UNIFY Harmonize your enterprise

OpenScape Desk Phone CP200/CP205/CP400/CP600 Phone Administration HFA

Administration Manual

A31003-C1000-M102-5-76A9

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standards and are certified by an external certification company.

Copyright © Unify Software and Solutions GmbH & Co. KG 09/2017
Mies-van-der-Rohe-Str. 6, 80807 Munich/Germany

All rights reserved.

Reference No.: A31003-C1000-M102-5-76A9

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.

UNIFY Harmonize your enterprise

unify.com

Content

1 Overview 8
1.1 Important Notes 8
1.2 Maintenance Notes 9
1.3 Product-oriented environmental protection 9
1.4 Labeling 9
1.5 About the Manual 10
1.6 Conventions for this Document 11
1.7 The OpenScape Desk Phone CP Family 11
1.7.1 OpenScape Desk Phone CP600 12
1.7.2 OpenScape Desk Phone CP400 13
1.7.3 OpenScape Desk Phone CP200/CP205 14
1.8 Administration Interfaces 15
1.8.1 Web-based Management (WBM) 15
1.8.2 DLS (OpenScape Deployment Service) 15
1.8.3 Local Phone Menu 15

2 Startup 16
2.1 Prerequisites 16
2.2 Assembling and Installing the Phone 16
2.2.1 Shipment 16
2.2.2 Connectors at the bottom side 17
2.2.3 Assembly 19
2.2.4 How to Connect the Phone 20
2.2.5 How to Better Use LAN Network Connections 21
2.2.6 Key Module 21
2.3 Quick Start 22
2.3.1 How to Access the Web Interface (WBM) 22
2.3.2 Access via Local Phone 23
2.3.2.1 OpenScape Desk Phone CP20X 23
2.3.2.2 OpenScape Desk Phone CP400/600 24
2.3.3 How to Set the Terminal Number 25
2.3.4 Basic Network Configuration 25
2.3.5 DHCP Resilience 26
2.3.6 Date and Time / SNTP 27
2.3.7 Extended Network Configuration 27
2.3.8 VLAN Discovery 28
2.3.8.1 Using a Vendor Class 28
2.3.8.2 Using Option #43 "Vendor Specific" 33
2.3.9 DLS Server Address 35
2.3.9.1 Using Vendor Class 35
2.3.9.2 Using Option #43 "Vendor Specific" 42

2.3.10 HFA Gateway Settings . . . 44
2.3.11 Using the Web Interface (WBM) . . . 44
2.3.12 Using the Local Menu . . . 44

3 Administration . . . 45
3.1 Bluetooth Interface . . . 45
3.1.1 Feature Access . . . 45
3.2 LAN Settings . . . 46
3.2.1 LAN Port Settings . . . 46
3.2.2 VLAN . . . 48
3.2.2.1 Automatic VLAN discovery using LLDP-MED . . . 48
3.2.2.2 Automatic VLAN discovery using DHCP . . . 49
3.2.2.3 Manual configuration of a VLAN ID . . . 50
3.3 IP Network Parameters . . . 52
3.3.1 Quality of Service (QoS) . . . 52
3.3.1.1 Layer 2 / 802.1p . . . 52
3.3.1.2 Layer 3 / Diffserv . . . 53
3.3.2 Use DHCP . . . 55
3.3.3 IP Address - Manual Configuration . . . 57
3.3.4 Default Route/Gateway . . . 58
3.3.5 Specific IP Routing . . . 59
3.3.6 DNS . . . 60
3.3.6.1 DNS Domain Name . . . 60
3.3.6.2 Terminal Hostname . . . 61
3.3.7 Configuration & Update Service (DLS) . . . 62
3.3.8 SNMP . . . 64
3.4 OpenScape Service Menu . . . 67
3.5 System Settings . . . 68
3.5.1 System Identity . . . 68
3.5.2 HFA Gateway Settings . . . 68
3.5.3 HFA Emergency Gateway Settings . . . 70
3.5.4 Server and Standby Server ports . . . 71
3.5.5 Redundancy . . . 72
3.5.6 Emergency number . . . 74
3.5.7 LIN . . . 74
3.5.8 Not Used Timeout . . . 75
3.5.9 Energy Saving . . . 76
3.5.9.1 Energy Efficient Ethernet (OpenScape Desk Phone CP205/CP400/600 only) 76
3.5.10 Date and Time . . . 76
3.5.10.1 SNTP is Available, but no Automatic Configuration by DHCP Server . . . 77
3.5.11 Security . . . 79
3.5.11.1 System . . . 79
3.5.11.2 Access control . . . 81
3.6 Dialing . . . 82
3.6.1 Canonical Dialing Configuration . . . 82

3.6.2 Canonical Dial Lookup . . . 85
3.7 Distinctive Ringing . . . 87
3.8 User Mobility . . . 91
3.9 Transferring Phone Software, Application, and Media Files . . . 92
3.9.1 FTP/HTTPS Server . . . 92
3.9.2 Common FTP/HTTPS Settings (Defaults) . . . 92
3.9.3 Phone Application . . . 95
3.9.3.1 Upgrade Using File . . . 95
3.9.3.2 Upgrade Using FTP/HTTPS Access Data . . . 95
3.9.3.3 Download/Update Phone Application . . . 99
3.9.4 Picture Clips . . . 101
3.9.4.1 FTP/HTTPS Access Data . . . 101
3.9.4.2 Download Picture Clip . . . 103
3.9.5 LDAP Template . . . 104
3.9.5.1 FTP/HTTPS Access Data . . . 104
3.9.5.2 Download LDAP Template . . . 106
3.9.6 Screensaver . . . 107
3.9.6.1 FTP/HTTPS Access Data . . . 107
3.9.6.2 Download Screensaver . . . 109
3.9.7 Ringer File . . . 110
3.9.7.1 FTP/HTTPS Access Data . . . 111
3.9.7.2 Download Ringer File . . . 113
3.9.8 Dongle Key . . . 114
3.9.8.1 FTP/HTTPS Access Data . . . 114
3.9.8.2 Download Dongle Key File . . . 116
3.10 UC Server . . . 117
3.11 Corporate Phonebook: Directory Settings . . . 118
3.11.1 LDAP . . . 118
3.11.2 Canonical Dial Settings . . . 119
3.11.3 Picture via LDAP . . . 120
3.12 Speech . . . 122
3.12.1 RTP Base Port . . . 122
3.12.2 Codec Preferences . . . 123
3.12.3 Display General Phone Information . . . 125
3.13 Security and Policies . . . 126
3.13.1 Password . . . 126
3.13.1.1 Troubleshooting: Lost Password . . . 127
3.13.2 Certificates . . . 127
3.13.2.1 Generic . . . 127
3.13.2.2 Authentication Policy . . . 128
3.14 Restart Phone . . . 129
3.15 Factory Reset . . . 129
3.16 SSH – Secure Shell Access . . . 130
3.17 Display License Information . . . 131

3.18 Web Services Interface (WSI) . . . 131
3.19 HPT Interface (For Service Staff) . . . 132
3.20 Diagnostics . . . 133
3.20.1 LLDP-MED . . . 134
3.20.2 Fault Trace Configuration . . . 136
3.20.3 EasyTrace Profiles . . . 142
3.20.3.1 Call Connection . . . 142
3.20.3.2 Call Log Problems . . . 143
3.20.3.3 Call recording . . . 143
3.20.3.4 DAS Connection . . . 144
3.20.3.5 DLS Data Errors . . . 144
3.20.3.6 HFA registration and security . . . 145
3.20.3.7 Help Application problems . . . 145
3.20.3.8 Key Input problems . . . 146
3.20.3.9 LAN Connectivity problems . . . 146
3.20.3.10 Messaging application problems . . . 147
3.20.3.11 Mobility problems . . . 147
3.20.3.12 Phone administration problems . . . 148
3.20.3.13 Phonebook (LDAP) problems . . . 148
3.20.3.14 Phonebook (local) problems . . . 149
3.20.3.15 Server based application problems . . . 149
3.20.3.16 Sidecar problems . . . 150
3.20.3.17 Speech problems . . . 150
3.20.3.18 Tone problems . . . 151
3.20.3.19 Web based management . . . 151
3.20.3.20 802.1x problems . . . 152
3.20.3.21 No Tracing for All Services . . . 153
3.20.4 Bluetooth advanced traces . . . 154
3.20.5 QoS Reports . . . 155
3.20.5.1 Conditions and Thresholds for Report Generation . . . 155
3.20.5.2 View Session Data . . . 158
3.20.6 Miscellaneous . . . 162
3.20.6.1 IP tests . . . 162
3.20.6.2 Memory Status Information . . . 163
3.20.6.3 Core dump . . . 165
3.20.7 Remote Tracing – Syslog . . . 166

4 Examples and HowTos . . . 167
4.1 Canonical Dialing . . . 167
4.1.1 Canonical Dialing Settings . . . 167
4.1.2 Canonical Dial Lookup . . . 168
4.1.2.1 Conversion examples . . . 169
4.2 How to Set Up the Corporate Phonebook (LDAP) . . . 171
4.2.1 Prerequisites . . . 171
4.2.2 Create an LDAP Template . . . 172

4.2.3 How to Load the LDAP Template into the Phone 174
4.2.4 Configure LDAP Access 175
4.3 An LLDP-Med Example 175

5 Technical Reference 176
5.1 Default Port List 176
5.2 Troubleshooting: Error Codes 177
5.3 Troubleshooting: Error Messages 178

Glossary 181

Index 188

1 Overview

1.1 Important Notes

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

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

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

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

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

For USA and Canada only:

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

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

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

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

1.2 Maintenance Notes

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

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

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

1.3 Product-oriented environmental protection

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

ENERGY STAR	ENERGY STAR is a U.S. Environmental Protection Agency voluntary program that helps businesses and individuals save money and protect our climate through superior energy efficiency. Products that earn the ENERGY STAR prevent greenhouse gas emissions by meeting strict energy efficiency criteria or requirements set by the U.S. Environmental Protection Agency. Unify is an ENERGY STAR partner participating in the ENERGY STAR program for Enterprise Servers and Telephony. The Unify products OpenScape DeskPhone CP200/400/600 have earned the ENERGY STAR. Learn more at energystar.gov.

Special setting instructions for energy-efficient use of the telephone can be found on page 78 in the User Manual.

1.4 Labeling

CE

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

1.5 About the Manual

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

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

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

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

1.6 Conventions for this Document

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

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

This document describes the software version V1.

1.7 The OpenScape Desk Phone CP Family

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

- Section 1.7.1, “OpenScape Desk Phone CP600”
- Section 1.7.2, “OpenScape Desk Phone CP400”
- Section 1.7.3, “OpenScape Desk Phone CP200/CP205”

1.7.1 OpenScape Desk Phone CP600

1	With the **Handset**, the user can pick up and conduct calls in the usual manner.
2	The **Microphone** is used in the speakerphone mode.
3	The **Display** provides intuitive support for telephone operation.
4	With the **Menu Key**, the user/administrator has access to the user/administrator menu.
5	With the **Navigation Keys**, the user/administrator can navigate through the various phone functions.
6	With the **Soft Keys**, the user/administrator can operate the phone´s functions.
7	Audio Keys: **+** and **-**: Increases/decreases the speaker/headset and handset volume. **Mute**: Turns off/on the microphone during conversations. **Speaker**: Turns on/off the hands-free mode (speakerphone). **Headset**: Switches the audio between handset/speakerphone and headset
8	The **Notification LED** visually signals incoming calls and new voice messages.
9	The **Keypad** is used for entering phone numbers and text.
10	The **Out-of-Office Key** provides an easy way to set up Call Forwarding and your Presence State.

Tabelle 1-1

1.7.2 OpenScape Desk Phone CP400

1	With the **Handset**, the user can pick up and conduct calls in the usual manner.
2	The **Microphone** is used in the speakerphone mode.
3	The **Display** provides intuitive support for telephone operation.
4	With the **Menu Key**, the user/administrator has access to the user/administrator menu.
5	With the **Navigation Keys**, the user/administrator can navigate through the various phone functions.
6	With the **Context Keys**, the user/administrator can operate the phone´s functions.
7	Audio Keys: **+** and **-**: Increases/decreases the speaker/headset and handset volume. **Mute**: Turns off/on the microphone during conversations. **Speaker**: Turns on/off the hands-free mode (speakerphone). **Headset**: Switches the audio between handset/speakerphone and headset
8	The **Notification LED** visually signals incoming calls and new voice messages.
9	The **Keypad** is used for entering phone numbers and text.
10	The **Out-of-Office Key** provides an easy way to set up Call Forwarding or your Presence State.
11	The **Free programmable Keys** can be set up with various functions defined by user.

Tabelle 1-2

1.7.3 OpenScape Desk Phone CP200/CP205

1	With the **Handset**, the user can pick up and conduct calls in the usual manner.
2	The **Microphone** is used in the speakerphone mode.
3	The **Display** provides intuitive support for telephone operation.
4	Conversation Keys: **Hold**: Places a call in hold. **Transfer**: Transfers a current call to another party. **Conference**: Initiates a conference call.
5	With the **Menu Key**, the user has access to the user menu.
6	With the **Messages Key**, the user has access to the voicemail and the call log.
7	With the **Navigation Keys**, the user/administrator can navigate through the various phone functions.
8	With the **Function Keys**, the user can comfortably operate the phone´s functions like Conversations, Phonebook, Call Forwarding and Redial.
9	The **Keypad** is used for entering phone numbers and text.
10	Audio Keys: **+** and **-**: Increases/decreases the speaker/headset and handset volume. **Mute**: Turns off/on the microphone during conversations. **Speaker**: Turns on/off the hands-free mode (speakerphone). **Headset**: Switches the audio between handset/speakerphone and headset
11	The **Notification LED** visually signals incoming calls and new voice messages.

Tabelle 1-3

1.8 Administration Interfaces

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

1.8.1 Web-based Management (WBM)

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

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

1.8.2 DLS (OpenScape Deployment Service)

The OpenScape Deployment Service (DLS) is an OpenScape Management application for administering phones and soft clients in both OpenScape and non-OpenScape networks. It has a Java-supported, web-based user interface, which runs on an internet browser. For further information, please refer to the OpenScape Deployment Service Administration Guide.

1.8.3 Local Phone Menu

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

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

2 Startup

2.1 Prerequisites

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

- An Ethernet connection to a network.

> ⚠ 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.

- A OpenScape Business (with DLI) or OpenScape 4000 Communications System (with Integrated Phone Software Management, IPSM).
- Usage of Voice VLANs is recommended.
- An FTP Server for file transfer, e. g. firmware, configuration data, application software. Starting with V1 software upgrade can be started via WBM by browsing for image file through a directory.
- A Dynamic Host Configuration Protocol (DHCP) server (recommended).
- DLS (OpenScape Deployment Service) for advanced configuration and software deployment (recommended).

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

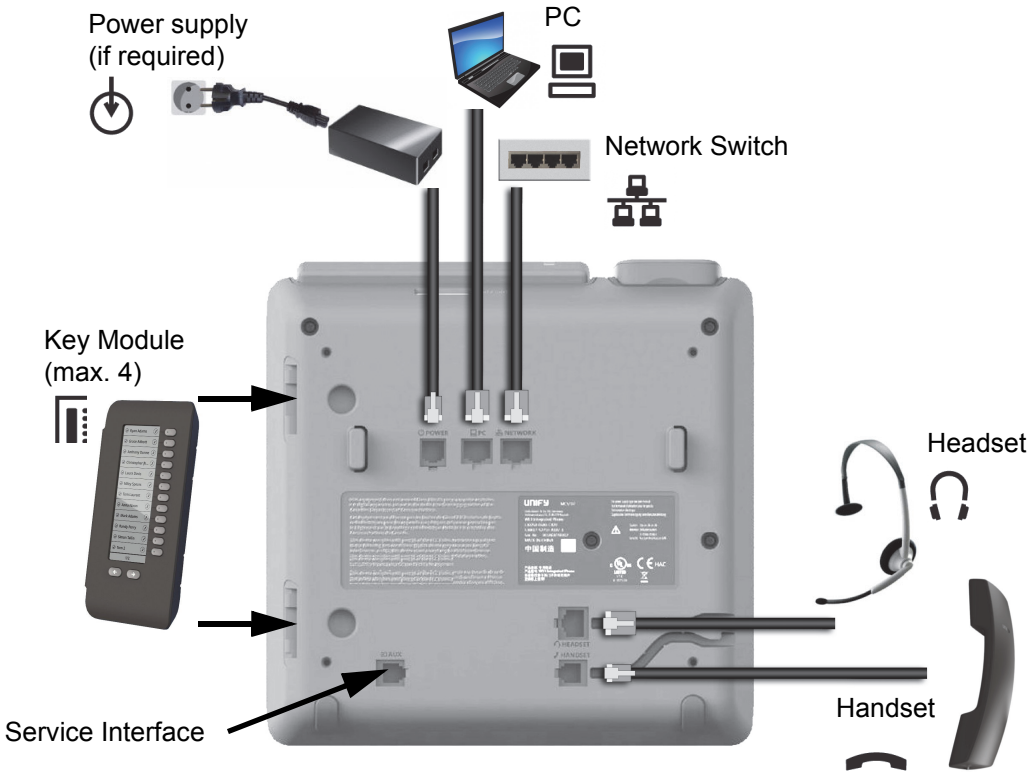
2.2 Assembling and Installing the Phone

2.2.1 Shipment

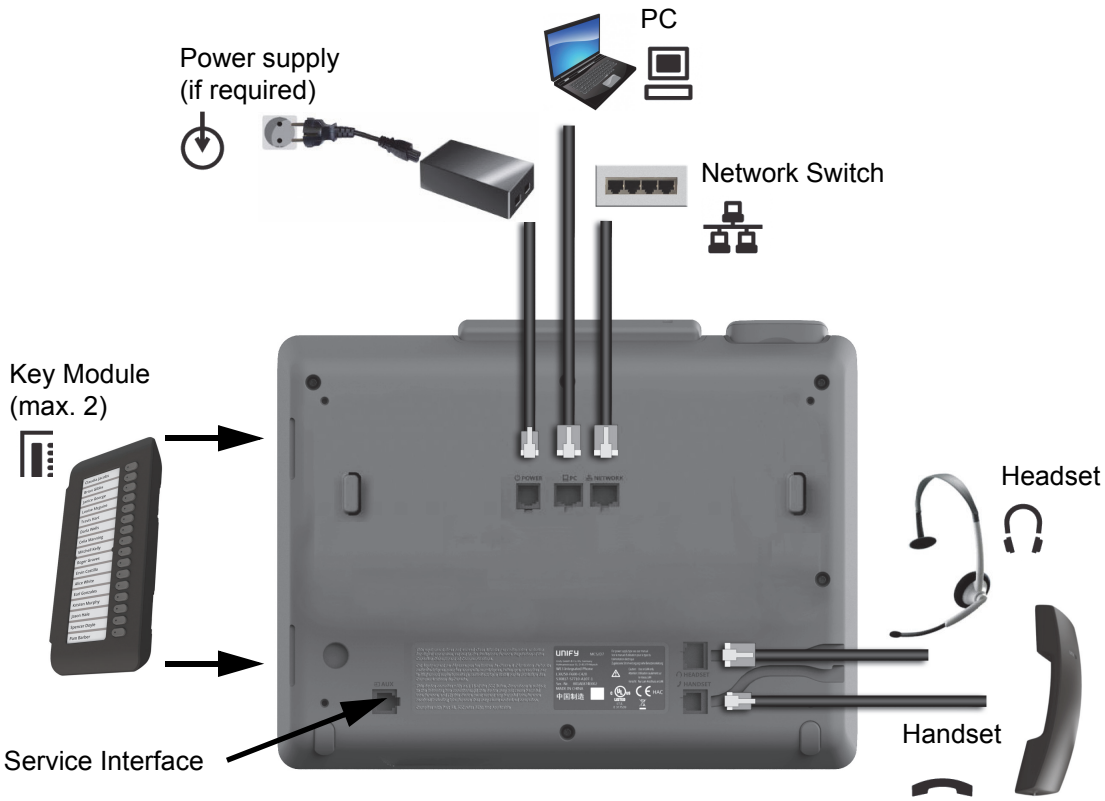
- Phone
- Handset
- Handset cable
- Document "Installation and Quick Reference Guide"

2.2.2 Connectors at the bottom side

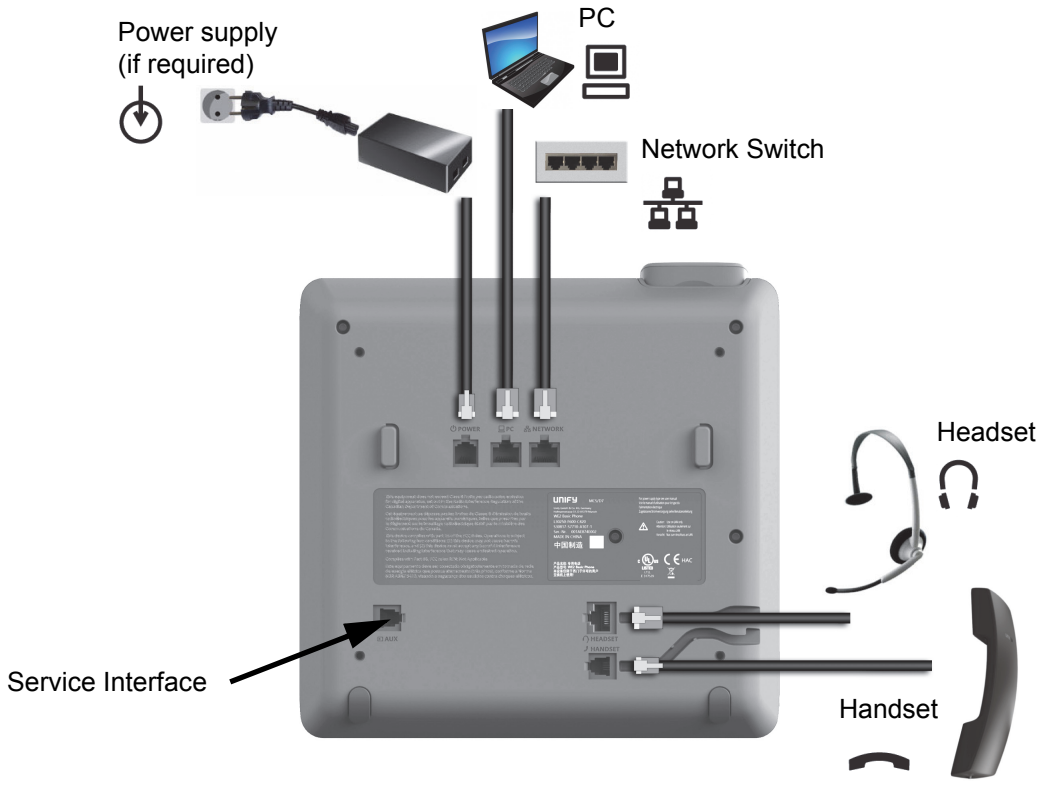
OpenScape Desk Phone CP600



OpenScape Desk Phone CP400



OpenScape Desk Phone CP200/CP205



2.2.3 Assembly

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

2.2.4 How to Connect the Phone

1. Plug the LAN cable into the connector at the bottom of the telephone and connect the cable to the LAN resp. switch. If PoE (Power over Ethernet) is to be used, the PSE (Power Sourcing Equipment) must meet the IEEE 802.3af specification.
   For details about the required power supply, see the following table:

Model	Power Consumption
OpenScape Desk Phone CP200/CP205	PoE (Power Class 1)
OpenScape Desk Phone CP400	PoE (Power Class 2)
OpenScape Desk Phone CP600[1]	PoE (Power Class 2)

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

2. If Power over Ethernet (PoE) is **NOT** supported or an OpenScape Desk Phone CP600 phone has more than one Key Module connected:
   Plug the power supply unit into the mains. Connect the plug-in power supply unit to the jack at the bottom of the phone.

Plug-in Power Supply	Order No.
Power Supply, power cable and plug (Type E+F) for EU	L30250-F600-C141
Power Supply, power cable and plug for Great Britain	L30250-F600-C142
Power Supply, power cable and plug for USA	L30250-F600-C143
Power Supply, power cable and plug for Switzerland	L30250-F600-C182
Power Supply, power cable and plug for Italy	L30250-F600-C183
Power Supply, power cable and plug for Australia	L30250-F600-C184
Power Supply, power cable and plug for South Africa	L30250-F600-C185
Power Supply without power cable	L30250-F600-C148

3. If applicable, connect the following optional jacks:
   - LAN connection to PC
   - Headset (accessory)

2.2.5 How to Better Use LAN Network Connections

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

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

2.2.6 Key Module

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

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

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

2.3 Quick Start

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

Alternatively, WBM, DLI or DLS (Deployment Service) administration tools 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.

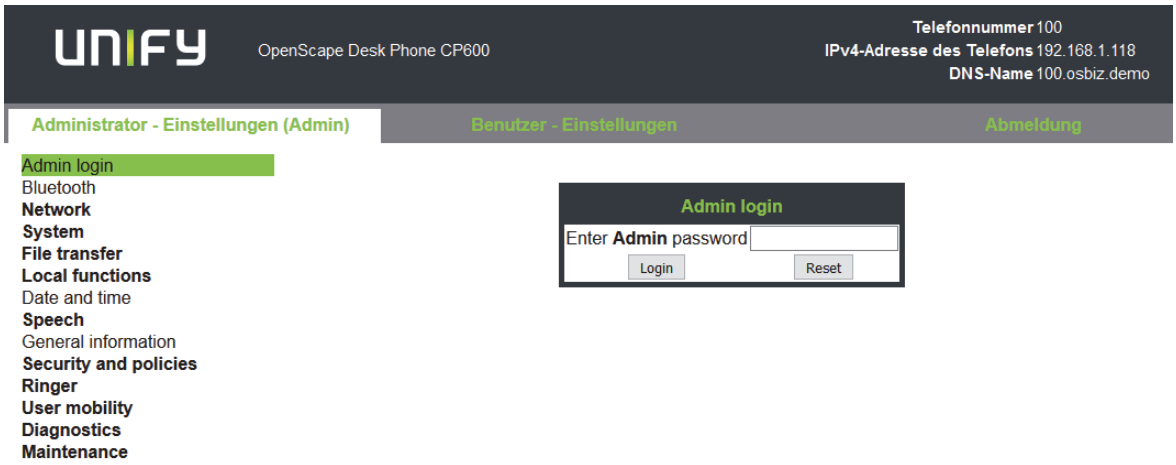
Any settings made by a DHCP server are not configurable by other configuration tools.

2.3.1 How to Access the Web Interface (WBM)

Prerequisites

- The phone´s IP address or URL is required for accessing the phone´s Web Interface via a web browser. By default, the phone will automatically search for a DHCP server on startup and try to obtain IP data and further configuration parameters from that central server.
- If no DHCP server is available in the IP network or if the DHCP parameter is disabled, the IP address, subnet mask and default gateway/route must be defined manually.
- To obtain the phone´s IP address, proceed as follows:

1. Access the local phone´s Admin menu as described in Section 2.3.2, "Access via Local Phone".
   - If DHCP is enabled (default): In the Admin menu, navigate to Network > IP configuration > IP address. The IP address is displayed.
   - If DHCP is disabled or if no DHCP server is available in the IP network, the IP address, Subnet Mask and Default Route/Gateway must be defined manually as described in How to Manually Configure the Phone´s IP address.
2. Open your web browser and enter the appropriate URL. Example: `https://192.168.1.15` or `https://myphone.phones`.
   For configuring the phone's DNS name, please refer to Section 3.3.6.2, "Terminal Hostname".
   If the browser displays a certificate notification, accept it. The start page of the web interface appears. In the upper right corner, the phone number, the phone's IP address, as well as the DNS name assigned to the phone are displayed. The left corner contains the user menu tree.



3. Click on the tab "Administrator Pages". In the dialog box, enter the admin password. The default password is 123456. It is highly recommended to change the password (see Section 3.13.1, “Password”) after your first login.

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

2.3.2 Access via Local Phone

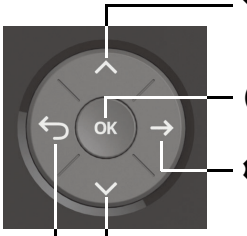
2.3.2.1 OpenScape Desk Phone CP20X

1. Press **1 3 0** simultaneously. You will be prompted to enter the administrator password.
2. Enter the administrator password (default password is **123456**). It is highly recommended to change the password (see Section 3.13.1, “Password”) after your first login.
3. Confirm with **OK** key.

2.3.2.2 OpenScape Desk Phone CP400/600

1. Access the Administration Menu

Press the ☰ or ⇆ key and use the **Up Arrow**, **Down Arrow** and **OK** keys consecutively to select the **Admin** menu.



- Scroll upwards
  Hold down: Jump to top of list
- Confirm input or perform action
- Navigate tab or move right
- Scroll downwards
  Hold down: Jump to bottom of list
- Cancel function, delete character left of cursor, navigate tab or go back one menu level

2. When the **Admin** menu is active, you will be prompted to enter the administrator password. The default admin password is "123456". It is highly recommended to change the password (see Section 3.13.1, “Password”) after your first login.

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

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

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

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

3. Navigate within the Administration Menu.

4. Select a parameter

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

5. Enter the parameter value

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

Key	Key Function during text input	Key function when held down
*▲	Enter special characters.	Ringer on/off when pressed short, ringer set to alerting with longpress.

Key	Key Function during text input	Key function when held down
# Abc 123	Toggle between lowercase characters, uppercase characters, and digits in the following order: (Abc) -> (abc) -> (123) -> (ABC) -> back to start.	Phonelock on/off.

With the OpenScape Desk Phone IP use the keypad for entering parameter values. Use the Navigation Keys or Navigation Block to navigate and execute administrative actions in the Administration Menu.

6. Save and exit

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

2.3.3 How to Set the Terminal Number

Prerequisites

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

1) Log on as administrator to the WBM by entering the access data for your phone.

2) In the Administrator menu (left column), select System > System Identity to open the "System Identity" dialog. Enter the terminal number, i. e. the HFA name / phone number.

2.3.4 Basic Network Configuration

For basic functionality, DHCP must provide the following parameters:

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

If no DHCP server is present, see Section 3.3.3, “IP Address - Manual Configuration” for IP address and subnet mask, and Section 3.3.4, “Default Route/Gateway” for the default route.

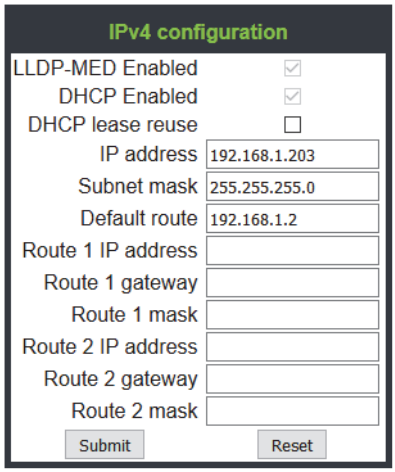
2.3.5 DHCP Resilience

Prerequisites

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

Step by Step

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



2.3.6 Date and Time / SNTP

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

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

The following DHCP options are required:

- SNTP IP Address (option #42 "NTP Servers"): IP Address or hostname of the SNTP server to be used by the phone.
- Time zone offset (option #2 "Time Offset"): Offset in seconds in relationship to the UTC time provided by the SNTP server. For manual configuration of date and time see 3.5.5 Date and Time.

2.3.7 Extended Network Configuration

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

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

For manual configuration of specific/static routing see Section 3.3.5, "Specific IP Routing".

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

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

For manual configuration of the DNS domain name see Section 3.3.6.1, "DNS Domain Name".

2.3.8 VLAN Discovery

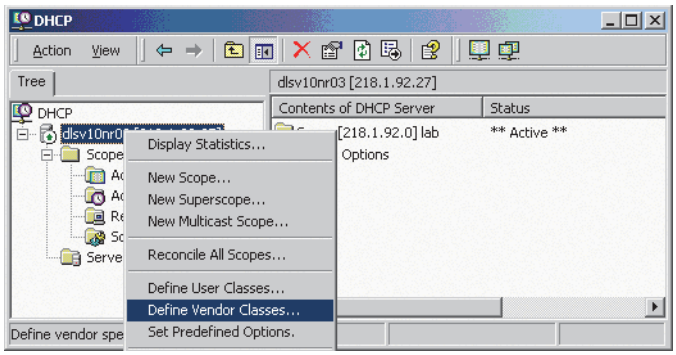
If the phone is to be located in a VLAN (Virtual LAN), a VLAN ID must be assigned. If the VLAN shall be provided by DHCP, **VLAN Discovery** must be set to "DHCP" (see Section 3.2.2, “VLAN”). The corresponding DHCP option is vendor-specific, thus a specific procedure is necessary.

2.3.8.1 Using a Vendor Class

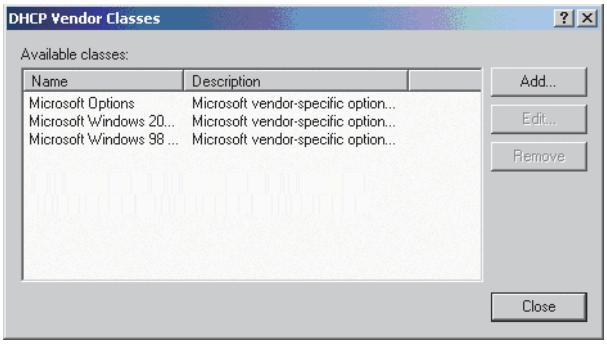
It is recommended to define a vendor class on the DHCP server, thus enabling server and phone to exchange vendor-specific data exclusively. The data is disclosed from other clients. The following steps are required for the configuration of the Windows DHCP server.

Setting up a new vendor class using the Windows DHCP Server

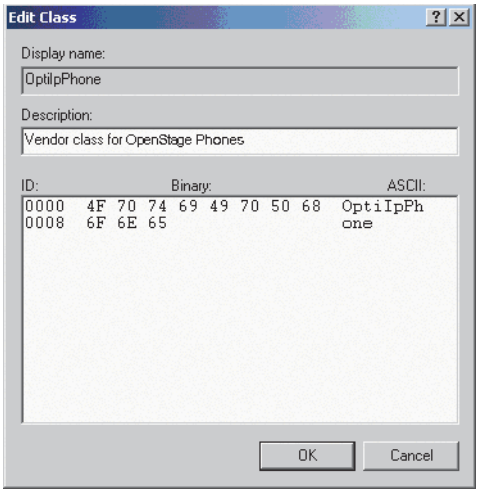
1. In the Windows Start menu, select **Start** > **Programs** > **Administrative Tools** > **DHCP**.
2. In the DHCP console menu, right-click the DHCP server in question and select **Define Vendor Classes...** in the context menu.



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



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



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

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

Add Options to the New Vendor Class

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

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

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

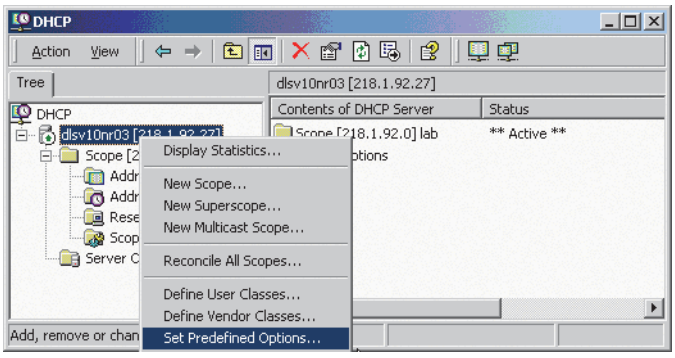
You can use the following command to configure the required option (without error message) so that it is also appears later in the DHCP console:

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

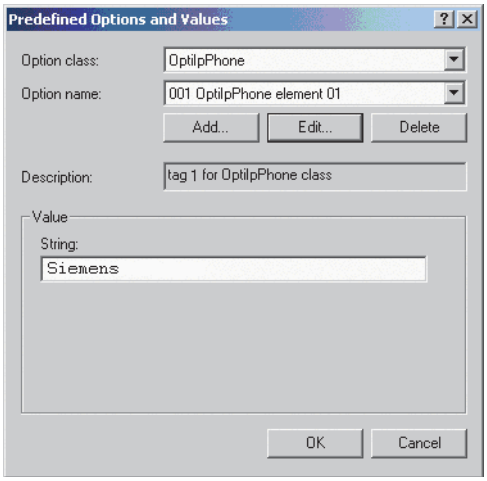
The value **SIEMENS** for optiPoint Element 1 can then be re-assigned over the DHCP console.

This error was corrected in Windows 2003 Server SP2.

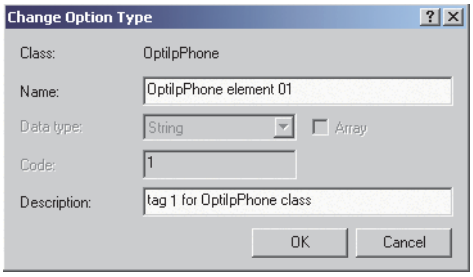
6. In the DHCP console menu, right-click the DHCP server in question and select Set Predefined Options from the context menu.



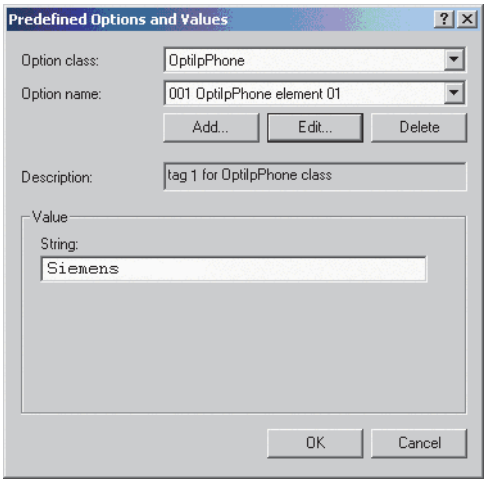
7. In the dialog, select the previously defined **OptiIpPhone** class and click on **Add...** to add a new option.



8. Enter the following data for the new option:
   1. First Pass: Option 1
   - Name: Free text, e. g. "OptiIpPhone element 01"
   - Data type: "String"
   - Code: "1"
   - Description: Free text.
   2. Second Pass: Option 2
   - Name: Free text, e. g. "OptiIpPhone element 02"
   - Data type: "Long"
   - Code: "2"
   - Description: Free text.



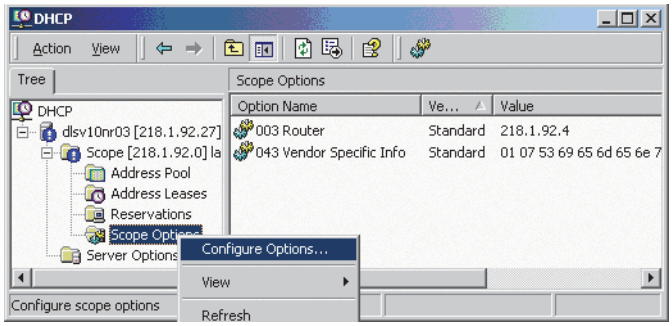
9. Enter the value for this option.
   1. First Pass: "Siemens"
   2. Second Pass: VLAN ID



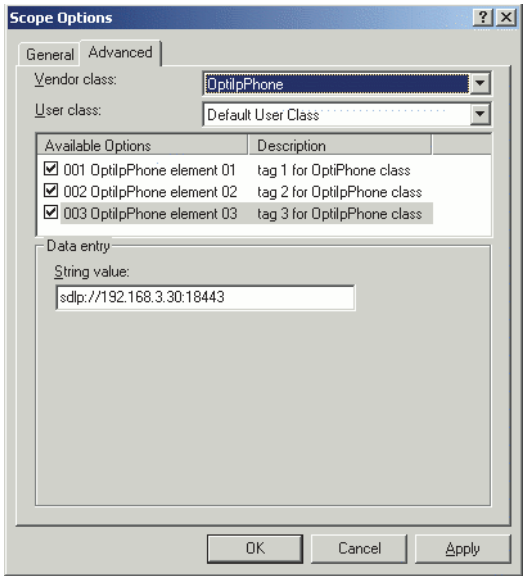
10. Press **OK**, repeat steps 7 to 9 for the second pass, and press **OK** again.

Defining the scope for the new vendor class

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



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



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

13. The DHCP console now shows the information that will be transmitted for the corresponding workpoints. Information from the **Standard** vendor is transmitted to all clients, whereas information from the **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 #2: VLAN ID
   #2  4  0 0  1  0
    02:04:00:00:00:0A;
   match if substring (option vendor-class-identifier, 0, 11) =
   "OptiIpPhone";
}
```

2.3.8.2 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

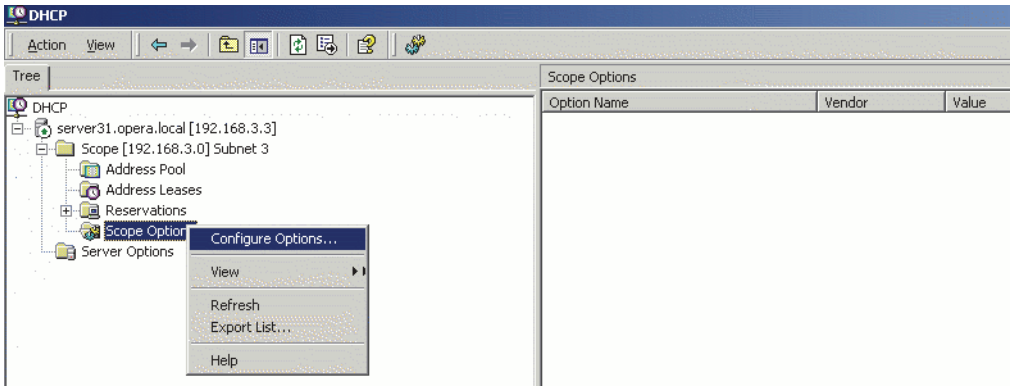
The following example shows a VLAN ID with the decimal value "10":

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

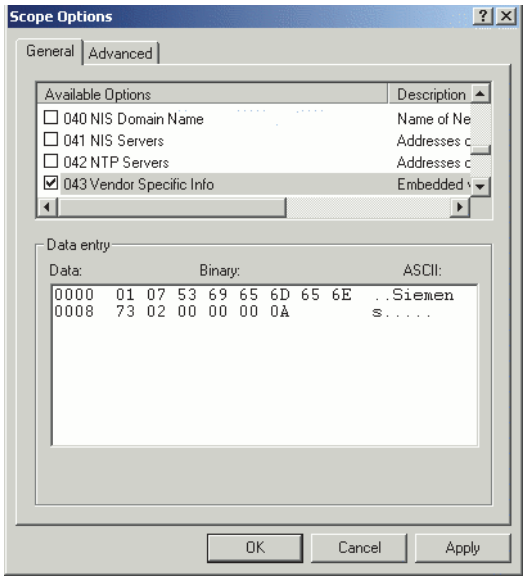
For manual configuration of the VLAN ID see Section 3.2.2.1, “Automatic VLAN discovery using LLDP-MED”.

Setup using the Windows DHCP Server

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



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



2.3.9 DLS Server Address

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

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

For manual configuration of the DLS server address see Section 3.3.7, “Configuration & Update Service (DLS)”.

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

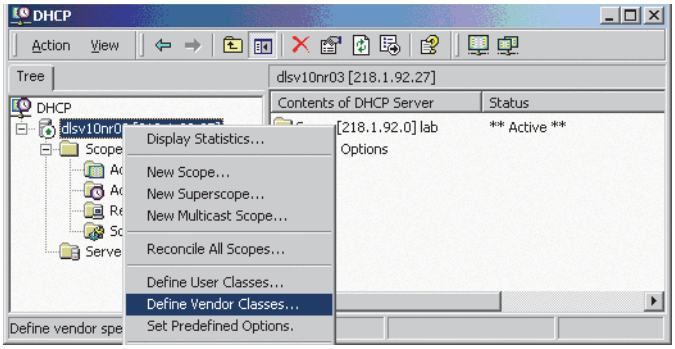
2.3.9.1 Using Vendor Class

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

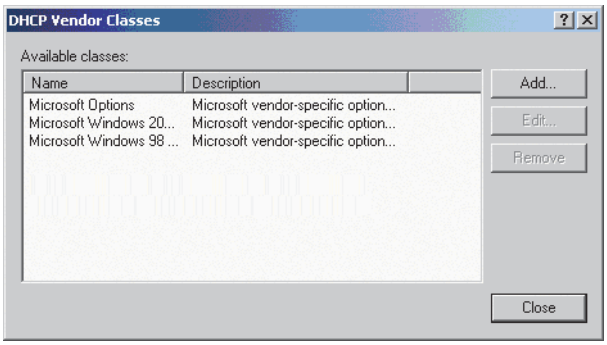
The following steps are required for the configuration of the Windows DHCP server.

Setting up a new vendor class using the Windows DHCP Server

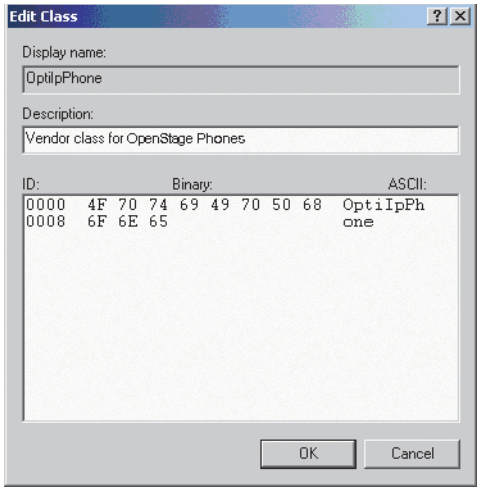
1. In the Windows Start menu, select **Start** > **Programs** > **Administrative Tools** > **DHCP**.
2. In the DHCP console menu, right-click the DHCP server in question and select **Define Vendor Classes...** in the context menu.



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



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



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

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

Add Options to the New Vendor Class

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

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

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

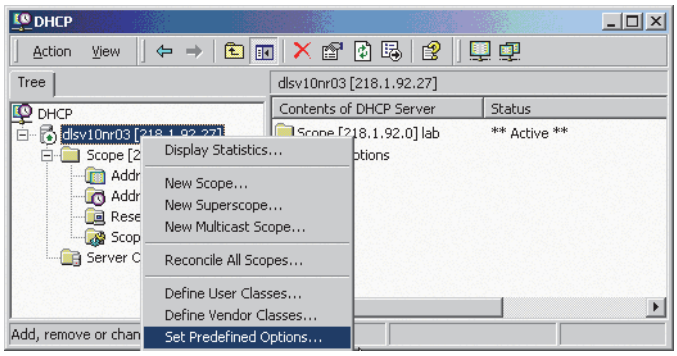
You can use the following command to configure the required option (without error message) so that it is also appears later in the DHCP console:

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

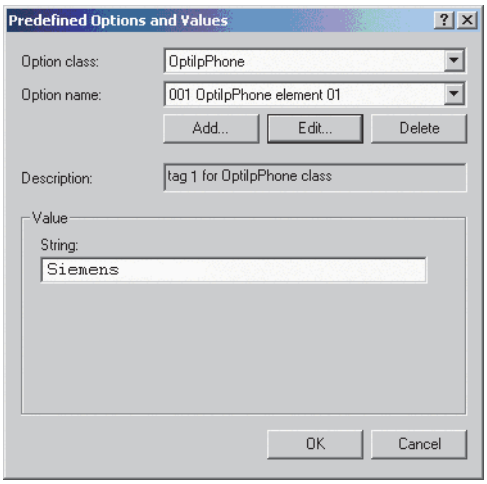
The value **SIEMENS** for optiPoint Element 1 can then be re-assigned over the DHCP console.

This error was corrected in Windows 2003 Server SP2.

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



7. In the dialog, select the previously defined **OptiIpPhone** class and click on **Add...** to add a new option.



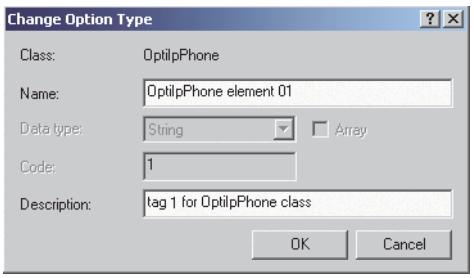
8. Enter the following data for the new option:

   1. First Pass: Option 1

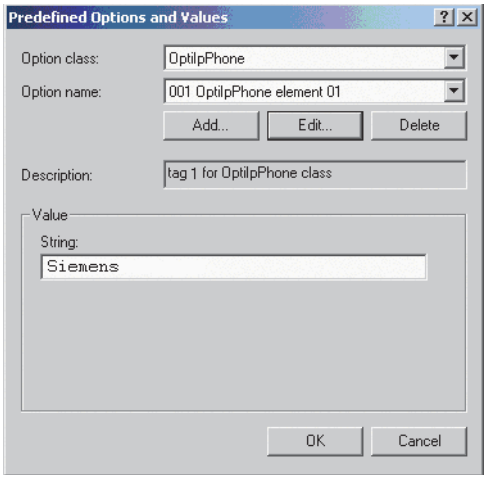
   - Name: Free text, e. g. "OptiIpPhone element 01"
   - Data type: "String"
   - Code: "1"
   - Description: Free text.

   2. Second Pass: Option 3

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



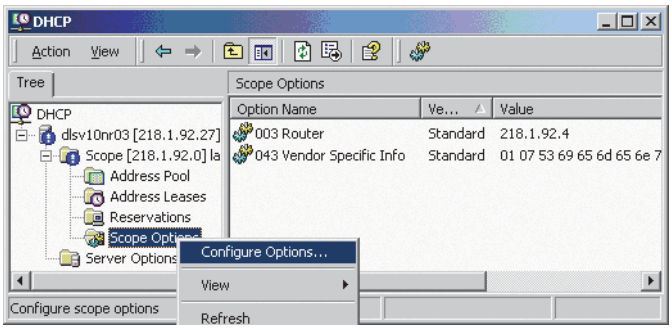
9. Enter the value for this option.
   1. First Pass: "Siemens"
   2. Second Pass: DLS address
      The DLS address has the following format:
      <PROTOCOL>:://<IP ADDRESS OF DLS SERVER>:<PORT NUMBER>
      Example: sdlp://192.168.3.30:18443



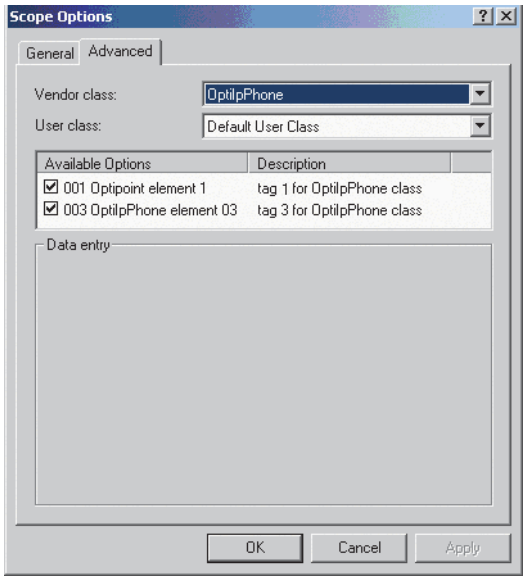
10. Press **OK**, repeat steps 7 to 9 for the second pass, and press **OK** again.

Defining the scope for the new vendor class

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



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



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

13. The DHCP console now shows the information that will be transmitted for the corresponding workpoints. Information from the **Standard** vendor is transmitted to all clients, whereas information from the **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";
}
```

2.3.9.2 Using Option #43 "Vendor Specific"

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

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

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

- **Tag 004: DLS hostname**

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

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

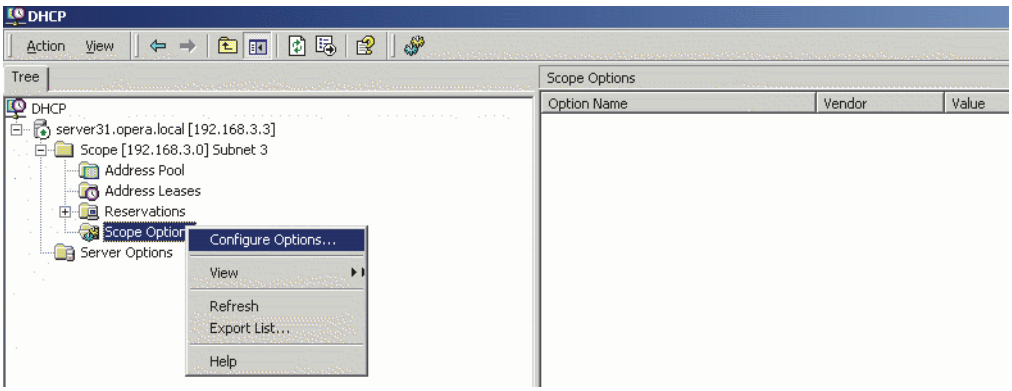
Code	**Length**	**Vendor name**						
1	7	S	i	e	m	e	n	s
01	07	53	69	65	6D	65	6E	73

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

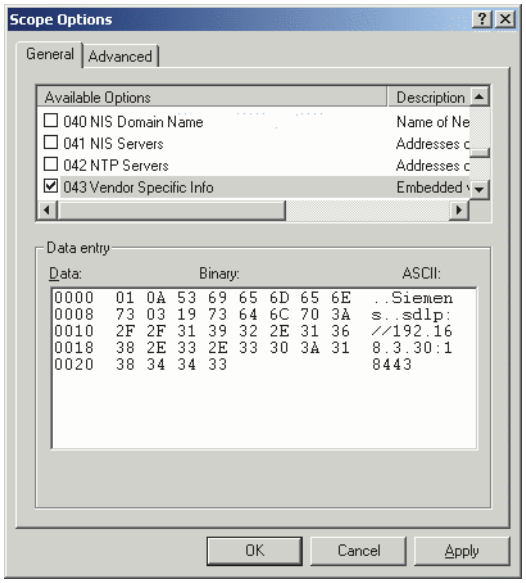
Code	**Length**	**DLS IP address**																						
3	25	s	d	l	p	:	/	/	1	9	2	.	1	6	8	.	2	.	1	9	:	1	8	4	4	3
03	19	73	64	6C	70	3A	2F	2F	31	39	32	2E	31	36	38	2E	32	2E	31	39	3A	31	38	34	34	33

Setup using the Windows DHCP Server

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



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



2.3.10 HFA Gateway Settings

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

2.3.11 Using the Web Interface (WBM)

1. Log in to the Administrator Pages of the WBM. For details about accessing the WBM, see Section 2.3.1, “How to Access the Web Interface (WBM)”.
2. In the menu at the lefthand side, go to **System** > **Gateway**.
3. Enter the IP address of the OpenScape Business or OpenScape 4000 Communication System in the **IP address** field.
4. In the **Subscriber number** field, enter the internal extension number of the phone. It can be 1 to 24 characters long.
5. Enter the subscriber password in the **Password** field.

2.3.12 Using the Local Menu

Take the following steps to configure the access to an HFA gateway (for further information see Section 2.3.2, “Access via Local Phone”):

1. In the administration menu, go to **System** > **Gateway**. For further instructions on entering data using the Local menu see Section 2.3.2, “Access via Local Phone”. The path is as follows:

   ```
   --- Administration
       --- System
           --- Gateway
               --- System type
               --- IP address
               --- Gateway ID
               --- Subscriber number
               --- Password
   ```

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

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

3 Administration

This chapter describes the configuration of every parameter available on the OpenScape Desk Phone CP phones. Please refer to Section 2.3.1, “How to Access the Web Interface (WBM)”.

3.1 Bluetooth Interface

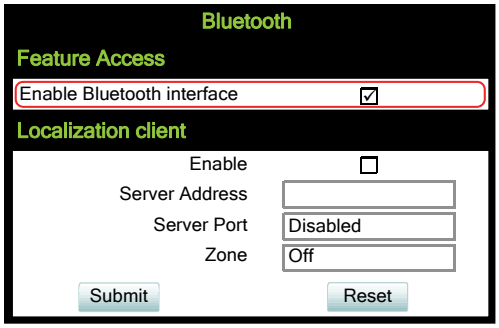
Bluetooth is available only on Open Scape Desk Phone CP600.

3.1.1 Feature Access

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

Administration via WBM

Bluetooth



Administration via Local Phone

| --- Bluetooth

3.2 LAN Settings

3.2.1 LAN Port Settings

The OpenScape Desk Phone CP200/205/400/600 phone provides an integrated switch which connects the LAN, the phone itself and a PC port. By default, the switch will auto negotiate transfer rate (10/100/1000 Mb/s autosensing, configurable, Gigabit not available on OpenScape Desk Phone CP200) and duplex method (full or half duplex) with whatever equipment is connected. Optionally, the required transfer rate and duplex mode can be specified manually using the **LAN Port Speed** parameter.

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

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

Do not use this connection for further OpenScape Desk Phone CP or OpenStage phones!

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

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

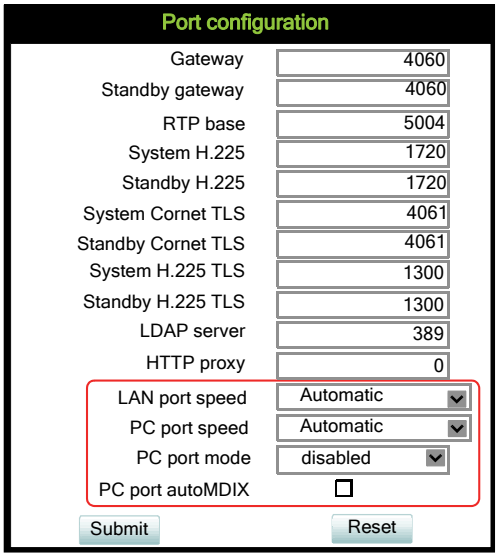
Data required

- **LAN port speed**: Settings for the ethernet port connected to a LAN switch.
  Value range: "Automatic," "10 Mbps half duplex", "10 Mbps full duplex", "100 Mbps half duplex", "100 Mbps full duplex", "1 Gbps full duplex" (OpenScape Desk Phone CP205, OpenScape Desk Phone CP400 and OpenScape Desk Phone CP600 only) .
  Default: "Automatic"

- **PC port speed** / **PC port type**: Settings for the ethernet port connected to a PC.
  Value range: "Automatic," "10 Mbps half duplex", "10 Mbps full duplex", "100 Mbps half duplex", "100 Mbps full duplex", "1 Gbps full duplex" (OpenScape Desk Phone CP205, OpenScape Desk Phone CP400 and OpenScape Desk Phone CP600 only).
  Default: "Automatic"
- **PC port mode** / **PC port status**: Controls the PC port.
  Value range: "disabled", "enabled", "mirror".
  Default: "disabled"
- **PC port autoMDIX**: Switches between MDI and MDI-X automatically.
  Value range: "On", "Off"
  Default: "Off"

Administration via WBM

Network > Port configuration



Administration via Local Phone

```
└--- Admin
    └--- Network
        └--- Port Configuration
            └--- Number
                |--- LAN port speed
                |--- PC port status
                |--- PC port speed
                └--- PC port autoMDIX
```

3.2.2 VLAN

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

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

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

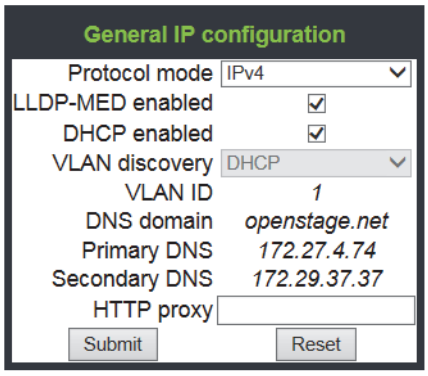
3.2.2.1 Automatic VLAN discovery using LLDP-MED

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

Administration via WBM

Network > General IP configuration

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



Administration via Local Phone

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

```
└--- Administration
    └--- Network
        └--- General IP configuration
            |--- Protocol Mode
            |--- LLDP-MED enabled
            |--- DHCP enabled
            |--- VLAN discovery
            |--- VLAN ID
            |--- DNS domain
            |--- Primary DNS
            |--- Secondary DNS
            |--- HTTP proxy
```

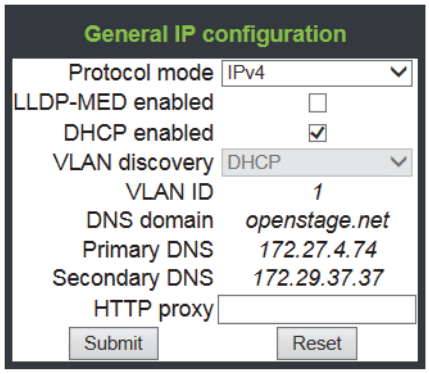
3.2.2.2 Automatic VLAN discovery using DHCP

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

Administration via WBM

Network > General IP configuration

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



Administration via Local Phone

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

```
└ --- Administration
    └ --- Network
        └ --- General IP configuration
            |--- Protocol Mode
            |--- LLDP-MED enabled
            |--- DHCP enabled
            |--- VLAN discovery
            |--- VLAN ID
            |--- DNS domain
            |--- Primary DNS
            |--- Secondary DNS
            |--- HTTP proxy
```

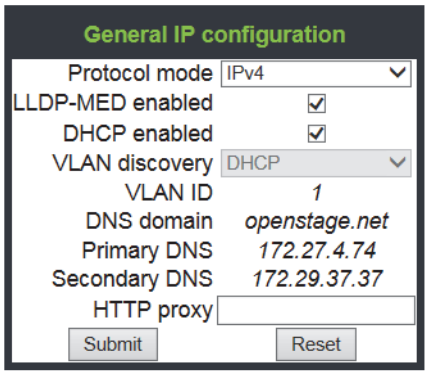
3.2.2.3 Manual configuration of a VLAN ID

To configure layer 2 VLAN manually, first make sure that VLAN discovery is set to "Manual" (see Section 3.2.2.1, “Automatic VLAN discovery using LLDP-MED”). Then, the phone must be provided with a VLAN ID between 1 and 4095. If you misconfigure a phone to an incorrect VLAN, the phone will possibly not connect to the network. In DHCP mode it will behave as though the DHCP server cannot be found, in fixed IP mode no server connections will be possible.

Administration via WBM

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

Network > General IP configuration



Administration via Local Phone

- Administration
  - Network
    - General IP configuration
      - Protocol Mode
      - LLDP-MED enabled
      - DHCP enabled
      - VLAN discovery
      - VLAN ID
      - DNS domain
      - Primary DNS
      - Secondary DNS
      - HTTP proxy

3.3 IP Network Parameters

3.3.1 Quality of Service (QoS)

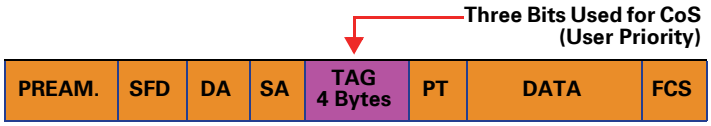
The QoS technology based on layer 2 and the two QoS technologies Diffserv and TOS/IP Precedence based on layer 3 are allowing the VoIP application to request and receive predictable service levels in terms of data throughput capacity (bandwidth), latency variations (jitter), and delay.

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

3.3.1.1 Layer 2 / 802.1p

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

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

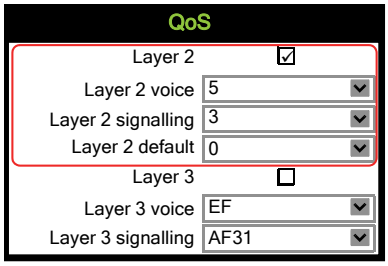


Data required

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

Administration via WBM

Network > QoS



Administration via Local Phone

```
└--- Admin
    └--- Network
        └--- QoS
            └--- Service
                ├--- Layer 2
                ├--- Layer 2 voice
                ├--- Layer 2 signalling
                └--- Layer 2 default
```

3.3.1.2 Layer 3 / Diffserv

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

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

1. Default
   Any traffic that does not meet the requirements of any of the other defined classes is placed in the default per-hop behaviour group. Typically, the forwarding has best-effort forwarding characteristics. The DSCP (Diffserv Codepoint) value for Default is "0 0 0 0 0 0".
2. Expedited Forwarding (EF referred to RFC 3246)
   Expedited Forwarding is used for voice (RTP streams) by default. It effectively creates a special low-latency path in the network. The DSCP (Diffserv Codepoint) value for EF is "1 0 1 1 1 0".
3. Assured Forwarding (AF referred to RFC 2597)
   Assured forwarding is used for signaling messages by default (AF31). It is less stringent than EF in a multiple dropping system. The AF values are containing two digits X and Y (AFXY), where X is describing the priority class and Y the drop level.
   Four classes X are reserved for AFXY: AF1Y (low priority), AF2Y, AF3Y and AF4Y (high priority).

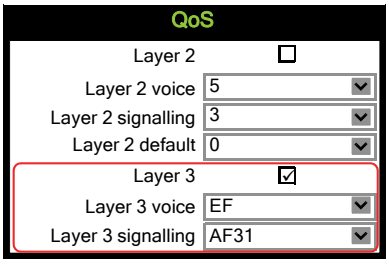
Three drop levels Y are reserved for AFXY: AFX1 (low drop probability), AFX2 and AFX3 (High drop probability). In the case of low drop level, packets are buffered over an extended period in the case of high drop level, packets are promptly rejected if they cannot be forwarded.

Data required

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

Administration via WBM

Network > QoS



Administration via Local Phone

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

3.3.2 Use DHCP

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

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

The change will only have effect if you restart the phone.
The phone is able to maintain its IP connection even in case of DHCP server failure. For further information, please refer to DHCP Resilience.

The following parameters can be obtained by DHCP:

Basic Configuration

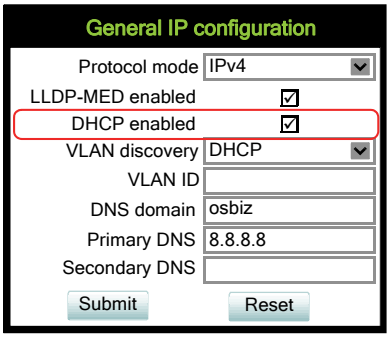
- IP Address
- Subnet Mask

Optional Configuration

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

Administration via WBM

Network > General IP configuration



Administration via Local Phone

- Admin
  - Network
    - General IP Configuration
      - **DHCP enabled**

3.3.3 IP Address - Manual Configuration

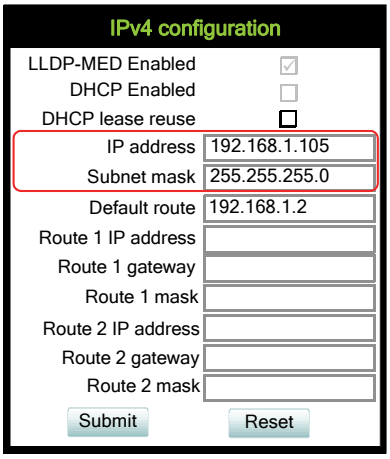
If not provided by DHCP dynamically, you must specify the phone's IP address and subnet mask manually.

Data required

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

Administration via WBM

Network > IPv4 configuration



Administration via Local Phone

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

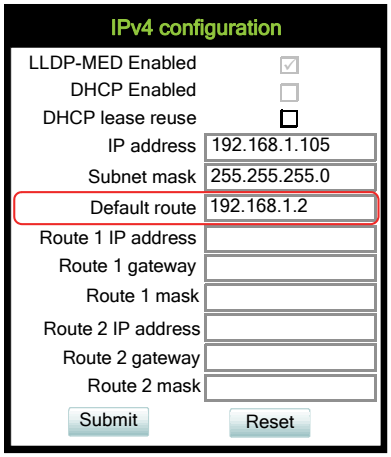
3.3.4 Default Route/Gateway

If not provided by DHCP dynamically (see Section 3.3.2, “Use DHCP”), enter the IP address of the router that links your IP network to other networks. If the value was assigned by DHCP, it can only be read.

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

Administration via WBM

Network > IPv4 configuration



Administration via Local Phone

└ --- Admin
  └ --- Network
    └ --- IPv4 Configuration
      └ --- **Default route**

3.3.5 Specific IP Routing

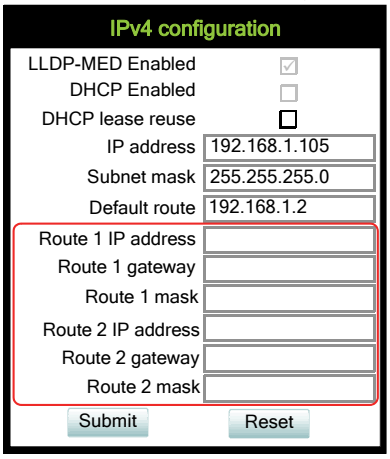
To have constant access to network subscribers of other domains, you can enter a total of two more network destinations, in addition to the default route/gateway. This is useful if the LAN has more than one router or if the LAN is divided into subnets.

Data required

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

Administration via WBM

Network > IPv4 configuration



Administration via Local Phone

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

3.3.6 DNS

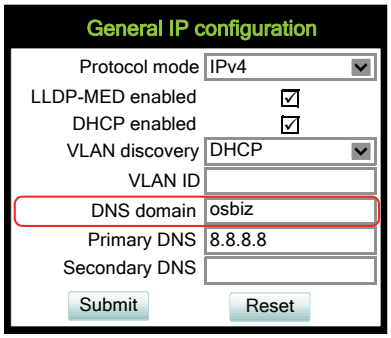
The main task of the domain name system (DNS) is to translate domain names to IP addresses. For some features and functions of the OpenScape Desk Phone CP phone, it is necessary to configure the DNS domain the phone belongs to, as well as the name servers needed for DNS resolving.

3.3.6.1 DNS Domain Name

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

Administration via WBM

Network > General IP configuration



Administration via Local Phone

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

3.3.6.2 Terminal Hostname

The phone's hostname can be customised.

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

The corresponding DNS domain is configured in Network > IP configuration > DNS domain (see Section 3.3.6.1, "DNS Domain Name").

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

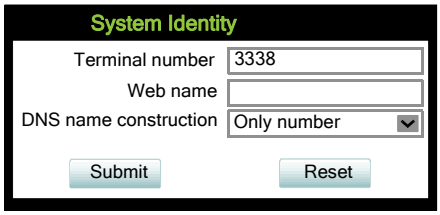
It is recommended to inform the user about the DNS name of the phone. The complete WBM address can be found under User menu > Network information > Web address.

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

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

Administration via WBM

System > System Identity



Administration via Local Phone

```
| --- Administration
        | --- Identity
              |--- Web name
              | --- DNS hostname
```

3.3.7 Configuration & Update Service (DLS)

The additional WBM and DLI are alternative administration tools. DLI uses the same technical inferface like DLS, but with less functionality.

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

DLS address, i.e. the IP address or hostname of the DLS server, and **Default mode port**, i.e. the port on which the DLS server is listening, are required to enable proper communication between phone and DLS. The **Contact gap** parameter controls a security function. It specifies a minimum time interval that must elapse between individual HTTP requests from the phone which are responding to a ContactMe request from the DLS. Any requests coming within that time will be ignored. The purpose is to prevent DoS (Denial of Service) attacks on the phone. Set **Revert to default security** to disable mutual authentication and return to DEFAULT mode. SECURE mode related settings are reset and certificates are removed.

The **Mode** determines whether the communication between the phone and the DLS is secure. A secure connection is established by exchanging credentials between the DLS and the phone for mutual authentication. After this, the communication is encrypted, and a different port is used.

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

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.

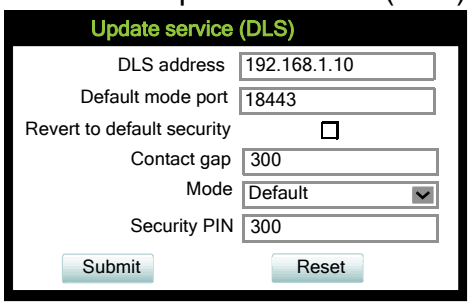
A Security PIN can be provided which is used for decrypting data provided by the DLS during bootstrap. For further information, please refer to the DLS documentation.

Data required

- **DLS address**: IP address or hostname of the server on which the Deployment Service is running.
- **Default mode port**: Port on which the DLS Deployment Service is listening.
  Default: 18443.
- **Revert to default security**: When set, security mode will be set to default. When using local phone administration, this will be set by selection option 'Default security' after pressing Save&exit.
- **Contact gap**: Minimum time interval in seconds that must elapse between responses to a ContactMe request from the DLS, in order to prevent DoS attacks.
  Default: 300.
- **Mode**: Determines whether the communication between the phone and the DLS is secure.
  Value range: "Default", "Secure".
  Default: "Default".
- **Security PIN**: Used for enhanced security.

Administration via WBM

Network > Update Service (DLS)



Administration via Local Phone

```
└ --- Admin
    └ --- Network
        └ --- Update service (DLS)
            |--- DLS address
            |--- Default mode port
            |--- Revert to default security
            |--- Contact gap
            |--- Mode
            └--- Security PIN
```

3.3.8 SNMP

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

OpenScape Desk Phone CP phones support SNMPv1.

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

Standard SNMP traps

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

- **coldStart**: sent if the phone does a full restart.
- **warmStart**: sent if only the phone software is restarted.
- **linkUp**: sent when IP connectivity is restored.

QoS Related traps

These traps are designed specifically for receipt and interpretation by the QDC collection system. The traps are common to SIP phones, HFA phones, Gateways, etc.

Traps specific to OpenScape Desk Phone CP 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.

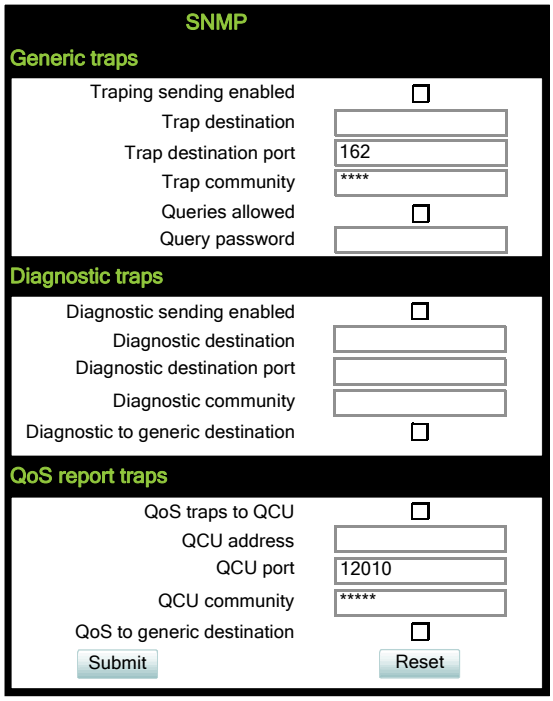
Data required

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

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

Administration via WBM

System > SNMP



Administration via Local Phone

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

3.4 OpenScape Service Menu

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

Administration via Local Phone

└--- Service Menu

3.5 System Settings

3.5.1 System Identity

3.5.2 HFA Gateway Settings

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

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

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

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

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

Data required:

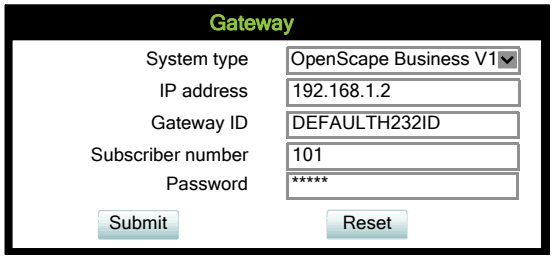
- **IP address**: IP address of the communication platform resp. HFA server.
- **Gateway ID**: The HFA server's port for signaling.
  Default: "4060".
- **Subscriber number**: The phone's extension.
- **Password**: Password for logging on to the HFA server.

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

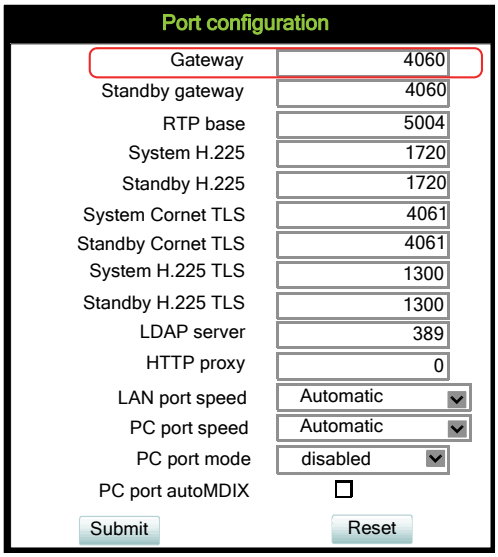
The **System type** is provided by the system the phone is connected to and therefore read-only.

Administration via WBM

System > Gateway



Network > Port configuration



Administration via Local Phone

- Admin
  - System
    - Gateway
      - **System type**
      - **IP address**
      - **Gateway ID**
      - **Subscriber number**
      - **Password**

- Admin
  - Network
    - Port configuration
      - **Gateway**

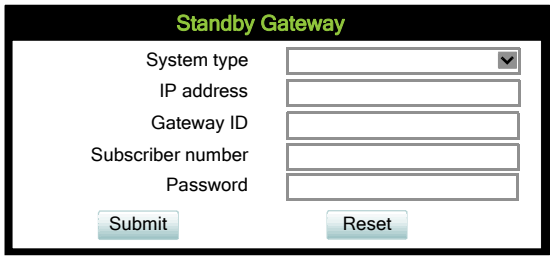
3.5.3 HFA Emergency Gateway Settings

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

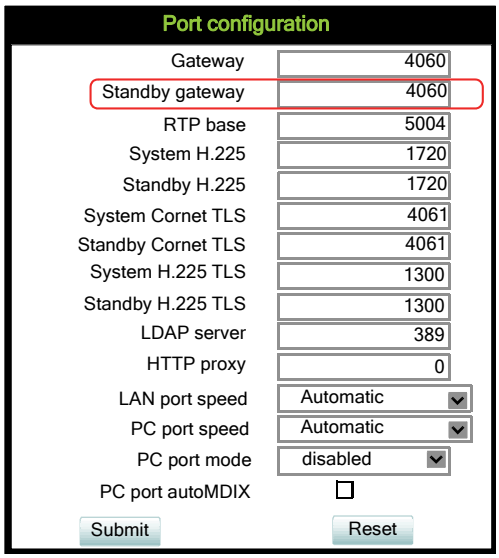
The settings are analog to those for the main system (see Section 3.5.2, “HFA Gateway Settings”).

Administration via WBM

System > Standby gateway



Network > Port configuration



Administration via Local Phone

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

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

3.5.4 Server and Standby Server ports

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

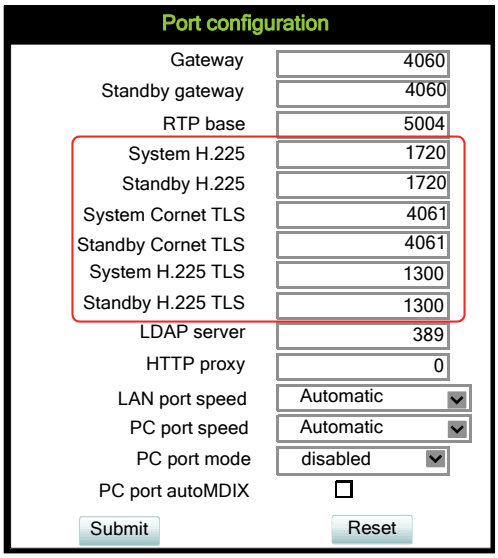
H.225.0 port determines the port used for non-secure H.225 signaling.
Default: 1720.

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

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

Administration via WBM

Network > Port configuration



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**

3.5.5 Redundancy

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

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

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

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

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

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

- **Timeout Standby**: Timeout between two "Retry count standby". The default is 30.
- **Timeout main**: Timeout between two "Retry count main" The default is 30.
- **TC test retry**: TC_Test retry determines the count of how many successfull TC_Tests the Main system need to answer before the phone switches back, if Auto switchback is enabled. The default is 3.
- **TC Test Expiry**: Determines how long the Previous connection needs to timeout to actually trigger any further SRSR activities.

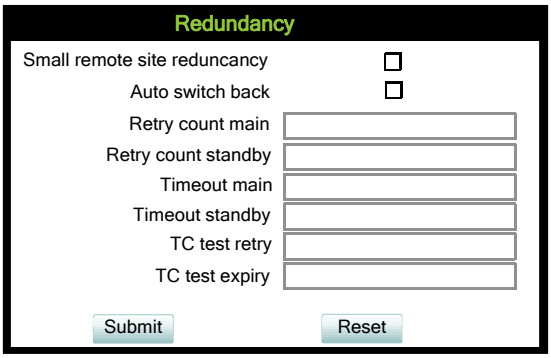
  How much time to wait from one unsuccessfull Retry count main sequence until the next happens and in which interval the phone will send itself a TC_Test message (in idle mode). The default is 30.

  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 timeing values the SRSR need to be deactivated and re-activated again to take effect!

Administration via WBM

System > Redundancy



Administration via Local Phone

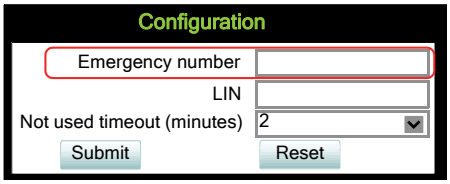
```
└ --- Admin
     └ --- System
          └ --- Redundancy
               |--- Small remote site
               |--- Auto switch back
               |--- Retry count main
               |--- Timeout main
               |--- Retry count stdby
               └ --- Timeout standby
```

3.5.6 Emergency number

E.911 emergency number. This number establishes a connection to the PSAP (Publiy Safety Answering Point). If a user dials this number, and an appropriate LIN (see Section 3.5.7, “LIN”) is configured, the user’s location is communicated to the PSAP. In the USA, the number is 911.

Administration via WBM

System > Features > Configuration



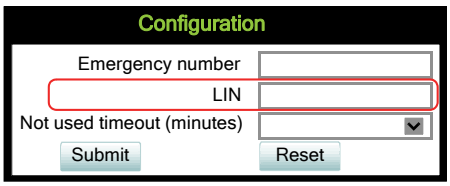
Administration via Local Phone

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

3.5.7 LIN

The **L**ocation **I**dentification **N**umber is a number code which provides detailed geographic information about the phone, including e. g. the office room. On issuing an emergency call using the E.911 emergency number (see Section 3.5.6, “Emergency number”), 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



Administration via Local Phone

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

3.5.8 Not Used Timeout

This is available only on OpenScape Desk Phone CP400/600 phones.

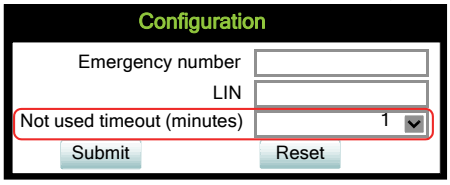
The timeout for the local user and admin menu is configurable. When the time interval is over, the menu is closed and the administrator/user is logged out.

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

The timeout ranges from 1 to 5 five minutes. The default value is 2.

Administration via WBM

System > Features > Configuration



Administration via Local Phone

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

3.5.9 Energy Saving

3.5.9.1 Energy Efficient Ethernet (OpenScape Desk Phone CP205/CP400/600 only)

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

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

3.5.10 Date and Time

To ensure that HFA security operates properly, the phone must obtain the correct date and time before logging on to the system. For this purpose, the phone must use the same SNTP server that is used by the system/PBX. If the DHCP server in your network provides the IP address of the SNTP server, no manual configuration is necessary. If not, you have to set the **SNTP IP address** parameter manually.

The date and time to be displayed can be obtained either from the SNTP server or from the system/PBX. To select SNTP-based date and time, set the **Time source** parameter to "SNTP". The default value is "System".

For correct display of the current time, the **Timezone offset** must be set appropriately. This is the time offset from UTC (Coordinated Universal Time). 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 timezones, 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 daylight saving, the administrator can choose whether daylight saving time is activated manually or automatically. If **Daylight saving** is enabled, and **Auto time change** is disabled, daylight saving time (DST) is in effect immediately. If **Auto time change** is enabled, daylight saving is controlled by the **DST zone** parameter. This selects the daylight saving timezone which is characterized by the start and end date for daylight saving time.

The **Difference (minutes)** provides the time difference for daylight saving time in minutes. This parameter is required also when **Auto time change** is enabled. In Germany, for instance, as in most countries, this is +60.

The **Current DISPLAY Time** is the date and time according to the timezone and daylight saving settings; this date and time is presented to the user. The **Current UTC Time** is the UTC time used by the phone and the system internally.

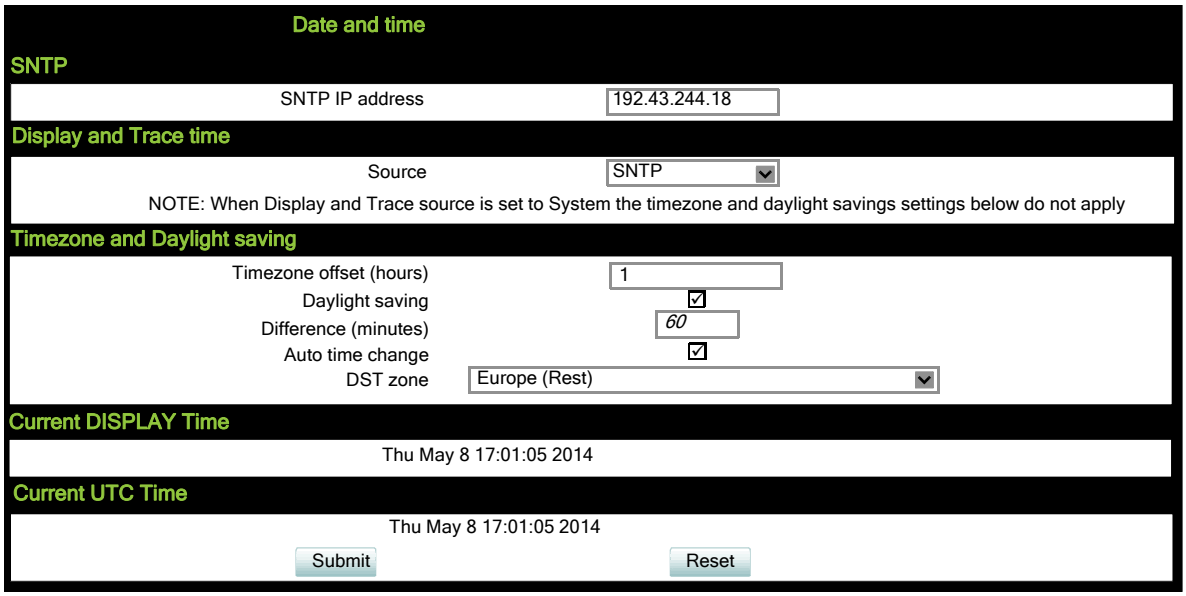
3.5.10.1 SNTP is Available, but no Automatic Configuration by DHCP Server

Data required

- **SNTP IP address**: IP address or hostname of the SNTP server.
- **Timezone offset (hours)**: Shift in hours corresponding to UTC.
- **Daylight saving**: Enables or disables daylight saving time in conjunction with **Auto time change**.
  Value range: "Yes", "No".
- **Difference (minutes)**: Time difference when daylight saving time is in effect.
- **Auto time change** / **Auto DST**: Enables or disables automatic control of daylight saving time according to the **DST zone**.
  Value range: "Yes", "No".
- **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".

Administration via WBM

Date and Time



Administration via Local Phone

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

3.5.11 Security

3.5.11.1 System

OpenScape Desk Phone CP phones support the following security option:

- PKI-based SPE (Signaling and Payload Encryption)

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

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

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 Section 3.13.2.2, “Authentication Policy”.

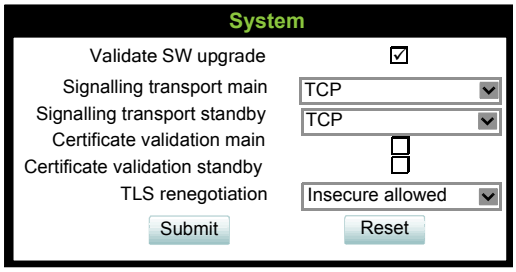
For further information on deploying SPE, please refer to the manual of the OpenScape system in use, and to the Deployment Service Administration manual.

Data required

- **Validate SW upgrade:** validates if the uploaded Phone software is compatible with the phone.
- **Signalling transport main**: Protocol to use for signalling when the main gateway is in use.
  Value range: "TCP", "TLS".
- **Signalling transport standby**: Protocol to use for signalling when the standby gateway is in use.
  Value range: "TCP", "TLS".
- **Certificate validation main**: Check the phone certificate against the gateway certificate when the main gateway is in use (read only).
  Value range: true, false.
- **Certificate validation standby**: Check the phone certificate against the gateway certificate when the main gateway is in use (read only).
  Value range: true, false.
- **TLS renegotiation**: Check whether Server accepts TLS renegotiation.
  Value range:
  Insecure allowed: Server without TLS renegotiation are accepted
  Secure (RFC5746): Only server with TLS renegotiation are allowed

Administration via WBM

System > Security > System



Administration via Local Phone

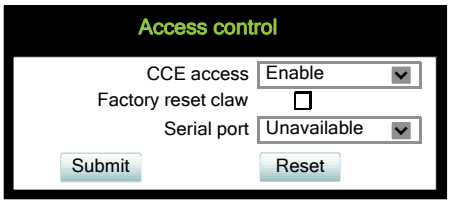
- Administration
  - System
    - Security
      - System
        - **Signalling main**
        - **Signalling stdby**
        - **Certificate main**
        - **Certificate stdby**
        - **TLS renegotiation**

3.5.11.2 Access control

The CCE access parameter controls TCP and UDP access for the CCE (CommsChannel Extender). This affects the operation of the OpenStage Manager, local CTI access, and HPT access. When Disable is selected, both TCP and UDP are disabled. With Enable, there are no restrictions.
With **Factory reset claw,** the 'hooded claw' keypad mechanism to initiate a factory reset without requiring an authenticated access can be enabled or disabled.
The **Serial port** parameter controls access to the serial port. When set to No password, a terminal connected to the port can interact with the phone's operating system without restrictions. When Passwd reqd is selected, the serial port requires a password for access (root user is not available). When Unavailable is chosen, the serial port is not accessible.
As a prerequisite, the root user needs to create a user and to define a password via Serial Access, so that access can be granted when the Password required prompt is issued.

Administration via WBM

System > Security > Access control



Administration via Local Phone

- Administration
  - System
    - Security
      - Access control
        - **CCE access**
        - **Factory reset claw**
        - **Serial port**

3.6 Dialing

3.6.1 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 appropiate 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.

To enable the number conversion, all parameters not marked as optional must be provided, and the canonical lookup settings must be configured (see Section 3.6.1, “Canonical Dialing Configuration”).

Data required

- **Local country code**: E.164 Country code, e.g. "49" for Germany, "44" for United Kingdom. Maximum length: 5.
- **National prefix digit**: Prefix for national connections, e.g. "0" in Germany and United Kingdom. Maximum length: 5.
- **Local national code**: Local area code or city code, e.g. "89" for Munich, "20" for London. Maximum length: 6.
- **Minimal local number length**: Minimum number of digits in a local PSTN number, e.g. 3335333 = 7 digits.
- **Local enterprise node**: Number of the company/PBX wherein the phone is residing. Maximum length: 10. (Optional)
- **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 IP, each number will start with 3, 4, or 5. Therefore, the digits to be entered are 3, 4, 5.
- **Internal numbers**

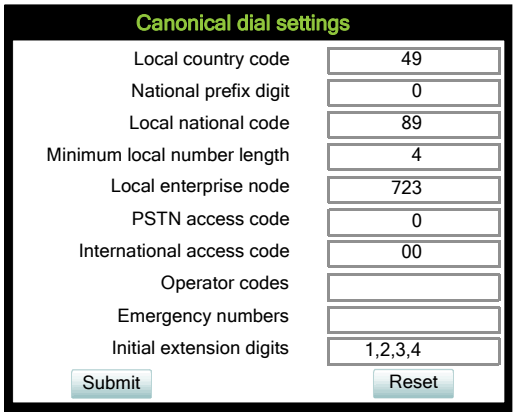
  To enable the phone to discern internal numbers from external numbers, it is crucial that a canonical lookup table is provided (Section 3.6.1, “Canonical Dialing Configuration”).

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

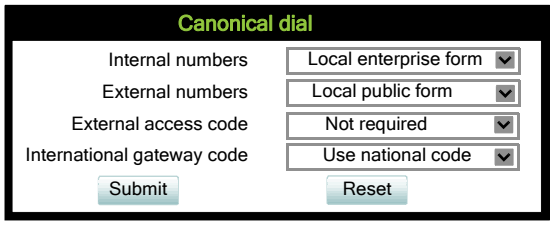
- **International gateway code**:
  - "Use national code": Default value. All international formatted numbers will be dialled explicitly by using the access code for the international gateway to replace the "+" prefix.
  - "Leave as +": All international formatted numbers will be prefixed with "+".

Administration via WBM

Local functions > Locality > Canonical dial settings



Local functions > Locality > Canonical dial



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(iona)l access**

3.6.2 Canonical Dial Lookup

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

In the local phonebook, and, mostly, in LDAP directories, numbers are stored in canonical format. In order to generate an appropriate dial string according to the settings in **Internal numbers** and **External numbers**, internal numbers must be discerned from external numbers. The canonical lookup table provides patterns which allow for operation.

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

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

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

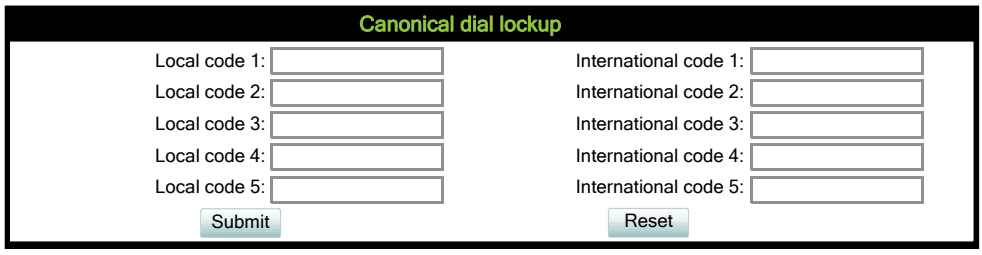
Up to 5 patterns can be defined. The **Local code 1 ... 5** parameters define up to 5 different local enterprise nodes, whilst **International code 1... 5** define up to 5 international codes, that is, fully qualified E.164 call numbers for use in a PSTN.

Data required

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

Administration via WBM

Locality > Canonical dial lookup



Administration via Local Phone

```
|--- Admin
    |--- Local Functions
        |--- Locality
            |--- Canonical lookup
                |--- Local code 1
                |--- International 1
                |--- Local code 2
                |--- International 2
                |--- Local code 3
                |--- International 3
                |--- Local code 4
                |--- International 4
                |--- Local code 5
                |--- International 5
```

3.7 Distinctive Ringing

The HFA server may provide information indicating a specific type of call within an incoming call. The phone can use this information to choose a ring tone according to the call type. A list of different ring types is maintained in the phone.

Any ringer sound may either be

- OpenScape specified tones
- Audio file (selected from the pool of ringer files on the phone)
- Constructed (from melody and tone sequence settings)

The ringer sounds are system controlled by default.

Once distinctive ringing is configured locally a system control of the ringer parameters is not possible. If system control of the ringer is desired the ringer mode must be set to “HiPath”.

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

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

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

Distinctive ringer naming

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

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

Ringer setting and preview

The configuration of distinctive ringers overlaps considerably with the general ringer configuration feature and the ability to preview (manually and automatically) what a ringer sounds like.

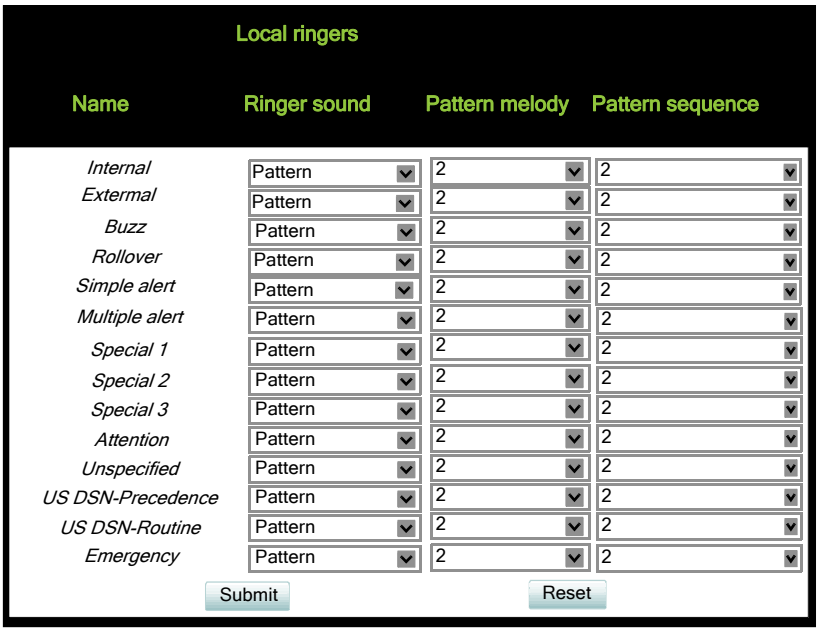
Data required

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

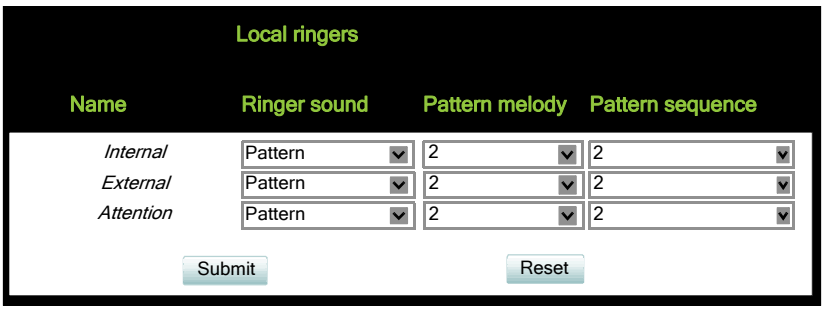
  Value range OpenScape Business: "Internal call", "External call", "Attention ringer"
  Default: "Internal call".
- **Ringer sound**: ‘Pattern’ or the name of the selected ring tone file. Sets the distinctive ringer to use the currently set pattern (melody and sequence). This is the pattern that will be used if the configured ring tone file cannot be played for any reason.
  Value range: "Pattern", "<audio file>"
  Default: "Pattern".
- **Pattern melody**: Selects the melody pattern that will be used if **Ringer sound** is set to "Pattern".
  Value range: "1"... "8"
  Default: "2".
- **Pattern sequence:** Determines the length for the melody pattern, and the interval between the repetitions of the pattern.
  Value range: "1": 1 sec ON, 4 sec OFF
  "2": 1 sec ON, 2 sec OFF
  "3": 0.7 sec ON, 0.7 sec OFF, 0.7 sec ON, 3 sec OFF
  Default: "2".
- **User changeable**: Selects if the user is allowed to change destinctive ringer settings.
  Value range: "Yes", "No"
  Default: "Yes".
- **Mode**: Determines the source of ringer tone.
  Value range: "HiPath ", "Local ringer"
  Default: "HiPath".

Administration via WBM

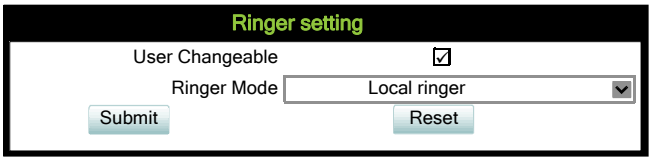
OpenScape 4000: Admin > Ringer > Local ringers



OpenScape Business: Admin > Ringer > Local ringers



Admin > Ringer >Ringer setting



Administration via Local Phone

- Admin
  - Settings
    - Ringer
      - Local ringer
        - **Name**
        - **Ringer sound**
        - **Ringer melody**
        - **Ringer sequence**
      - Ringer Setting
        - **Options**
        - **User changeable**
        - **Mode**

3.8 User Mobility

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

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

3.9 Transferring Phone Software, Application, and Media Files

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

For all user data, which includes files as well as phonebook content, the following amounts of storage place are available:
- OpenScape Desk Phone CP600: 100 MB
- OpenScape Desk Phone CP400: 100 MB
- OpenScape Desk Phone CP200/CP205: 25 MB

3.9.1 FTP/HTTPS Server

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

3.9.2 Common FTP/HTTPS Settings (Defaults)

For each one of the various file types, e.g. phone software, or logos, specific FTP/HTTPS access data can be defined. If some or all file types have the parameters **Download method**, **FTP Server**, **FTP Server port**, **FTP Account**, **FTP Username**, **FTP path**, and **HTTPS base URL** in common, they can be specified here. These settings will be used for a specific file type if its **Use defaults** parameter is set to "Yes".

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

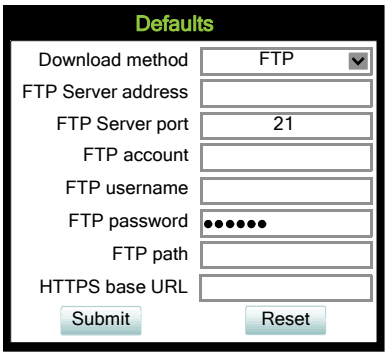
Data required

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS".
  Default: "FTP".
- **FTP Server**: IP address or hostname of the FTP server in use.
- **FTP Server port**: Port number of the FTP server in use. For HTTPS, port 443 is assumed, unless a different port is specified in the HTTPS base URL.
  Default: 21.
- **FTP Account**: Account at the server (if applicable).
- **FTP Username**: User name for accessing the server.
- **FTP Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.

- **HTTPS base URL**: IP address or hostname of the HTTPS server in use. If no port number is specified here, port 443 is used. Only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > Defaults



Administration via Local Phone

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

3.9.3 Phone Application

The firmware for the phone can be updated by downloading a new software file to the phone.

If an incorrect software image is being attempted to be loaded onto the phone, the phone will reject the request and return to normal operation without reboot. As part of this security mechanism, new software binds are identified by a "Supported Hardware Level" information built into the header.

Prerequisite: The phone knows it’s own hardware level (from the part number and/or by a dynamical check of its HW level).

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

1. If new software bind has hardware level header included (in the bind header): Hardware level of new bind is compared with phone’s hardware level.
   - If compatible (or if Override is set): Proceed with update
   - If NOT compatible: Abandon update and return to original application
2. If new software bind does NOT have hardware level header included (in the bind header): Software version of new bind is compared with minimum known supported SW level.
   - If compatible (or if Override is set): Proceed with update
   - If NOT compatible: Abandon update and return to original application

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

3.9.3.1 Upgrade Using File

Use an image file choosen by browsing to upgrade the phone.

Closing or navigating away from this screen will cancel the file upload.

3.9.3.2 Upgrade Using FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.9.2, “Common FTP/HTTPS Settings (Defaults)”) are to be used, **Use defaults** must be set to "Yes", and only the **Filename** must be specified.

Data required (in every case)

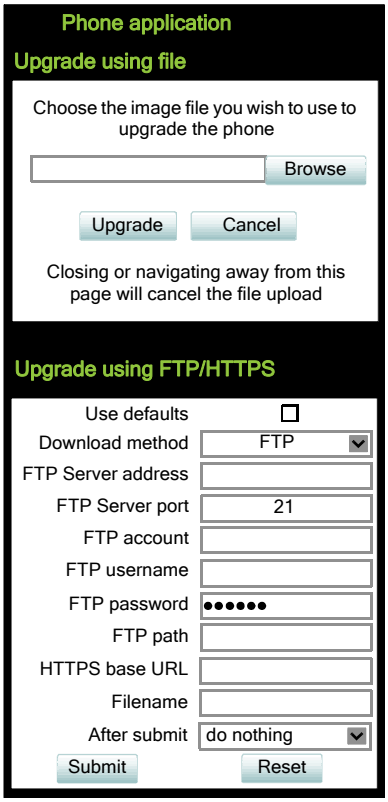
- **Use defaults**: Specifies whether the default FTP/HTTPS access settings shall be used.
  Value range: "Yes", "No".
- **Filename**: Specifies the file name of the phone software.

Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS".
  Default: "FTP".
- **Server**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21.
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".
- **After submit**: Specifies actions after submit button is pressed.
  Value range: "do nothing", "start download".
  Default: "do nothing".

Administration via WBM

File transfer > Phone application



Administration via Local Phone

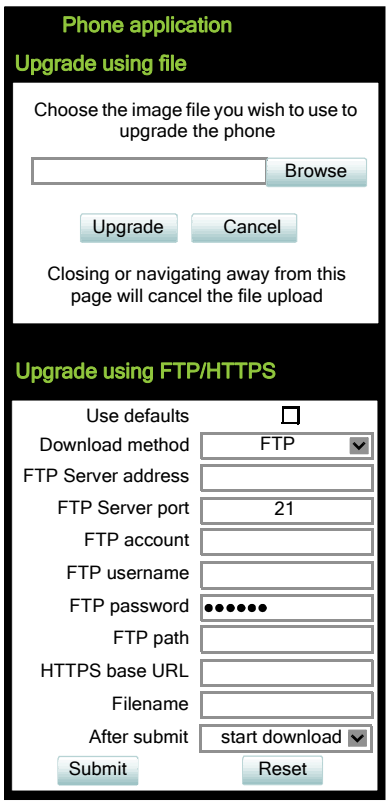
- Admin
  - File Transfer
    - Phone app
      - **Use default**
      - **Download method**
      - **Server**
      - **Port**
      - **Account**
      - **Username**
      - **Password**
      - **FTP path**
      - **HTTPS base URL**
      - **Filename**

3.9.3.3 Download/Update Phone Application

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

Start Download via WBM

File transfer > Phone application



In the File transfer > Phone application dialog, set **After submit** to "start download" and press the **Submit** button.

Start Download via Local Phone

In the administration menu, set the focus to **Phone app**.

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

- On Desk Phone CP200/CP205:
  Press the **OK** key. A context menu opens. In the context menu, select **Download**. The download will start immediately.
- On Desk Phone CP400/600:
  Press the Soft Key labeled **Download**. The download will start immediately.

3.9.4 Picture Clips

Picture clips are available only on OpenScape Desk Phone CP600 phones.

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 and PNG.

3.9.4.1 FTP/HTTPS Access Data

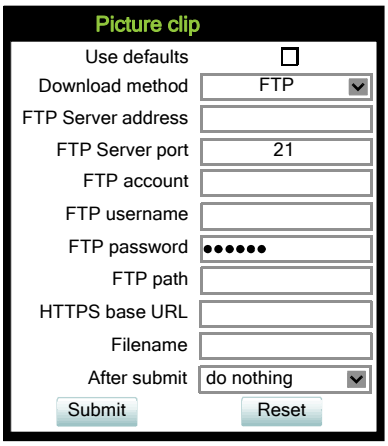
If the default FTP/HTTPS access settings (see Section 3.9.2, “Common FTP/HTTPS Settings (Defaults)”) are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

Data required (in any case)

- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used.
  Value range: "Yes", "No".
- **Filename**: Specifies the file name of the image file.
- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS".
  Default: "FTP".
- **Server**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21.
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".
- **After submit**: Specifies actions after submit button is pressed.
  Value range: "do nothing", "start download".
  Default: "do nothing".

Administration via WBM

File transfer > Picture clip



Administration via Local Phone

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

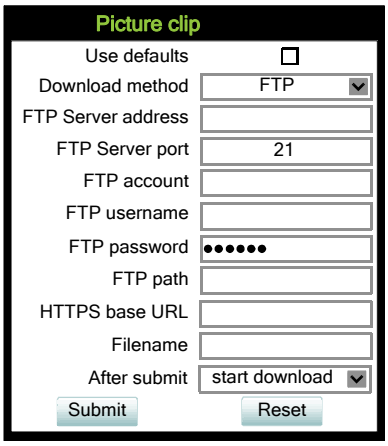
- On Desk Phone CP400/600:
  Press the Soft Key labeled **Download**. The download will start immediately.

3.9.4.2 Download Picture Clip

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

Start Download via WBM

File transfer > Phone application



In the File transfer > Picture clip dialog, set **After submit** to "start download" and press the **Submit** button.

Start Download via Local Phone

In the administration menu, set the focus to **Picture clip**.

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

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

3.9.5 LDAP Template

LDAP template is available only on OpenScape Desk Phone CP400/600 phones.

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 OpenScape Desk Phone CP phones support LDAPv3.

3.9.5.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.9.2, “Common FTP/HTTPS Settings (Defaults)”) are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

Data required (in any case)

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

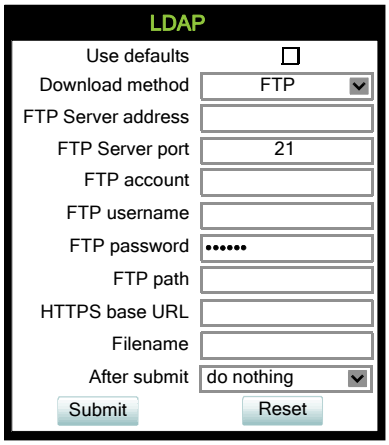
Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS"
  Default: "FTP"
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.

- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > LDAP



Administration via Local Phone

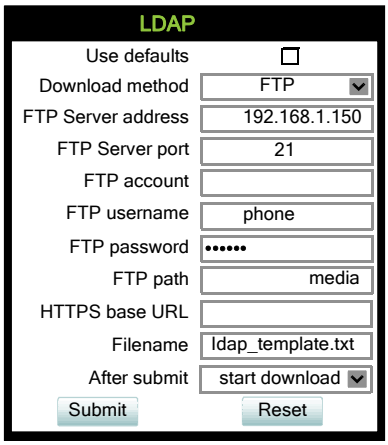
```
└ --- Admin
     └ --- File Transfer
          └ --- LDAP
               |--- Use default
               |--- Download method
               |--- Server
               |--- Port
               |--- Account
               |--- Username
               |--- Password
               |--- FTP path
   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

3.9.5.2 Download LDAP Template

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

The OpenScape Desk Phone CP phone supports LDAPv3.

Start Download via WBM



In the **File transfer** > LDAP dialog, set **After submit** to "start download" and press the **Submit** button.

Start Download via Local Phone

In the administration menu, set the focus to **LDAP**.

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

- On Desk Phone CP200/CP205:
  Press the OK key. A context menu opens. In the context menu, select Download. The download will start immediately.
- On Desk Phone CP400/600:
  Press the Soft Key labeled Download. The download will start immediately.

3.9.6 Screensaver

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

Screensavers are available only on OpenScape Desk Phone CP600.

The file size for a screensaver image is limited to 300 KB. If the file is too large or the contents of the file are not valid, the file will not be stored in the phone.

For screensaver images, the following specifications are valid:

- Data format: JPG or PNG. JPG is recommended.
- Screen format: 4:3. The images are resized to fit in the screen, so that images with a width/height ratio differing from 4:3 will appear with deviant proportions.
- Resolution: The phone's screen resolution is the best choice for image resolution:
  – OpenScape Desk Phone CP400/600: 320x240

3.9.6.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.9.2, "Common FTP/HTTPS Settings (Defaults)") are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

Data required (in any case)

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

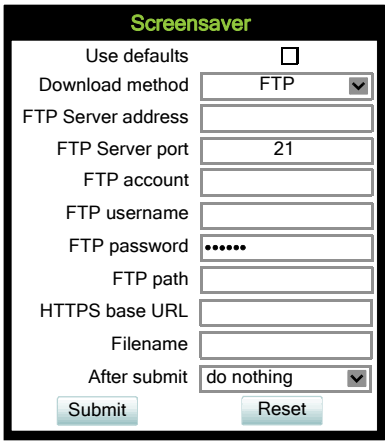
Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS"
  Default: "FTP"
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21

- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > Screensaver



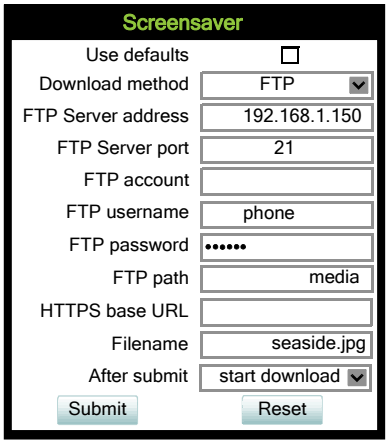
Administration via Local Phone

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

3.9.6.2 Download Screensaver

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

Start Download via WBM



In the **File transfer** > Screensaver dialog, set **After submit** to "start download" and press the **Submit** button.

Start Download via Local Phone

In the administration menu, set the focus to **Screensaver**.

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

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

3.9.7 Ringer File

The download of ringer files via WBM or local menu is possible only for OpenScape Desk Phone CP400/600.

Custom ring tones can be uploaded to the phone.

The file size for a ringer file is limited to 1 MB. If the file is too large or the contents of the file are not valid, the file will not be stored in the phone. This limitation is only enforced on WBM.

The following file formats are supported:

- WAV format. The recommended specifications are:
  - Audio format: PCM
  - Bitrate: 16 kB/sec
  - Sampling rate: 8 kHz
  - Quantization level: 16 bit
- MIDI format.
- MP3 format (OpenScape Desk Phone CP400/600 only). The OpenScape Desk Phone CP400/600 phones are able to play MP3 files from 32 kbit/s up to 320 kbit/s. As the memory for user data is limited to 8 MB, a constant bitrate of 48 kbit/sec to 112 kbit/s and a length of max. 1 minute is recommended. Although the phone software can play stereo files, mono files are recommended, as the phone has only 1 loudspeaker.
  See the following table for estimated file size (mono files):

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

3.9.7.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.9.2, “Common FTP/HTTPS Settings (Defaults)”) are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

Data required (in any case)

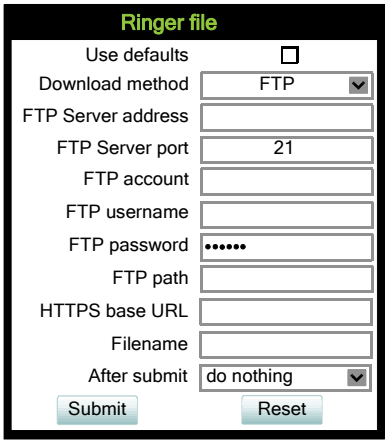
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used.
  Value range: "Yes", "No"
  Default: "No"
- **Filename**: Specifies the file name of the phone software.
- **After submit**: Specifies action after submit button is pressed.
  Value range: "do nothing", "start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

Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS"
  Default: "FTP"
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > Ringer file



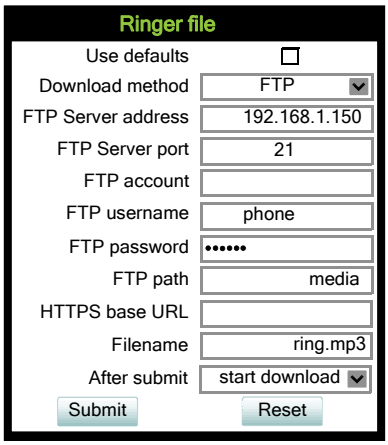
Administration via Local Phone

- Admin
  - File Transfer
    - Ringer
      - **Use default**
      - **Download method**
      - **Server**
      - **Port**
      - **Account**
      - **Username**
      - **Password**
      - **FTP path**
      - **HTTPS base URL**
      - **Filename**

3.9.7.2 Download Ringer File

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

Start Download via WBM



In the File transfer > Ringer dialog, set **After submit** to "start download" and press the **Submit** button.

Start Download via Local Phone

In the administration menu, set the focus to **Ringer**.

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

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

3.9.8 Dongle Key

The HPT dongle key is a special file that contains a secret hash number which is required to connect the HPT tool to the phone. This testing tool is used exclusively by the service staff.

3.9.8.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.9.2, “Common FTP/HTTPS Settings (Defaults)”) are to be used, **Use default** must be set to „Yes“, and only the **Filename** must be specified.

Data required (in any case)

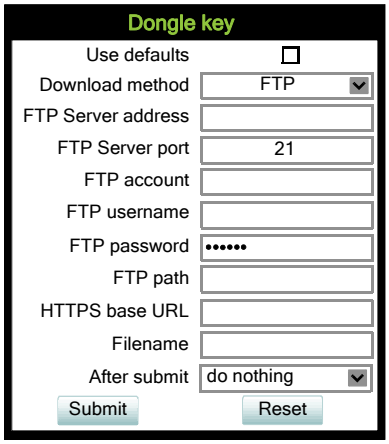
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used.
  Value range: „Yes“, „No“
  Default: „No“
- **Filename**: Specifies the file name of the phone software.
- **After submit**: Specifies actions after submit button is pressed.
  Value range: "do nothing", "start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

Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: „FTP“, „HTTPS“
  Default: „FTP“
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to „HTTPS“.

Administration via WBM

File transfer > Dongle key



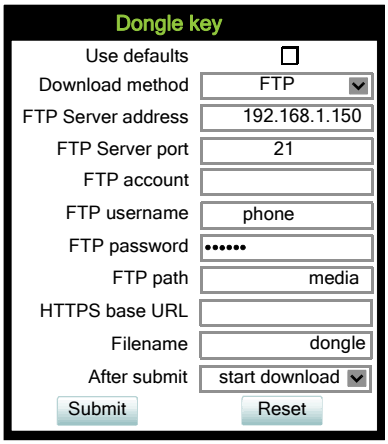
Administration via Local Phone

- Admin
  - File Transfer
    - Dongle key
      - **Use default**
      - **Download method**
      - **Server**
      - **Port**
      - **Account**
      - **Username**
      - **Password**
      - **FTP path**
      - **HTTPS base URL**
      - **Filename**

3.9.8.2 Download Dongle Key File

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

Start Download via WBM



In the **File transfer** > Dongle key dialog, set **After submit** to „start download“ and press the **Submit** button.

Start Download via Local Phone

In the administration menu, set the focus to **Dongle key**.

```
└ --- Admin
    └ --- File Transfer
        └ --- Dongle key
```

- On Desk Phone CP200/CP205:
  Press the **OK** key. A context menu opens. In the context menu, select **Download**. The download will start immediately.
- On Desk Phone CP400/600:
  Press the Soft Key labeled **Download**. The download will start immediately.

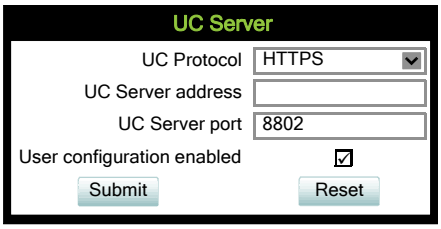
3.10 UC Server

Data required

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

Administration via WBM

Local functions > Locality > UC Server



Administration via Local Phone

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

3.11 Corporate Phonebook: Directory Settings

3.11.1 LDAP

LDAP is possible only for OpenScape Desk Phone CP400/600.

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

The OpenScape Desk Phone CP phones support LDAPv3.

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

For a quick guide on setting up LDAP on an OpenScape Desk Phone CP phone, please refer to Section 4.2, “How to Set Up the Corporate Phonebook (LDAP)”.

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

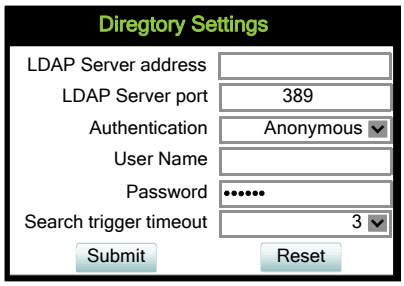
Data required

- **Server address**: IP address or hostname of the LDAP server.
- **Server port**: Port on which the LDAP server is listening for requests.
  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.
- **Search trigger timeout**: Timespan between entering the last character and search string submission to the LDAP server.

Administration via WBM

Local functions > Directory Settings



Administration via Local Phone

```
└--- Admin
    └--- Local Functions
        └--- LDAP
            |--- Server address
            |--- LDAP server port
            |--- Authenticate
            |--- User name
            |--- Password
            └--- Search trigger (s)
```

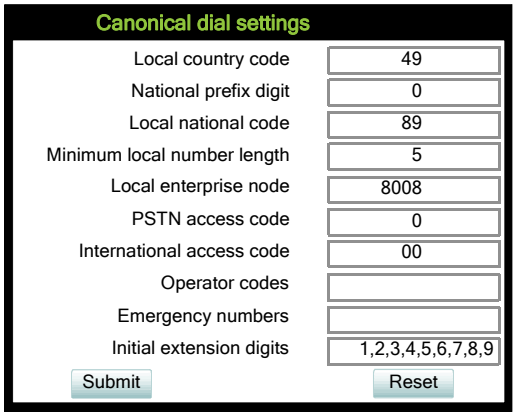
3.11.2 Canonical Dial Settings

For contact data retrieval from the directory server, upon arrival of a call, the remote telephone number is converted according to the canonical dial settings (see also Section 3.11.2, “Canonical Dial Settings”). The format of the resulting number should match the format the numbers are stored in the directory server. It is recommended to convert the numbers to fully qualified format, i.e. adding country and area code to the subscriber number. This way it is ensured that the number used for lookup is unique.

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

Administration via WBM

Local functions > Locality > Canonical dial settings



- 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**
        - **Inital extension digits**

3.11.3 Picture via LDAP

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

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

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

- Direct retrieval of pictures stored within the ldap directory (preferred mechanism)

- Indirect (two step) retrieval in case the directory server contains a reference (url) to the picture instead – in this case the picture is retrieved from another server via http using the url.

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

3.12 Speech

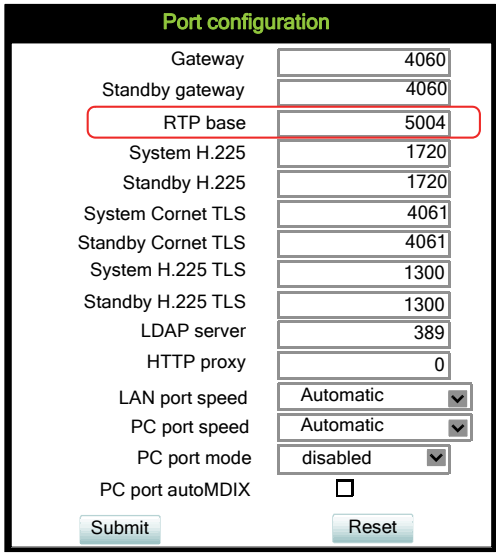
3.12.1 RTP Base Port

The port used for RTP is negotiated during the establishment of a HFA connection. The RTP base port number defines the starting point from which the phone will count up when negotiating. The default value is 5004.

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

Administration via WBM

Network > Port Configuration



Administration via Local Phone

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

3.12.2 Codec Preferences

If **Silence suppression** is activated, the transmission of data packets is suppressed on no conversation, that is, if the user doesn't speak.

The OpenScape Desk Phone CP phone provides the codecs **G.711**, **G.722**, and **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.

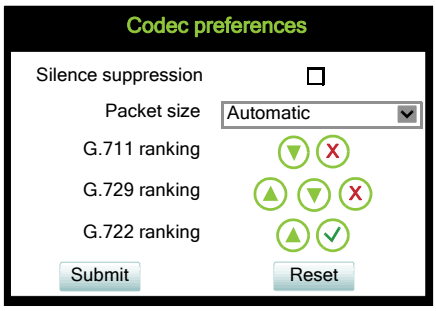
The **Packet size**, i. e. length in milliseconds, of the RTP packets for speech data, can be set to 10ms, 20ms, 30ms, 60ms or to automatic detection.

Data required

- **Silence suppression**: Suppression of data transmission on no conversation.
  Value range: "On", "Off"
  Default: "Off"
- **Packet size**: Size of RTP packets in milliseconds.
  Value range: "10 ms", "20ms", "30ms", "60ms", "Automatic"
  Default: "Automatic"
- **G.711**: Parameters for the G. 711 codec.
  Value Range: "Choice 1", "Choice 2", "Choice 3", "Disabled", "Enabled"
  Default: "Choice 1"
- **G.729**: Parameters for the G. 729 codec.
  Value Range: "Choice 1", "Choice 2", "Choice 3", "Disabled", "Enabled"
  Default: "Choice 2"
- **G.722**: Parameters for the G. 722 codec.
  Value Range: "Choice 1", "Choice 2", "Choice 3", "Disabled", "Enabled"
  Default: "Disabled"

Administration via WBM

Speech > Codec preferences



Administration via Local Phone

- Admin
  - Speech
    - Codec Preferences
      - **Silence suppression**
      - **Packet size**
      - **G.711**
      - **G.729**
      - **G.722**

3.12.3 Display General Phone Information

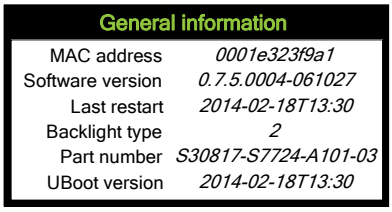
General information about the status of the phone can be displayed if desired.

Displayed Data

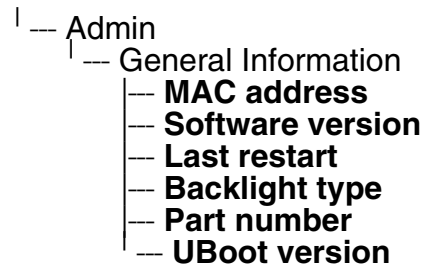
- **MAC address**: Shows the phone's MAC address.
- **Software version**: Shows the version of the phone's firmware.
- **Last restart**: Shows date and time of the last reboot.
- **Backlight type**: indicates whether the phone has a backlight, and, if applicable, the type
- of backlight.
  Value range: 0 (no backlight); 1 (cathode tube backlight); 2 (LED backlight).
- **Part number**: Shows the part number of the phone's hardware
- **UBoot version**: Shows the version of the boot loader.

Display on the WBM

General information



Display on the Local Phone



3.13 Security and Policies

3.13.1 Password

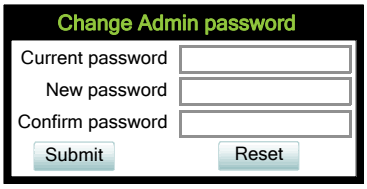
The passwords for user and administrator can be set here. They have to be confirmed after entering. The default factory setting for the administrator password is "123456"; it should be changed after the first login (see Change Admin and User password). The factory setting for the user password is "not set", i. e. no password.

The admin has to define the initial user password once the user is willing to use a 1st party CTI application. After this the user should change this user password via WBM immediately. The user himself cannot set the initial password due to security reasons.

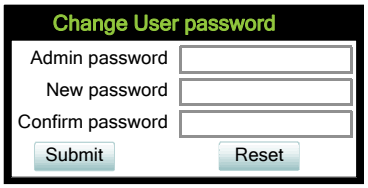
Usable characters are 0-9 A-Z a-z ."*#,?!'+-()@/:_

Administration via WBM

Security and Policies > Password > Change Admin password



Security and Policies > Password > Change User password



Administration via Local Phone

- Admin
  - Security and policies
    - Change admin password
      - **Current admin**
      - **Admin**
      - **Confirm new password**
    - Change user password
      - **Admin password**
      - **New user password**
      - **Confirm new user**

3.13.1.1 Troubleshooting: Lost Password

If the administration and/or user password is lost, and there is no DLS available, new passwords must be provided. In case of lost administration password, a factory reset is necessary. In case of lost user password, the administrator may reset the user password. Take the following steps to initiate a factory reset:

1. On the phone, press the settings/service key to activate the administration menu (the Menu key toggles between the user's configuration menu and the administration menu).
2. Press the number keys 2-8-9 simultaneously. The factory reset menu opens. If not, the key combination is deactivated due to security reason.
3. In the input field, enter the special password for factory reset: "124816".
4. Confirm by pressing OK.

3.13.2 Certificates

3.13.2.1 Generic

Online Certificate Check

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

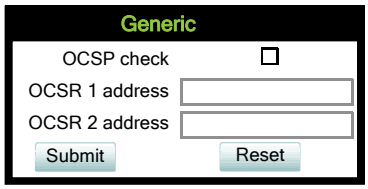
When **OCSP check** is activated, the configured OCSR is requested to check if the certificate has been revoked.

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

Security and Policies > Certificates > Generic



Administration via Local Phone

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

3.13.2.2 Authentication Policy

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

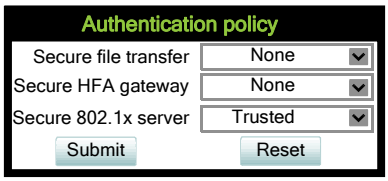
Secure file transfer sets the authentication level for the HTTPS server to be used (see Section 3.9.2, “Common FTP/HTTPS Settings (Defaults)”).

Secure HFA gateway sets the authentication level for the HFA gateway connected to the phone (see Section 3.5.11, “Security”).

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

Administration via WBM

Security and Policies > Certificates > Authentication policy



Administration via Local Phone

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

3.14 Restart Phone

If necessary, the phone can be restarted from the administration menu or via pressing number keys 1-4-7 simultaneously.

Administration via WBM

Maintenance > Restart Phone

Administration via Local Phone

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

3.15 Factory Reset

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

Administration via WBM

Maintenance > Factory reset

Administration via Local Phone

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

3.16 SSH – Secure Shell Access

The phone’s operating system can be accessed via SSH for special troubleshooting tasks.Hereby, the administrator is enabled to use the built-in Linux commands. As soon as SSH access has been enabled using the WBM, the system can be accessed by the user "admin" for a specified timespan. When this timespan has expired, no connection is possible any more. The user "admin" has the following permissions:

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

It is not possible to logon as root via SSH.

When **Enable access** is enabled, and the parameters described underneath are specified, SSH access is activated. By default, SSH access is disabled.

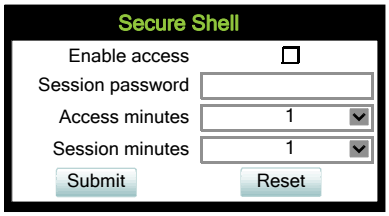
With the **Session password** parameter, a password for the "admin" user is created. This password is required. It will be valid for the timespan specified in the parameters described underneath.

Access minutes defines the timespan in minutes within which the SSH connection must be established. After it has expired, a logon via SSH is not possible. The possible values ranges from 1 to 10.

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

Administration via WBM

Maintenance > Secure Shell



3.17 Display License Information

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

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

Administration via Local Phone

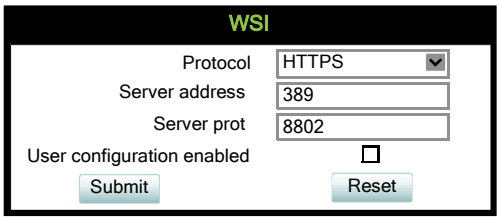
```
|--- Admin
     |--- Licence information
```

3.18 Web Services Interface (WSI)

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

Administration via WBM

Local functions > WSI



Administration via Local Phone (Disable)

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

3.19 HPT Interface (For Service Staff)

For special diagnosis and maintenance tasks, the service staff may employ the HPT tool, which is able to control and observe an OpenScape Desk Phone CP phone remotely. For security reasons, this tool can only be used when a dongle key file is uploaded to the phone (see Section 3.9.8, “Dongle Key”). This key is accessable to the service staff only. It is specific for a particular HFA firmware version, but it will also be valid for previous versions.

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 HPT interface is enabled by downloading the dongle key file to the phone (see Section 3.9.8, “Dongle Key”). It can be disabled via local menu or WBM. Thereby, the dongle key file is deleted. To enable the HPT interface again, the file must be downloaded anew.

The session data is written to a log file on the phone. It can be downloaded from the Diagnostics > Fault trace configuration menu (see Section 3.20.2, “Fault Trace Configuration”).

Administration via WBM

Maintenance > HPT interface

Administration via Local Phone (Disable)

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

3.20 Diagnostics

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

3.20.1 LLDP-MED

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

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

For details on LLDP-MED, please refer to the ANSI/TIA-1057 standard.

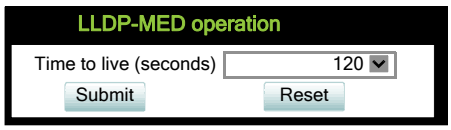
For a network configuration example that shows LLDP-MED in operation, please refer to Section 4.3, “An LLDP-Med Example”.

Displayed Data

- **Extended Power**: Power Consumption; relevant for PoE.
- **Network policy (voice)**: VLAN ID and QoS (Quality of Service) parameters for voice transport.
- **Network policy (signalling)**: VLAN ID and QoS (Quality of Service) parameters for signalling.
- **LLDP-MED capabilities**: The LLDP-MED TLVs supported by the phone and the switch as well as the specific device class they belong to.
- **MAC_Phy configuration**: Identifies the possible duplex and bit-rate capability of the sending device, its current duplex and bit-rate capability, and whether theses 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**: **T**ime **T**o **L**ive. This parameter determines how long the TLVs are valid. When expired, the device will send a new set of TLVs.

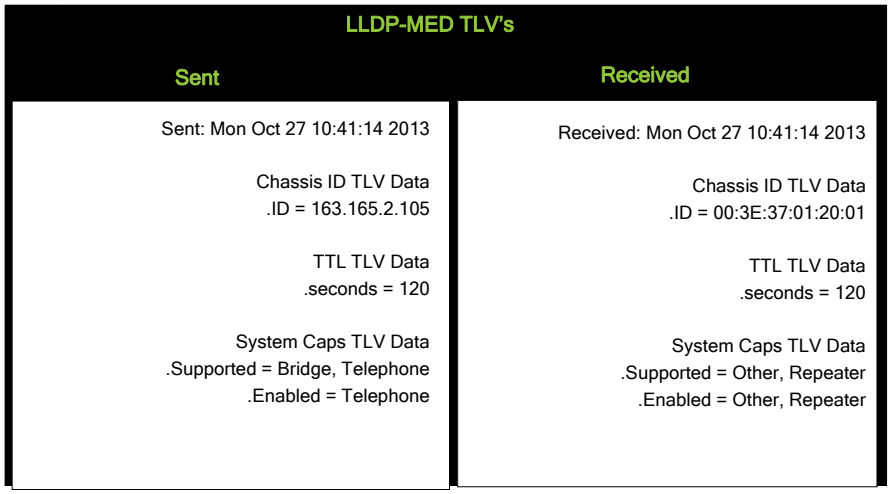
Administration via WBM

Admin > Network > LLDP-MED operation



View Data From WBM

Diagnostics > LLDP-MED TLVs



View Data From Local Menu

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

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

3.20.2 Fault Trace Configuration

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

The **File size (bytes)** parameter sets the maximum file size. When it is reached, the data is saved as old file, and a new file is generated. From then on, the trace data is written to the new file. When the maximum file size is reached again, the data is saved as old file once more, thereby overwriting the previous old file. The default value is 1048576.

The absolute maximum file size is 6290000 bytes. However, on OpenScape Desk Phone CP phones, a maximum size not greater than 1000 000 bytes is recommended due to the amount of available memory.

The **Trace timeout (minutes)** determines when to stop tracing. When the timeout is reached, the trace settings for all components are set to OFF, but ERROR and STATUS messages are still written to the trace file ad infinitum. When the trace file has reached its maximum size, the data is saved, and a new file is created (for more information, see **File size (bytes)** above). If the value is 0, the trace data will be written without time limit.

If **Automatic clear before start** is checked, the existing trace file will be deleted on pressing the **Submit** button, and a new, empty trace file will be generated. By default, it is unchecked.

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

- **Download trace file**
  The trace data according to the settings specified for the services.
- **Download old trace file**
  The trace file is stored in permanent memory. When the file has reached its size limit, it will be saved as old trace file, and the current exception file is emptied for future messages. The old trace file can be viewed here.
- **Download saved trace file**
  Normally, the trace file is saved only in the phone RAM. When the phone restarts in a controlled manner, the trace file will be saved in permanent memory.
- **Download syslog file**
  Messages from the phone's operating system, including error and exception messages.
- **Download old syslog file**
  Old messages from the phone's operating system.
- **Download saved syslog file**
  Saved messages from the phone's operating system.
- **Download exception file**
  If an exceptions occurs in a process running on the phone, a message is written to this file. These messages are incorporated in the syslog file (see **Download syslog file** also).

- **Download old exception file**
  The exception file is stored permanent memory. When the file has reached its size limit, it will be saved as old exception file, and the current exception file is emptied for future messages. The old exception file can be viewed here.
- **Download H.323 trace file**
- **Download upgrade trace file**
  The trace log created during a software upgrade.
- **Download upgrade error file**
  The error messages created during a software upgrade. These messages are incorporated in the syslog file (see **Download syslog file** also).
- **Download Database file**
  Configuration parameters of the phone in SQLite format.
- **Download HPT remote service log file**
  Log data from the HPT service.

By pressing **Submit**, the trace settings are submitted to the phone. With **Reset**, the recent changes can be canceled.

The following trace levels can be selected:
- **OFF**: Default value. Only error messages are stored.
- **FATAL**: Only fatal error messages are stored.
- **ERROR**: Error messages are stored.
- **WARNING**: Warning messages are stored.
- **LOG**: Log messages are stored.
- **TRACE**: Trace messages are stored. These contain detailed information about the processes taking place in the phone.
- **DEBUG**: All types of messages are stored.

Brief Descriptions of the Components/Services

- **802.1x service**
  Provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. The service is used for certain closed wireless access points.
- **Administration**
  Deals with the changing and setting of parameters within the phone database, from both the User and Admin menus.
- **AGP Phonelet**
  Phonelet that manages XML applications.
- **Application framework**

All applications within the phone, e.g. Call view, Call log, or Phonebook, are run within the application framework. It is responsible for the switching between different applications and bringing them into and out of focus as appropriate.

- **Application menu**
  This is where applications to be run on the phone can be started and stopped.
- **Call Log**
  The Call log application displays the call history of the phone.
- **Call View**
  Handles the representation of telephony calls on the phone screen.
- **Certificate management**
  Handles the verification and exchange of certificates for security and verification purposes.
- **Clock Service**
  Handles the phone's time and date, including daylight saving and SNTP 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, e.g. OpenScape Desk Phone CP200/205/400/600 HFA.
- **CSTA service**
  Any CSTA messages are handled by this service. CSTA messages are used within the phone by all services as a common call progression and control protocol.
- **Data Access service**
  Allows other services to access the data held within the phone database.
- **Desktop**
  Responsible for the shared parts of the phone display. Primarily these are the status bar at the top of the screen and the FPK labels.
- **Digit analysis service**
  Analyses and modifies digit streams which are sent to and received by the phone, e.g. canonical conversion.
- **Directory service**
  Performs a look up for data in the phonebook, trying to match incoming and outgoing numbers with entries in the phonebook.
- **DLS client management**
  Handles interactions with the DLS (Deployment Service).

- **H.323 messages**
  Used on HiPath 4000 systems as SME platforms do not use H.323 with HFA V3, this traces the H.323 messages which are exchanged between the phone, gateway and other phones for DMC calls.
- **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.
- **HFA service agent**
  This trace will enable the Stimulus FPK Programming and HFA Stimulus, Messages Menu Phonelet and HFA Phonelet Utilities that are directly managed by PBX
- **HTTP Service**
  Handles the HTTP Service messages.
- **Instrumentation service**
  Used by the Husim 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.
- **Mobility service**
  Handles the mobility feature whereby users can log onto different phones and have them configured to their own profile.
- **OBEX service (Not applicable for OpenScape Desk Phone CP200/CP205)**
  Involved with Bluetooth accesses to the phone.
  Bluetooth is available only on OpenScape Desk Phone CP600 phones.
- **OpenStage client management**
  This trace allows you to control the data flow of the system in case a configuration item on Local Menu,WEBM or DLS is deleted/updated/added. It resides in the middle of all services and provides interface to all other services for data management.
- **Password management service**
  Verifies passwords used in the phone.

- **Performance Marks**
  Aid for measuring the performance of the phone. For events triggered by the user, a performance mark is written to the trace file, together with a timestamp in the format hh:mm:ss yyyy.milliseconds, and information about the event. The timespan between two performance marks is an indicator for the performance of the phone.

  The trace level must be set to "TRACE" or "DEBUG".

- **Phonebook**
  Responsible for the phonebook application.
- **Physical interface service**
  Handles any interactions with the phone via the keypad, mode keys, fixed feature buttons, clickwheel and slider.
- **Security Log Service**
  Handles the Security Log 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.
- **Tone generation service**
  Handles the generation of the tones and ringers on the phone.
- **Transport service**
  Provides the IP (LAN) interface between the phone and the outside world.
- **USB backup service**
  Used to make backup/restore to/from USB stick by using password. This item is available in the phone GUI.
- **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.
- **Voice recognition**
  Used by the voice dial facility for recognizing spoken dialing commands.
- **Web server service**
  Provides access to the phone via web browser.

Administration via WBM

Diagnostics > Fault trace configuration

Fault trace configuration

File size (bytes): 65536 | Trace timeout (minutes): 0 | Automatic clear before start ☐

Trace levels for components

802.1 x service	OFF	Administration	OFF
AGP Phonelet	OFF	Application framework	OFF
Application menu	OFF	Call log	OFF
Call View	OFF	Certificate management	OFF
Clock Service	OFF	Communications	OFF
Component registrar	OFF	CSTA service	OFF
Data Access service	OFF	Desktop	OFF
Digit analysis service	OFF	Directory service	OFF
DLS client management	OFF	H.323 messages	OFF
Health service	OFF	Help	OFF
HFA service agent	OFF	HTTP Service	OFF
Instrumentation service	OFF	Journal service	OFF
Media control service	OFF	Media procession service	OFF
Mobility service	OFF	OBEX service	OFF
OpenStage client management	OFF	Password management service	OFF
Performance Marks	OFF	Phonebook	OFF
Physical interface service	OFF	Security Log Service	OFF
Service framework	OFF	Service registry	OFF
Sidecar service	OFF	Tone generation service	OFF
Transport service	OFF	USB backup service	OFF
Voice generation service	OFF	Voice mail	OFF
Voice recognition	OFF	Web server service	OFF

Download trace file | Download saved trace file | Download upgrade trace file | Download old trace file

Download syslog file | Download old syslog file | Download saved syslog file | Download Database file

Download upgrade error file | Download HPT remote service log file | Download dial plan file

Submit | Reset

3.20.3 EasyTrace Profiles

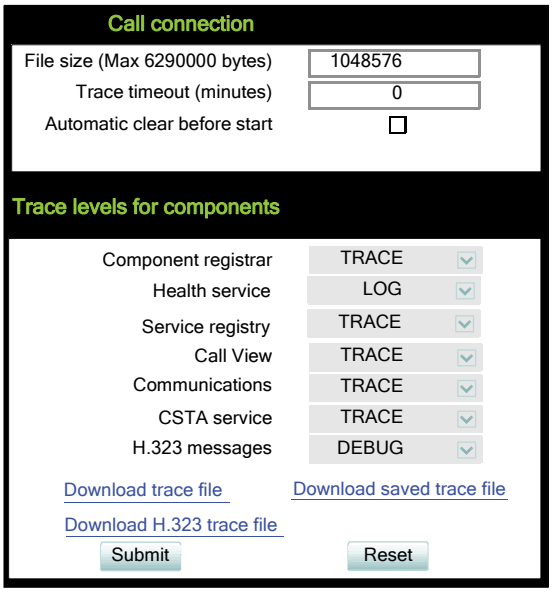
In order to simplify tracing for a specific problem, the tracing levels can be adjusted using pre-defined settings. The EasyTrace profiles provide settings for a specific area, e. g. call connection. On pressing **Submit**, those pre-defined settings are sent to the phone. If desired, the settings can be modified anytime using the general mask for trace configuration under **Diagnostics** > Fault Trace Configuration (see Section 3.20.2, “Fault Trace Configuration”).

If desired, the tracing for all services can be disabled (see Section 3.20.3.21, “No Tracing for All Services”).

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

3.20.3.1 Call Connection

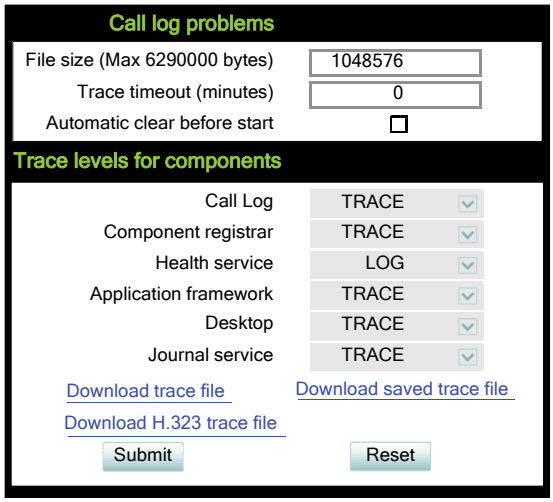
Diagnostics > EasyTrace Profiles > Call connection



This EasyTrace profile contains the tracing of H.323 messages. Please note that after changing the level for the tracing of H.323 messages, the phone must be rebooted.

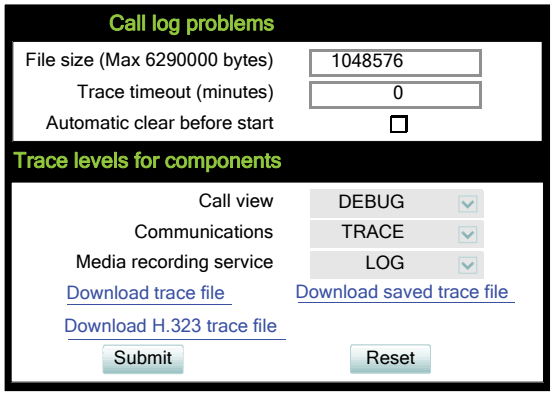
3.20.3.2 Call Log Problems

Diagnostics > EasyTrace Profiles > Call log problems



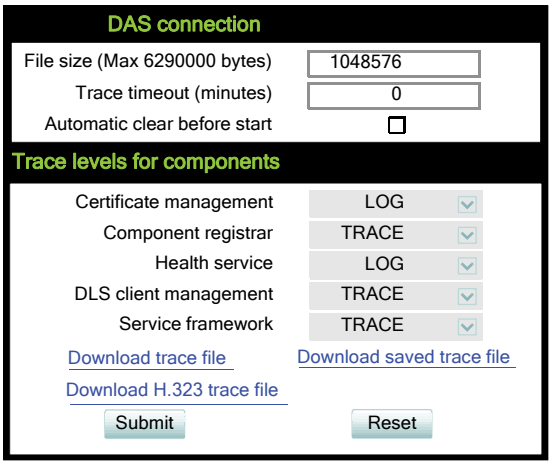
3.20.3.3 Call recording

Diagnostics > EasyTrace Profiles > Call recording



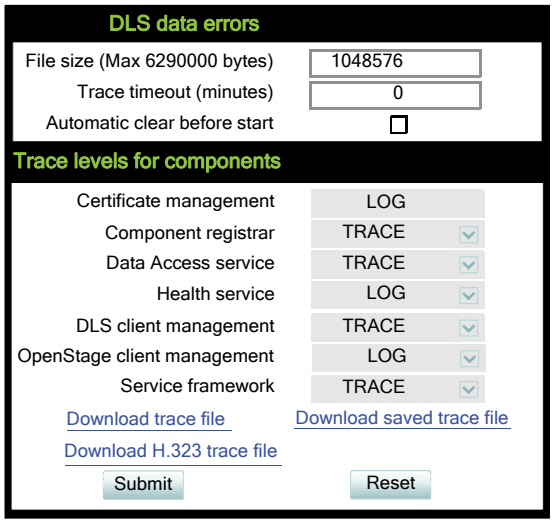
3.20.3.4 DAS Connection

Diagnostics > EasyTrace Profiles > DAS connection



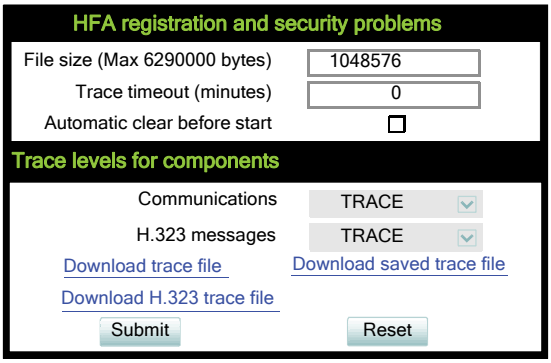
3.20.3.5 DLS Data Errors

Diagnostics > EasyTrace Profiles > DLS data errors



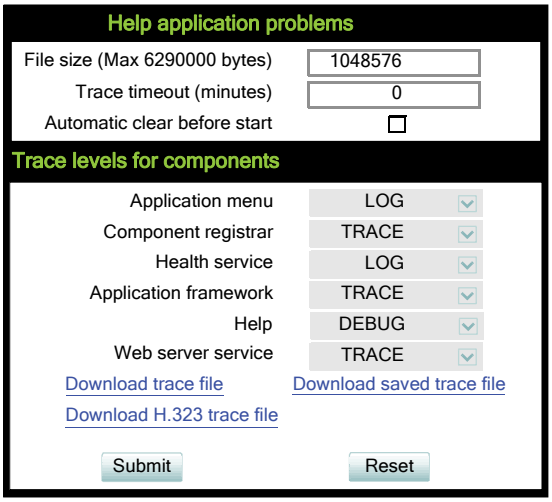
3.20.3.6 HFA registration and security

Diagnostics > EasyTrace Profiles > HFA registration and security



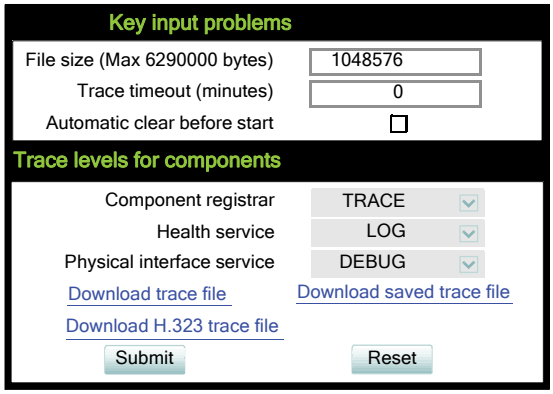
3.20.3.7 Help Application problems

Diagnostics > EasyTrace Profiles > Help application problems



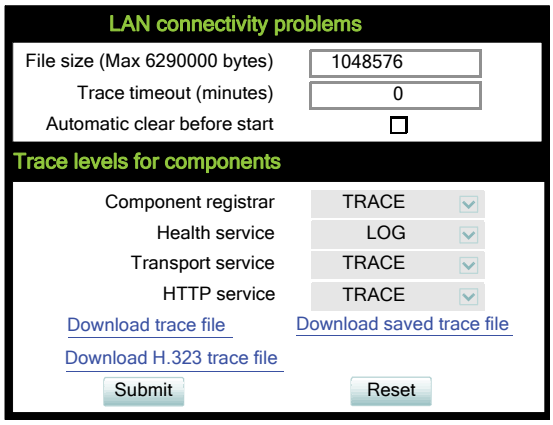
3.20.3.8 Key Input problems

Diagnostics > EasyTrace Profiles > Key input problems



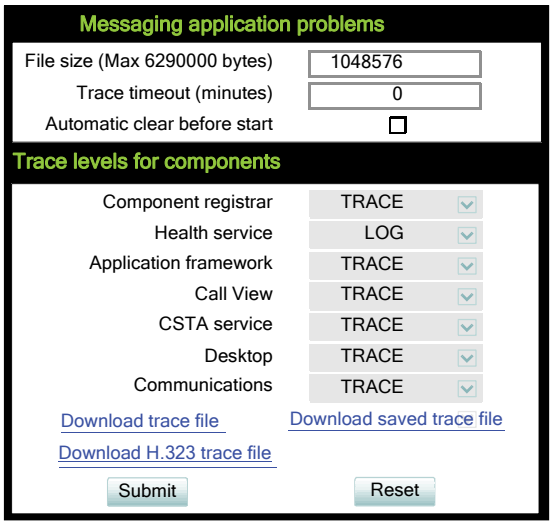
3.20.3.9 LAN Connectivity problems

Diagnostics > EasyTrace Profiles > LAN connectivity problems



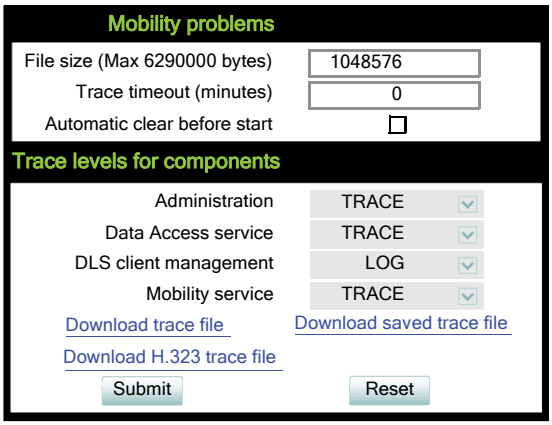
3.20.3.10 Messaging application problems

Diagnostics > EasyTrace Profiles > Messaging application problems



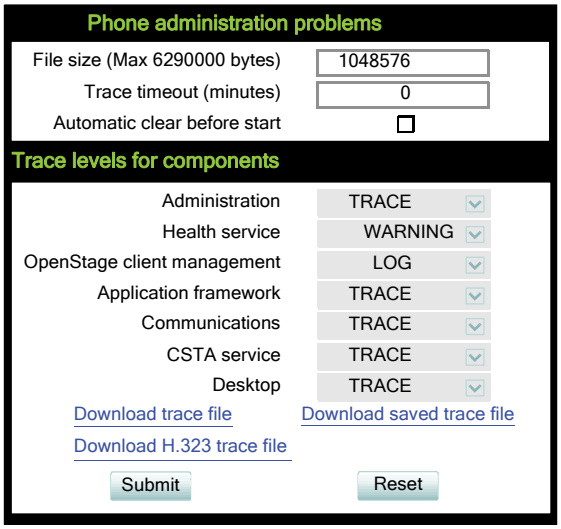
3.20.3.11 Mobility problems

Diagnostics > EasyTrace Profiles > Mobility problems



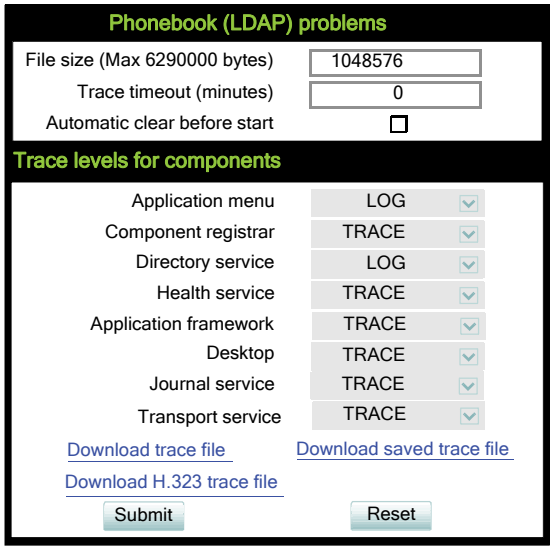
3.20.3.12 Phone administration problems

Diagnostics > EasyTrace Profiles > Phone administration problems



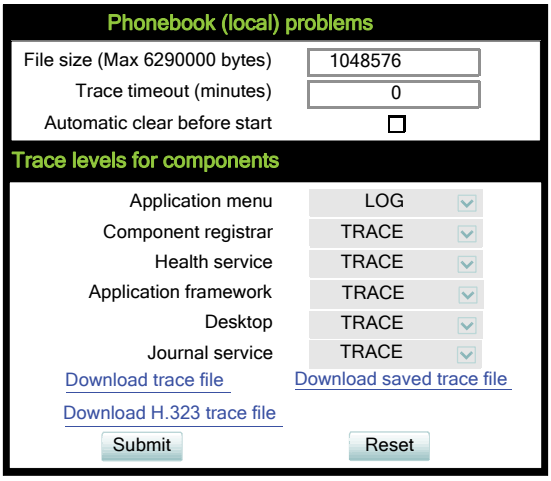
3.20.3.13 Phonebook (LDAP) problems

Diagnostics > EasyTrace Profiles > Phonebook (LDAP) problems



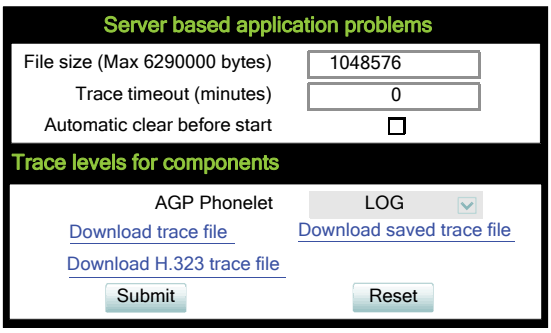
3.20.3.14 Phonebook (local) problems

Diagnostics > EasyTrace Profiles > Phonebook (local) problems



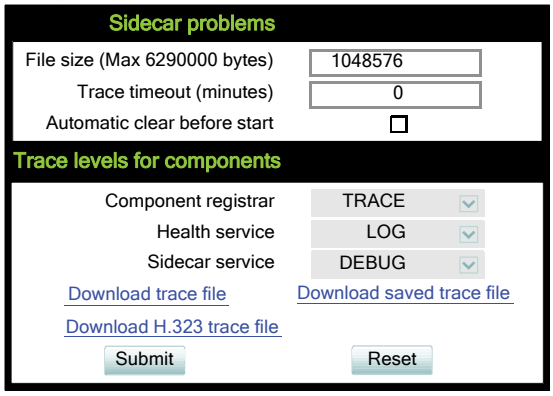
3.20.3.15 Server based application problems

Diagnostics > EasyTrace Profiles > Server based application problems



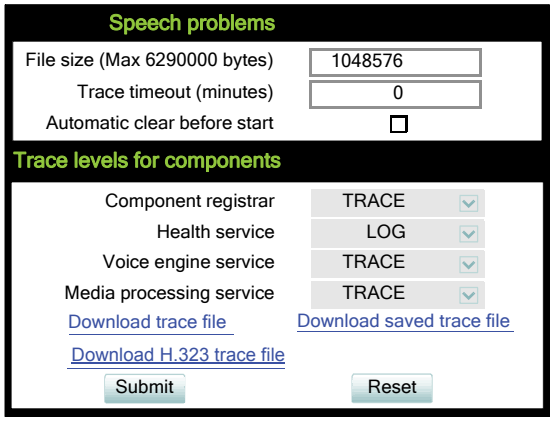
3.20.3.16 Sidecar problems

Diagnostics > Easy Trace Profiles > Sidecar problems



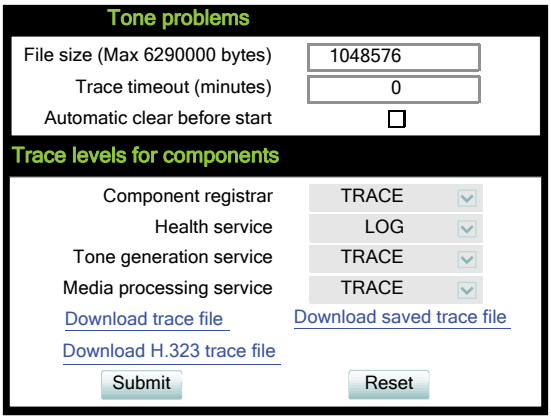
3.20.3.17 Speech problems

Diagnostics > EasyTrace Profiles > Speech problems



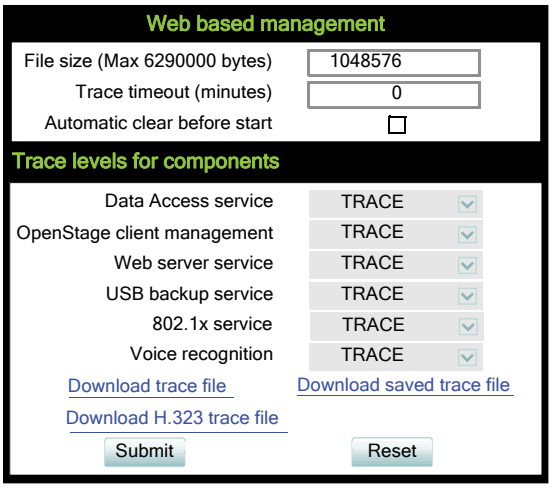
3.20.3.18 Tone problems

Diagnostics > EasyTrace Profiles > Tone problems



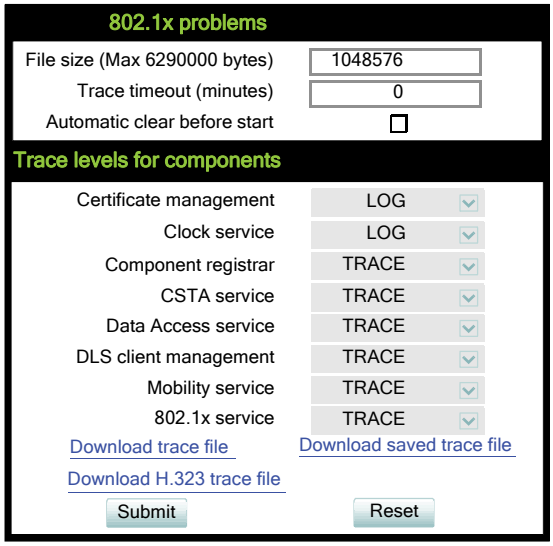
3.20.3.19 Web based management

Diagnostics > EasyTrace Profiles > Web based management



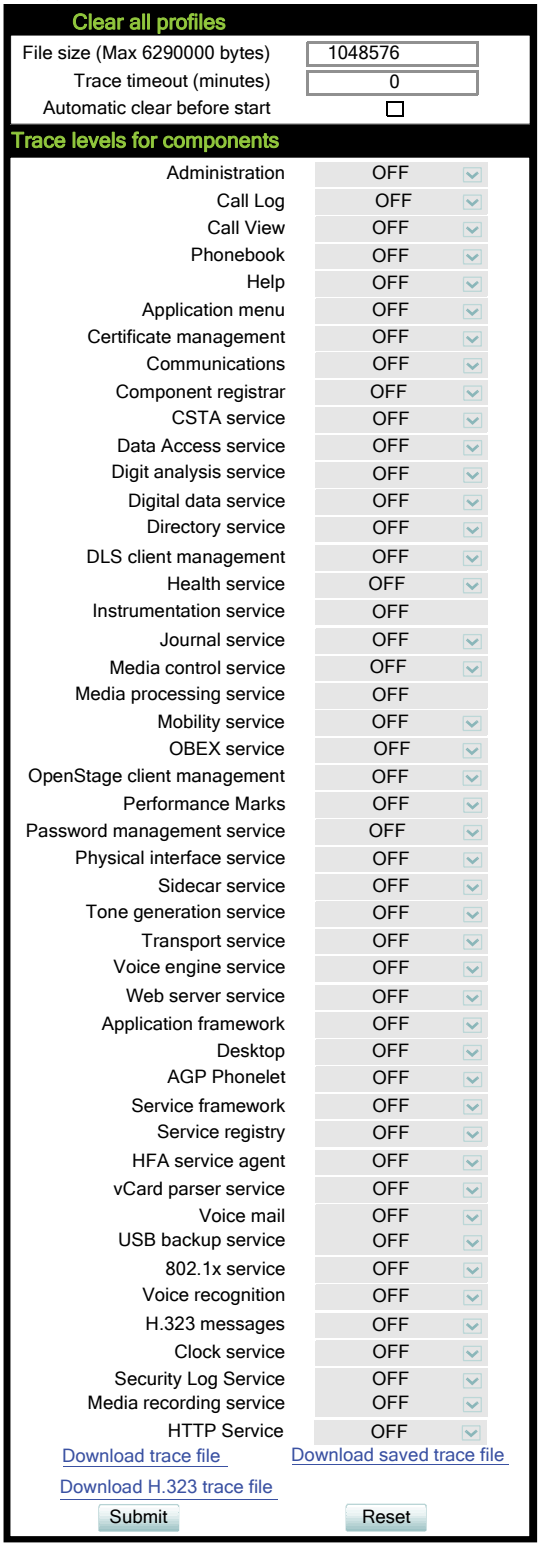
3.20.3.20 802.1x problems

Diagnostics > EasyTrace Profiles > 802.1x problems



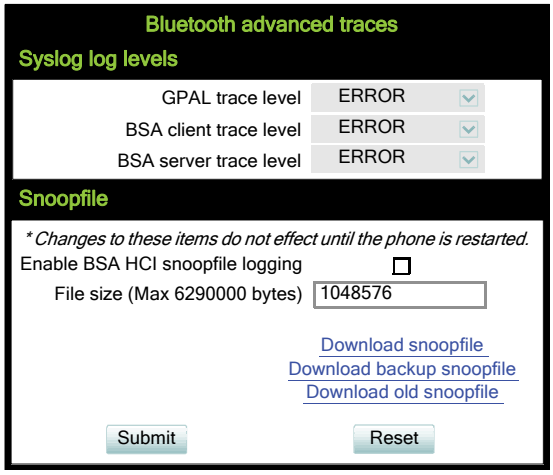
3.20.3.21 No Tracing for All Services

Diagnostics > EasyTrace Profiles > Clear all profiles



3.20.4 Bluetooth advanced traces

Diagnostics > Bluetooth advanced traces



3.20.5 QoS Reports

3.20.5.1 Conditions and Thresholds for Report Generation

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

The generation of QoS (Quality of Service) reports which are sent to a QCU server (see Section 3.3.8, “SNMP”) is configured here.

Data required

- **Report mode**: Sets the conditions for generating a QoS report.
  Value range:
  - "OFF": No reports are generated.
  - "EOS Threshold exceeded": Default value. A report is created if a) a telephone conversation longer than the **Minimum session length** has just ended, and b) a threshold value has been exceeded during the conversation.
  - "EOR Threshold exceeded": A report is created if a) the report interval has just passed, and b) a threshold value has been exceeded during the observation interval.
  - "EOS (End of Session)": A report is created if a telephone conversation longer than the **Minimum session length** has just ended.
  - "EOR (End of Report Interval)": A report is created if the report interval has just passed.
- **Report interval (seconds)**: Time interval between the periodical observations.
  Default: 60
- **Observation interval (seconds)**: During this time interval, the traffic is observed.
  Value: 10
- **Minimum session length (100 millisecond units)**: When the Report mode is set to "EOS Threshold exceeded" or "EOS (End of Session)", a report can be created only if the duration of the conversation exceeds this value.
  Default: 20
- **Maximum jitter (milliseconds)**: When the jitter exceeds this value, a report is generated.
  Default: 20
- **Average round trip delay (milliseconds)**: When the average round trip time exceeds this value, a report is generated.
  Default: 100

Non-compressing codecs:

The following threshold values apply to non-compressing codecs.

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

Compressing codecs:

The following threshold values apply to compressing codecs.

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

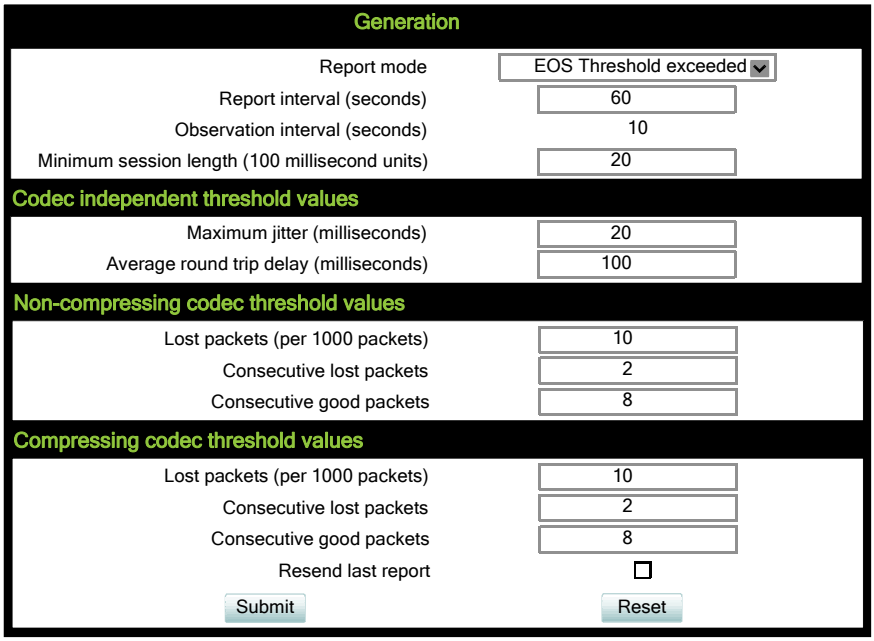
General:

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

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

Administration via WBM

Diagnostics > QoS Reports > Generation



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**

3.20.5.2 View Session Data

OpenScape Desk Phone CP phones generate QoS reports using a HiPath specific format, QDC (**Q**oS **D**ata **C**ollection). The reports created for the last 6 sessions, i. e. conversations, can be viewed on the WBM.

To enable the generation of reports, please ensure that:

- the switch **QoS traps to QCU** (System > SNMP) is activated (see Section 3.3.8, “SNMP”);
- the conditions for the generation of reports are set adequately (see Section 3.20.5.1, “Conditions and Thresholds for Report Generation”).

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

A QoS report contains the following data:

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

- **Maximum jitter**: Maximum jitter (in ms) found during the report interval.
- **Maximum inter-arrival jitter**: Maximum of the interarrival jitter values (in ms). The interarrival jitter is the smoothed absolute value of the jitter measurements. It is calculated continuously. For details about the calulation, 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 phoneis connected in the shelf.
- **Endpoint type**: Type of the local phone.
- **Version**: Software version of the local phone.
- **Subscriber number type**: Type of subscriber number assigned to the local phone. The possible types are:
  - 1: local number, extension only
  - 2: called number, network call
  - 3: E.164 number of the local phone
- **Subscriber number**: Subscriber number of the local phone.
- **Call ID**: SIP call id.
- **MAC address**: MAC address of the local phone.

Data viewing via WBM

Diagnostics > QoS reports > View Session Data

View Session Data

Select a report to view: QoS Statistics 1

Submit

Start of report period - seconds	2011/10/16 21:51:29 UTC
End of report period - seconds	2011/10/16 21:56:36 UTC
SNMP specific trap type	2
IP address (local)	192.168.1.235
Port number (local)	5012
IP address (remote)	192.168.1.202
Port number (remote)	5010
SSRC (receiving)	1481715715
SSRC (sending)	3244864262
Codec	G.711 PCMU
Maximum packet size	20
Silence suppression	0
Count of good packets	15203
Maximum jitter	2
Maximum inter-arrival jitter	0
Periods jitter threshold exceeded	0
Round trip delay	433
Round trip delay threshold exceeded	☐
Count of lost packets	0
Count of discarded packets	0
Periods of lost packets	0
Consecutive packet loss (CPL)	255,255,255,255,255,255,255,255,255,255
Periods of consecutive lost packets	255
Consecutive good packets (CGP)	255,255,255,255,255,255,255,255,255,255
Periods of consecutive good packets	255
Count of jitter buffer overruns	0
Count of jitter buffer under-runs	0
Codec change on the fly	
Periods with at least one threshold exceeded	0
HiPath Switch ID	Asterisk PBX 1.6.2.19
LTU number	255
Slot number	255
Endpoint type	OpenStage 80
Version	V3 R0.50.0 SIP 110924
Subscriber number type	0
Subscriber number	3339
Call ID	05b4445aeaf00008
MAC address	0001e325eaca

3.20.6 Miscellaneous

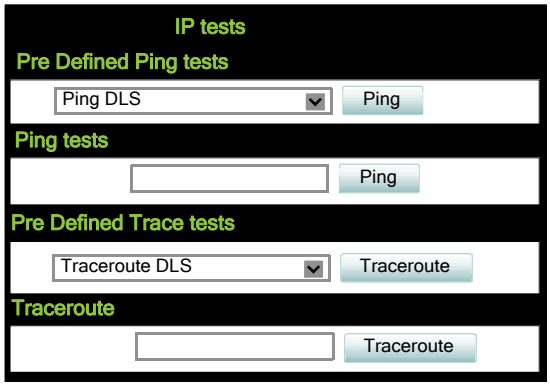
3.20.6.1 IP tests

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

Data required

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

Administration via WBM



3.20.6.2 Memory Status Information

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

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

When **Disable reboot** is checked, no reboot will take place when a memory problem has been found. However, recovery requires a reboot.

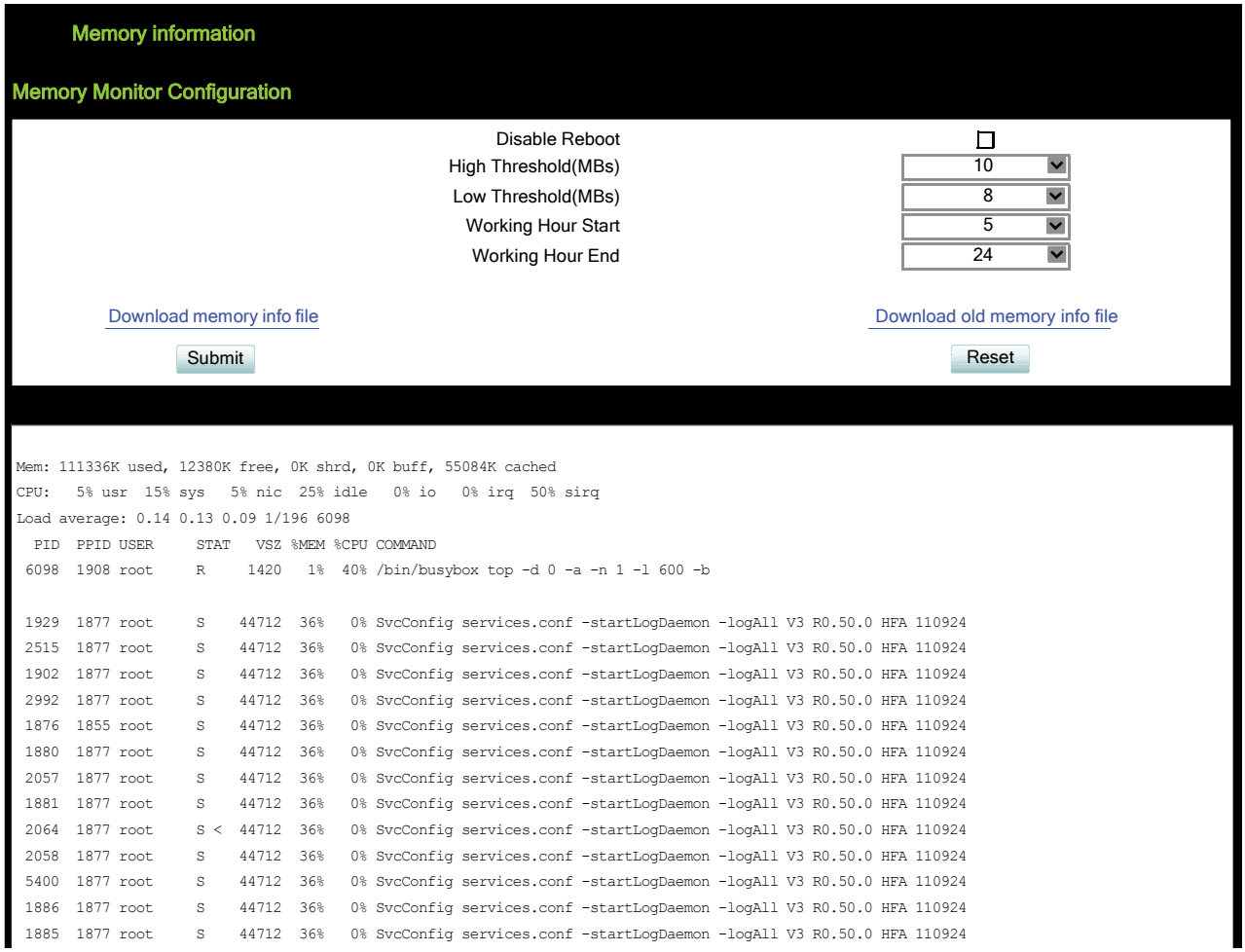
The recovery process will be triggered when the available main memory (RAM) falls below a given threshold value. As memory consumption is assumed to be higher during working hours, two thresholds are configurable. The **High Threshold (MBs)** parameter defines the threshold for off-time. For OpenScape Desk Phone CP200/CP205, the default value is 10 MB, and for OpenScape Desk Phone CP400/600, it is 30 MB. With **Low Threshold (MBs)**, the threshold for off-time is defined. For OpenScape Desk Phone CP200/CP205, the default value is 8 MB, and for OpenScape Desk Phone CP400/600, 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 occured, information about the incident is written to a log file which can be viewed via the **Download memory info file** link. If there has been a previous case of memory shortage, the corresponding log file can be viewed via **Download memory info file**.

Administration via WBM

Diagnostics > Miscellaneous > Memory information



3.20.6.3 Core dump

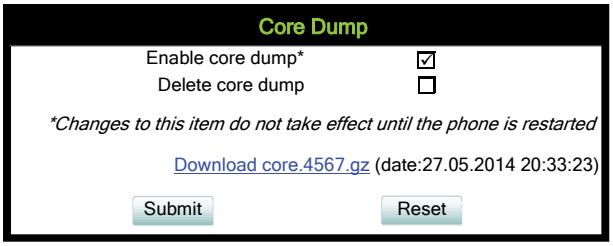
If **Enable core dump** is checked, a core dump will be initiated in case of a severe error. The core dump will be saved to a file. By default, this function is activated.

If **Delete core dump** is activated, the current core dump file is deleted on **Submit**. By default, this is not activated.

If one or more core dump file exist, hyperlinks for downloading will be created automatically.

Administration via WBM

Diagnostics > Miscellaneous > Core Dump



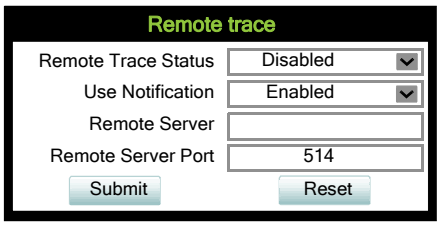
3.20.7 Remote Tracing – Syslog

All trace messages created by the components of the phone software can be sent to a remote server using the syslog protocol. This is helpful especially for long-term observations with a greater number of phones.

To enable remote tracing, **Remote trace status** must be set to "Enabled". Furthermore, the IP address of the server receiving the syslog messages must be entered in **Remote ip**, and the corresponding server port must be given in **Remote port**.

Administration via WBM

Maintenance > Remote trace



Administration via Local Phone

└ --- Admin
  └ --- Maintenance
    └ --- Remote trace
      ├--- **Remote trace status**
      ├--- **Remote ip**
      └ --- **Remote port**

4 Examples and HowTos

4.1 Canonical Dialing

4.1.1 Canonical Dialing Settings

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

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

4.1.2 Canonical Dial Lookup

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>	722	Enterprise node prefix (here: Munich).
International code <2>	+4989722	Equivalent prefix to access numbers on this node from the PSTN. Here, the prefix used by the PSTN for direct inward dialing is identical to the enterprise node prefix.

4.1.2.1 Conversion examples

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

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

User entry		2345
External numbers		Local public form
External access code		Not required
International gateway code		Use national code
Number stored in the phone book		+441159432345
Dial string sent when dialing from the phone book	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		7222345
External numbers		Local public form
External access code		Not required
International gateway code		Use national code
Number stored in the phone book		+49897222345
Dial string sent when dialing from the phone book	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 phone book		+4411511234567
Dial string sent when dialing from the phone book	External numbers = Local public form	234567
	External numbers = National public form	011511234567
	External numbers = International form	004411511234567

4.2 How to Set Up the Corporate Phonebook (LDAP)

LDAP is available only on phones.

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

4.2.1 Prerequisites

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

4.2.2 Create an LDAP Template

The user interface of the corporate phonebook application provides a form which is used both for search and retrieval.

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.

INFO:
In an LDAP template, the entries must be sorted according to the sequential number of the template labels, as shown in the example underneath. It is also recommended to use pre-sorted entries, which will reduce the use of resources.

Generic Example (Standard Attributes)

OpenStage Field	LDAP Template Lables	LDAP Attribute	Example Value
Last name	ATTRIB01	sn	Doe
First name	ATTRIB02	givenName	John
Business 1	ATTRIB03	telephoneNumber	9991234
Business 2	ATTRIB04	facsimileTelephoneNumber	9992345
Mobile	ATTRIB05	mobile	017711223344
Private	ATTRIB06	homePhone	441274333444
Company	ATTRIB07	o	Example Inc.
Address 1	ATTRIB08	departmentNumber	0815
Address 2	ATTRIB09		
Job function	ATTRIB10	title	Product Manager
Email	ATTRIB11	mail	doe@example.com

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

```
OpenStage LDAP TEMPLATE (v.1)
SEARCHBASE="dc=example,dc=com"
ATTRIB01="sn"
```

```
ATTRIB02="givenname"
ATTRIB03="telephoneNumber"
ATTRIB04="facsimileTelephoneNumber"
ATTRIB05="mobile"
ATTRIB06="homePhone"
ATTRIB07="o"
ATTRIB08="departmentNumber"
ATTRIB09=""
ATTRIB10="title"
ATTRIB11="mail"
EOF
```

Microsoft Active Directory Specific Example

OpenStage Field	LDAP Template Attribute	LDAP Attribute	Example Value
Last name	ATTRIB01	sn	Doe
First name	ATTRIB02	givenName	John
Business 1	ATTRIB03	ipPhone	9991234
Business 2	ATTRIB04	otherTelephone	9992345
Mobile	ATTRIB05	mobile	017711223344
Private	ATTRIB06	homePhone	441274333444
Company	ATTRIB07	company	Example Inc.
Address 1	ATTRIB08	department	Administration
Address 2	ATTRIB09		
Job function	ATTRIB10	title	Product Manager
Email	ATTRIB11	mail	doe@example.com

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

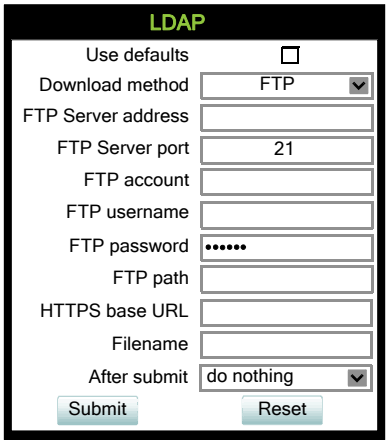
```
OpenStage LDAP TEMPLATE (v.1)
SEARCHBASE="dc=example,dc=com"
ATTRIB01="sn"
ATTRIB02="givenname"
ATTRIB03="ipPhone"
ATTRIB04="otherTelephone"
ATTRIB05="mobile"
ATTRIB06="homePhone"
```

```
ATTRIB07="company"
ATTRIB08="department"
ATTRIB09=""
ATTRIB10="title"
ATTRIB11="mail"
EOF
```

4.2.3 How to Load the LDAP Template into the Phone

When you have configured the LDAP template, you can upload it to the phone:

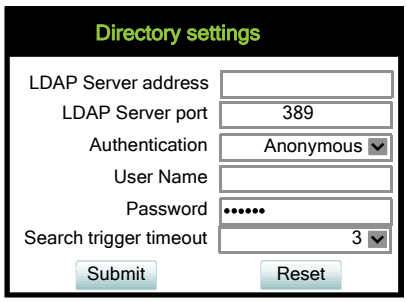
1. Save the template under a suitable name, for example, `ldap-template.txt`.
2. Copy the template file to the FTP server designated for deploying LDAP templates.
3. Upload the file using the WBM (see Section 3.9.5, “LDAP Template”), or, alternatively, the Local menu, or the DLS (see the Deployment Service Administration Manual). For an example configuration, see the following WBM screenshot (WBM path: **File transfer** > LDAP):



4.2.4 Configure LDAP Access

To enter the access data using the WBM, take the following steps:

1. Navigate to **Local Functions** > Directory Settings.
2. Enter the following parameters:
   - **Server address** (IP address or hostname of the LDAP server)
   - **Server port** (port used by the LDAP, typically 389)
   - **Authentication** (authentication method for the connection to the LDAP server)
   - **User name** (only required if simple authentication is selected); **Password** (relating to the user name).



3. Press **Submit**.

4.3 An LLDP-Med Example

The following example illustrates the mode of operation of LLDP-MED. In order to evoke a reaction from LLDP-MED, the LAN switch has been set to auto-negotiation, whereas the phone's LAN port (see Section 3.2.1, "LAN Port Settings") is set to 100Mbit/s, hence a fixed value. This configuration error is detected and displayed by LLDPMED. Please note the status of MAC_Phy config displayed in the local phone´s Admin menu.

1. Log in as administrator on the local phone´s **Admin** menu.
2. In the **Admin menu, navigate to Network > LLDP-MED Operation** using the navigation keys, and click OK.
3. In the LLDP-MED Operation submenu (see *LLDP-MED Operation*), navigate to MAC_Phy config and note the status displayed:
4. Select the MAC_Phy config submenu by pressing OK and navigate to the parameters displayed by using the navigation keys.
   The following status is displayed for the MAC_Phy config parameters:
   AutoSet enabled = Incompatible
   MAU = Incompatible

5 Technical Reference

5.1 Default Port List

The following table contains all default ports, resp. port ranges, and protocols used by the services running on OpenScape Desk Phone IP HFA 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
TCP is used	4060	32786 - 61000	HFA / TCP
TLS is used	4061	32786 - 61000	HFA / TLS
XML applications in phone, connecting to an application server	---	32786 - 61000	HTTP / TCP HTTPS / TCP-TLS
XML Push service	8085	---	HTTP / TCP
XML Push service	443	---	HTTPS / TCP-TLS
Directory access via LDAP	---	32786 - 61000	TCP
DLS contact me service - workpoint side	8085	---	HTTP / TCP
Default communication with the DLS workpoint interface	---	18443	HTTPS / TCP - SSL / TLS
Secure communication with the DLS workpoint interface	---	18444	HTTPS / TCP - SSL / TLS
Connection to the control port of FTP server	21	32786 - 61000	FTP / TCP
FTP client; uses the FTP server in active mode	32786 - 61000	20	FTP / TCP
HTTPS file download server	443	32786 - 61000	HTTPS / TCP - SSL/TLS
Web server for WBM access	8085	---	HTTP / TCP
Secure Web Server for WBM access	443	---	HTTPS / TCP - SSL / TLS
HPT- debug IF (Available only if a dongle file is present on phone.)	65532	---	TCP - SSL/TLS
SSH (Secure Shell Remote Login)	22	---	TCP

5.2 Troubleshooting: Error Codes

For a set of error cases, specific error codes are defined. These error codes are shown in brackets on the display, following a general error note. Example: „No Telephony possible (LP1)“.

Problem	Description	Error code
Network Problem	No network connection	LI1
Not Initialised	Waiting for data	I1
Unable to use LAN	802.1x error	LX1
Unable to use LAN	Physical connection missing	LP1
Unable to Register	Server timeout	RT2
Unable to Register	Server failed	RF2
Unable to Register	Authentication failed	RA2
Unable to Register	No number configured	RN2
Unable to Register	No server configured	RS2
Unable to Register	No registrar configured	RG2
Unable to Register	No DNS domain configured	RD2
Unable to Register	Rejected by server	RR2
Unable to Register	No phone IP address set	RI2
Survivability	Backup route active	B8
Survivability	Backup not configured	RS8
Survivability	Backup timeout	RT8
Survivability	Backup authentication failed	RA8
Cloud-Deployment abandoned by user	Cloud-Deployment abandoned by user Occurs when the pin prompt is dismissed	AU

Tabelle 5-1 Troubleshooting Error Codes

A special “fast-busy” tone (also called congestion tone) is played if a temporary network problem causes a user-initiated call action to fail. Typical call actions: making an outgoing call; picking up a call from Manual Hold; or Group pickup. Phone users and mobile users logged on to the phone. The special tone is triggered if one of the following SIP response codes is received from the server:
606, 408, or 503.

http://wiki.unify.com/wiki/_SIP_FAQ#Error_codes

5.3 Troubleshooting: Error Messages

The following table lists the possible error messages for OpenScape HFA phones and provides possible causes and explanations, where applicable.

Error Message	Error Code	Error Condition	Error Cause
No Telephony possible	D02	Unable to contact DHCP	
No Telephony possible	H[2	Unable to register HFA main line	Logoff: Forced client logoff due to an incorrect PreSharedSecret
No Telephony possible	H02	Unable to register HFA main line	General Error
No Telephony possible	H12	Unable to register HFA main line	No IP address
No Telephony possible	H22	Unable to register HFA main line	No default route
No Telephony possible	H32	Unable to register HFA main line	No mask
No Telephony possible	H42	Unable to register HFA main line	No gateway IP address
No Telephony possible	H52	Unable to register HFA main line	No subscriber number
No Telephony possible	H62	Unable to register HFA main line	Tc-logon timeout
No Telephony possible	Ha2	Unable to register HFA main line	Logon: Rejected due to missing LIN
No Telephony possible	HA2	Unable to register HFA main line	Logon: Maintenance busy
No Telephony possible	Hb2	Unable to register HFA main line	Logon: Rejected due to invalid LIN
No Telephony possible	HB2	Unable to register HFA main line	Logon: No port available
No Telephony possible	Hc2	Unable to register HFA main line	Logon: Rejected due to mobile terminal blokked

Table 5-2 Error Messages

Error Message	Error Code	Error Condition	Error Cause
No Telephony possible	Hd2	Unable to register HFA main line	Logon: Rejected due to incompatible security profile
No Telephony possible	HD2	Unable to register HFA main line	Logon: No port ext available
No Telephony possible	He2	Unable to register HFA main line	Logon: Rejected due to TCP usage while TLS is required
No Telephony possible	HE2	Unable to register HFA main line	Logon: Client not registered
No Telephony possible	HF2	Unable to register HFA main line	Logon: Rejected due to Logoff
No Telephony possible	HG2	Unable to register HFA main line	Logon: Rejected due to Logoff progress
No Telephony possible	HH2	Unable to register HFA main line	Logon: Rejected due to Shutdown
No Telephony possible	HI2	Unable to register HFA main line	Logon: Rejected due to duplicate Logon
No Telephony possible	HJ2	Unable to register HFA main line	Logon: Rejected due to already logged on
No Telephony possible	HK2	Unable to register HFA main line	Logon: Rejected due to PIN not present
No Telephony possible	HL2	Unable to register HFA main line	Logon: Rejected due to password not present
No Telephony possible	HM2	Unable to register HFA main line	Logon: Rejected due to password not correct
No Telephony possible	HN2	Unable to register HFA main line	Logon: Rejected due to invalid license
No Telephony possible	HQ2	Unable to register HFA main line	Logoff: Normal Logoff
No Telephony possible	HR2	Unable to register HFA main line	Logoff: Client not logged on
No Telephony possible	HS2	Unable to register HFA main line	Logoff: Client logged off

Table 5-2 Error Messages

Error Message	Error Code	Error Condition	Error Cause
No Telephony possible	HT2	Unable to register HFA main line	Logoff: Forced client logoff
No Telephony possible	HU2	Unable to register HFA main line	Logoff: Timeout expired
No Telephony possible	HV2	Unable to register HFA main line	Logoff: OMCaction
No Telephony possible	HW2	Unable to register HFA main line	Logoff: HFA mobile user logged on
No Telephony possible	HX2	Unable to register HFA main line	Logoff: Switch back to central system
No Telephony possible	HY2	Unable to register HFA main line	Logoff: No bearer channel
No Telephony possible	HZ2	Unable to register HFA main line	Logoff: New logon requested from the server
No Telephony possible	IR1	Not Initialised	CorNet-TC logon Conf received
No Telephony possible	IS1	Not Initialised	CorNet-TC logon sent
No Telephony possible	LP1	Unable to use the LAN	Physical Connection
No Telephony possible	LX1	Unable to use the LAN	802.1x errors
No Telephony possible	RA2	Unable to register main line	Authentication failed
No Telephony possible	TP2	Unable to establish a TLS connection	To PC
No Telephony possible	TT2	Unable to establish a TLS connection	No SNTP server
Reduced Telephony functions	M3	Unable to contact the DLS for mobility logon	

Table 5-2 Error Messages

Glossary

A

ADPCM
Adaptive **D**ifferential **P**ulse **C**ode **M**odulation. A compressed encoding method for audio signals which are to be transmitted by a low bandwidth. As opposed to regular -> PCM, 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.

C

CSTA
Computer **S**upported **T**elecommunications **A**pplications. An abstraction layer for telecommunications applications allowing for the interaction of -> CTI computer applications with telephony devices and networks.

CTI
Computer **T**elephony **I**ntegration. This term denotes the interaction of computer applications with telephony devices and networks.

D

DFT
Digital **F**eature **T**elephone. A phone with no line keys.

DHCP
Dynamic **H**ost **C**onfiguration **P**rotocol. Allows for the automatic configuration of network endpoints, like IP Phones and IP Clients.

DiffServ
Differentiated **Serv**ices. Specifies a layer 3 mechanism for classifying and managing network traffic and providing quality of service (-> QoS) guarantees on -> IP networks. DiffServ can be used to provide low-latency, guaranteed service for e. g. voice communication.

DLS
The Deployment Service (DLS) is a OpenScape management application for the administration of workpoints, i. e. IP Phones and IP Clients, in both HiPath- and non-HiPath networks.

DNS
Domain **N**ame **S**ystem. Performs the translation of network domain names and computer hostnames to -> IP addresses.

DTMF

Dual **T**one **M**ulti **F**requency. A means of signaling between a phone and e. g. a voicemail facility. The signals can be transmitted either in-band, i. e. within the speech band, or out-band, i. e. in a separate signaling channel.

E

EAP

Extensible **A**uthentication **P**rotocol. An authentication framework that is frequently used in WLAN networks. It is defined in RFC 3748.

F

FTP

File **T**ransfer **P**rotocol. Used for transferring files in networks, e. g., to update telephone software.

G

G.711

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

G.722

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

G.729

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

Gateway

Mediation components between two different network types, e. g., -> IP network and ISDN network.

H

HTTP

Hyper**t**ext **T**ransfer **P**rotocol. A standard protocol for data transfer in -> IP networks.

I

IP
Internet **P**rotocol. A data-oriented network layer protocol used for transferring data across a packet-switched internetwork. Within this network layer, reliability is not guaranteed.

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

J

Jitter
Latency fluctuations in the data transmission resulting in distorted sound.

L

LAN
Local **A**rea **N**etwork. 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 **C**rystal **D**isplay. Display of numbers, text or graphics with the help of liquid crystal technology.

LDAP
Lightweight **D**irectory **A**ccess **P**rotocol. Simplified protocol for accessing standardized directory systems, e.g., a company telephone directory.

LED
Light **E**mitting **D**iode. Cold light illumination in different colours at low power consumption.

M

MAC Address
Media **A**ccess **C**ontrol address. Unique 48-bit identifier attached to network adapters.

MDI-X

Media **D**ependent **I**nterface 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 **I**nformation **B**ase. A type of database used to manage the devices in a communications network.

MWI

Message **W**aiting **I**ndicator. A signal, typically a LED, to notify the user that new mailbox messages have arrived.

P

PBX

Private **B**ranch E**x**change. Private telephone system that connects the internal devices to each other and to the ISDN network.

PCM

Pulse **C**ode **M**odulation. A digital representation of an analog signal, e. g. audio data, which consists of quantized samples taken in regular time intervals.

PING

Packet **In**ternet **G**ro(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 **o**ver **E**thernet. The IEEE 802.3af standard specifies how to supply power to compliant devices over Ethernet cabling (10/100Base-T).

Port

Ports are used in -> IP networks to permit several communication connections simultaneously. Different services often have different port numbers.

PSTN

Public **S**witched **T**elephone **N**etwork. The network of the world's public circuit-switched telephone networks.

Q

QoS

Quality **o**f **S**ervice. 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).

R

RAM
Random **A**ccess **M**emory. Memory with read / write access.

ROM
Read **O**nly **M**emory. Memory with read only access.

RTCP
Realtime **T**ransport **C**ontrol **P**rotocol. Controls the -> RTP stream and provides information about the status of the transmission, like QoS parameters.

RTP
Realtime **T**ransport **P**rotocol. This application layer protocol has been designed for audio communication.

S

SDP
Session **D**escription **P**rotocol. Describes and initiates multimedia sessions, like web conferences. The informations provided by SDP can be processed by -> SNMP.

SNMP
Simple **N**etwork **M**anagement **P**rotocol. Used for monitoring, controlling, and administration of network and network devices.

SNTP
Simple **N**etwork **T**ime **P**rotocol. Used to synchronize the time of a terminal device with a timeserver.

Subnet Mask
To discern the network part from the host part of an -> IP address, 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 -> MAC Addresses: data targeted to a specific device is directed to the switch port that device is attached to.

T

TCP
Transfer **C**ontrol **P**rotocol. 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 **L**ayer **S**ecurity. Ensures privacy between communicating applications. Typically, the server is authenticated, but mutual authentication is also possible.

U

URI
Uniform **R**esource **I**dentifier. A compact string of characters used to identify or name a resource.

URL
Uniform **R**esource **L**ocator. A special type of -> URI which provides means of acting upon or obtaining a representation of the resource by describing its primary access mechanism or network location.

V

VLAN
Virtual **L**ocal **A**rea **N**etwork. 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 **o**ver **IP**. A term for the protocols and technologies enabling the routing of voice conversations over the internet or through any other -> IP-based network

W

WAP
Wireless **A**pplication **P**rotocol. A collection of protocols and technologies aiming at enabling access to internet applications for wireless devices. WAP can also be used by the OpenScape Desk Phone CP phone.

WBM
Web **B**ased **M**anagement. A web interface which enables configuration of the device using a standard web browser.

WML

Wireless **M**arkup **L**anguage. An XML-based markup language which supports text, graphics, hyperlinks and forms on a -> WAP-browser.

WSP

Wireless **S**ession **P**rotocol. The protocol is a part of the -> WAP specification. Its task is to establish a session between the terminal device and the WAP gateway.

Index

A

Administration Menu (Local Menu) 23, 24

B

Bluetooth
- Interface activation/deactivation 45

C

Canonical Dial Lookup 85
Canonical Dialing 82
Codec Preferences 123
Connectors 17
Core dump 165
Corporate Phonebook 118
CSTA 181
CTI 181

D

Date and Time (SNTP) 76
Daylight Saving 76
Default Route 58
DFT 181
DHCP 55, 181
Diffserv 53
Directory Settings 118
DLS (Deployment Service) 15, 35, 62, 181
DNS 60, 181
- Domain Name 60

Dongle Key (Download) 114
DST Zone (Daylight Saving Time Zone) 77

E

Easy Trace Profiles 142
- 802.1x 152, 154
- Call Connection 142
- Call Log 143
- DAS Connection 144
- DLS Data Errors 144
- Help Application 145
- Key Input 146
- LAN Connectivity 146
- Local Phonebook 148, 149
- Mobility 147
- No Tracing for All Services 153
- Phone administration 148
- Server based applications 149
- Speech 150
- Tone 151
- Web Based Management 151

Emergency Number 82
Energy Saving 76
Error Codes 177
External Access Code 83
External Numbers 83

F

Factory Reset 129
Fault Trace Configuration 136
FTP Settings 92

G

G.711 123
G.722 123
G.729 123
Gateway 58
General Information 125

I

Initial Digits 83
Internal Numbers 83
International Code (Local Country Code) 82
International Gateway Code 84
International Prefix (International Access Code) 82
IP
- Address 25, 57
- Address (Manual configuration) 57
- IP 183
- Specific Routing 59

K

Key module (phone types) 21

L

LAN 183

Monitoring 134
Port 46
Layer 2 52
Layer 3 53
LDAP 118, 183
LDAP Template (Download) 104
License Information 131
LLDP-MED 134
Local Country Code (International Code) 82
Local Enterprise Number 82
Local National Code (Local Area Code) 82

M

MAC Address 183
MDI-X 46, 184
MIB 184
Monitoring 134
MWI (Message Waiting Indicator) 184

N

National Prefix (Trunk Prefix) 82
Network port configuration 47

O

OCSP 127
Operator Code 82

P

Password
Change 126
Lost 127
PBX 184
PC port 46
Phone
Restart 129
Phone software (Download) 95
Phonebook 118
Picture Clips (Download) 101
PoE (Power over Ethernet) 20, 184
Port configuration 47
Port List 176
Power Consumption/Supply 20
PSTN 184
PSTN Access Code 82

Q

QCU 65
QoS 52
QoS Reports 155
Quick Start 22

R

Remote Tracing – Syslog 166
Reset Factory 129
Restart Phone 129
Ringer File 110
RTP 185
Base Port 122

S

Screensaver (Download) 107
Secure
file transfer 128
SIP server 128
Shipment 16
Silence suppression 123
SNMP 64, 185
SSH – Secure Shell Access 130
Subnet Mask 25
Subnet Mask (Manual configuration) 57

T

TCP 186
Timezone Offset 76
TLS 186
Trace Configuration 136
Trace Profiles 142
Traps 64

U

UDP 186
Update Service 62

V

Vendor Class (DHCP) 28, 35
VLAN 28, 48

W

WBM (Web Based Management) 15, 22, 186