1. Open System > Standby gateway.
2. Open Network > Port number configuration.

Administration via local phone

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

|--- Admin
    |--- Network
        |--- Port configuration
            |--- Standby gateway
```

Server and standby server ports

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

Administration via WBM

1. Open Network > Port number configuration.
 - H.225.0 port determines the port used for non-secure H.225 signaling. Default: 1720.
 - CorNet-TLS port determines the port used for secure communication by the HFA server.
 - H.225.0 TLS port determines the port used for secure H.225 signaling.

Administration via local phone

```

|--- Admin

    |--- Network

        |--- Port configuration

            |--- Server port configuration

                |--- H.225.0 port

                |--- TC TLS port

                |--- H.225.0 TLS port

            |--- Standby server port configuration

                |--- H.225.0 port

                |--- TC TLS port

                |--- H.225.0 TLS port

```

Redundancy

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

Administration via WBM

1. Open System > **Redundancy**.
 - When "Small remote side redundancy" is activated, the phone switches to the standby HFA server if the connection to the main server is lost. By default, this is disabled.
 - When "Auto switch back" is activated, the phone will switch back to the main server as soon as the connection is re-established. By default, this is disabled.
 - "Retry count main" sets the number of trials to establish a connection to the main server before the phone switches over to the standby server. The default is 1.
 - The "Timeout main" determines the time interval between the last try to get a connection to the main server and the establishing of a connection to the standby server. The default is 30.
 - "Retry Count Standby" sets the number of trials to establish a connection to the standby server before the phone switches back to the main server. The default is 3.
 - "Timeout Standby" sets the timeout between two "Retry count standby". The default is 30.
 - "Timeout main" sets the timeout between two "Retry count main". The default is 30.

- “TC test retry” determines the count of how many successful TC tests the main system needs to answer before the phone switches back with Auto switchback enabled. The default is 3.
- “TC Test Expiry” determines how long the Previous connection needs to timeout to actually trigger any further SRSR activities.
How much time to wait from one unsuccessful retry count main sequence until the next happens and in which interval the phone will send itself a TC test message (in idle mode). The default is 30.
Lowering this value will significantly increase Network load but the phone might detect failures faster but at an increased risk of false positive detections due to short time Network outage.
After a change of the timing values the SRSR need to be deactivated and re-activated again to take effect.

Administration via local phone

```
|--- Admin
    |--- System
        |--- Redundancy
            |--- Small remote site
            |--- Auto switch back
            |--- Retry count main
            |--- Timeout main
            |--- Retry count stdby
            |--- Timeout standby
```

Emergency number

E.911 emergency number. This number establishes a connection to the PSAP (Public Safety Answering Point). If a user dials this number, and an appropriate LIN (see "LIN" → page 76) is configured, the user location is communicated to the PSAP. In the US, the number is 911.

Administration via WBM

1. Open System > Features > Configuration.

Configuration	
General	
Emergency number	<input type="text"/>
Voice mail number	<input type="text"/>
MWI LED	AlertBar only <input type="button" value="v"/>
Missed call LED	AlertBar LED <input type="button" value="v"/>
AlertBar LED hint	<input type="checkbox"/>
Allow refuse	<input type="checkbox"/>
Hot/Warm phone	No action <input type="button" value="v"/>
Hot/Warm destination	<input type="text"/>
Initial digit timer (seconds)	30 <input type="text"/>
Allow uaCSTA	<input checked="" type="checkbox"/>
Server features	<input checked="" type="checkbox"/>
Not used timeout (minutes)	2 <input type="button" value="v"/>
Transfer on hangup	<input type="checkbox"/>
Bridging enabled	<input type="checkbox"/>
Dial plan enabled	<input type="checkbox"/>
FPK program timer	On <input type="button" value="v"/>
Selected Dial Action on calls	No action <input type="button" value="v"/>
DSS monitored	<input type="checkbox"/>
Show icon for all forwarding types	<input type="checkbox"/>
Automatic key module switchback	<input checked="" type="checkbox"/>
Simultaneous key module switching	<input checked="" type="checkbox"/>

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

Administration via local phone

```

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

```

LIN

The Location Identification Number (LIN) is a number code that provides detailed geographic information about the phone, including the office room. On issuing an emergency call using the E.911 emergency number (see "[Emergency number](#)" → page 75), this code is transferred to an ALI (Automatic Location Information) system in the public Network. When the ALI has looked up the location data in its database, it transmits

the data along with the call to the PSAP. The emergency operator is presented with the location data in readable form, so he can dispatch help as appropriate.

Administration via WBM

1. Open System > Features > **Configuration**.

Administration via local phone

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

Not used timeout

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

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

The timeout may be helpful in case a user does a long press on a line key unintentionally, and thereby invokes the key configuration menu. The menu will close after the timeout, and the key will return to normal line key operation.

Administration via WBM

1. Open System > Features > Configuration.

Configuration	
General	
Emergency number	<input type="text"/>
Voice mail number	<input type="text"/>
MWI LED	AlertBar only <input type="button" value="v"/>
Missed call LED	AlertBar LED <input type="button" value="v"/>
AlertBar LED hint	<input type="checkbox"/>
Allow refuse	<input type="checkbox"/>
Hot/Warm phone	No action <input type="button" value="v"/>
Hot/Warm destination	<input type="text"/>
Initial digit timer (seconds)	30 <input type="text"/>
Allow uaCSTA	<input checked="" type="checkbox"/>
Server features	<input checked="" type="checkbox"/>
Not used timeout (minutes)	2 <input type="button" value="v"/>
Transfer on hangup	<input type="checkbox"/>
Bridging enabled	<input type="checkbox"/>
Dial plan enabled	<input type="checkbox"/>
FPK program timer	On <input type="button" value="v"/>
Selected Dial Action on calls	No action <input type="button" value="v"/>
DSS monitored	<input type="checkbox"/>
Show icon for all forwarding types	<input type="checkbox"/>
Automatic key module switchback	<input checked="" type="checkbox"/>
Simultaneous key module switching	<input checked="" type="checkbox"/>

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

Administration via local phone

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

Enable telephony settings

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

Users can access limited menu options and set basic telephony settings without the need of a password. Since the administrator enables the option "Enable telephony settings", the item "Configure telephone" appears on the telephone screen while navigating from the idle menu to Service/Settings.

The user password is not required to navigate to this option. The option is disabled by default.

Administration via WBM

1. Open System > Features > **Configuration**.

Administration via local phone

```
|--- Admin
      |--- System
            |--- Features
                  |--- Configuration
                          |--- Telephony settings
                                  |--- Enable telephony settings
```

Energy saving

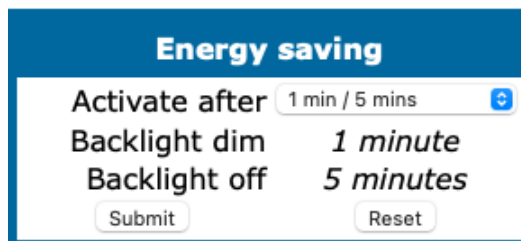
Backlight time setting

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.



Energy saving	
Activate after	1 min / 5 mins
Backlight dim	1 minute
Backlight off	5 minutes
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

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

Administration via local phone

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

Energy efficient Ethernet

The OpenScape Desk Phone CP110 / CP210 / CP410 / CP710 phones support the standard IEEE 802.3az (Energy efficient Ethernet).

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

System

OpenScape Desk Phone CP phones support the following security option:

- PKI-based SPE (Signaling and Payload Encryption)

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

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

Certificate validation main/standby shows whether the phone certificate used for encrypted logon via TLS is checked against the certificate on the gateway (read only). For configuration see ["Authentication policy" → page 133](#).

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

- Open System > Security > System.

System	
Validate SW upgrade	<input checked="" type="checkbox"/>
DoS protection	<input type="checkbox"/>
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

- 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
                |--- Signalling main
                |--- Signalling stdb
                |--- Certificate main
                |--- Certificate stdb
                |--- TLS renegotiation
```

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.
- **The Server TLS interface**

Administration via local phone

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

Security log

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

Note The security log cannot be disabled.

Administration via WBM

1. Open System > Security > Logging.

- The **Max. lines** parameter defines the maximum number of entry lines that can be kept in the security log before old entries are overwritten by new entries.

- **Automatic archive to DLS** controls whether the log is sent to the DLS. When activated, the DLS is used to automatically archive the security log so that no log entries is lost.
- **Archive when at:** This value sets the trigger for log archiving. Automatic archiving of new security log entries will occur when the percentage of unarchived entries in the log is as specified or more. The value may be set to 0% by both the phone and the DLS and this value will prevent the phone from archiving or telling the DLS that it needs archiving.
- The security log upload may be accomplished in two ways:
 - If "Automatic archive to DLS" is enabled, if the security log reaches the threshold % for unachieved entries, the phone will initiate an upload.
 - If "Automatic archive to DLS" is NOT enabled and the security log reaches the threshold % for unachieved entries, the phone only sets the "archive-me" flag, it does not initiate the archive. It is up to the DLS to recognize the flag and initiate an upload.
- **Last archived** shows the date when the security log was last archived to the DLS.

Administration via local phone

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

Date and time

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

For correct display of the current time, the Timezone offset must be set appropriately. This is the time offset from UTC (Universal Time Coordinated). If, for instance, the phone is located in Munich, Germany, the offset is +1 (or simply 1); if it is located in Los Angeles, USA, the offset is -8. For countries or areas with half-our time zones, like

South Australia or India, non-integer values can be used, for example 10.5 for South Australia (UTC +10:30).

If the phone is located in a country with DST (Daylight Saving Time), you can choose whether DST is toggled manually or automatically.

- For manual toggling, disable "Auto time change" and enable or disable "Daylight saving"; the change is in effect immediately.
- For automatic toggling, enable "Auto time change". Daylight saving is controlled by the DST zone / time zone parameter. This parameter determines when DST starts or ends, and must be set according to the location of the phone.

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

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

Settings via SNTP

Administration via WBM

1. Open Date and time.

Date and time	
Time source	
SNTP primary	<input type="text" value="192.168.12.1"/>
SNTP backup	<input type="text" value="172.25.14.51"/>
Timezone offset (hours)	<input type="text" value="2"/>
Daylight saving	
Daylight saving	<input checked="" type="checkbox"/>
Difference (minutes)	<input type="text" value="60"/>
Auto time change	<input checked="" type="checkbox"/>
DST zone	<input type="text" value="Not set"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

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

"New Zealand", "New Zealand (Chatham)".

- Default setting for US is "United States". After a factory reset, the system is reset to this value.

Administration via Local Phone

```
|--- Administration
  |--- Date and Time
    |--- Time source
      |--- SNTP primary
      |--- SNTP backup
      |--- Timezone offset
    |--- Daylight saving
      |--- Daylight saving
      |--- Difference (mins)
      |--- Auto DST
      |--- DST zone
```

Dialing

Canonical dialing configuration

Call numbers taken from a directory application, LDAP for instance, are mostly expressed in canonical format. Moreover, call numbers entered 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. If, for instance, 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".


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.

Note To enable the number conversion, all parameters not marked as optional must be provided, and the canonical lookup settings must be configured (see "[Canonical dialing look-up](#)" → page 159).

Administration via WBM

1. Open Local functions > Locality > Canonical dial settings.

Canonical dial settings


Warning – changes to these settings could prevent calls being matched to existing conversations

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

- Local country code: E.164 country code, e.g. "49" for Germany, "44" for United Kingdom
 - Maximum length: 5
- National prefix digit: prefix for national connections, e.g. "0" in Germany and United Kingdom
 - Maximum length: 5
- Local national code: local area code or city code, e.g. "89" for Munich, "20" for London
 - Maximum length: 6
- Minimal local number length: minimum number of digits in a local PSTN number, e.g. 3335333 = 7 digits
- Local enterprise node: number of the company/PBX wherein the phone is residing
 - Maximum length: 10 (optional)
- 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 / Initial digits: List of initial digits of all possible extensions in the local enterprise Network. When a call number could not be matched as a public Network number, the phone checks if it is part of the local enterprise Network. This is done by comparing the first digit of the call number to the value(s) given here. If it matches, the call number is recognized as a local enterprise number and processed accordingly. If, for instance, the extensions 3000-5999 are configured in the OpenScape Desk Phone, each number will start with 3, 4, or 5. Therefore, the digits to be entered are 3, 4, 5.

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 lookup table is provided ("[Canonical dialing look-up](#)" → page 159).

- **"Local enterprise form"**: Default value. Any extension number is dialed in its simplest form. For an extension on the local enterprise node, the node ID is omitted. If the extension is on a different enterprise node, then the appropriate node ID is prefixed to the extension number. Numbers that do not correspond to an enterprise node extension are treated as external numbers.
- **"Always add node"**: Numbers that correspond to an enterprise node extension are always prefixed with the node ID, even those on the local node. Numbers that do not correspond to an enterprise node extension are treated as external numbers.
- **"Use external numbers"**: All numbers are dialled using the external number form.
- External numbers
 - **"Local public form"**: Default value. All external numbers are dialed in their simplest form. Thus a number in the local public Network region does not have the region code prefix. Numbers in the same country but not in the local region are dialled as national numbers. Numbers for a different country are dialled using the international format.
 - **"National public form"**: All numbers within the current country are dialled as national numbers, thus even local numbers will have a region code prefix (as dialling from a mobile). Numbers for a different country are dialled using the international format.

- **"International form"**: All numbers are dialled using their full international number format.
- External access code
 - **"Not required"**: The access code to allow a public Network number to be dialled is not required.
 - **"For external numbers"**: Default value. All public Network numbers 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 dialled 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
|--- Admin
  |--- Local Functions
    |--- Locality
      |--- Canonical dial
        |--- Internal numbers
          |--- External numbers
          |--- External access code
          |--- Internat(ional) access
```

Canonical dial look-up

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

In the local phone book, and, mostly, in LDAP directories, numbers are stored in canonical format. In order to generate an appropriate dial string according to the settings in Internal numbers and External numbers, internal numbers must be discerned

from external numbers(see "Canonical dialing configuration" → page 85). The canonical look-up table provides patterns which allow for operation.

Furthermore, these patterns enable the phone to identify callers from different local or international telephone networks by looking up the caller’s number in the phone book. As incoming numbers are not always in canonical format, their composition must be analyzed first. For this purpose, an incoming number is matched against one or more patterns consisting of country codes, national codes, and enterprise nodes. Then, the result of this operation is matched against the entries in the local phone book.

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

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

You can view and edit the first five entries via the WBM. The Local code 1...5 parameters define up to 5 different local enterprise nodes, whilst International code 1...5 define up to 5 international codes, that is, fully qualified E.164 call numbers for use in a PSTN. The whole list of entries are not visible on the phone but can be seen and handled using the DLS.

Administration via WBM

1. Open Locality > Canonical dial lookup.

Canonical dial lookup

Warning – changes to these settings could prevent calls being matched to existing conversations

Equivalent number forms

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

- **Local code 1...5:** Local enterprise code for the node / PBX the phone is connected to.
 - Example: "7007" for Unify office in Munich.
- **International code 1...5:** Sequence of "+", local country code, local area code, and local enterprise node corresponding to one or more phone book entries.
 - Example: "+49897007" for Unify office in Munich.

Administration via local phone

```
|--- Administrator settings
  |--- Local Functions
    |--- Locality
      |--- Canonical dial lookup
        |--- Local code 1
        |--- International code1
        |--- Local code 2
        |--- International code 2
        |--- Local code 3
        |--- International code 3
        |--- Local code 4
        |--- International code4
        |--- Local code 5
        |--- International code5
```

Ringer setting

Distinctive ringing

The server may provide information indicating a specific type of call within an incoming call. The phone can use this information to choose a ring tone according to the call type from the "Distinctive ringer table".

Administration via WBM

1. Open Admin > Ringer setting > Distinctive.

Distinctive

This page allows you to set up interworking with other IP phone systems that support distinctive ringing

Name	Ringer sound	Pattern melody	Pattern sequence	Duration (sec)	Audible
Bellcore-dr1	Pattern	2	2	60	Ring
Bellcore-dr2	Pattern	2	2	60	Ring
Bellcore-dr3	Pattern	2	2	60	Ring
alert-emergen	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring
	Pattern	2	2	60	Ring

Submit
Reset

- When the string sent via alert-info matches the string specified in the Name parameter, the corresponding ringer is triggered. For instance, the OpenScope Voice system may send the string `Bellcore-dr1` to indicate that a call is from within the same business group, and the Name parameter is set to "Bellcore-dr1". To select a specific ring tone for calls from the same business group, the other parameters corresponding to that Name must be set accordingly.
- The ringer sound parameter determines whether a pattern, i. e. melody, or a specific sound file shall be used as ringer.
- Pattern melody selects the melody pattern that 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
- The Duration parameter determines how long the phone will ring on an incoming call. The range is 0-300 sec.
- With the Audible parameter, the ringer can be muted. In this case, an incoming call is indicated only visually.

Special ringers

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

Abstract names used for Special Ringers:

- "Bellcore-dr1" - normal (internal) alerting or ring-back;
- "Bellcore-dr2" - external alerting or ring-back;
- "Bellcore-dr3" - recall alerting or ring-back (e.g., following transfer).
- "alert-internal" - normal (internal) alerting or ring-back;
- "alert-external" - external alerting or ring-back;
- "alert-recall" - recall alerting or ring-back (e.g., following transfer)
- "alert-emergency" - emergency alerting or ring-back.
- "Line-<DN of Line>-Reserved" - distinctive alerting for a line with number <DN of Line>

Once made available (by the administrator) to the user, the Special Ringers for the call types listed can be selected and configured via the User menu (see "[Special ringers](#)" → [page 93](#)).

Note The ringer settings may be locked by DLS and therefore also the special ringers will not be available for the user. See DLS Documentation for details.

Administration via local phone

```
|--- Admin
  |--- Ringer setting
    |--- Distinctive
      |--- <1 .... 15>
        |--- Name
          |--- Ringer sound
          |--- Pattern melody
          |--- Pattern sequence
          |--- Duration
          |--- Audible
```

Map to specials

The "Mapping table" is not accessible by local menu, WBM, or DLS but is predefined with Ringer name defaults. 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.

The "Mapping table" has been configured to identify the distinctive ringer names as a special ringer type and the User has access to configure a different audio file or pattern for this distinctive ringer via their "Special ringer table". Any change made by the User to this special ringer is reflected in the "Distinctive ringer table" and any change made by Admin in the "Distinctive ringer table" is reflected in the "Special ringer table".

Administration via WBM

1. Open Ringer setting > Map To Specials.

Map to specials	
Internal	Bellcore-dr1 ▼
External	Bellcore-dr2 ▼
Recall	Bellcore-dr3 ▼
Emergency	alert-emerge ▼
Special1	▼
Special2	▼
Special3	▼
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

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

Special ringers

This section is available to the user and does not require a password.

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.

Call type	Ringer sound	Pattern melody	Pattern sequence
Internal	Pattern	2	1.0 sec. ON, 2.0 sec. OFF
Internal	Pattern	2	1.0 sec. ON, 2.0 sec. OFF

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
```

Mobility

The Mobility feature requires the OpenScape Deployment Service (DLS). If the phone is mobility enabled by the DLS, a mobile user can log on to the phone and thereby have his own user settings transferred to the phone. These user data are stored in the DLS database and include, for instance, SIP registration settings, dialing properties, key layouts, as well as the user's phone book.

If the mobile user changes some settings, the changed data is sent to the DLS server. This ensures that his user profile is updated if necessary.

Administration via WBM

1. Open Mobility.

Mobility	
Unauthorised logoff trap	<input type="checkbox"/>
Logoff trap delay	<input type="text" value="300"/>
Timer medium priority	<input type="text" value="60"/>
Mobility feature	<input type="checkbox"/>
Managed profile	<input type="checkbox"/>
Error count local	<input type="text" value="0"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

- **Unauthorized logoff trap:** An SNMP trap is sent on an unauthorized log-off attempt. If "Unauthorized Logoff Trap" is set to "Yes", a message is sent to the SNMP server if an unauthorized attempt is made to log off the mobile user.
 - Value range: "Yes", "No"
 - Default: "No"
- **Logoff trap delay:** Time span in seconds between the unauthorized log-off attempt and the SNMP trap. Logoff Trap Delay defines the time span in seconds between the unauthorized log-off attempt and the trap message to the SNMP server.
 - Default: 300
- **Timer medium priority:** Time span in seconds between a data change in the phone and its transfer to the DLS server. Timer Medium Priority determines the time span in seconds between a change of user data in the phone and the transfer of the changes to the DLS server.
 - Default: 60
- **Mobility feature:** Indicates whether the mobility feature is enabled. The Mobility Feature parameter indicates whether the mobility feature is enabled by the DLS or not.
- **Managed Profile:** Display only field.
- **Error Count Local:** Display only field.

Administration via local phone

```
|--- Admin
  |--- Mobility
    |--- Unauthorized Logoff Trap
      |--- Logoff Trap Delay
      |--- Timer Medium Priority
      |--- Mobility Feature
    |--- Managed Profile
      |--- Error Count Local
```

Bluetooth mobility

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

Bluetooth specification requires pairing of devices before connecting. Pairing is a security mechanism during which several parameters unique to both devices (among others Bluetooth hardware addresses of both devices) are combined in a number called a link key. The link key is then used to establish a session over secure channel. Bluetooth hardware address is the only datum that needs to be transferred together with the link-key setr for the link-keys to work on different hardware.

The Bluetooth hardware address is part of the mobile user data profile and is assigned to the device on log-on. When the user logs off, Bluetooth address is again unassigned. This way the Bluetooth hardware address and the link-keys travel with the mobile user and the user can seamlessly use the paired Bluetooth devices.

The pool of mobile Bluetooth addresses, which can be assigned to device, must be set up on the DLS server.

In case of large installations, DLS admin must ensure that any chance of address collision in possible mobile scenarios is avoid.

Free programmable keys

The key programming can be accessed via the WBM, via the local phone and via DMS.

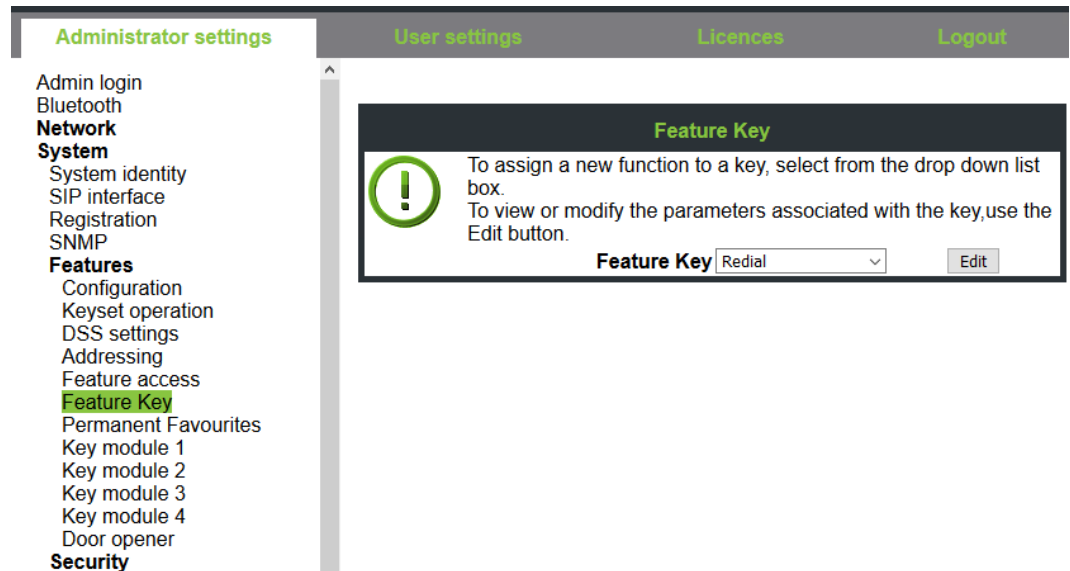
- The OpenScape Desk Phone CP710 comes with 12 free programmable keys with LED (red / green / amber), all of which can be programmed on two separate levels. The 6 first programmable keys are permanently displayed on the left panel. The 6 last programmable keys are available in Favorites. The number of programmable keys can be increased by attaching one or more OpenScape Key Modules to the phone.
- The OpenScape Desk Phone CP210 phone provides four free programmable keys (FPKs). This is called „Phone keys“.

Feature key for CP710

The OpenScape Desk Phone CP710 has a feature key at the right lower corner. The feature key is configurable in WBM and DLS.

Administration via WBM

1. Open System > Features > Feature key.



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

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 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 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.

The solution is to replace invalid characters in the names of files to be downloaded onto the phone with a dummy character.

This should cover any download mechanism:

- WBM download of user files (such as ringtones)
- WBM download of binds
- FTP or HTTPS download of files to the phone

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

WBM checks the file name and file extension entered in any FTP / HTTPS file transfer panel only contains valid characters and that the file extensions (file type) are valid.

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

FTP / HTTPS server

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

Common FTP / HTTPS settings (defaults)

For each one of the various file types, e.g. phone software, or logos, specific FTP / HTTPS access data can be defined. If some or all file types have the parameters "Download method", "FTP Server", "FTP Server port", "FTP Account", "FTP Username", "FTP path", and "HTTPS base URL" in common, they can be specified here. These settings 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 scenarios:

- Update has been allowed due to override flag being set
- Whole part number is not recognized
- Block 4 of part number is not recognized
- Downloaded software does not have a hardware level included

Administration via WBM

1. Open File transfer > Defaults.

The screenshot shows a web form titled "Defaults" with the following fields and controls:

- Download method:** A dropdown menu with "FTP" selected.
- FTP server address:** An empty text input field.
- FTP server port:** A text input field containing "21".
- FTP account:** An empty text input field.
- FTP username:** An empty text input field.
- FTP password:** A text input field with masked characters (dots).
- FTP path:** An empty text input field.
- Submit:** A button at the bottom left.
- Reset:** A button at the bottom right.

- **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 HW 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 uploading a local file. This can be done only by WBM administration.

Administration via WBM

1. Open File transfer > Phone application.

Phone application

Upgrade using file

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

Durchsuchen... Keine Datei ausgewählt.

Upgrade Cancel

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

Upgrade using FTP/HTTPS

Use defaults

Filename

After submit do nothing

Submit Reset

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

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

Upgrade using FTP / HTTPS

If the default FTP / HTTPS access settings (see "[Common FTP / HTTPS settings \(defaults\)](#)" → [page 99](#)) 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".
- **File name:** Specifies the file name of the phone software.

Data required (if not derived from Defaults)

- **Download method:** Selects the protocol to be used. Value range: "FTP", "HTTPS". Default: "FTP".
- **Server:** IP address or 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

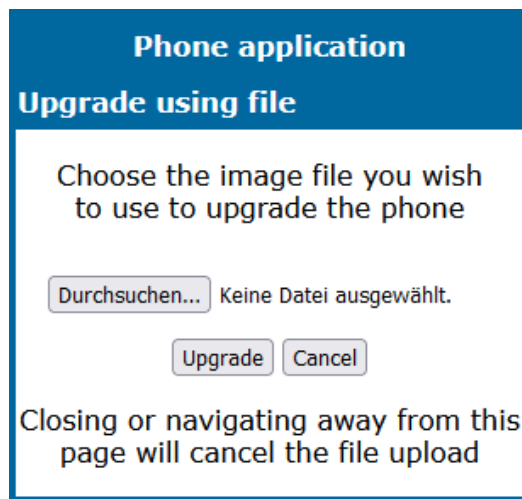
```
|--- Admin
  |--- File Transfer
    |--- Phone application
      |--- Use default
      |--- Download method
      |--- Server
      |--- Port
      |--- Account
      |--- Username
      |--- Password
      |--- FTP path
      |--- HTTPS base URL
      |--- File name
```

Download / update phone application

If applicable, phone software should be deployed using the Deployment Service (DLS). Alternatively, the download can be triggered from the WBM interface or from the Local phone menu. When the download has been successful, the phone will restart using the new software.

Updating with a download

1. Download the update file to your desktop and unpack the file.
2. Open File transfer > Phone application.



3. Select "Search" and locate the file on your local hard drive.
4. Click **Upgrade**.
5. Wait until the upgrade process is finished and the phone restarts.

Updating via FTP or HTTPS

1. Open File transfer > Phone application.

Upgrade using FTP/HTTPS

Use defaults

Download method FTP

FTP server address

FTP server port 21

FTP account

FTP username

FTP password

FTP path

Filename

After submit do nothing

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

Start Download via Local Phone

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

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

Picture clips

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

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

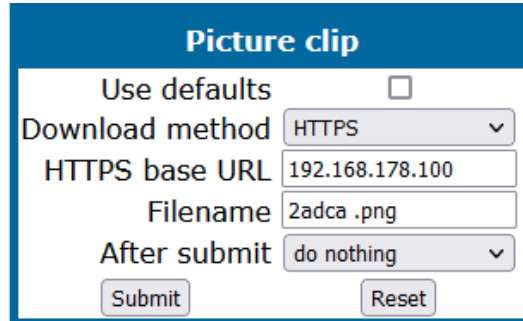
FTP / HTTPS access data

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

(defaults)" → page 99).

Administration via WBM

1. Open File transfer > Picture clip.



Picture clip

Use defaults

Download method HTTPS

HTTPS base URL

Filename

After submit do nothing

- **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

If applicable, picture clips should be deployed using the Deployment Service (DLS). Alternatively, the download can be triggered from the web interface or from the local phone menu.

Start Download via WBM

1. Open File transfer > Phone application.

Phone application

Upgrade using file

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

Keine Datei ausgewählt.

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

Upgrade using FTP/HTTPS

Use defaults

Filename

After submit ▼

2. For "After submit" select "start download".
3. Click **Submit**.

Start Download via Local Phone

```
|--- Admin
  |--- File Transfer
    |--- Picture clip
```

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

Upload picture clips via LDAP

conversation, so that he can easily recognize his conversation partners. The LDAP template identifies if avatars are available for LDAP entries and how they are accessed by the phone.

The LDAP directory must contain avatar pictures in JPEG / JIFF format (plain or base 64 encoded) or a URL that points to a web-server that can provide a picture for the contact.

Example: Plain JPEG picture attributes are "jpegPhoto" or "thumbnailPhoto". URL attribute can be "photoURL".

For best display the square format is recommended.

Maximum picture size is 100 kB. The phone shows an avatar in two sizes:

- 32x32 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 (for more information, see "[Create an LDAP template](#)" → page 162).

If the configured address of the web server (Avatar server) is not empty, the attribute content is treated as the variable part of the URL to access the picture from a WEB server — see Configuration via DLS and WBM in this chapter. The phone then constructs a full path to the picture file on the web server, i.e. adds the attribute value to the Avatar server field value. The photoURL attribute may be a direct URL which ends up with <filename>.jpg. The address can include a HTTP address or a HTTPS address. HTTPS is assumed by default.

If configured address of the web server (Avatar server) is empty, the attribute value is treated as a LDAP DN and the LDAP server is asked for the content of the attribute. The content must be plain JPEG or base64 encoded.

Example

Avatar server value is „https://my.image.server.com/internal“ . The photoURL attribute is „employee1.jpg“ . Phone will sent http request for https://my.image.server.com/internal/employee1.jpg.

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

Configuration via Admin menu

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

Configuration via DLS

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

Administration via WBM

1. Open Admin > Local functions > Directory settings.

Directory settings	
LDAP server address	<input type="text"/>
Transport	TCP <input type="button" value="v"/>
Secure port	636 <input type="text"/>
LDAP server port	389 <input type="text"/>
Authentication	Anonymous <input type="button" value="v"/>
User name	<input type="text"/>
Password	••••••
Avatar server	<input type="text"/>
LDAP for manual search only	<input type="checkbox"/>
Firstname and lastname for quick search	<input type="checkbox"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

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

LDAP template

The LDAP template is an ASCII text file that uses an allocation list to assign directory server attributes to input and output fields on an LDAP client. The LDAP template must be modified correctly for successful communication between the directory server and the LDAP client.

The OpenScope 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 99).

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 phone software.
- **After submit:** Specifies actions after submit button is pressed. Value range: "do nothing", "start download". Default: "do nothing".

Data required (if not derived from Defaults)

- **Download method:** Selects the protocol to be used. Value range: "FTP", "HTTPS" Default: "FTP"
- **Server address:** IP address or 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 OpenScope 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 is displayed when the phone is in idle mode. It performs a slide show consisting of images which can be uploaded using the web interface.

Screen savers are available only on OpenScope Desk Phone 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: 320x240 px

FTP / HTTPS access data

If the default FTP / HTTPS access setting are used, Use default must be set to "Yes", and only the file name must be specified (see "[Common FTP / HTTPS settings \(defaults\)](#)" → page 99).

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 phone software.
- **After submit:** Specifies actions after submit button is pressed.
 - Value range: "do nothing", "start download"
 - Default: "do nothing".

Data required (if not derived from Defaults)

- **Download method:** Selects the protocol to be used.
 - Value range: "FTP", "HTTPS"
 - Default: "FTP"
- **Server address:** IP address or 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 screensaver

If applicable, screensavers should be deployed using the DLS (Deployment Service). Alternatively, the download can be triggered from the web interface or from the local phone menu.

Start Download via WBM

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 OpenScope Desk Phone CP710 phones are able to play MP3 files from 32 kbit/s up to 320 kbit/s. As the memory for user data is limited to 8 MB, a constant 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 99).

Administration via WBM

1. Open File transfer > Ringer file.

The screenshot shows a web form titled "Ringer file" with a blue header. The form contains the following elements:

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

- **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 phone software.
- **After submit:** Specifies action after submit button is pressed.
 - Value range: "do nothing", "start download"
 - Default: "do nothing"

Data required (if not derived from Defaults)

- **Download method:** Selects the protocol to be used.
 - Value range: "FTP", "HTTPS"
 - Default: "FTP"
- **Server address:** IP address or 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.

UC server

Administration via WBM

1. Open Local functions > Locality > UC **Server**.
 - UC Protocol: selects the protocol to be used.
 - Value range: "HTTP", "HTTPS".
 - UC Server address: IP address or host name of the UC server in use.
 - UC Server port: port number of the UC server in use.
 - Default: 8802.
 - User configuration enabled: indicates whether the user configuration is enabled.

Administration via local phone

```
|--- Admin
    |--- Local functions
        |--- UC Server
            |--- UC Protocol
            |--- UC server address
            |--- UC Server port
            |--- User configuration enabled
```

Send request via HTTP / HTTPS

With this function, the phone can send a specific HTTP or HTTPS request to a server. The function is available at any time, irrespective of registration and call state. Possible uses are HTTP-controlled features on the system, or functions on a web server that can only be triggered by HTTP / HTTPS request, e.g. login or logout for flexible working hours.

- The protocol parameter defines whether HTTP or HTTPS is used for sending the URL to the server.

- The web server address is the IP address or DNS name of the remote server to which the URL is sent.
- The port is the target port at the server to which the URL is sent.
- The path is the server-side path to the desired function, i.e. the part of the URL that follows the IP address or DNS name (example: web page /checkin.html).
- In the parameters field, one or more key/value pairs in the format "<key>->=<value>" can be added to the request, separated by an ampersand(&).

Example

phonenumber=3338&action=huntGroupLogon

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

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

If the web server requires user authentication, the parameters "Web server user ID" and "Web server password" can be used. If not null, the values are appended between the serverside path (Path) and the additional parameters (Parameter).

Administration via WBM

1. Open System > Features > Send URL.

Send URL

Name

Message details

Protocol

Web server address

Port

Path

Parameters

Method

Authenticate phone

Web server user ID

Web server password

- **Name** defines or changes the name (label) of the key.
- **Protocol**: transfer protocol to be used.
 - Value range: "HTTP", "HTTPS"
- **Web server address**: IP address or DNS name of the remote server.
- **Port**: target port at the server.
- **Path**: server-side path to the function.
- **Parameters**: optional parameters to be sent to the server.
- **Method**: HTTP method used for transfer.
 - Value range: "GET", "POST"
- **Web server user ID**: user id for user authentication at the server.
- **Web server password**: password for user authentication.

Settings of the corporate directory

LDAP

The Lightweight Directory Access Protocol (LDAP) enables access to a directory server via an LDAP client. Various personal information is stored there, e.g. the name, organization, and contact data of persons working in an organization. When the LDAP client has found a person's data, e. g. by looking up the surname, the user can call this person directly using the displayed number.

The user can access the LDAP directory using the entry Directories > Corporate directory.

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

Note The OpenScope Desk Phone CP phones support LDAPv3.

For connecting the phone LDAP client to an LDAP server, the required access data must be configured. The parameter "Server" address specifies the IP address of the LDAP server. The parameter "Transport" defines whether the phone must continue to use an unencrypted TCP connection to the LDAP server, or to use an encrypted TLS connection to a separate LDAPS port on the LDAP server, or to use an encrypted TLS connection to a separate LDAPS port on the LDAP server. Depending on the setting of "Transport" the secure port (for TLS) or the server port (for TCP) are defined. If the authentication is not set to "Anonymous", the user must authenticate himself with the server by providing a user name and a corresponding password. The user name and password are defined by the administrator. The user name is the string in the LDAP bind request, e. g. "C=GB,O=SIEMENS COMM,OU=COM,L=NTH,CN=BAYLIS MICHAEL". The internal structure will depend on the specific corporate directory.

For a guide on setting up LDAP on an OpenScope Desk Phone, refer to "[How to set up the "Corporate directory" \(LDAP\)](#)" → page 162.

A search field for LDAP requests is supported. The search string is submitted to the LDAP server as soon as the OK key is pressed or when the search trigger timeout expires.

Administration via WBM

1. Open Local functions > Directory Settings.

Directory settings	
LDAP server address	<input type="text"/>
Transport	TCP <input type="button" value="v"/>
Secure port	636 <input type="text"/>
LDAP server port	389 <input type="text"/>
Authentication	Anonymous <input type="button" value="v"/>
User name	<input type="text"/>
Password	•••••• <input type="text"/>
Avatar server	<input type="text"/>
LDAP for manual search only	<input type="checkbox"/>
Firstname and lastname for quick search	<input type="checkbox"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

- **LDAP Server address:** IP address or host name of the LDAP server
- **Transport:** defines transport mode, whether LDAP interface uses TCP and is unencrypted, or uses TLS and is encrypted
 - Value range: "TCP", "TLS"
 - Default: "TCP"
- **Secure Port:** defines the port of the appropriate TLS interface on LDAP server when Transport is set to TLS
 - Default: "636"
- **LDAP Server port:** port on which the LDAP server is listening for requests, when Transport is set to TCP
 - Default: 389
- **Authentication:** authentication method used for connecting to the LDAP server
 - Value range: "Anonymous", "Simple"
 - Default: "Anonymous"
- **User name:** user name used for authentication with the LDAP server in the LDAP bind request
- **Password:** password used for authentication with the LDAP server
- **Contact details update:** The update source for call party names can be set as one or more of the following: Directory, Signaling or Local.
- **Avatar server:** HTTP or HTTPS address, where the pictures are located. The complete HTTP or HTTPS address is built from <Avatar server> + <Avatar>. <Avatar> is the attribute name from the LDAP template field <Avatar>. The specified LDAP attribute must contain the file name of the picture contained in the URL specified in <Avatar Server>. Example: <Avatar Server> = "https://mypicture.server/picturepath" <Avatar> = picturename. When the phone does an LDAP lookup for user A, the field "Picturename" returns picturename = UserA.jpg. The phone will look for the picture at: https://mypicture.server/picturepath/UserA.jpg.

Administration via local phone

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

Contact details update

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

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

- Existing contact names are updated for new calls (if one or more sources are specified and matched)
- Existing contact names are not updated (if the local source is used, i.e. no sources set)

Source of the contact details

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

- LDAP
- Signalling

Administration via WBM

1. Open Local functions > Name update sources.



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

- Directory: LDAP (if an LDAP entry matches the call, the contact is updated 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
```

System phone book

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

Note that if an OCAB system is used, the IP of the OCAB board needs to be configured in Admin > Local functions > UC Server to access the system Directory (see "[UC server](#)" → page 117).

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

The phone will perform a reverse look-up of the number provided from the system on outgoing and incoming calls so configuring of canonical dial settings is mandatory (see "[Canonical dialing settings](#)" → page 159).

Any further information available in the system phone book is stored for this contact as well.

This reverse look-up is only performed if no result is returned from a configured LDAP server.

Picture via LDAP

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

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

The OpenScape Desk Phone CP410 / CP710 requests the look-up for all numbers for which the local phone book does not have a picture. In case the phone book contains names for the number but without picture the name and picture from the directory server are displayed. If there is no entry for the number in the directory server the name from the local phone book is displayed, so the directory server data overrides the local phone book.

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

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

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

Canonical dial settings


For contact data retrieval from the directory server, upon arrival of a call, the remote telephone number is converted according to the canonical dial settings (see also "[Canonical dialing settings](#)" → [page 159](#)). The format of the resulting number should match the format the numbers are stored in the directory server. It is recommended to convert the numbers to fully qualified format, i.e. adding country and area code to the subscriber number. This way it is ensured that the number used for look-up is unique.

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

Administration via WBM

1. Open Local functions > Locality > Canonical dial **settings**.

Canonical dial settings



Warning – changes to these settings could prevent calls being matched to existing conversations

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

Administration via local phone

```
|--- Administration
```

```
  |--- Local Functions
```

```
    |--- Locality
```

```
      |--- Canonical dial settings
```

```
        |--- Local country code
```

```
        |--- National prefix digit
```

```
        |--- Local national code
```

```
        |--- Minimum local number length
```

```
        |--- Local enterprise node
```

```
        |--- PSTN access code
```

```
        |--- International code
```

```
        |--- Operator code
```

```
        |--- Emergency number
```

```
|--- Initial extension digits
```

Speech

RTP base port

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

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

Administration via WBM

1. Open Network > Port number configuration.

Port number configuration	
SIP server	5060
SIP registrar	5060
SIP gateway	5060
SIP local	5060
Backup proxy	5060
RTP base	5010
LDAP server	389
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

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

Administration via local phone

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

Codec preferences

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

The OpenScope Desk Phone CP phone provides the codecs

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

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

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

Administration via WBM

1. Open Speech > Codec preferences.

Codec preferences

Silence suppression

Allow "HD" icon

Packet size Automatic

OPUS ranking ▼ ✗

G.711 ranking ▲ ▼ ✗

G.729 ranking ▲ ▼ ✗

G.722 ranking ▲ ✓

OPUS settings

Max bandwidth Wideband

Bitrate type VBR

Max complexity

FEC

DTX

PLR

- **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**: 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 codec is visible in codec table only for systems that support it.

OPUS settings

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

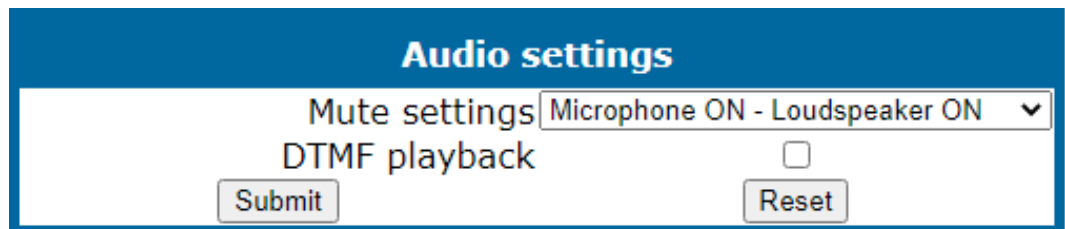
```
|--- Admin
  |--- Speech
    |--- Codec Preferences
      |--- Silence suppression
      |--- Packet size
        |--- OPUS
        |--- G.711
        |--- G.729
        |--- G.722
      |--- OPUS settings
```

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 digits received using [RFC2833](#) coding (i.e. Rtp events) in the current active audio device (headset / loudspeaker / handset).

Security and policies

Changing a password

The passwords for user and administrator can be changed.

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

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

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

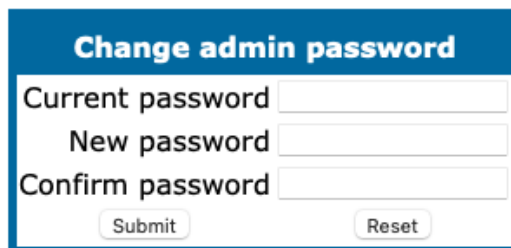
Usable characters are 0-9 A-Z a-z ."#,'?'+-()@/;:_*

Default passwords

- **Admin menu:** 123456
- **User menu:** no password
- **Factory Reset:** 124816
- **Soft Restart:** Press keys 1-4-7 simultaneously and enter Admin password.
- **Factory Reset:** Press keys 2-8-9 simultaneously and enter Reset password.

Changing the administrator password

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



Change admin password

Current password

New password

Confirm 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**.

Certificates

Generic

Online Certificate Check

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

- When OCSP check is activated, the configured OCSR is requested to check if the certificate has been revoked.
- OCSR 1 address specifies the IP address (or FQDN) of a primary OCSP responder.
- OCSR 2 address specifies the IP address (or FQDN) of a secondary OCSP responder.

Administration via WBM

1. Open Security and Policies > Certificates > **Generic**.

Generic policy	
Expires after (days)	<input type="text" value="0"/>
Warn before (days)	<input type="text" value="0"/>
Force changed	<input type="checkbox"/>
Tries allowed	<input type="text" value="3"/>
No change for (hours)	<input type="text" value="0"/>
Suspended for (mins)	<input type="text" value="1"/>
History valid for (days)	<input type="text" value="180"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Administration via local phone

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

Authentication policy

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

Administration via WBM

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

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

Submit Reset

- Secure file transfer sets the authentication level for the HTTPS server to be used (see "[Common FTP / HTTPS settings \(defaults\)](#)" → page 99).
- Secure HFA gateway sets the authentication level for the HFA gateway connected to the phone (see "[HFA gateway settings](#)" → page 71).
- 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
```

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

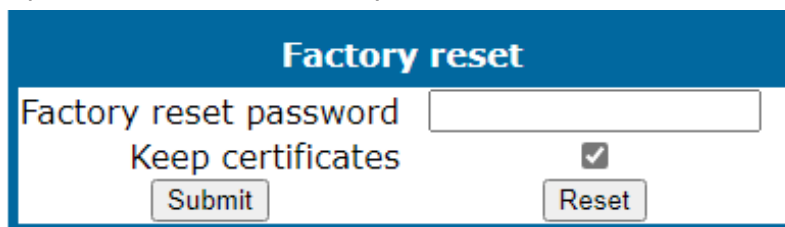
```
|--- Admin
    |--- Maintenance
        |--- Restart
```

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.



The screenshot shows a web form titled "Factory reset". It has a text input field for "Factory reset password", a checkbox labeled "Keep certificates" which is checked, and two buttons: "Submit" and "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.

Secure shell

Enable access	<input type="checkbox"/>
Session password	<input style="width: 150px;" type="text"/>
Access minutes	<input style="width: 50px;" type="text" value="3"/> ▼
Session minutes	<input style="width: 50px;" type="text" value="5"/> ▼

Access Phone Behind a NAT settings

Remote SSH enable access	<input type="checkbox"/>
Remote SSH server address	<input style="width: 150px;" type="text"/>
Remote SSH server port	<input style="width: 150px;" type="text"/>
Remote SSH username	<input style="width: 150px;" type="text"/>
Remote SSH HPT port forwarding	<input type="checkbox"/>
Remote SSH Webm port forwarding	<input type="checkbox"/>
Remote SSH known hosts	<input style="width: 150px;" type="text"/>

Submit
Reset

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

- Session minutes defines the maximum length in minutes for an SSH connection. After it has expired, the "admin" user is logged out.
 - Values: 5, 10, 20, 30, 60.

Display license information

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

The license information can also be viewed by users with the user login if logging on as administrator is not permitted.

Administration via local phone

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

Web Services Interface (WSI)

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

Administration via WBM

1. Open Local **functions** > **WSI**.

Administration via local phone

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

HPT interface (for service staff)

For special diagnosis and maintenance tasks, the service staff may employ the HPT tool, which is able to control and observe OpenScape Desk Phone CP110 / CP210 / CP410 phones remotely.

There are 2 types of HPT sessions, control session and observation session.

- A control session allows for activating phone functions remotely. When a control session is established, the following changes will occur:
 - The display shows a message indicating that remote service is active.
 - Handset, microphone, speaker, headset, and microphone are disabled.
- An observation session allows for supervising events on the phone, like, for instance, pressing a key, incoming calls or navigating in the menus. Before an observation session is started, the user is prompted for allowing the observation. During an observation session, the phone operates normally, including loudspeaker, microphone and ringer. Thus, the local user can demonstrate an error towards the service staff that is connected via HPT.

The session data is written to a log file on the phone. It can be downloaded from the Diagnostics > Fault trace configuration menu (see "[Fault trace configuration](#)" → [page 140](#)).

Administration via WBM

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

Administration via Local Phone

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

AlertBar LED hint

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

The administrator can control how the Alert LED is automatically turned off.

Administration via WBM

1. Open System > Features > Configuration.

The screenshot shows the 'Configuration' page with the 'General' tab selected. The settings are as follows:

Setting	Value
Emergency number	<input type="text"/>
Voice mail number	<input type="text"/>
MWI LED	AlertBar only ▼
Missed call LED	AlertBar LED ▼
AlertBar LED hint	<input type="checkbox"/>
Allow refuse	<input type="checkbox"/>
Hot/Warm phone	No action ▼

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.

Diagnostics

Note Some of the diagnostic tools and functions may reveal personal data of the user, such as caller lists. Thus, with regards to data privacy, it is recommended to inform the user when diagnostic functions are executed.

LLDP-MED

When the phone is connected to a switch with LLDP-MED capabilities, it can receive a VLAN ID and QoS parameters and advertise its own Network-related properties. The data is exchanged in TLV (Type-Length-Value) format.

Both sent and received LLDP-MED data can be monitored at the administrator interface.

Note For details on LLDP-MED, refer to the ANSI/TIA-1057 standard. For a Network configuration example that shows LLDP-MED in operation, refer to "[LLDP-Med example](#)" → page 167.

View Data From WBM

1. Open Diagnostics > LLDP-MED TLVs.

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

- **Extended Power:** Power Consumption; relevant for PoE.
- **Network policy (voice):** VLAN ID and QoS (Quality of Service) parameters for voice transport.
- **Network policy (signalling):** VLAN ID and QoS (Quality of Service) parameters for signalling.
- **LLDP-MED capabilities:** The LLDP-MED TLVs supported by the phone and the switch as well as the specific device class they belong to.
- **MAC_Phy configuration:** Identifies the possible duplex and bit-rate capability of the sending device, its current duplex and bit-rate capability, and whether these settings are the result of auto-negotiation during the initialization of the link, or of manual set override actions.
- **System capabilities:** The devices advertise their potential and currently enabled functions, e. g. "Bridge", "Telephone".
- **TTL:** Time To Live. This parameter determines how long the TLVs are valid. When expired, the device will send a new set of TLVs.
- **Inventory:** Inventory information of a CP phone such as "Manufacturer Name", "Model Name", "Hardware Revision", "Firmware Revision", "Software Revision", "Serial Number", "Asset ID"

View Data From Local Menu

If both sent and received values are concordant, OK is appended to the parameter. If not, an error message is displayed.

```

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

```

Fault trace configuration

Error tracing and logging can be configured separately for all components, i. e. the services and applications running on the 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.

Fault trace configuration

File size (Max 6290000 bytes)

Trace timeout (minutes)

Automatic clear before start

Trace levels for components

802.1x service	OFF	▼	Administration	OFF	▼
Application framework	OFF	▼	Application menu	OFF	▼
Broadsoft service	OFF	▼	Call log	OFF	▼
Call view	OFF	▼	Certificate management	OFF	▼
Clock service	OFF	▼	Communications	OFF	▼
Component registrar	OFF	▼	CPE Service	OFF	▼
CSTA service	OFF	▼	Data access service	OFF	▼
Desktop	OFF	▼	Digit analysis service	OFF	▼
Directory service	OFF	▼	DLS client management	OFF	▼
GPALAudio Core	OFF	▼	GPALAudio Framework	OFF	▼
Health service	OFF	▼	Instrumentation service	OFF	▼
Journal service	OFF	▼	Media control service	OFF	▼
Media recording service	OFF	▼	Mobility service	OFF	▼
OpenStage client management	OFF	▼	Password management service	OFF	▼
Phonebook	OFF	▼	Performance marks	OFF	▼
Physical interface service	OFF	▼	RingCentral Service	OFF	▼
Security log service	OFF	▼	Service framework	OFF	▼
Service registry	OFF	▼	SIP call control	OFF	▼
SIP messages	OFF	▼	SIP signalling	OFF	▼
SIP MST stack	OFF	▼	Team service	OFF	▼
Tone generation service	OFF	▼	Transport service	OFF	▼
HTTP service	OFF	▼	Voice engine service	OFF	▼
Voice mail	OFF	▼	Web server service	OFF	▼

- The “File size (bytes)” parameter sets the maximum file size. When it is reached, the data is saved as old file, and a new file is generated. From then on, the trace data is written to the new file. When the maximum file size is reached

again, the data is saved as old file once more, thereby overwriting the previous old file. The default value is "1048576".

- The "Trace timeout (minutes)" determines when to stop tracing. When the timeout is reached, the trace settings for all components are set to OFF, but ERROR and STATUS messages are still written to the trace file infinitely. When the trace file has reached its maximum size, the data is saved, and a new file is created (for more information, see File size (bytes) above). If the value is 0, the trace data is written without time limit.
- If "Automatic clear before start" is enabled, the existing trace file is deleted on clicking **Submit**, and a new, empty trace file is generated. By default, it is unchecked.

Log files

You can read the log files by clicking on the appropriate hyperlinks (the hyperlinks work only if the file in question has been created). The following logs can be viewed:

- **Download trace file:** The trace data according to the settings specified for the services.
- **Download old trace file:** The trace file is stored in permanent memory. When the file has reached its size limit, it is saved as old trace file, and the current exception file is emptied for future messages. The old trace file can be viewed here.
- **Download saved trace file:** Normally, the trace file is saved only in the phone RAM. When the phone restarts in a controlled manner, the trace file is saved in permanent memory.
- **Download syslog file:** Messages from the phone's operating system, including error and exception messages.
- **Download old syslog file:** Old messages from the phone's operating system.
- **Download saved syslog file:** Saved messages from the phone's operating system.
- **Download exception file:** If an exceptions occurs in a process running on the phone, a message is written to this file. These messages are incorporated in the syslog file.
- **Download old exception file:** The exception file is stored permanent memory. When the file has reached its size limit, it is saved as old exception file, and the current exception file is emptied for future messages. The old exception file can be viewed here.
- **Download upgrade trace file:** The trace log created during a software upgrade.
- **Download upgrade error file:** The error messages created during a software upgrade. These messages are incorporated in the syslog file.
- **Download dial plan file:** If a dial plan has been uploaded to the phone, it is displayed here, along with its status (enabled or disabled) and error status. For details, refer to ["Dial Plan" →1](#)
- **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

- **Administration:** Deals with the changing and setting of parameters within the phone database, from both the User and Admin menus.
- **AGP Phonelet:** Deals with AGP Phonelet.
- **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:** 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:** 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.
- **Help:** Handles the help function.

- **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 processing service:** This is a layer of software between the media control service, the tone generation, and voice engine services. It is also involved in the switching of audio devices such as the handset and loudspeaker.
- **Media recording service:** Logs the data flow generated with call recording.
- **Mobility service:** Handles the mobility feature whereby users can log onto different phones and have them configured to their own profile.
- **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.
- **Directory:** Responsible for the Directory application.
- **Performance Marks:** Aid for measuring the performance of the phone. For events triggered by the user, a performance mark is written to the trace file, together with a timestamp in the format "hh:mm:ss yyyy.milliseconds", and information about the event. The timespan between two performance marks is an indicator for the performance of the phone.

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:** 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.

- **USB backup service:** Used to make backup and restore to and from a USB stick by using a password. This item is available in the phone GUI.
- **Video service engine:** Handles the video functionality.
- **Voice engine service:** Provides a switching mechanism for voice streams within the phone. This component is also involved in QDC, Music on hold and voice instrumentation.
- **Voice mail:** Handles the voice mail functionality.
- **Web server service:** Provides access to the phone via web browser.
- **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 140).

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

Phone administration problems

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

Phone administration problems	
File size (Max 6290000 bytes)	<input type="text" value="1048576"/>
Trace timeout (minutes)	<input type="text" value="0"/>
Automatic clear before start	<input type="checkbox"/>
Trace levels for components	
Administration	<input type="text" value="DEBUG"/>
Clock service	<input type="text" value="DEBUG"/>
Data access service	<input type="text" value="DEBUG"/>
OpenStage client management	<input type="text" value="DEBUG"/>
Password management service	<input type="text" value="DEBUG"/>
Web server service	<input type="text" value="DEBUG"/>
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>
Download trace file	Download saved trace file

Audio related problems

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

Audio related problems

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

Trace levels for components

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

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

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

Call proceeding problems

- Open Diagnostics > EasyTrace Profiles > Call proceeding **problems**.

Call proceeding problems

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

Trace levels for components

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

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

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

Conversations / LDAP problems

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

Conversations / LDAP problems

File size (Max 6290000 bytes)	<input style="width: 90%;" type="text" value="1048576"/>
Trace timeout (minutes)	<input style="width: 90%;" type="text" value="0"/>
Automatic clear before start	<input type="checkbox"/>

Trace levels for components

Call view	<input style="width: 90%;" type="text" value="DEBUG"/>
ConversationAPI	<input style="width: 90%;" type="text" value="DEBUG"/>
CSTA service	<input style="width: 90%;" type="text" value="DEBUG"/>
Digit analysis service	<input style="width: 90%;" type="text" value="DEBUG"/>
Directory service	<input style="width: 90%;" type="text" value="DEBUG"/>
Exchange service	<input style="width: 90%;" type="text" value="DEBUG"/>
Journal service	<input style="width: 90%;" type="text" value="DEBUG"/>

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

Keystore problems

1. Open Diagnostics > EasyTrace Profiles > Keystore **problems**.

Keystore problems

File size (Max 6290000 bytes)	<input style="width: 90%;" type="text" value="1048576"/>
Trace timeout (minutes)	<input style="width: 90%;" type="text" value="0"/>
Automatic clear before start	<input type="checkbox"/>

Trace levels for components

Call view	<input style="width: 90%;" type="text" value="DEBUG"/>
Communications	<input style="width: 90%;" type="text" value="DEBUG"/>
CSTA service	<input style="width: 90%;" type="text" value="DEBUG"/>
Sidcar service	<input style="width: 90%;" type="text" value="DEBUG"/>
SIP messages	<input style="width: 90%;" type="text" value="DEBUG"/>
Team service	<input style="width: 90%;" type="text" value="DEBUG"/>

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

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

Mobility / DLS problems

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

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

Network problems

1. Open Diagnostics > EasyTrace Profiles > Network **problems**.

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

Security problems

1. Open Diagnostics > EasyTrace Profiles > Security **problems**.

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

Bluetooth problems

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

1. Open Diagnostics > EasyTrace Profiles > Bluetooth **problems**.

Advanced audio traces

This feature allows the admin to turn on EPT (Broadcom EndPoint) traces, so that audio related issues can be collected directly from the users' phones. This helps to analyze those audio issues faster and come to a solution.

The following information can be collected:

- EPT traces
- The status of the EPT component
- The existence of the eptMsg thread that processes the microphone packets

Administration via WBM

1. Open Diagnostics > **Advanced audio traces**.
 - **EPT trace level:** can be configured from 0 (tracing disabled) up to 5 (maximum trace level).
 - **Automatic clear before start:** if checked, the ept file is cleared after pressing the Submit button.
 - **Capture and stop:**
 - if checked, tracing will continue until the maximum number of lines is reached and then it will stop. Also, this feature will remain enabled after restart.
 - if unchecked, the trace file will continuously wrap around, overwriting the older lines.
 - **Number of lines (Max 100000):** the maximum number of lines in the eptlog file.
 - **Download eptlog file:** opens a new web page presenting the contents of the trace file "eptlog.txt".

- **Download saved eptlog file:** saves the trace file "eptlog.txt.save.gz" captured before the last reboot, if there was any. To save the flash memory space, this file is compressed.
- **Download audio status:** the current status of the audio devices, streams and the gain setting. The origin of the information differs according to the platform:
 - **CP_LO phone models:** information from /proc/ept filesystem and from pxcon tool.
 - **CP_HI phone models:** information from mxcon tool.

QoS reports

Conditions and thresholds for report generation

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

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

Administration via WBM

1. Open Diagnostics > QoS Reports > Generation.

Generation	
Report mode	OFF
Report interval (seconds)	60
Observation interval (seconds)	10
Minimum session length (100 millisecond units)	20
Codec independent threshold values	
Maximum jitter (milliseconds)	20
Average round trip delay (milliseconds)	100
Non-compressing codec threshold values	
Lost packets (per 1000 packets)	10
Consecutive lost packets	2
Consecutive good packets	8
Compressing codec threshold values	
Lost packets (per 1000 packets)	10
Consecutive lost packets	2
Consecutive good packets	8
Resend last report	<input type="checkbox"/>
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

- **Report mode:** Sets the conditions for generating a QoS report. Value range:
 - **"OFF":** No reports are generated.
 - **"EOS Threshold exceeded":** Default value. A report is created if a) a telephone conversation longer than the Minimum session length has just ended, and b) a threshold value has been exceeded during the conversation.

- **"EOR Threshold exceeded"**: A report is created if a) the report interval has just passed, and b) a threshold value has been exceeded during the observation interval.
- **"EOS (End of Session)"**: A report is created if a telephone conversation longer than the Minimum session length has just ended.
- **"EOR (End of Report Interval)"**: A report is created if the report interval has just passed.
- **Report interval (seconds)**: Time interval between the periodical observations.
 - Default: 60
- **Observation interval (seconds)**: During this time interval, the traffic is observed.
 - Value: 10
- **Minimum session length (100 millisecond units)**: When the Report mode is set to "EOS Threshold exceeded" or "EOS (End of Session)", a report can be created only if the duration of the conversation exceeds this value.
 - Default: 20
- **Maximum jitter (milliseconds)**: When the jitter exceeds this value, a report is generated.
 - Default: 20
- **Average round trip delay (milliseconds)**: When the average round trip time exceeds this value, a report is generated.
 - Default: 100

Non-compressing codecs

The following threshold values apply to non-compressing codecs:

- **Lost packets (per 1000 packets)**: When the number of lost packets exceeds this maximum value during the observation interval, a report is created.
 - Default: 10.
- **Consecutive lost packets**: When the number of lost packets following one another exceeds this maximum value during the observation interval, a report is created.
 - Default: 2.
- **Consecutive good packets**: When the number of good packets following one another falls below this minimum value, a report is created.
 - Default: 8.

Compressing codecs

The following threshold values apply to compressing codecs:

- **Lost packets (per 1000 packets)**: When the number of lost packets exceeds this maximum value during the observation interval, a report is created.
 - Default: 10.
- **Consecutive lost packets**: When the number of lost packets following one another exceeds this maximum value during the observation interval, a report

is created.

- Default: 2.
- **Consecutive good packets:** When the number of good packets following one another falls below this minimum value, a report is created.
 - Default: 8.

General:

- **Resend last report:** If checked, the previous report is sent once again on pressing Submit. By default, this is unchecked.

The transmission of report data can be triggered manually by pressing Send now in the local menu.

Administration via local phone

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

View report

OpenScope Desk Phone CP phones generate QoS reports using a HiPath specific format, QDC (QoS Data Collection). The reports created for the last 6 sessions, i. e. conversations, can be viewed on the WBM.

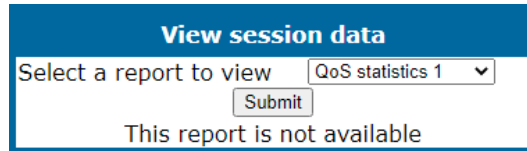
To enable the generation of reports, ensure that:

- The switch QoS traps to QCU (System > SNMP) is activated (see ["SNMP" → page 63](#));
- The conditions for the generation of reports are set adequately.

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

Data viewing via WBM

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



2. Click **Submit**.

A QoS report contains the following data:

- **Start of report period - seconds:** NTP time in seconds for the start of the report period.
- **Start of report period - fraction of seconds:** Additional split seconds to be added to the seconds for an exact start time.
- **End of report period - seconds:** NTP time in seconds for the end of the report period.
- **End of report period - fraction of seconds:** Additional split seconds to be added to the seconds for an exact end time.
- **SNMP specific trap type:** The trap type is a 5 bit value calculated from a list of threshold-exceeding bits. Every time a threshold is exceeded, the associated bit is set, otherwise it is cleared. The trace type bits are defined as follows:
 - **Bit 0:** Jitter threshold was exceeded.
 - **Bit 1:** Delay threshold was exceeded.
 - **Bit 2:** Threshold for lost packets was exceeded.
 - **Bit 3:** Threshold for consecutive lost packets was exceeded.
 - **Bit 4:** Threshold for consecutive good packets was exceeded.
- **IP address (local):** IP address of the local phone.
- **Port number (local):** RTP receiving port of the local phone.
- **IP address (remote):** IP address of the remote phone that took part in the session.
- **Port number (remote):** RTP sending port of the local phone.
- **SSRC (receiving):** RTP Source Synchronization Identifier of the local phone.
- **SSRC (sending):** RTP Source Synchronization Identifier of the remote phone.
- **Codec:** Number of the Payload Type applied in the session; see RFC 3551 (Table 4 and 5).
- **Maximum packet size:** Maximum size (in ms) of packets received during the report interval.
- **Silence suppression:** Number of silence suppression activation objects found in the RTP stream received. A silence suppression activation object is defined as a period of silence when no encoded voice signals were transmitted by the sender.
- **Count of good packets:** Total amount of good packets.
- **Maximum jitter:** Maximum jitter (in ms) found during the report interval.

- **Maximum inter-arrival jitter:** Maximum of the interarrival jitter values (in ms). The interarrival jitter is the smoothed absolute value of the jitter measurements. It is calculated continuously. For details about the calculation, see RFC 3550.
- **Periods jitter threshold exceeded:** Number of observation intervals in which the threshold for maximum jitter was exceeded.
- **Round trip delay:** Average value of delay calculated for each RTCP packet. The first value is available after about 15 sec.
- **Round trip delay threshold exceeded:** Set to "true" if the average round trip delay threshold value was exceeded in the report interval.
- **Count of lost packets:** Number of packets lost in the course of speech decoding.
- **Count of discarded packets:** Number of the packets discarded without transferring the contents.
- **Periods of lost packets:** Number of observation intervals in which the threshold for lost packets was exceeded.
- **Consecutive packet loss (CPL):** List of sequences consecutive packets that were all lost, grouped according to the amount of packets per sequence. The first number in the list counts single lost packets, the second number counts sequences of two lost packets, and so on. The last number counts sequences of more than 10 lost packets.
- **Periods of consecutive lost packets:** Number of observation intervals in which the threshold for consecutive lost packets was exceeded.
- **Consecutive good packets (CGP):** List of sequences consecutive packets that were all processed, grouped according to the amount of packets per sequence. The first number in the list counts single good packets, the second number counts sequences of two good packets, and so on. The last number counts sequences of more than 10 good packets. All values are reset to 0 after an interval without packet loss.
- **Periods of consecutive good packets:** Number of intervals in which the count of lost packets went below the threshold.
- **Count of jitter buffer overruns:** Number of packets rejected because the jitter buffer was full.
- **Count of jitter buffer under-runs:** Increased by one whenever the decoder requests new information on decoding and finds an empty jitter buffer.
- **Codec change on the fly:** The value is 1, if there has been a codec or SSRC change during the observation period, and 0, if there has been no change.
- **Periods with at least one threshold exceeded:** Number of observation intervals with at least one threshold exceedance. If there is no data, the value is 255. The threshold values included are:
 - maximum jitter;
 - lost packets;
 - consecutive lost packets;
 - consecutive good packets.
- **HiPath Switch ID:** Unique number identifying the HiPath switch to which the endpoints are assigned.
- **LTU number:** In HiPath 4000 only, the shelf identification is taken from the shelf containing a gateway.

- **Slot number:** The slot number where the phone is connected in the shelf.
- **Endpoint type :** Type of the local phone.
- **Version:** Software version of the local phone.
- **Subscriber number type:** Type of subscriber number assigned to the local phone. The possible types are:
 - **1:** local number, extension only
 - **2:** called number, network call
 - **3:** E.164 number of the local phone
- **Subscriber number:** Subscriber number of the local phone.
- **Call ID:** SIP call id.
- **MAC address:** MAC address of the local phone.

Miscellaneous

IP tests

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

Administration via WBM

1. Open Diagnostics > Miscellaneous > IP tests.

The screenshot shows the 'IP tests' configuration page. It has a blue header with the title 'IP tests'. Below the header, there are four sections:

- Pre defined ping tests:** A dropdown menu with 'Ping DLS' selected and a 'Ping' button.
- Ping tests:** An empty text input field and a 'Ping' button.
- Pre defined trace tests:** A dropdown menu with 'Traceroute DLS' selected and a 'Traceroute' button.
- Traceroute:** An empty text input field and a 'Traceroute' button.

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

Memory status information

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

The amount of free memory is checked on a regular basis in order to prevent problems caused by low memory. This check determines whether a recovery is necessary.

Administration via WBM

1. Open Diagnostics > Miscellaneous > Memory information.

Memory information

Memory monitor configuration

Disable reboot

High threshold(MBs)

Low threshold(MBs)

Working hour start

Working hour end

[Download memory info file](#) [Download old memory info file](#) [Download thread info for admin](#)

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

Device memory information

```
Mem: 123988K used, 117156K free, 604K shrd, 0K buff, 46900K cached
CPU:  0% usr  28% sys  66% nic 66% idle  0% io  0% irq  0% irq
Load average: 2.15 2.15 2.04 1/251 1392
PID  PPID USER  STAT  VSZ %VSZ KCPU COMMAND
511  1 root    S  17844  7%  app_dsp
608  583 root    S  132n 56%  0% SvcConfig services.conf -startLogDaemon -logAll V2 R0.3.66 SIP 220505
1065 608 root    SN 36432 15%  0% (QT Gui CallView) PhoneletLauncher callview.phd V2 R0.3.66 SIP 220505 WPI Siemens SIP US en DD.MM.YYYY 24HR 0 NO_APP_PROP
1032 608 root    SN 35808 15%  0% (QT Gui DesktopP) PhoneletLauncher desktopphonelet.phd V2 R0.3.66 SIP 220505 WPI Siemens SIP US en DD.MM.YYYY 24HR 0 NO_APP_PROP
583  1 root    S  34448 14%  0% SvcConfig healthservice.conf
1093 608 root    SN 34252 14%  0% (QT Gui AdminPho) PhoneletLauncher admin.phd V2 R0.3.66 SIP 220505 WPI Siemens SIP US en DD.MM.YYYY 24HR 0 NO_APP_PROP
1134 608 root    SN 31256 13%  0% (QT Gui CalllogP) PhoneletLauncher calllog.phd V2 R0.3.66 SIP 220505 WPI Siemens SIP US en DD.MM.YYYY 24HR 0 NO_APP_PROP
1092 608 root    SN 31140 13%  0% (QT Gui LDAppPho) PhoneletLauncher ldapp.phd V2 R0.3.66 SIP 220505 WPI Siemens SIP US en DD.MM.YYYY 24HR 0 NO_APP_PROP 192x48+0 -chlid
1091 608 root    SN 30700 13%  0% (QT Gui Messages) PhoneletLauncher MessagesPhonelet.phd V2 R0.3.66 SIP 220505 WPI Siemens SIP US en DD.MM.YYYY 24HR 0 NO_APP_PROP
1066 608 root    SN 27208 11%  0% (QT Gui Applaunch) PhoneletLauncher Applauncher.phd V2 R0.3.66 SIP 220505 WPI Siemens SIP US en DD.MM.YYYY 24HR 0 NO_APP_PROP
1036  1 appweb  SN 15740  7%  0% ./appweb --config opera_appweb_latestflsonly.conf
1387 1036 appweb  SN 14048  6%  0% /Opera_Deploy/appweb/web/page.cnd
582  1 root    S  11672  5%  0% SplashScreenapp
718  1 root    S  7324  3%  0% /usr/sbin/stunnel /Opera_Deploy/stunnel_server_allTlsVersions.conf
709 608 root    S  4220  2%  0% /sbin/dhclient -4 -d -q -sf /Opera_Deploy/networking/dhcpv4Event.sh -lf /data/networking/dhcpv4Leases.none -cf /data/networking/dhcpv4.conf eth0
1  0 root    S  3024  1%  0% init
312  1 root    S  3024  1%  0% /sbin/syslogd -L -s 2000 -O /tmp/logs/messages
```

- When "Disable reboot" is checked, no reboot will take place when a memory problem has been found. However, recovery requires a reboot. The recovery process is triggered when the available main memory (RAM) falls below a given threshold value. As memory consumption is assumed to be higher during working hours, two thresholds are configurable.
- The High Threshold (MBs) parameter defines the threshold for off-time:
 - For OpenScape Desk Phone CP110/210, the default value is 10 MB.
 - For OpenScape Desk Phone CP410/710, it is 30 MB.
- With Low Threshold (MBs), the threshold for off-time is defined:
 - For OpenScape Desk Phone CP110/210, the default value is 8 MB.
 - For OpenScape Desk Phone CP410/710, it is 20 MB.
- The beginning and end of the working hours are defined in 24 hours format with Working Hour Start (Default: 5) and Working Hour End (Default: 24).

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

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

Core dump

Administration via WBM

1. Open Diagnostics > Miscellaneous > Core Dump.

- 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 set to “Enabled”. Furthermore, the IP address of the server receiving the syslog messages must be entered in Remote ip, and the corresponding server port must be given in Remote port.
- With version V2, the User notification parameter controls whether the user is notified about the remote tracing or not. If “Use notification” is enabled, a blinking **symbol** (🔑 on OpenScape Desk Phone CP210) will inform the user when remote tracing is active, i.e. when “Remote Trace Status” is set to “Enabled”.

Administration via Local Phone

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

Key modules

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

- On an OpenScape Desk Phone CP710 a key module provides 12 additional free programmable keys. A maximum of two key modules can be connected to the phone.

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 does not switch automatically back to the "Normal" level, unless configured to do so.

2. Open System > Features > Configuration.

Configuration

General

Emergency number	<input type="text"/>
Voice mail number	<input type="text"/>
MWI LED	AlertBar only ▾
Missed call LED	AlertBar LED ▾
AlertBar LED hint	<input type="checkbox"/>
Allow refuse	<input type="checkbox"/>
Hot/Warm phone	No action ▾
Hot/Warm destination	<input type="text"/>
Initial digit timer (seconds)	30
Allow uaCSTA	<input checked="" type="checkbox"/>
Server features	<input checked="" type="checkbox"/>
Not used timeout (minutes)	2 ▾
Transfer on hangup	<input type="checkbox"/>
Bridging enabled	<input type="checkbox"/>
Dial plan enabled	<input type="checkbox"/>
FPK program timer	On ▾
Selected Dial Action on calls	No action ▾
DSS monitored	<input type="checkbox"/>
Show icon for all forwarding types	<input type="checkbox"/>
Automatic key module switchback	<input checked="" type="checkbox"/>
Simultaneous key module switching	<input checked="" type="checkbox"/>

3. To configure the phone to automatically switch back to the Normal level, enable **Automatic key module switchback**. The phone will start a 15 seconds timer and then switch to the non shifted level on all the attached KM400/KM600.

Examples and how-tos

Canonical dialing

Canonical dialing settings

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

Parameter	Example value	Explanation
Local country code	44	International country code for the UK.
National prefix digit	0	Used in front of national codes when dialed without international prefix.
Local national code	115	Area code within the UK (here: Nottingham).
Minimum local number length	7	Number of digits in a local PSTN number (e. g. 3335333 = 7 digits).
Local enterprise node	780	Prefix to access Nottingham numbers from within the company Network.
PSTN access code	9	Prefix to make an international call in the UK.
Operator codes	0, 7800	Set of numbers to access the local operators.
Emergency numbers	999, 555	Set of numbers to access emergency services.
Initial extension digits	2, 3, 4, 5, 6, 8	1 st digits of numbers that are used for extension numbers on the local node.

Canonical dialing look-up

The following example shows settings suitable for recognizing incoming numbers and assigning them to entries in the local phone-book, and for generating correct dial strings from phone book entries, depending on whether the number is internal or external.

Parameter	Example value	Explanation
Local code <1>	780	Enterprise node prefix (here: Nottingham).
International code <1>	+44115943	Equivalent prefix to access numbers on this node from the PSTN. Here, the prefix used by the PSTN (DID/DDI: direct inward dialing) is 943, which differs from the enterprise node prefix used within the enterprise Network.
Local code <2>	7007	Enterprise node prefix (here: Munich).
International code <2>	+49897007	Equivalent prefix to access numbers on this node from the PSTN. Here, the prefix used by the PSTN for direct inward dialing is identical to the enterprise node prefix.

Conversion examples

In the following examples, numbers entered into the local Directory by the user are converted according to the settings given above.

Example 1: Internal number, same node as the local phone

User entry		2345
External numbers		Local public form
External access code		Not required
International gateway code		Use national code
Number stored in the Directory		+441159432345
Dial string sent when dialing from the Directory	Internal numbers = Local enterprise form	1234
	Internal numbers = Always add node	7802345
	Internal numbers = Use external numbers	9432345

Example 2: Internal number, different node

User entry		70072345
External numbers		Local public form
External access code		Not required
International gateway code		Use national code
Number stored in the Directory		+498970072345
Dial string sent when dialing from the Directory	Internal numbers = Local enterprise form	2345
	Internal numbers = Always add node	7802345
	Internal numbers = Use external numbers	9432345

Example 3: External number, same local national code as the local phone

User entry		011511234567
External numbers		Local public form
External access code		Not required
International gateway code		Use national code
Number stored in the Directory		+4411511234567
Dial string sent when dialing from the Directory	External numbers = Local public form	234567
	External numbers = National public form	011511234567
	External numbers = International form	004411511234567

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

The “Corporate directory” function is based on an LDAP client that can be connected to the company’s LDAP service. A variety of LDAP servers can be used, for instance Microsoft Active Directory, OpenLDAP, or Apache Directory Server.

Prerequisites

- An LDAP server is present and accessible to the phone’s Network. The standard server port for LDAP is 389, the standard transport for LDAP is TCP.
- Query access to the LDAP server must be provided. Unless anonymous access is used, a user name and password must be provided. It might be feasible to use a single login and password for all OpenScape Desk Phone CP phones.
- To enable dialing internal numbers from the corporate phone book, an LDAP entry must be provided that contains the proper number format required by OpenScape Desk Phone CP for OpenScape Voice.
- In Microsoft Active Directory, the standard LDAP attribute `telephoneNumber` is typically populated as follows: `+1<area code><call number>`. However, in a standard configuration, OpenScape Desk Phone CP will not handle this dial string correctly, due to the +1 prefix. Therefore, it is recommended to use the “ipPhone” field, which is typically unused in Active Directory. It can be found in the Telephones tab of the Active Directory User Manager.

Create an LDAP template

The task of an LDAP template is to map the phone’s search and display fields to LDAP attributes that can be delivered by the server. In the LDAP template, the fields are represented by hard-coded names: `ATTRIB01`, `ATTRIB02`, and so on. These field names are assigned to LDAP attributes, as appropriate.

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

Note In an LDAP template for OpenScape Desk Phone CP, the entries must be sorted according to the sequential number of the template labels, as shown in the example underneath.

Administration via WBM

1. Open Local functions > LDAP template.

LDAP template

This page allows you to specify the LDAP attribute fields that will be used by the phone, plus how the field is used.

Use	Field name	Usage type
Search base	<input style="width: 100%;" type="text"/>	
Last name	<input style="width: 100%;" type="text"/>	▼
First name	<input style="width: 100%;" type="text"/>	▼
Work 1	<input style="width: 100%;" type="text"/>	▼
Work 2	<input style="width: 100%;" type="text"/>	▼
Mobile	<input style="width: 100%;" type="text"/>	▼
Home	<input style="width: 100%;" type="text"/>	▼
Company	<input style="width: 100%;" type="text"/>	▼
Address 1	<input style="width: 100%;" type="text"/>	▼
Address 2	<input style="width: 100%;" type="text"/>	▼
Role	<input style="width: 100%;" type="text"/>	▼
Email	<input style="width: 100%;" type="text"/>	▼
Nickname	<input style="width: 100%;" type="text"/>	
Avatar	<input style="width: 100%;" type="text"/>	

Generic example (standard attributes)

OpenScope Desk Phone CP field	LDAP template labels	LDAP attribute	Example value
Last name	ATTRIB01	surnameNational	Doe
First name	ATTRIB02	givenNameNational	John
Work 1	ATTRIB03	telephoneNumber	9991234
Work 2	ATTRIB04	alternatePhone	9992345
Mobile	ATTRIB05	mobile	017711223344
Home	ATTRIB06	otherTelephone	441274333444
Company	ATTRIB07	ou	Example Inc.
Address 1	ATTRIB08	departmentText	0815
Address 2	ATTRIB09		

OpenScape Desk Phone CP field	LDAP template labels	LDAP attribute	Example value
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 → 107

Given "example.com" as the LDAP subtree to be searched, the LDAP template file looks like this:

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

Microsoft Active Directory specific example

OpenScape Desk Phone CP field	LDAP template attribute	LDAP attribute	Example value
Last name	ATTRIB01	sn	Doe
First name	ATTRIB02	givenName	John
Business 1	ATTRIB03	ipPhone	9991234
Business 2	ATTRIB04	otherTelephone	9992345

OpenScape Desk Phone CP field	LDAP template attribute	LDAP attribute	Example value
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

Given "example.com" as the LDAP subtree to be searched, the LDAP template file looks like this:

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

Upload the LDAP template to the phone

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 108).
4. Optionally, use the local menu or the DLS (see the Deployment Service Administration Manual).

Example

1. Open File transfer > LDAP.

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
 - **Permanent LDAP enabled**
3. Click **Submit**.

LLDP-Med example

The following example illustrates the mode of operation of LLDP-MED. To evoke a reaction from LLDP-MED, the LAN switch has been set to auto-negotiation, whereas the phone's LAN port is set to 100 Mbit/s, hence a fixed value (see "[LAN port settings](#)" → [page 43](#)). This configuration error is discovered by LLDP-MED. The following screenshots from the phone local menu show the error messages.

This [screenshot](#) shows the LLDP-MED operation submenu (see "[LLDP-MED](#)" → [page 138](#)).

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 using the navigation keys.
3. Click **OK**.
4. In the LLDP-MED operation submenu, navigate to MAC_Phy config.
5. Note the status displayed.
6. Select the MAC_Phy config submenu by pressing **OK**.
7. Navigate to the parameters displayed by using the navigation keys. The following status is displayed for the MAC_Phy config parameters:
 - AutoSet enabled = Incompatible
 - MAU = Incompatible

Technical reference

Default port list

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

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

Service	Server Default Port	Client Default Port	Protocol Stack
Secure communication with the DLS workpoint interface	---	18444	HTTPS / TCP - SSL / TLS
Connection to the control port of FTP server	21	32786 - 61000	FTP / TCP
FTP client; uses the FTP server in active mode	32786 - 61000	20	FTP / TCP
HTTPS file download server	443	32786 - 61000	HTTPS / TCP - SSL/TLS
Client application which sends QDC data to the QCU	---	32786 - 61000	SNMP / UDP
Part of SNMP-Agent - sending Traps	---	32786 - 61000	SNMP / UDP
Part of SNMP-Agent - receive Set/Get commands	161	---	SNMP / UDP
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
OpenStage Phone Manager	65531	---	HTTP / TCP
OpenStage Phone Manager	65530	---	HTTP / UDP

Troubleshooting error codes

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

Example

“No Telephony possible (LP)”

Network Errors

Error code	Priority	Problem	Description
LP	0	Unable to use LAN connection	Physical connection error
LX	1	Unable to use LAN connection	802.1x errors
L1	2	Unable to register HFA main line	No IP address - Manual config mode
L2	3	Unable to register HFA main line	No default route - Manual config mode
L3	4	Unable to register HFA main line	No default route - Manual config mode
LI	5	Unable to use LAN connection	Network Configuration Error â General IP error - Manual config mode
D0	6	Unable to contact DHCP	Network Configuration Error - DHCP failure
TT	7	Unable to establish a TLS connection	No SNTP server

HFA Configuration Errors

Error code	Priority	Problem	Description
H4	8	Unable to register HFA main line	No gateway IP address

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

Communication Errors

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

Error code	Priority	Problem	Description
		HFA main line	gress
HH	11	Unable to register HFA main line	Logon: Rejected due to shutdown
HI	11	Unable to register HFA main line	Logon: Rejected due to duplicate Logon
HJ	11	Unable to register HFA main line	Logon: Rejected due to already logged on
HK	11	Unable to register HFA main line	Logon: Rejected due to PIN not present
HL	11	Unable to register HFA main line	Logon: Rejected due to password not present
HM	11	Unable to register HFA main line	Logon: Rejected due to password not correct
HN	11	Unable to register HFA main line	Logon: Rejected due to invalid license
Ha	11	Unable to register HFA main line	Logoff: Rejected due to missing LN
HQ	11	Unable to register HFA main line	Logoff: Normal Logoff
HR	11	Unable to register HFA main line	Logoff: Client not logged on
HS	11	Unable to register HFA main line	Logoff: Client logged off
HT	11	Unable to register HFA main line	Logoff: Forced client logoff
HU	11	Unable to register HFA main line	Logoff: Timeout expired
HV	11	Unable to register HFA main line	Logoff: OMC action

Error code	Priority	Problem	Description
HW	11	Unable to register HFA main line	Logoff: Hfa mobile user logged on
HX	11	Unable to register HFA main line	Logoff: Switch back to central system
HY	11	Unable to register HFA main line	Logoff: No bearer channel
HZ	11	Unable to register HFA main line	Logoff: New logon requested from the server
H[11	Unable to register HFA main line	Logoff: Forced client logoff due to an incorrect PreShared secret
H0	12	Unable to register HFA main line	General Error
UC1	13	UC (WSI) server not accessible	Invalid UC server access configuration
UC2	14	UC logon rejected/not available	No access to UC service (UC mode)
EX	15	Exchange failure	<ul style="list-style-type: none"> • Exchange: check username and password • Exchange: untrusted server • connection to Exchange server failed
CI	16	Circuit failure	<ul style="list-style-type: none"> • Circuit: check username and password • Circuit: untrusted server • connection to Circuit server failed
NT	17	SNTP server unavailable	No SNTP connection

Glossary

Address of Record (AoR)

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

ADPCM

Adaptive Differential Pulse Code Modulation. A compressed encoding method for audio signals which are transmitted by a low bandwidth. A sample is coded as the difference between its predicted value and its real value. As this difference is usually smaller than the real, absolute value itself, a lesser number of bits can be used to encode it.

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 OpenScope management application for the administration of workpoints, i. e. IP Phones and IP Clients, in both HiPath- and non-HiPath networks.

DNS

Domain Name System. Performs the translation of Network domain names and computer hostnames.

DTMF

Dual Tone Multi Frequency. A means of signaling between a phone and e. g. a voice-mail facility. The signals can be transmitted either in-band, i. e. within the speech band, or out-band, i. e. in a separate signaling channel.

EAP

Extensible Authentication Protocol. An authentication framework that is frequently used in WLAN networks. It is defined in RFC 3748.

FTP

File Transfer Protocol. Used for transferring files in networks, e. g., to update telephone software.

G.711

ITU-T standard for audio encoding, used in e.g. ISDN. It requires a 64 kBit/s bandwidth.

G.722

ITU-T standard for audio encoding using split band Network. The audio bandwidth is 7 kHz at a sampling rate of 16 kHz. There are several transfer rates ranging from 32 to 64 kBit/s, which correspond to different compression degrees. The voice quality is very good.

G.729

ITU-T standard for audio encoding with low bandwidth requirements, mostly used in VoIP. The standard bit rate is 8 kBit/s. Music or tones such as ring tones or fax tones cannot be transported reliably with this codec.

Gateway

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

HTTP

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

IP

Internet Protocol. A data-oriented Network layer protocol used for transferring data across a packet-switched Network. Within this Network layer, reliability is not guaranteed.

IP address

The unique address of a terminal device in the Network. It consists of four number blocks of 0 to 255 each, separated by a point.

Jitter

Latency fluctuations in the data transmission resulting in distorted sound.

LAN

Local Area Network. A computer Network covering a local area, like an office, or group of buildings.

Layer 2

2nd layer (Data Link Layer) of the 7-layer OSI model for describing data transmission interfaces.

Layer 3

3rd layer (Network Layer) of the 7-layer OSI model for describing the data transmission interfaces.

LCD

Liquid Crystal Display. Display of numbers, text or graphics with the help of liquid crystal technology.

LDAP

Lightweight Directory Access Protocol. Simplified protocol for accessing standardized directory systems, e.g., a company telephone directory.

LED

Light Emitting Diode. Cold light illumination in different colours at low power consumption.

MAC Address

Media Access Control address. Unique 48-bit identifier attached to Network adapters.

MDI-X

Media Dependent Interface crossover (X). The send and receive pins are inverted. This MDI allows the connection of two endpoints without using a crossover cable. When Auto MDI-X is available, the MDI can switch between regular MDI and MDI-X automatically, depending on the connected device.

MIB

Management Information Base. A type of database used to manage the devices in a communications Network.

MWI

Message Waiting Indicator. A signal, typically a LED, to notify the user that new mail-box 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 → 174 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.

Provide feedback to further optimize this document to edoku@atos.net.

As reseller please address further presales related questions to the responsible presales organization at Unify or at your distributor. For specific technical inquiries you may use the support knowledge base, raise - if a software support contract is in place - a ticket via our partner portal or contact your distributor.

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO 9001 and ISO 14001 standards and are certified by an external certification company.

Copyright © Unify Software and Solutions GmbH & Co. KG 08/2022
All rights reserved.

Reference No.: A31103-C1100-M102-13-76A9

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products.

An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.

Availability and technical specifications are subject to change without notice.

Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG. All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

atos.net

The logo for Atos, featuring the word "Atos" in a bold, white, sans-serif font. The letter 'o' is stylized with a circular cutout in the center.