



OpenScape Desk Phone IP Phone Administration HFA

Administration Manual

A31003-D3030-M100-02-76A9

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 GmbH & Co. KG 07/2014
Hofmannstr. 51, 81379 Munich/Germany

All rights reserved.

Reference No.: A31003-D3030-M100-02-76A9

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 GmbH & Co. KG. All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

Content

1 Overview	1-6
1.1 Important Notes	1-6
1.2 Maintenance Notes	1-7
1.3 About the Manual	1-7
1.4 Conventions for this Document	1-8
1.5 The OpenScape Desk Phone Family	1-9
1.5.1 OpenScape Desk Phone IP 55G	1-9
1.5.2 OpenScape Desk Phone IP 35G	1-11
1.6 Administration Interfaces	1-13
1.6.1 Web-based Management (WBM)	1-13
1.6.2 DLS (OpenScape Deployment Service)	1-13
1.6.3 Local Phone Menu	1-13
2 Startup	2-14
2.1 Prerequisites	2-14
2.2 Assembling and Installing the Phone	2-14
2.2.1 Shipment	2-14
2.2.2 Connectors at the bottom side	2-15
2.2.3 Assembly	2-16
2.2.4 How to Connect the Phone	2-17
2.2.5 How to Better Use LAN Network Connections	2-18
2.2.6 Key Module	2-19
2.2.7 Using Multilingual User Interface	2-19
2.3 Quick Start	2-20
2.3.1 How to Access the Web Interface (WBM)	2-20
2.3.2 How to Set the Terminal Number	2-21
2.3.3 Basic Network Configuration	2-22
2.3.4 Extended Network Configuration	2-23
2.3.5 VLAN Discovery	2-23
2.3.5.1 Using a Vendor Class	2-23
2.3.5.2 Using Option #43 "Vendor Specific"	2-29
2.3.6 DLS Server Address	2-31
2.3.6.1 Using Vendor Class	2-31
2.3.6.2 Using Option #43 "Vendor Specific"	2-38
2.3.7 HFA Gateway Settings	2-40
2.3.8 Using the Web Interface (WBM)	2-40
2.3.9 Using the Local Menu	2-40
3 Administration	3-42
3.1 Access via Local Phone	3-42
3.2 LAN Settings	3-45

Content

3.2.1 LAN Port Settings	3-45
3.2.2 VLAN	3-47
3.2.2.1 Automatic VLAN discovery using LLDP-MED	3-49
3.2.2.2 Manual configuration of a VLAN ID	3-51
3.3 IP Network Parameters	3-52
3.3.1 Quality of Service (QoS)	3-52
3.3.1.1 Layer 2 / 802.1p	3-52
3.3.1.2 Layer 3 / Diffserv	3-53
3.3.2 Use DHCP	3-55
3.3.3 IP Address - Manual Configuration	3-57
3.3.4 Default Route/Gateway	3-58
3.3.5 Specific IP Routing	3-59
3.3.6 DNS	3-60
3.3.6.1 DNS Domain Name	3-60
3.3.6.2 DNS Servers	3-61
3.3.6.3 Terminal Hostname	3-63
3.3.7 Configuration & Update Service (DLS)	3-64
3.3.8 SNMP	3-66
3.4 OpenScape Service Menu	3-69
3.5 System Settings	3-70
3.5.1 System Identity	3-70
3.5.2 HFA Gateway Settings	3-70
3.5.3 HFA Emergency Gateway Settings	3-72
3.5.4 Server and Standby Server ports	3-73
3.5.5 Redundancy	3-74
3.5.6 Emergency number	3-76
3.5.7 LIN	3-76
3.5.8 Not Used Timeout.	3-77
3.5.9 Feature access	3-77
3.5.10 Energy Saving (OpenScape Desk Phone IP 55G)	3-79
3.5.11 Date and Time	3-79
3.5.11.1 SNTP is Available, but no Automatic Configuration by DHCP Server	3-80
3.5.12 Security	3-82
3.5.12.1 System	3-82
3.5.12.2 Access control	3-84
3.6 Dialing	3-85
3.6.1 Canonical Dialing Configuration	3-85
3.6.2 Canonical Dial Lookup	3-89
3.7 Distinctive Ringing	3-91
3.8 User Mobility	3-95
3.8.1 Platform Specific Behaviour	3-96
3.9 Transferring Phone Software, Application, and Media Files	3-98
3.9.1 FTP/HTTPS Server	3-98
3.9.2 Common FTP/HTTPS Settings (Defaults)	3-98

3.9.3 Phone Application	3-100
3.9.3.1 FTP/HTTPS Access Data	3-100
3.9.3.2 Download/Update Phone Application	3-102
3.9.4 Picture Clips	3-103
3.9.4.1 FTP/HTTPS Access Data	3-103
3.9.4.2 Download Picture Clip	3-105
3.9.5 LDAP Template	3-106
3.9.5.1 FTP/HTTPS Access Data	3-106
3.9.5.2 Download LDAP Template	3-108
3.9.6 Logo	3-109
3.9.6.1 FTP/HTTPS Access Data	3-109
3.9.6.2 Download Logo	3-111
3.9.7 Screensaver	3-112
3.9.7.1 FTP/HTTPS Access Data	3-112
3.9.7.2 Download Screensaver	3-114
3.9.8 Ringer File	3-115
3.9.8.1 FTP/HTTPS Access Data	3-116
3.9.8.2 Download Ringer File	3-118
3.9.9 Dongle Key	3-119
3.9.9.1 FTP/HTTPS Access Data	3-119
3.9.9.2 Download Dongle Key File	3-121
3.10 Corporate Phonebook: Directory Settings	3-122
3.10.1 LDAP	3-122
3.10.2 Picture via LDAP	3-124
3.10.2.1 "Softgate V6" settings for central access to subscriber pictures	3-125
3.10.2.2 Local Phone Configuration	3-125
3.10.2.3 Phone Canonical Settings	3-128
3.11 Speech	3-129
3.11.1 RTP Base Port	3-129
3.11.2 Codec Preferences	3-130
3.11.3 Display General Phone Information	3-132
3.12 Applications	3-133
3.12.1 XML Applications/Xpressions(OpenScape Desk Phone IP 55G)	3-133
3.12.1.1 Setup/Configuration	3-133
3.12.1.2 HTTP Proxy	3-139
3.12.1.3 Modify an Existing Application	3-141
3.12.1.4 Remove an Existing Application	3-142
3.13 Password	3-143
3.14 Troubleshooting: Lost Password	3-144
3.15 Restart Phone	3-144
3.16 Factory Reset	3-144
3.17 SSH – Secure Shell Access	3-145
3.18 Display License Information	3-146
3.19 HPT Interface (For Service Staff)	3-146

Content

3.20	Diagnostics	3-147
3.20.1	LLDP-MED	3-148
3.20.2	Fault Trace Configuration	3-150
3.20.3	EasyTrace Profiles	3-156
3.20.3.1	Call Connection	3-156
3.20.3.2	Call Log Problems	3-157
3.20.3.3	DAS Connection	3-157
3.20.3.4	DLS Data Errors	3-158
3.20.3.5	HFA registration and security	3-158
3.20.3.6	Help Application	3-159
3.20.3.7	Key Input	3-159
3.20.3.8	LAN Connectivity	3-160
3.20.3.9	Messaging	3-160
3.20.3.10	Mobility	3-161
3.20.3.11	Phone administration	3-161
3.20.3.12	Local Phonebook	3-162
3.20.3.13	LDAP Phonebook	3-162
3.20.3.14	Server based applications	3-163
3.20.3.15	Sidecar	3-163
3.20.3.16	Speech	3-163
3.20.3.17	Tone	3-164
3.20.3.18	USB Backup/Restore	3-164
3.20.3.19	Web Based Management	3-165
3.20.3.20	802.1x problems	3-165
3.20.3.21	No Tracing for All Services	3-166
3.20.4	QoS Reports	3-167
3.20.4.1	Conditions and Thresholds for Report Generation	3-167
3.20.5	Miscellaneous	3-170
3.20.5.1	IP tests	3-170
3.20.5.2	Memory Status Information	3-171
3.20.5.3	Core dump	3-173
3.20.6	Remote Tracing – Syslog	3-174
4	Examples and HowTos	4-175
4.1	Canonical Dialing	4-175
4.1.1	Canonical Dialing Settings	4-175
4.1.2	Canonical Dial Lookup	4-176
4.1.2.1	Conversion examples	4-177
4.2	How to Create Logo Files for OpenScape Desk Phone	4-179
4.2.1	For OpenScape Desk Phone IP 55G	4-179
4.3	How to Set Up the Corporate Phonebook (LDAP)	4-182
4.3.1	Prerequisites	4-182
4.3.2	Create an LDAP Template	4-183
4.3.3	How to Load the LDAP Template into the Phone	4-186
4.3.4	Configure LDAP Access	4-187

4.3.5 Test	4-187
4.4 An LLDP-Med Example	4-190
5 Technical Reference	5-192
5.1 Default Port List	5-192
5.2 Troubleshooting: Error Codes	5-193
5.3 Troubleshooting: Error Messages	5-195
Glossary	6-199
Index	7-207

1 Overview

1.1 Important Notes



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



For safety reasons the phone should only be operating using the supplied plug in power unit.



Use only original accessories. The use of other accessories may be hazardous and will render the warranty, extended manufacturer's liability and the CE marking invalid.



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 operate 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 About the Manual

The instructions within this manual will help you in administering and maintaining the OpenScape phone. 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 phone and who have a fundamental understanding of VoIP, HFA, and IP networking. The tasks described in this guide are not intended for end users. Many of these tasks affect the ability of a phone to function on the network and require an understanding of IP networking and telephony concepts.

These instructions are laid out in a user-oriented manner, which means that you are led through the functions of the OpenScape phone 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/>).

Overview

Conventions for this Document

1.4 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.

As some WBM input masks have been changed with firmware updates, the screenshots are selected after the following rules:

- If a later version contains more or less parameters compared to previous software versions, the screenshot of the older version is shown.
- If the title of a mask (e.g. "Pixel saver" vs. "Energy saving") or the name of a parameter (e.g. "Time Zone" vs. "DST zone") has changed, the later version is shown.
- If a parameter has moved from one mask to another, both older and later versions are shown. The same is true for the local menu paths.

1.5 The OpenScape Desk Phone Family

The OpenScape Desk Phone Family comprises the following devices.

- Section 1.5.1, “OpenScape Desk Phone IP 55G”
- Section 1.5.2, “OpenScape Desk Phone IP 35G”

1.5.1 OpenScape Desk Phone IP 55G



Overview

The OpenScape Desk Phone Family

1	You can make and receive calls as normal using the handset .
2	The large graphic display permits intuitive operation of the phone.
3	<p>The Mode Keys allow easy operation of the applications featured on your telephone. To select a tab within a function press the relevant key repeatedly until the required tab is displayed.</p> <p>Phone: Display telephony interface Directory: Display phonebooks Call Log: Display call lists Message: Display voicemails Services: Display Program/Service menu/Applications menu</p>
4	Use the Navigation Block to conveniently navigate through the applications on your telephone.
5	You can customise your telephone by assigning phone numbers and functions to the Programmable Keys
6	<p>The Function Keys allow you to call up frequently used functions during a call (e.g. call forwarding, call transfer)</p> <p>Forward: Activate/deactivate call forwarding. Transfer: Transfers calls to other destinations. Conference: Provides access to the conferencing features. Hold: Places an ongoing call on hold or reconnects a held call.</p>
7	<p>The Audio Keys allow you to optimally configure the audio features on your telephone</p> <p>Speaker: Turns on/off the hands-free mode (speakerphone). Headset: Switches the audio sound to the headset or back from the headset to the handset speaker/speakerphone. Vol. + and Vol. -: Increases/decreases the speaker/headset and handset volume. Mute: Turns off/on the microphone during conversations. This feature is used to prevent the listening party from hearing what is being said at the calling party's location or to prevent noise from being transmitted to all participants in conference calls.</p>
8	The Softkeys allow you to call up context-dependent functions (e.g. Repeat dialling).
9	Incoming calls and new voicemails are visually signalled via the Call Display .
10	The Keypad can be used to enter phone numbers and write text.

Tabelle 1-1

1.5.2 OpenScape Desk Phone IP 35G



Overview

The OpenScape Desk Phone Family

1	With the Handset , the user can pick up and dial calls in the usual manner.
2	The Display provides intuitive support for telephone operation and allows the user to control the phone settings via the local User menu (the display offers two lines with up to 33 characters each).
3	<p>The Fixed Function Keys (not re-programmable) provide access to frequently used telephony functions, as follows:</p> <p>Messages: Provides access to the Call Log, allowing the user to view and manage the lists of Missed Calls, Dialled Calls, Received Calls, Forwarded Calls and to access and manage the Voice Mail.</p> <p>Settings: Provides access to the User menus for locally controlling the phone settings.</p> <p>Speaker: Turns on/off the hands-free mode (speakerphone).</p> <p>Headset: Switches the audio sound to the headset or back from the headset to the handset speaker/speaker phone.</p> <p>Vol.+ and Vol.-: increases/decreases the speaker/headset volume.</p> <p>Mute: Turns on/off the microphone during conversations. This feature is used to prevent the listening party from hearing what is being said at the calling party's location or to prevent noise from being transmitted to all participants in conference calls.</p>
4	With the Navigation Keys , the user can navigate through the various phone functions, applications and configuration menus.
5	<p>The Fixed Function Keys (re-programmable via WBM) provide access to frequently used telephony functions, as follows:</p> <p>Transfer: Transfers calls to other destinations.</p> <p>Conference: Provides access to the conferencing features. By default, pressing this key automatically seizes an outgoing line and turns on the hands-free mode.</p> <p>Hold: Places an ongoing call on hold or reconnects a held call.</p>
6	The Keypad is provided for input of phone numbers, codes and text.
7	<p>The Free Programmable Keys enable the user to customise the telephone in line with his/her personal needs by assigning individual phone numbers and functions.</p> <p>Preset default values:</p> <ul style="list-style-type: none">• Forward• Pick up• Do Not Disturb (DND).
8	Inbound calls are visually signalled via the Alert Bar .

Tabelle 1-2

1.6 Administration Interfaces

You can configure the OpenStage phone by using any of the methods described in this chapter.

1.6.1 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.

1.6.2 DLS (OpenScape Deployment Service)

The OpenScape Deployment Service (DLS) is an OpenScape Management application for administering phones and soft clients in communication 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.

1.6.3 Local Phone Menu

This method provides direct configuration of the OpenScape phone. 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 OpenStage phone acts as an endpoint client on an IP telephony network, and has the following network requirements:

- An Ethernet connection to a network with HFA clients and servers.



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

- A OpenScape Business or OpenScape 4000 V7 Communications System
- Usage of Voice VLANs is recommended.
- An FTP Server for file transfer, e. g. firmware, configuration data, application software
- 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.

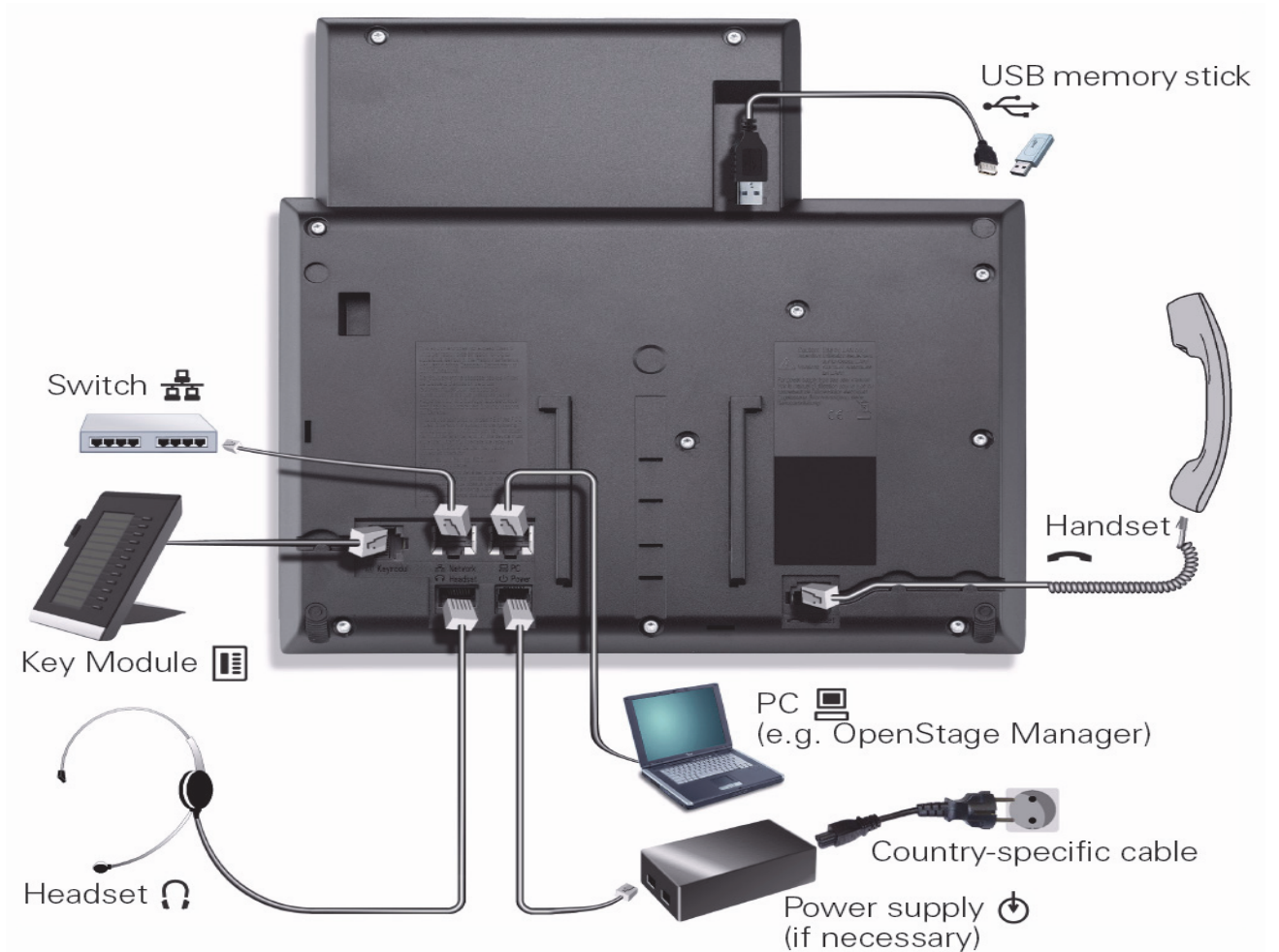
2.2 Assembling and Installing the Phone

2.2.1 Shipment

- Phone
- Handset
- Handset cable
- Subpackage:
 - Document "Information and Important Operating Procedures"
 - Emergency number sticker

2.2.2 Connectors at the bottom side

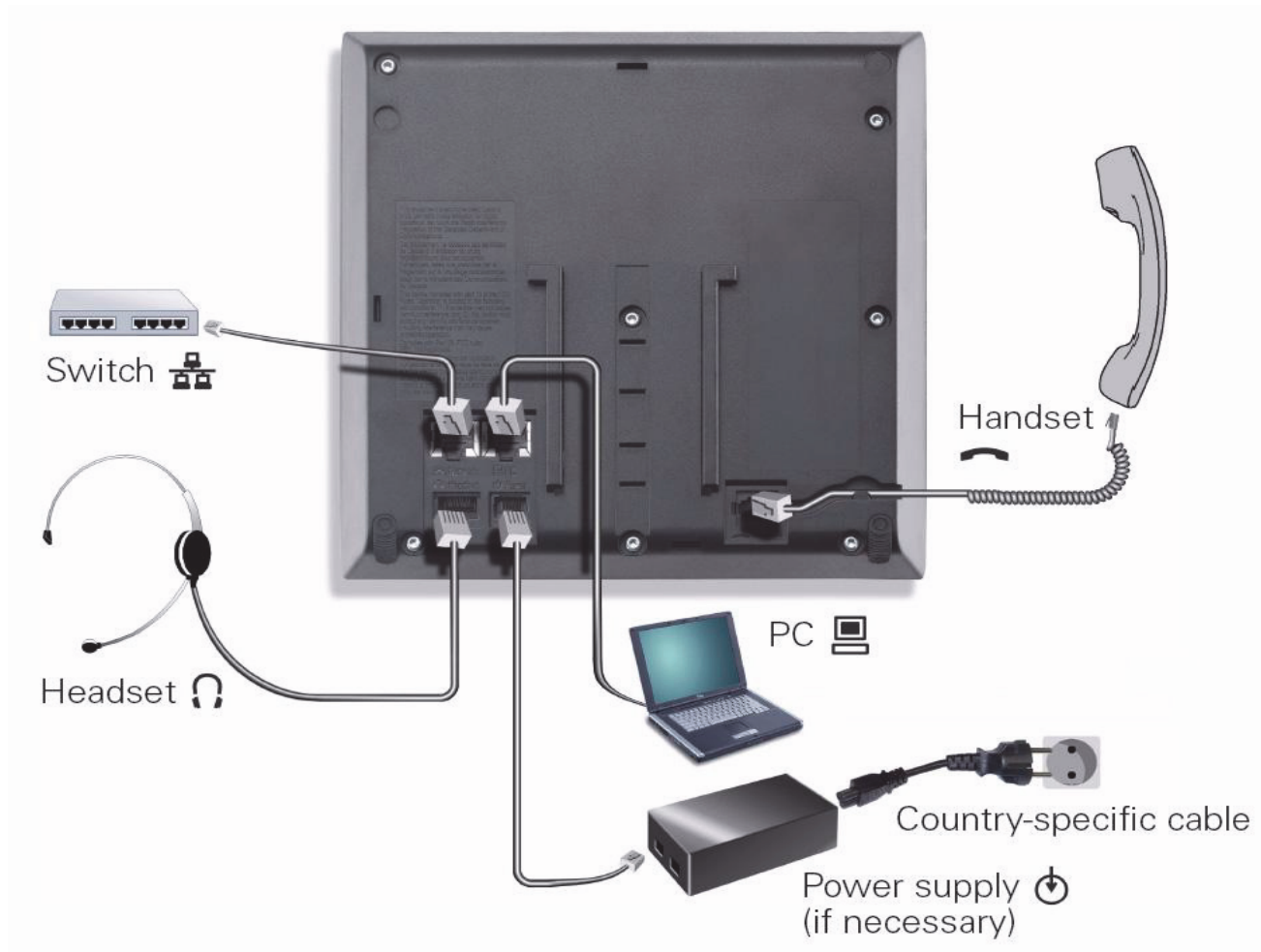
OpenScape Desk Phone IP 55G



Startup


Assembling and Installing the Phone

OpenScape Desk Phone IP 35G



2.2.3 Assembly


1. Handset

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. Emergency Number Sticker

Write your telephone number and those for the fire and police departments on the included label and attach it to the telephone housing underneath the handset (see arrow).

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/Supply
OpenScape Desk Phone IP 35G ¹	Power Class 2
OpenScape Desk Phone IP 35G + 2nd Key Module	Power Class 2
OpenScape Desk Phone IP 55G ⁴	Power Class 3
OpenScape Desk Phone IP 55G + 2nd Key Module	Power Class 3

¹ Includes 1 Key Module.

2. Only if Power over Ethernet (PoE) is **NOT** supported:







The order no. for the plug-in power supply is region specific:
EU: C39280-Z4-C510
UK: C39280-Z4-C512
USA: C39280-Z4-C511

Plug the power supply unit into the mains. Connect the plug-in power supply unit to the  jack at the bottom of the phone.

Startup

Assembling and Installing the Phone

3. If applicable, connect the following optional jacks:

-  LAN connection to PC
-  Headset (accessory)
-  Connection to add-on device (accessory)
-  USB master for connection to a USB device (e. g. accessory USB Acoustic Adapter)



To prevent damage on the OpenScape Desk Phone IP phone, connect an USB stick using the adapter cable C39195-Z7704-A5.



Do not connect a USB hub to the phone's USB port, as this may lead to stability problems.

2.2.5 How to Better Use LAN Network Connections

The OpenScape Desk Phone IP 55G provides 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 IP or OpenStage phones!



2.2.6 Key Module

A key module provides 12 additional program keys. Key modules are available for OpenScape Desk Phone IP 55G phones. A maximum of 2 key modules can be connected to one phone.

The following table shows which key modules can be connected to the particular phone types.

Phone Type	OpenScape Key Module 55
OpenScape Desk Phone IP 35G	-
OpenScape Desk Phone IP 55G	2

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

2.2.7 Using Multilingual User Interface

For further information on Using the Multilingual User Interface, please refer to platform documentation.

OpenScape 4000 V7

OpenScape 4000 V7, Section 3 - Feature Usage Examples, Service Documentation

Chapter "Multilingual User Interface"

Relevant AMOs: ZAND, SDAT, SBSCU, TAPRO

OpenScape Business

OpenScape Business V1, Administrator Documentation

Chapter "Multilingual Text Output"

2.3 Quick Start

This section describes a typical case: the setup of an OpenScape Desk Phone IP 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, the DLS (Deployment Service) administration tool can be used. Its Plug & Play functionality allows to provide the phone with configuration data by assigning an existing data profile to the phone's MAC address or E.164 number. For further information, see the Deployment Service Administration Manual.



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

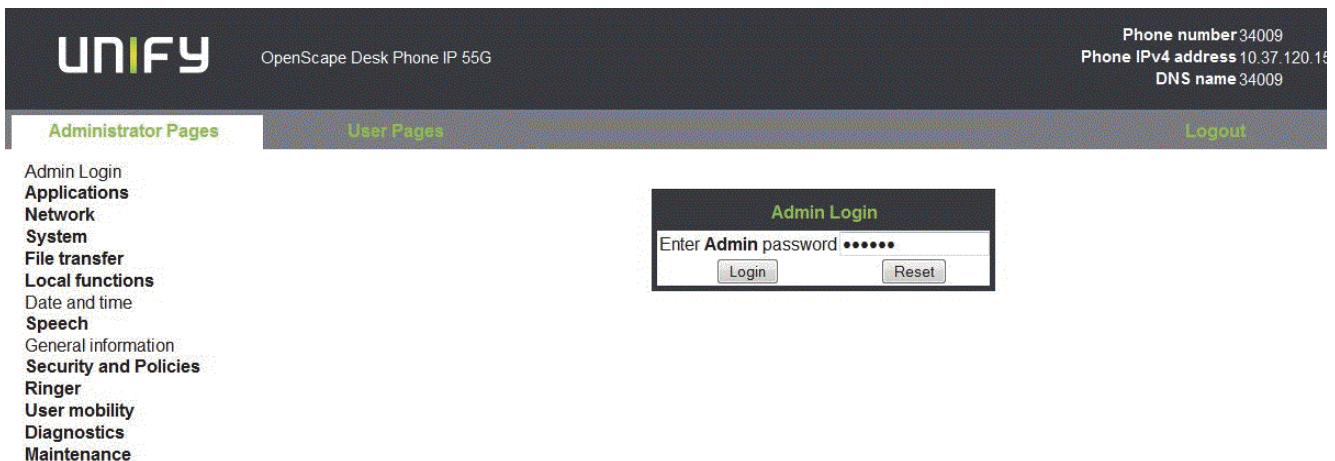
2.3.1 How to Access the Web Interface (WBM)

Prerequisites

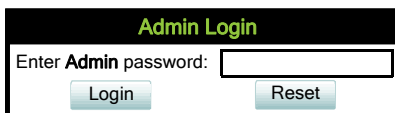
- The phone's IP address or URL is required for accessing the phone's Web Interface via a web browser. By default, the phone will automatically search for a DHCP server on startup and try to obtain IP data and further configuration parameters from that central server.
- If no DHCP server is available in the IP network or if the DHCP parameter is disabled, the IP address, subnet mask and default gateway/route must be defined manually.
- To obtain the phone's IP address, proceed as follows:
 1. Access the local phone's Admin menu as described in Access via Local Phone.
 - If DHCP is enabled (default): In the Admin menu, navigate to Network > 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 (MS Internet Explorer or Firefox) and enter the appropriate URL. Example: `https://192.168.1.15` or `https://myphone.phones`.

For configuring the phone's DNS name, please refer to Section 3.3.6.3, "Terminal Host-name".

If the browser displays a certificate notification, accept it. The start page of the web interface appears. In the upper right corner, the phone number, the phone's IP address, as well as the DNS name assigned to the phone are displayed. The left corner contains the user menu tree.



3. Click on the tab "Administrator Pages". In the dialog box, enter the admin password. The default password is 123456.



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

2.3.2 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. For further information, please refer to Terminal Identity.

2.3.3 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.

2.3.4 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".

2.3.5 VLAN Discovery

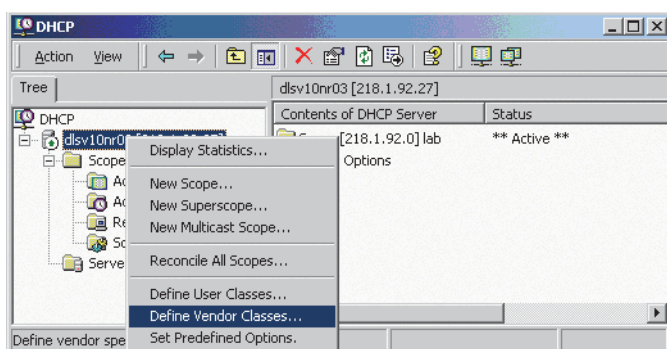
If the phone is to be located in a VLAN (Virtual LAN), a VLAN ID must be assigned. If the VLAN shall be provided by DHCP, **VLAN Discovery** must be set to "DHCP" (see Section 3.2.2.1, "Automatic VLAN discovery using LLDP-MED"). The corresponding DHCP option is vendor-specific, thus a specific procedure is necessary.

2.3.5.1 Using a Vendor Class

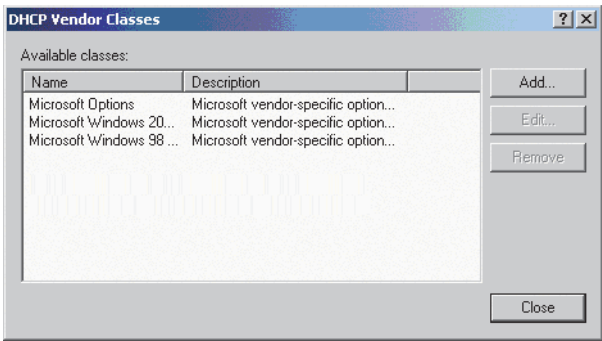
It is recommended to define a vendor class on the DHCP server, thus enabling server and phone to exchange vendor-specific data exclusively. The data is disclosed from other clients. The following steps are required for the configuration of the Windows DHCP server.

Setting up a new vendor class using the Windows DHCP Server

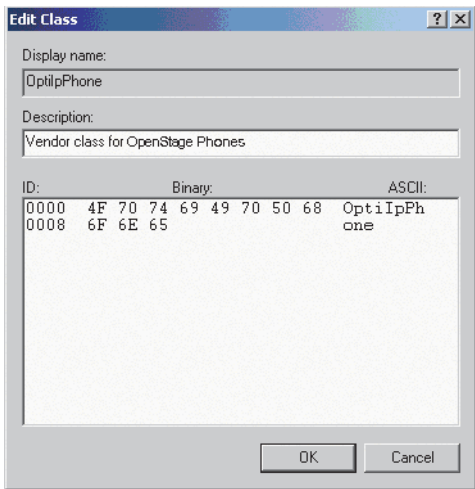
1. In the Windows Start menu, select **Start > Programs > Administrative Tools > DHCP**.
2. In the DHCP console menu, right-click the DHCP server in question and select **Define Vendor Classes...** in the context menu.



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



4. Define a new vendor class with the name **OptilpPhone** 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"
```

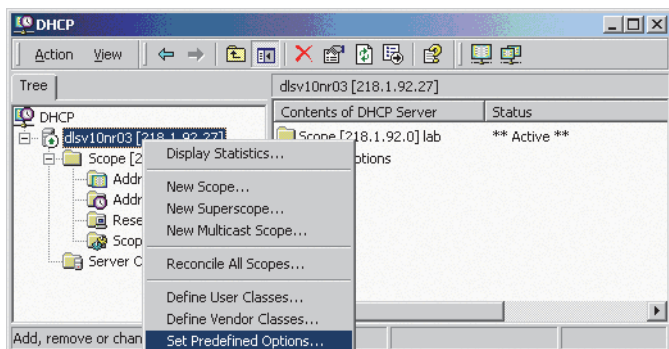
The value **SIEMENS** for optiPoint Element 1 can then be re-assigned over the DHCP console.

This error was corrected in Windows 2003 Server SP2.

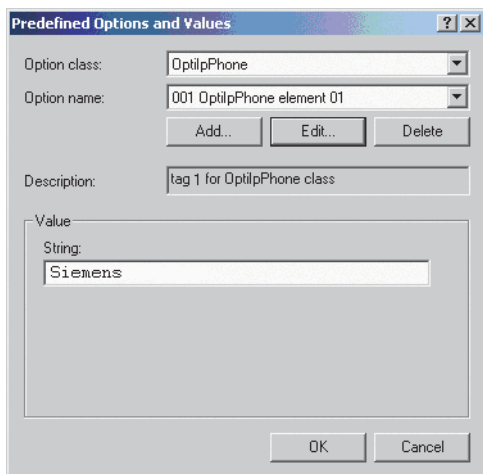
Startup

Quick Start

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



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



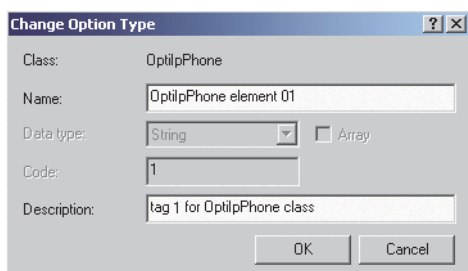
8. Enter the following data for the new option:

1. First Pass: Option 1

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

2. Second Pass: Option 2

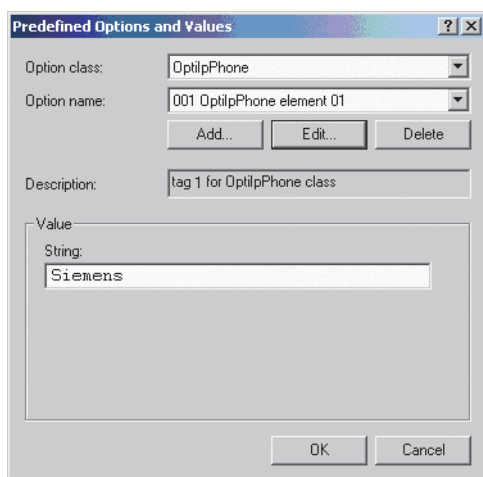
- Name: Free text, e. g. "OptilpPhone element 02"
- Data type: "Long"
- Code: "2"
- Description: Free text.



9. Enter the value for this option.

1. First Pass: "Siemens"

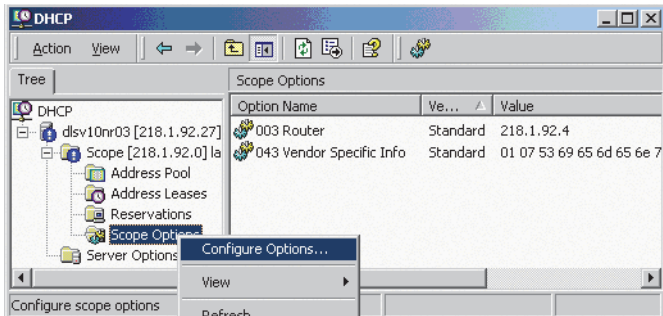
2. Second Pass: VLAN ID



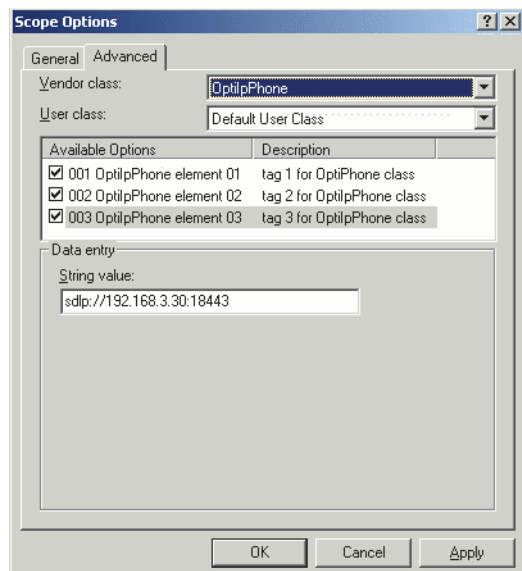
10. Press **OK**, repeat steps 7 to 9 for the second pass, and press **OK** again.

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 (**OptilpPhone**) and, under **User class**, select **Default User Class**.



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

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 **OptilpPhone** vendor is transmitted only to the clients (workpoints) in this vendor class.

Setup using a DHCP server on Unix/Linux

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

```
class "OptiIpPhone" {
    option vendor-encapsulated-options
    # The vendor encapsulated options consist of hexadecimal values for
    the option number (for instance, 01), the length of the value (for in-
    stance, 07), and the value (for instance, 53:69:65:6D:65:6E:73). The
    options can be written in separate lines; the last option must be fol-
    lowed by a `;` instead of a `:`.
    # Tag/Option #1: Vendor "Siemens"
    #1 7 S i e m e n s
    01:07:53:69:65:6D:65:6E:73:
    # Tag/Option #2: VLAN ID
    #2 4 0 0 1 0
    02:04:00:00:00:0A;
    match if substring (option vendor-class-identifier, 0, 11) =
    "OptiIpPhone";
}
```

2.3.5.2 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

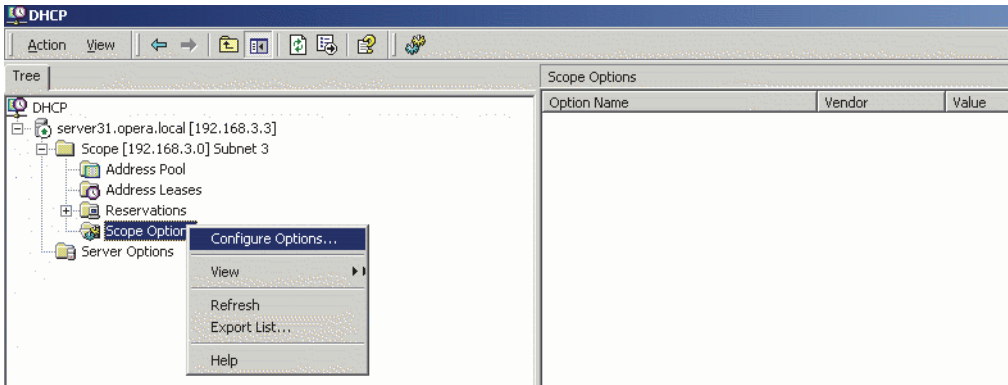
The following example shows a VLAN ID with the decimal value "10":

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

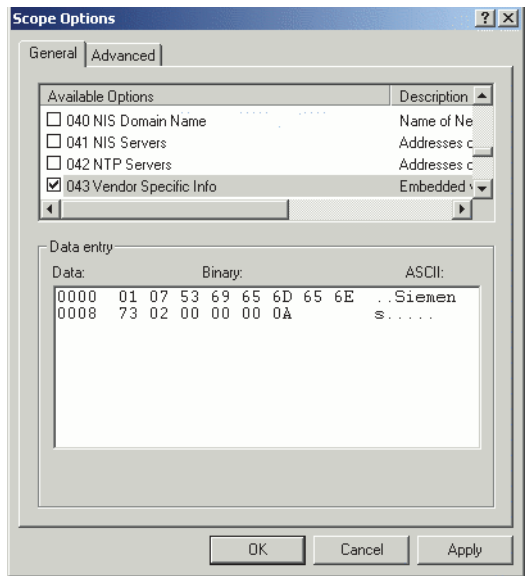
For manual configuration of the VLAN ID see Section 3.2.2.2, "Manual configuration of a VLAN ID".

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.



2.3.6 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 DHCP, as this method enables full Plug & Play and ensures the authenticity of the DLS server.

For manual configuration of the DLS server address see 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.

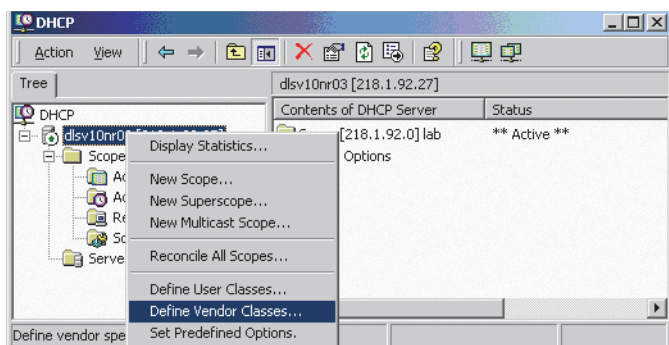
2.3.6.1 Using Vendor Class

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

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

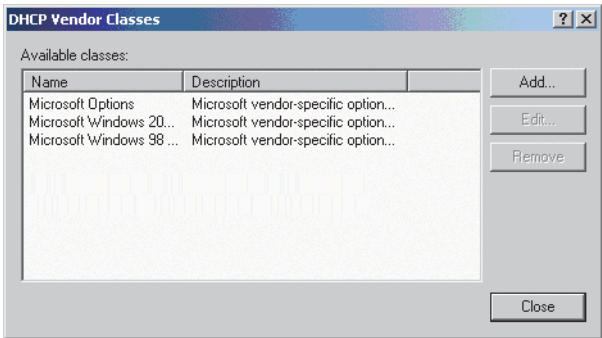
Setting up a new vendor class using the Windows DHCP Server

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

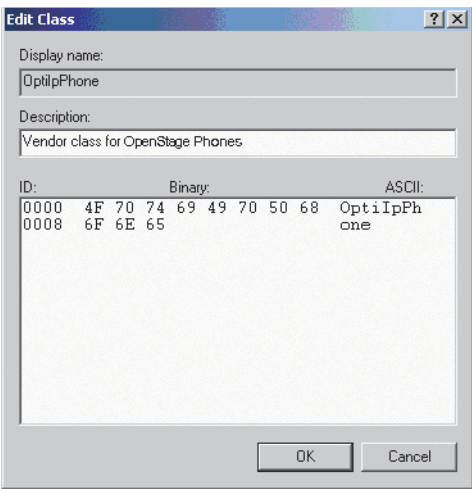


Startup
Quick Start

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



4. Define a new vendor class with the name **OptilpPhone** 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).

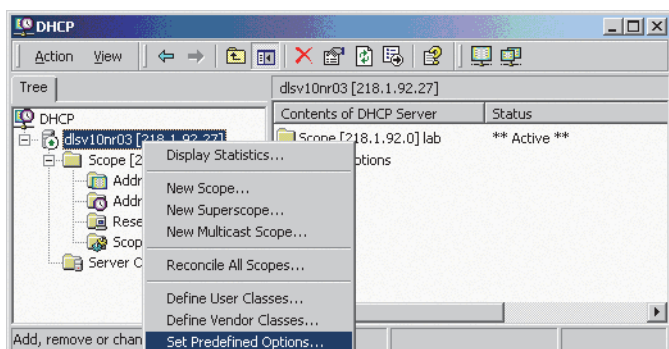
You can use the following command to configure the required option (without error message) so that it also appears later in the DHCP console:

```
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.

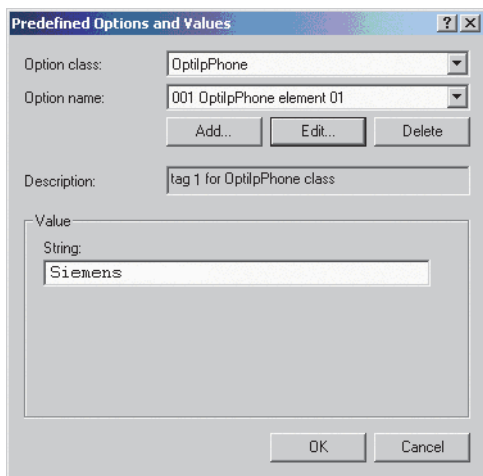
6. In the DHCP console menu, right-click the DHCP server in question and select Set Pre-defined Options from the context menu.



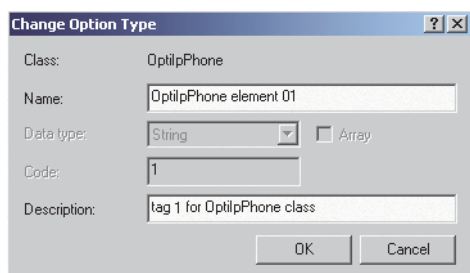
Startup

Quick Start

7. In the dialog, select the previously defined **OptilpPhone** 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. "OptilpPhone element 01"
 - Data type: "String"
 - Code: "1"
 - Description: Free text.
 2. Second Pass: Option 3
 - Name: Free text, e. g. "OptilpPhone element 03"
 - Data type: "String"
 - Code: "3"
 - Description: Free text.



9. Enter the value for this option.

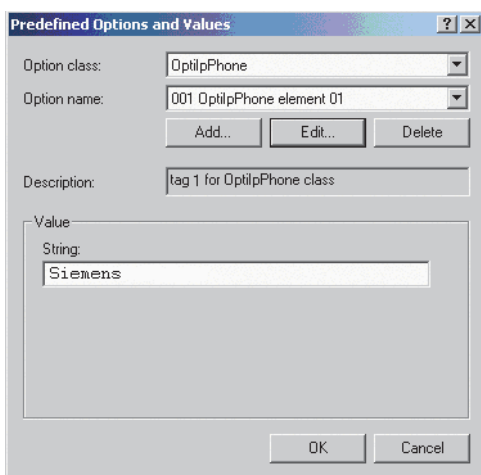
1. First Pass: "Siemens"

2. Second Pass: DLS address

The DLS address has the following format:

<PROTOCOL>:://<IP ADDRESS OF DLS SERVER>:<PORT NUMBER>

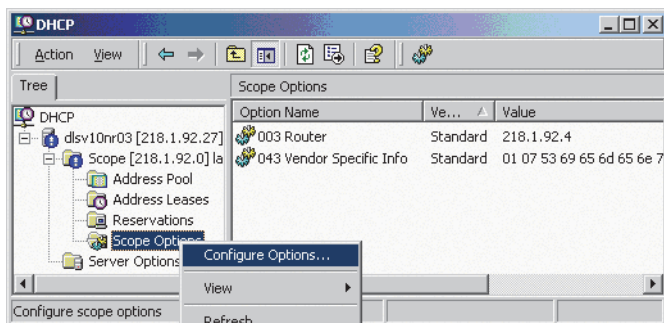
Example: sdip://192.168.3.30:18443



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

Defining the scope for the new vendor class

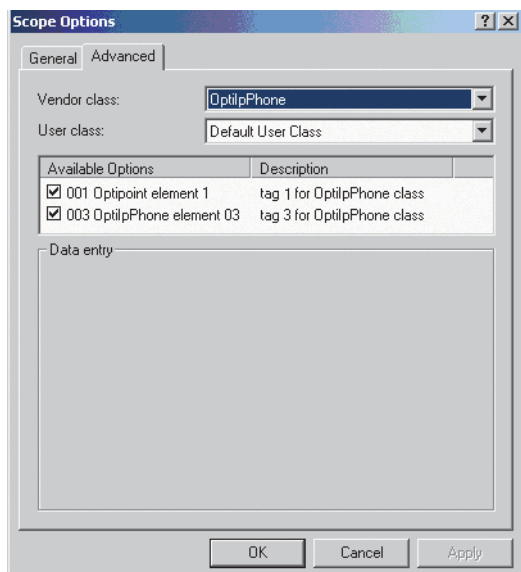
11. Select the DHCP server in question and the **Scope** and right-click **Scope Options**. Select **Configure Options...** in the context menu.



Startup

Quick Start

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



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

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 **OptilpPhone** vendor is transmitted only to the clients (workpoints) in this vendor class.

Setup using a DHCP server on Unix/Linux

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

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

2.3.6.2 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):

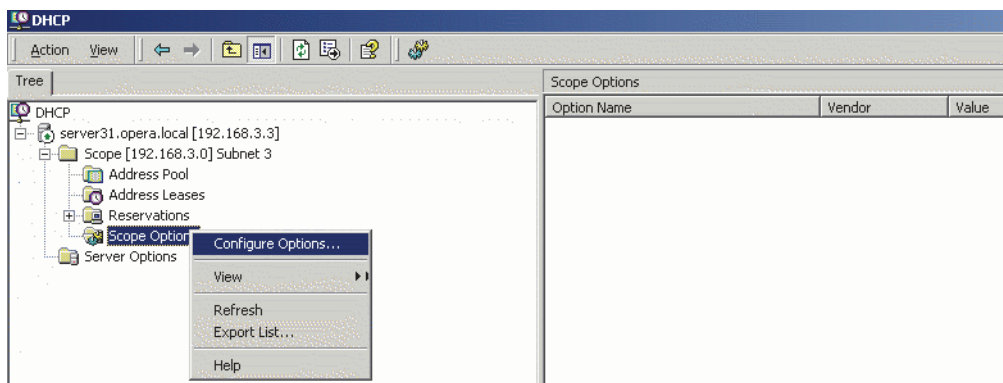
Code	Length	Vendor name						
1	7	S	i	e	m	e	n	s
01	07	53	69	65	6D	65	6E	73

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:

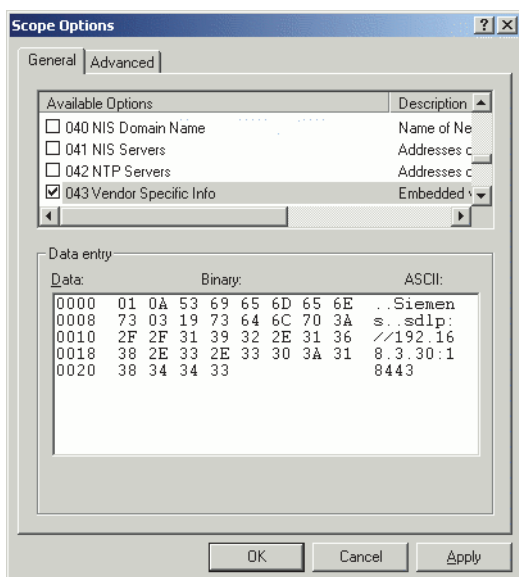
Code	Length	DLS IP address																								
3	25	s	d	l	p	:	/	/	1	9	2	.	1	6	8	.	2	.	1	9	:	1	8	4	4	3
03	19	73	64	6C	70	3A	2F	2F	31	39	32	2E	31	36	38	2E	32	2E	31	39	3A	31	38	34	34	33

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.



2.3.7 HFA Gateway Settings

To connect the OpenScape Desk Phone IP phone to the OpenScape Business or OpenScape 4000 V7 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.

2.3.8 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 V7 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.


2.3.9 Using the Local Menu

Take the following steps to configure the access to an HFA gateway (for further information see Section 3.1, "Access via Local Phone"):

1. Press the mode key (≡) once or twice to activate the administration menu (the key toggles between the user's configuration menu and the administration menu).
2. When the Admin menu is active, you will be prompted to enter the administrator password. The default admin password is "123456". It is recommended to change the password (see Section 3.11, "Password") after your first login.
3. In the administration menu, go to **System > Gateway**. For further instructions on entering data using the Local menu see Section 3.1, "Navigate within the Administration Menu". The path is as follows:

```
├ Administration
│   └ System
│       └ Gateway
│           ├── System type
│           ├── IP address
│           ├── Gateway ID
│           ├── Subscriber number
│           └ Password
```

4. Enter the IP address of the HFA gateway provided by your OpenScape Communication System.

5. Enter the phone's Gateway Id, which will also serve as internal phone number.
6. Enter the password associated with the Gateway Id.
7. After the data has been entered, select **Save & exit** and press .

3 Administration

This chapter describes the configuration of every parameter available on the OpenScape Desk Phone IP phones. For access via the local phone menu, see the following; for access using the web interface (WBM), please refer to Section 2.3.1, “How to Access the Web Interface (WBM)”.

3.1 Access via Local Phone

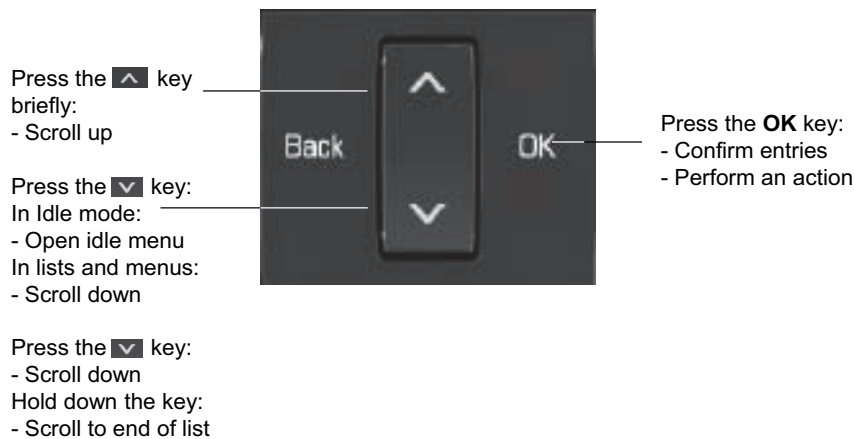


The data entered in input fields is parsed and controlled by the phone. Thus, data is accepted only if it complies to the value range.

1. Access the Administration Menu
Press the Services (Settings on DPIP 35G), Up Arrow or Down Arrow and OK keys consecutively to select the Admin menu.
2. When the Administration Menu is active, you will be prompted to enter the admin password.
The default admin password is "123456". It is recommended to change the password (see Section 3.13, “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

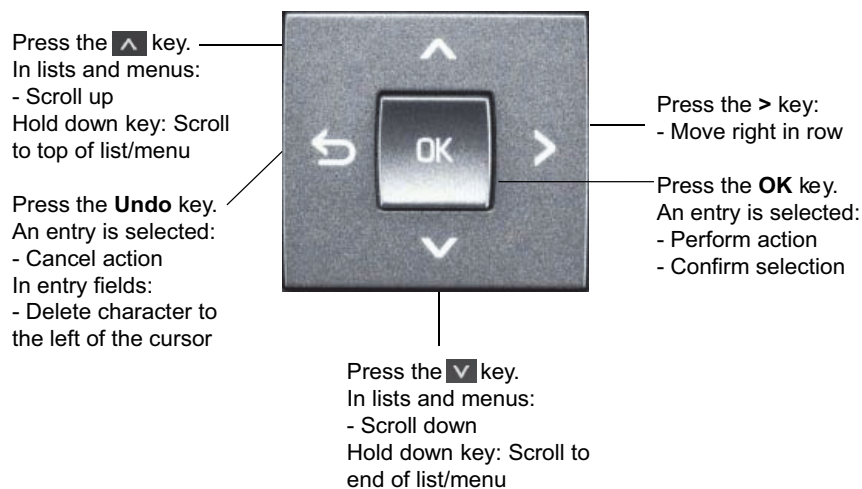
OpenScape Desk Phone IP 35G

Use the Navigation Keys to navigate and execute administrative actions in the Administration Menu.



OpenScape Desk Phone IP 55G

Use the Navigation Block to navigate in lists and menus, and between input fields. Use the central OK key to confirm options and trigger actions.



Administration



Access via Local Phone

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.
	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 33G/55G 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.

3.2 LAN Settings

3.2.1 LAN Port Settings

The OpenScape Desk Phone IP 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) 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 IP 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", "1000 Mbps half duplex" (Desk Phone IP 55G), "1000 Mbps full duplex" (Desk Phone IP 55G) .
Default: "Automatic"

Administration

LAN Settings

- **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", "1000 Mbps half duplex" (Desk Phone IP 55G), "1000 Mbps full duplex" (Desk Phone IP 55G).
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

Port configuration	
Gateway	4060
Standby gateway	4060
RTP base	5004
System H.225	1720
Standby H.225	1720
System Cornet TLS	4061
Standby Cornet TLS	4061
System H.225 TLS	1300
Standby H.225 TLS	1300
Download server (default)	21
LDAP server	389
HTTP Proxy	0
LAN port speed	Automatic
PC port speed	Automatic
PC port mode	disabled
PC port autoMDIX	<input type="checkbox"/>

Submit Reset

Administration via Local Phone

```
|__ Admin
|__ Network
|__ Port Configuration
|__ Number
|__ LAN port type
|__ PC port status
|__ PC port type
|__ 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:

- Manually
- By DHCP
- By LLDP-MED

Administration via WBM

Network > IP configuration

You must click on **change mode** first. Afterwards, the **IP configuration mode** dialog opens.

IP configuration

[change mode](#)

LLDP-MED Enabled ☐

DHCP Enabled ☐

IP address 192.168.1.105

Subnet mask 255.255.255.0

Default route 192.168.1.2

DNS domain

Primary DNS 192.168.1.105

Secondary DNS 192.168.1.2

Route 1 IP address

Route 1 gateway

Route 1 mask

Route 2 IP address

Route 2 gateway

Route 2 mask

VLAN discovery ☒

VLAN ID

HTTP proxy

Submit Reset

Network > IP configuration > **change mode**

To enable VLAN discovery by DHCP, select **DHCP used** in the **Discovery mode** menu. Afterwards, click **Submit**.

IP configuration mode

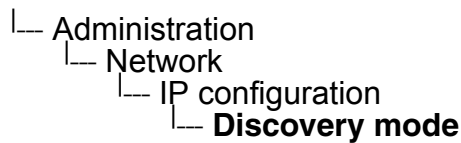
Discovery mode DHCP used

[back to IP configuration](#)

Submit Reset

Administration via Local Phone

To enable VLAN discovery by DHCP, select **DHCP used** in the **Discovery mode** menu.



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 > IP configuration

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

IP configuration

[change mode](#)

LLDP-MED Enabled ☐

DHCP Enabled ☐

IP address 192.168.1.105

Subnet mask 255.255.255.0

Default route 192.168.1.2

DNS domain

Primary DNS 192.168.1.105

Secondary DNS 192.168.1.2

Route 1 IP address

Route 1 gateway

Route 1 mask

Route 2 IP address

Route 2 gateway

Route 2 mask

VLAN discovery ☒

VLAN ID

HTTP proxy

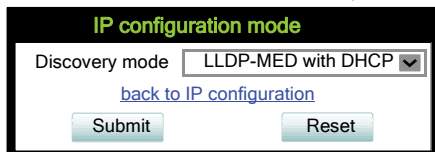
Submit Reset

Administration

LAN Settings

Network > IP configuration > **change mode**

To enable VLAN discovery by LLDP-MED, select **LLDP-MED with DHCP** in the **Discovery mode** menu. Afterwards, click **Submit**.



The screenshot shows a web interface titled "IP configuration mode". Inside, there is a "Discovery mode" label followed by a dropdown menu currently displaying "LLDP-MED with DHCP" with a downward arrow. Below the dropdown is a blue hyperlink labeled "back to IP configuration". At the bottom of the form are two buttons: "Submit" and "Reset".

Administration via Local Phone

To enable VLAN discovery by DHCP, select **LLDP-MED with DHCP** in the **Discovery mode** menu.

└─ Administration
 └─ Network
 └─ IP configuration
 └─ **Discovery mode**

3.2.2.2 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

Network > IP configuration

The screenshot shows the 'IP configuration' web page. At the top, there is a green header 'IP configuration' and a link 'Disable DHCP'. Below this, there are several configuration options: 'LLDP-MED Enabled' (checkbox), 'DHCP Enabled' (checkbox), 'IP address' (text box with '192.168.1.105'), 'Subnet mask' (text box with '255.255.255.0'), 'Default route' (text box with '192.168.1.2'), 'DNS domain' (text box), 'Primary DNS' (text box with '192.168.1.105'), 'Secondary DNS' (text box with '192.168.1.2'), 'Route 1 IP address' (text box), 'Route 1 gateway' (text box), 'Route 1 mask' (text box), 'Route 2 IP address' (text box), 'Route 2 gateway' (text box), 'Route 2 mask' (text box), 'VLAN discovery' (dropdown menu with 'DHCP' selected), 'VLAN ID' (text box, highlighted with a red circle), and 'HTTP proxy' (text box). At the bottom, there are 'Submit' and 'Reset' buttons.

Administration via Local Phone

└─ Admin
 └─ Network
 └─ IP Configuration
 └─ **VLAN ID**

3.3 IP Network Parameters

3.3.1 Quality of Service (QoS)

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

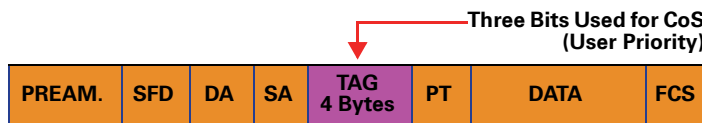


Layer 2 and 3 QoS for voice transmission can be set via LLDP-MED (see LLDP-MED). If so, the value can not be changed by any other interface.

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

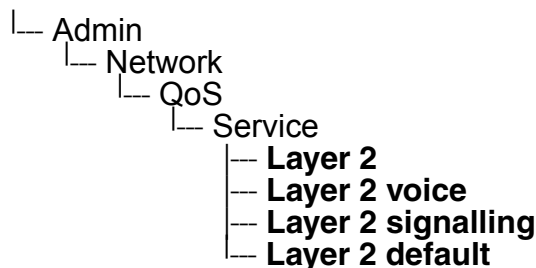
- **Layer 2:** Activates or deactivates QoS on layer 2.
Value range: "Yes", "No"
Default: "Yes"
- **Layer 2 voice:** Sets the CoS (Class of Service) value for voice data (RTP streams).
Value range: 0-7
Default: 5
- **Layer 2 signalling:** Sets the CoS (Class of Service) value for signaling.
Value range: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

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

Administration via Local Phone



3.3.1.2 Layer 3 / Diffserv

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

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

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

Administration

IP Network Parameters

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

QoS

Layer 2 ☐

Layer 2 voice 5

Layer 2 signalling 3

Layer 2 default 0

Layer 3 ☒

Layer 3 voice EF

Layer 3 signalling AF31

Administration via Local Phone

```
├─ Admin
│   └─ Network
│       └─ QoS
│           └─ Service
│               ├── Layer 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)
- SNTP IP Address (NTP Server option 42)
- Timezone offset (Time Server Offset option 2)
- Primary/Secondary DNS (DNS Server option 6)
- DNS Domain Name (DNS Domain option 15)
- Vendor Unique (option 43)

Administration
IP Network Parameters

Administration via WBM

Network > IP configuration

IP configuration

Disable DHCP

LLDP-MED Enabled☐

DHCP Enabled☐

IP address192.168.1.105

Subnet mask255.255.255.0

Default route192.168.1.2

DNS domain

Primary DNS192.168.1.105

Secondary DNS192.168.1.2

Route 1 IP address

Route 1 gateway

Route 1 mask

Route 2 IP address

Route 2 gateway

Route 2 mask

VLAN discoveryDHCP

VLAN ID

HTTP proxy

SubmitReset

Administration via Local Phone



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 > IP configuration

IP configuration

[Disable DHCP](#)

LLDP-MED Enabled ☐

DHCP Enabled ☐

IP address 192.168.1.105

Subnet mask 255.255.255.0

Default route 192.168.1.2

DNS domain

Primary DNS 192.168.1.105

Secondary DNS 192.168.1.2

Route 1 IP address

Route 1 gateway

Route 1 mask

Route 2 IP address

Route 2 gateway

Route 2 mask

VLAN discovery DHCP

VLAN ID

HTTP proxy


Submit Reset

Administration via Local Phone

Admin
 Network
 IP 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 > IP configuration

IP configuration

[Disable DHCP](#)

LLDP-MED Enabled☐

DHCP Enabled☐

IP address192.168.1.105

Subnet mask255.255.255.0

Default route192.168.1.2

DNS domain

Primary DNS192.168.1.105

Secondary DNS192.168.1.2

Route 1 IP address

Route 1 gateway

Route 1 mask

Route 2 IP address

Route 2 gateway

Route 2 mask

VLAN discoveryDHCP

VLAN ID

HTTP proxy

Submit

Reset

Administration via Local Phone



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 > IP configuration

IP configuration

[Disable DHCP](#)

LLDP-MED Enabled ☐

DHCP Enabled ☐

IP address 192.168.1.105

Subnet mask 255.255.255.0

Default route 192.168.1.2

DNS domain

Primary DNS 192.168.1.105

Secondary DNS 192.168.1.2

Route 1 IP address

Route 1 gateway

Route 1 mask

Route 2 IP address

Route 2 gateway

Route 2 mask

VLAN discovery DHCP ☒

VLAN ID

HTTP proxy

Submit Reset

Administration via Local Phone

```
├── Admin
│   ├── Network
│   │   ├── IP 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 IP 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 > IP configuration

IP configuration

[Disable DHCP](#)

LLDP-MED Enabled☐

DHCP Enabled☐

IP address192.168.1.105

Subnet mask255.255.255.0

Default route192.168.1.2

DNS domain

Primary DNS192.168.1.105

Secondary DNS192.168.1.2

Route 1 IP address

Route 1 gateway

Route 1 mask

Route 2 IP address

Route 2 gateway

Route 2 mask

VLAN discoveryDHCP

VLAN ID

HTTP proxy

SubmitReset

Administration via Local Phone



3.3.6.2 DNS Servers

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



Depending on the configuration chosen for survivability, DNS SRV is required. For details, please refer to Resilience and Survivability.

Data required

- **Primary DNS:** IP address of the primary DNS server.
- **Secondary DNS:** IP address of the secondary DNS server.

Administration via WBM

Network > IP configuration

Enter the IP addresses of the primary and the secondary DNS server. Afterwards, click **Submit**.

IP configuration

[Disable DHCP](#)

LLDP-MED Enabled ☐

DHCP Enabled ☐

IP address

Subnet mask

Default route

DNS domain

Primary DNS

Secondary DNS

Route 1 IP address

Route 1 gateway

Route 1 mask

Route 2 IP address

Route 2 gateway

Route 2 mask

VLAN discovery

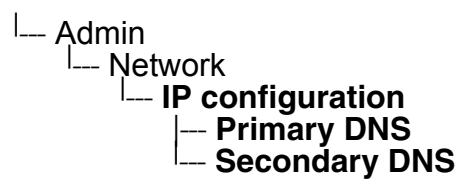
VLAN ID

HTTP proxy

Administration

IP Network Parameters

Administration via Local Phone



3.3.6.3 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:

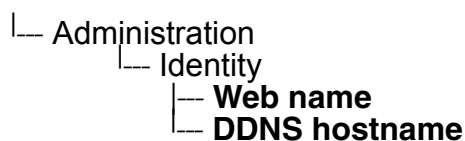
- "None": No hostname is send to the DHCP server during DHCP configuration.
- "MAC based": The DNS name is built from the prefix "OIP" followed by the phone's MAC address.
- "Web name": The DNS name is set to the the string entered in **Web name**.
- "Only number": The DNS name is set to the **Terminal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

System Identity	
Terminal number	3338
Web name	
DNS name construction	Only number
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Administration via Local Phone



3.3.7 Configuration & Update Service (DLS)

The OpenScape Deployment Service (DLS) is a OpenScape Management Application for administering workpoints in both HiPath and non-HiPath networks. 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.

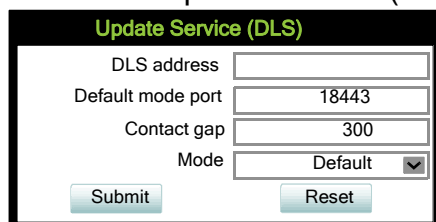
DLS address, i.e. the IP address or hostname of the DLS server, and **Default modeport**, i.e. the port on which the DLS server is listening, are required to enable proper communication between phone and DLS. The **Contact gap** parameter controls a security function. It specifies a minimum time interval 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. The **Security 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.

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.
- **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".

Administration via WBM

Network > Update Service (DLS)



Update Service (DLS)	
DLS address	<input type="text"/>
Default mode port	<input type="text" value="18443"/>
Contact gap	<input type="text" value="300"/>
Mode	<input type="text" value="Default"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Administration via Local Phone

```
|__ Admin
  |__ Network
    |__ Update Service (DLS)
      |__ DLS address
      |__ Default mode port
      |__ Contact gap
      |__ Mode
```

Administration

IP Network Parameters

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 IP phones support SNMPv1.

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

Standard SNMP traps

OpenScape Desk Phone IP 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 OpenStage 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

SNMP

Generic traps

Traping sending enabled

☐

Trap destination

Trap destination port

162

Trap community

Queries allowed

☐

Query password

Diagnostic traps

Diagnostic sending enabled

☐

Diagnostic destination

Diagnostic destination port

Diagnostic community

Diagnostic to generic destination

☐

QoS report traps

QoS traps to QCU

☐

QCU address

QCU port

12010

QCU community

QoS to generic destination

☐

Submit

Reset

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 by 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 IP 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:

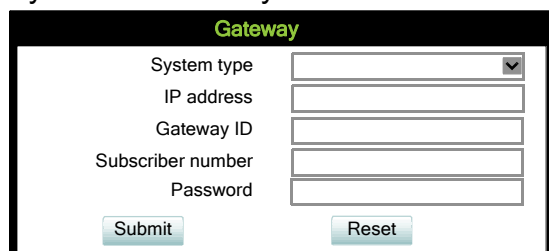
- **IP address:** IP address of the communication platform resp. HFA server.
- **Gateway ID:** The HFA server's port for signaling.
Default: "4060".
- **Subscriber number:** The phone's extension.
- **Password:** Password for logging on to the HFA server.

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 V7 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



The screenshot shows a web-based configuration interface titled "Gateway" in green text. It contains five input fields: "System type" (a dropdown menu with a checkmark icon), "IP address", "Gateway ID", "Subscriber number", and "Password". Below the input fields are two buttons: "Submit" and "Reset".

Network > Port configuration

Port configuration	
Gateway	4060
Standby gateway	4060
RTP base	5004
System H.225	1720
Standby H.225	1720
System Cornet TLS	4061
Standby Cornet TLS	4061
System H.225 TLS	1300
Standby H.225 TLS	1300
Download server (default)	21
LDAP server	389
HTTP Proxy	0
LAN port speed	Automatic
PC port speed	Automatic
PC port mode	disabled
PC port autoMDIX	<input type="checkbox"/>

Submit Reset

Administration via Local Phone

```

├─ Admin
│   └─ System
│       └─ Gateway
│           ├── System type
│           ├── IP address
│           ├── Gateway ID
│           ├── Subscriber number
│           └─ Password

```

```

├─ Admin
│   └─ Network
│       └─ Port configuration
│           └─ Number
│               └─ Gatekeeper

```

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”).

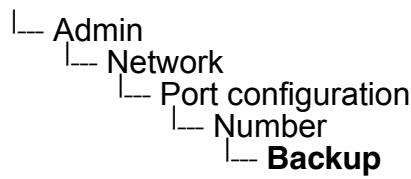
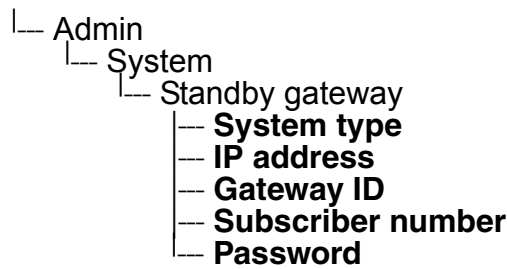
Administration via WBM

System > Standby gateway

Standby Gateway

System type	<input type="text"/>
IP address	<input type="text"/>
Gateway ID	<input type="text"/>
Subscriber number	<input type="text"/>
Password	<input type="text"/>

Administration via Local Phone



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-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

Port configuration	
Gateway	4060
Standby gateway	4060
RTP base	5004
System H.225	1720
Standby H.225	1720
System CorNet TLS	4061
Standby CorNet TLS	4061
System H.225 TLS	1300
Standby H.225 TLS	1300
Download server (default)	21
LDAP server	389
HTTP Proxy	0
LAN port speed	Automatic
PC port speed	Automatic
PC port mode	disabled
PC port autoMDIX	<input type="checkbox"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

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 will switch over to the standby HFA server in case the connection to the main server is lost. By default, this is disabled.

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

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

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

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 successful TC_Tests the Main system needs to answer before the phone switches back, if Auto switchback is enabled. The default is 3.
- **TC Test Expiry**: Determines how long the Previous connection needs to timeout to actually trigger any further SRSR activities.

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

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

After a change of the timing values the SRSR needs to be deactivated and re-activated again to take effect!

Administration via WBM

Redundancy

Small remote site reduncancy	<input type="checkbox"/>
Auto switch back	<input type="checkbox"/>
Retry count main	<input type="text"/>
Retry count standby	<input type="text"/>
Timeout main	<input type="text"/>
Timeout standby	<input type="text"/>
TC test retry	<input type="text"/>
TC test expiry	<input type="text"/>

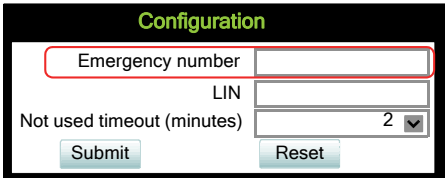
Administration via Local Phone

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

3.5.6 Emergency number

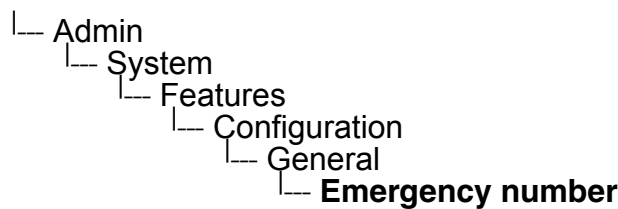
E.911 emergency number. This number establishes a connection to the PSAP (Publiy Safety Answering Point). If a user dials this number, and an appropriate LIN (see Section 3.5.7, “LIN”) is configured, the user’s location is communicated to the PSAP. In the USA, the number is 911.

Administration via WBM



The screenshot shows a web-based management interface titled "Configuration". It contains three input fields: "Emergency number" (with a red border), "LIN" (with a red border), and "Not used timeout (minutes)" (a dropdown menu currently set to "2"). Below these fields are two buttons: "Submit" and "Reset".

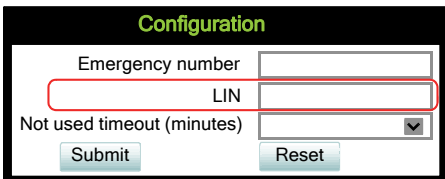
Administration via Local Phone



3.5.7 LIN

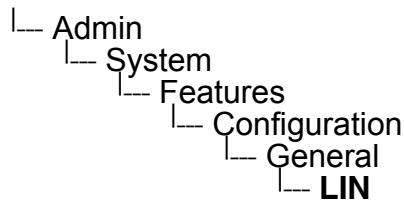
The **Location Identification Number** is a number code which provides detailed geographic information about the phone, including e. g. the office room. On issuing an emergency call using the E.911 emergency number (see Section 3.5.6, “Emergency number”), this code is transferred to an ALI (Automatic 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



The screenshot shows a web-based management interface titled "Configuration". It contains three input fields: "Emergency number", "LIN" (with a red border), and "Not used timeout (minutes)" (a dropdown menu currently set to "2"). Below these fields are two buttons: "Submit" and "Reset".

Administration via Local Phone



3.5.8 Not Used Timeout

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

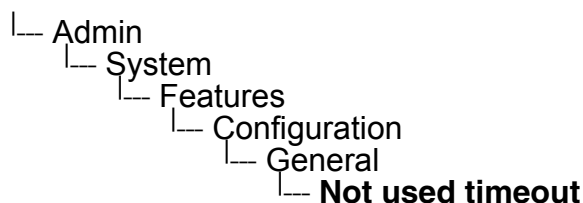
The timeout ranges from 1 to 5 five minutes. The default value is 2.

Administration via WBM

System > Features > Configuration

The screenshot shows a web browser interface for the 'Configuration' menu. It has a title bar 'Configuration' in green. Below it are three input fields: 'Emergency number', 'LIN', and 'Not used timeout (minutes)'. The 'Not used timeout (minutes)' field is highlighted with a red rectangle and shows a value of '1' with a dropdown arrow. At the bottom are 'Submit' and 'Reset' buttons.

Administration via Local Phone

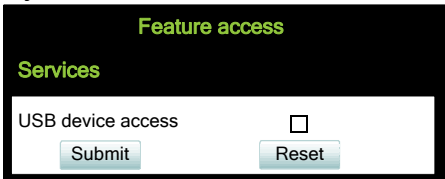


3.5.9 Feature access

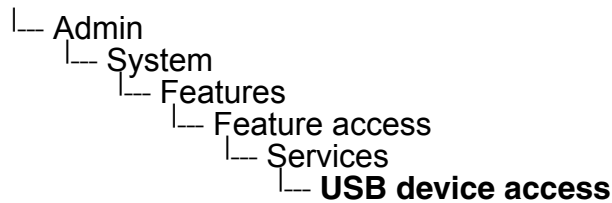
The access to USB devices is configurable.

Administration via WBM

System > Features > Feature access



Administration via Local Phone

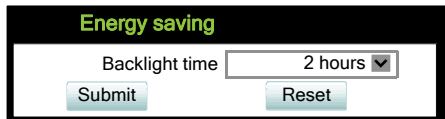


3.5.10 Energy Saving (OpenScape Desk Phone IP 55G)

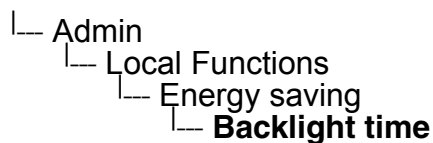
After the phone has been inactive within the timespan specified in **Backlight time**, the display backlight is switched off. The length of this timespan ranges from 1 minute, 5 minutes, 30 minutes, 60 minutes, 2 hours, 4 hours to 8 hours. The default value is 1 minute.

Administration via WBM

Local functions > Energy saving



Administration via Local Phone



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

If the phone is located in a country with daylight saving, the administrator can choose whether daylight saving time is activated manually or automatically. If **Use 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 **Time zone** parameter. This selects the daylight saving time zone 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.

3.5.11.1 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

Date and time	
SNTP	
SNTP IP address	<input type="text" value="192.43.244.18"/>
Display and Trace time	
Source	<input type="text" value="SNTP"/>
NOTE: When Display and Trace source is set to System the timezone and daylight savings settings below do not apply	
Timezone and Daylight saving	
Timezone offset (hours)	<input type="text" value="1"/>
Use daylight saving	<input checked="" type="checkbox"/>
Difference (minutes)	<input type="text" value="60"/>
Auto time change	<input checked="" type="checkbox"/>
Time zone	<input type="text" value="Europe (Rest)"/>
Current DISPLAY Time	
<input type="text" value="Thu May 8 17:01:05 2014"/>	
Current UTC Time	
<input type="text" value="Thu May 8 17:01:05 2014"/>	
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

Administration via Local Phone

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

3.5.12 Security

3.5.12.1 System

OpenScape Desk Phone IP phones support two security options, which are mutually exclusive:

- H.235 Authentication and Encryption
- 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).

Secure H.235 main/standby sets the stage of security for communication between phone and gatekeeper. When set to "None", there is no voice encryption. When set to "Partial", only the data sent from the phone to the gatekeeper is encrypted. With "Full", the data sent in both directions is encrypted.

The **Time H.235 main/standby** parameter defines a time window in milliseconds for the gateway. The gateway only accepts messages which arrive within this time window.

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

Certificate validation main/standby determines whether the phone certificate used for encrypted logon via TLS is checked against the certificate on the gateway.



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

- **Secure H.235 main:** Security stage for communication when the main gateway is in use. Value range: "None", "Partial", "Full".
- **Secure H.235 standby:** Security stage for communication when the standby gateway is in use. Value range: "None", "Partial", "Full".
- **Time H.235 main:** Time window length in ms when the main gateway is in use.
- **Time H.235 standby:** Time window length in ms when the main gateway is in use.
- **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. Value range: true, false.

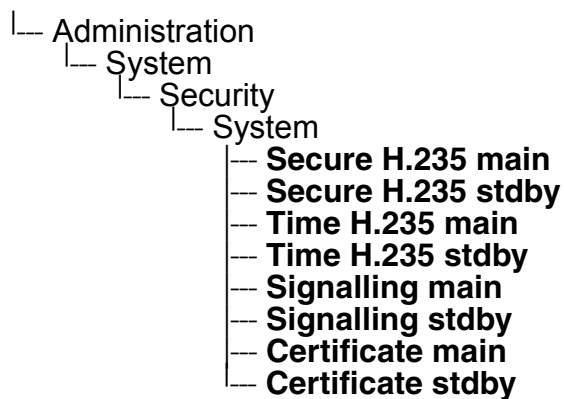
- **Certificate validation standby:** Check the phone certificate against the gateway certificate when the main gateway is in use.
Value range: true, false.

Administration via WBM

System > Security > System

System	
Secure H.235 main	None
Secure H.235 standby	None
Time H.235 main	240
Time H.235 standby	240
Signalling transport main	TCP
Signalling transport standby	TCP
Certificate validation main	<input type="checkbox"/>
Certificate validation standby	<input type="checkbox"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Administration via Local Phone



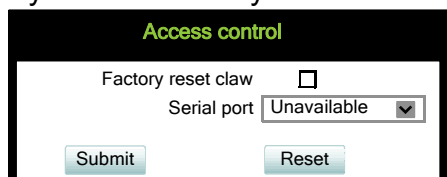
Administration

System Settings

3.5.12.2 Access control

Administration via WBM

System > Security > Access control



Access control

Factory reset claw ☐

Serial port Unavailable

Administration via Local Phone

```
├ Administration
│   └ System
│       └ Security
│           └ Access control
│               └ 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 appropriate dial string, a conversion from canonical format may be required. The following parameters determine the local settings of the phone, like **Local country code** or **Local national code**, and define rules for converting from canonical format to the format required by the PBX.



To enable the number conversion, all parameters not marked as optional must be provided, and the canonical lookup settings must be configured (see Section 3.6.2, "Canonical Dial Lookup").

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 system, 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 3.6.2, "Canonical Dial Lookup").

- "Local enterprise form": Any extension number is dialled 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": All external numbers are dialled 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": 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

Locality > Canonical dial settings

Canonical dial settings	
Local country code	<input type="text" value="49"/>
National prefix digit	<input type="text" value="0"/>
Local national code	<input type="text" value="89"/>
Minimum local number length	<input type="text" value="4"/>
Local enterprise node	<input type="text" value="723"/>
PSTN access code	<input type="text" value="0"/>
International access code	<input type="text" value="00"/>
Operator codes	<input type="text"/>
Emergency numbers	<input type="text"/>
Initial extension digits	<input type="text" value="1,2,3,4"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Local functions > Locality > Canonical dial

Canonical dial	
Internal numbers	<input type="text" value="Local enterprise form"/>
External numbers	<input type="text" value="Local public form"/>
External access code	<input type="text" value="Not required"/>
International gateway code	<input type="text" value="Use national code"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Administration

Dialing

Administration via Local Phone

- |— Admin
 - |— Local Functions
 - |— Locality
 - |— Canonical settings
 - |— **Local country code**
 - |— **National prefix digit**
 - |— **Local national code**
 - |— **Minimum local number length**
 - |— **Local enterprise node**
 - |— **PSTN access code**
 - |— **International access code**
 - |— **Operator code**
 - |— **Emergency number**
 - |— **Initial extension digits**

- |— Admin
 - |— Local Functions
 - |— Locality
 - |— Canonical dial
 - |— **Internal numbers**
 - |— **External numbers**
 - |— **External access code**
 - |— **International 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** (-> Section 3.6.1), 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** (-> Section 3.6.1)
- **Local area code** (-> Section 3.6.1)
- **Local enterprise code** (-> Section 3.6.1)

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 one or more phone book entries.
Example: "+49897007" for Unify Munich.

Administration via WBM

Locality > Canonical dial lookup

Canonical dial lookup	
Local code 1: <input type="text"/>	International code 1: <input type="text"/>
Local code 2: <input type="text"/>	International code 2: <input type="text"/>
Local code 3: <input type="text"/>	International code 3: <input type="text"/>
Local code 4: <input type="text"/>	International code 4: <input type="text"/>
Local code 5: <input type="text"/>	International code 5: <input type="text"/>
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

Administration

Dialing

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. The admin can set if the users are allowed to change their ringer sounds.

If the user is allowed (default setting), the user can decide to use either OpenScape system tones (default setting) or locally created sounds for each of the CorNet TS (Octet 12) ringer types; either constructed (8x3-seq/melody matrix) or ring tone file.

If the user setting is not allowed, the user cannot change ringer settings (except the ringer volume setting). Regardless of these setting, admin can set/change the ringer settings.

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

Administration

Distinctive Ringing

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 V7, for "Speaker call" function the call type "Rollover call" is used in the CorNet AU_RINGER_START message.
Value range OpenScape 4000 V7: "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 distinctive 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 V7: Admin > Ringer > Local ringers

Local ringers

Name	Ringer sound	Pattern melody	Pattern sequence
<i>Internal</i>	Pattern ▼	2 ▼	2 ▼
<i>External</i>	Pattern ▼	2 ▼	2 ▼
<i>Buzz</i>	Pattern ▼	2 ▼	2 ▼
<i>Rollover</i>	Pattern ▼	2 ▼	2 ▼
<i>Simple alert</i>	Pattern ▼	2 ▼	2 ▼
<i>Multiple alert</i>	Pattern ▼	2 ▼	2 ▼
<i>Special 1</i>	Pattern ▼	2 ▼	2 ▼
<i>Special 2</i>	Pattern ▼	2 ▼	2 ▼
<i>Special 3</i>	Pattern ▼	2 ▼	2 ▼
<i>Attention</i>	Pattern ▼	2 ▼	2 ▼
<i>Unspecified</i>	Pattern ▼	2 ▼	2 ▼
<i>US DSN-Precedence</i>	Pattern ▼	2 ▼	2 ▼
<i>US DSN-Routine</i>	Pattern ▼	2 ▼	2 ▼
<i>Emergency</i>	Pattern ▼	2 ▼	2 ▼

Submit Reset

OpenScape Business: Admin > Ringer > Local ringers

Local ringers

Name	Ringer sound	Pattern melody	Pattern sequence
<i>Internal</i>	Pattern ▼	2 ▼	2 ▼
<i>External</i>	Pattern ▼	2 ▼	2 ▼
<i>Attention</i>	Pattern ▼	2 ▼	2 ▼

Submit Reset

Administration

Distinctive Ringing

Admin > Ringer >Ringer setting

Ringer setting

User Changeable☒

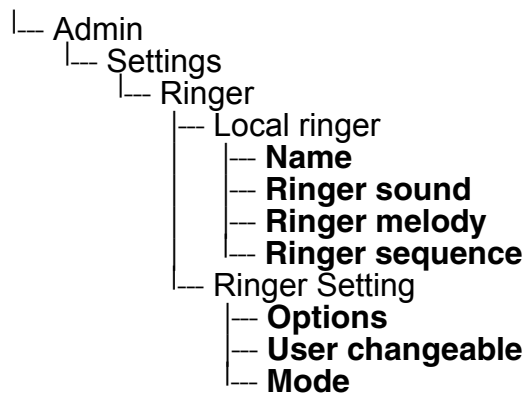
Ringer Mode

Local ringer

Submit

Reset

Administration via Local Phone



3.8 User Mobility

If user mobility is enabled, the user can log on at another phone and at the same time transfer the user data (only possible in case of DPIP55G Data Mobility). The transferable user data comprises the following:

- the user's phone book, including call groups;
- the picture clips associated with phone book entries;
- the canonical settings (see Section 3.5.11, "Date and Time");
- the call log;
- the user password.



For user data mobility, the DLS (Deployment Service) must be available.

The **Set Mobility Mode** parameter controls the phone's mobility features, i. e. it adjusts the mobility level. The following settings are possible:

- **Basic** (Default): This is the original behaviour before the introduction of data mobility in V1R3. 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, a pristine, empty phone book and call log will be provided. The user data of the precedent user will be hidden to the new user.
- **Data Mobility**: The user data of phone A, i. e. the user's home phone, is sent to the DLS, which acts as a cache for mobility purposes. The local phone book, the picture clips, the canonical settings, and the user password are updated each time a change is made. The call log is sent to the DLS every hour and when the user logs off. As soon as the user logs on to phone B, the data is transferred to phone B. Please note that user data mobility must be activated both on phone A and B.



In case a user wants to move from an OpenScape Desk Phone IP to an optiPoint phone, DLS-based data mobility is not possible.

3.8.1 Platform Specific Behaviour

Regarding data mobility, there are some differences, depending on whether a OpenScape Business or OpenScape 4000 V7 is in use.

OpenScape 4000 V7

When the user logs on to phone B, phone A is in "cancel mobility" state. This means that the user, or someone else, can trigger a restore of the initial user at phone A. Thus, the user will be logged off from phone B and logged on at phone A. To prevent an unauthorized person from doing this, the cancel mobility process can be password-protected. This password is entered in the **Cancel mobility password** menu.

OpenScape Business

With this platform, mobility is achieved by storing all user data in the DLS. Hence, for each participant who wishes to use data mobility, a mobile user must be created on the DLS. For details, please refer to the Deployment Service Administration Manual.

Logon attempts: Tries of unsuccessful Logon attempts before the phone switches back from the Mobile user to Non Mobile user after the connection to the gateway failed.

Admin > User Mobility > Set Mobility Mode

OpenScape Desk Phone IP 55G

Set Mobility Mode

Mobility Type

Logon attempts

OpenScape Desk Phone IP 35G

Set Mobility Mode

Logon attempts

Admin > User Mobility > Cancel mobility password

Cancel Mobility password

New password

Confirm password

Administration via Local Phone

- |_ Admin
 - |_ Mobility
 - |_ **Mobility Mode**
 - |_ **Logon attempts**
 - |_ **Mobility password**
 - |_ **Confirm password**

Administration

Transferring Phone Software, Application, and Media Files

3.9 Transferring Phone Software, Application, and Media Files

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



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

- OpenScape Desk Phone IP 35G: 4 MB
- OpenScape Desk Phone IP 55G: 8 MB

3.9.1 FTP/HTTPS Server

There are no specific requirements regarding the FTP server for transferring files to the OpenScape Desk Phone IP. 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

The screenshot shows a web-based configuration interface titled 'Defaults'. It contains several input fields for configuring file transfer settings. The 'Download method' is set to 'FTP' via a dropdown menu. Other fields include 'FTP Server address', 'FTP Server port' (set to 21), 'FTP account', 'FTP username', 'FTP password' (masked with dots), 'FTP path', and 'HTTPS base URL'. At the bottom, there are 'Submit' and 'Reset' buttons.

Defaults	
Download method	FTP
FTP Server address	
FTP Server port	21
FTP account	
FTP username	
FTP password	••••••
FTP path	
HTTPS base URL	
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Administration via Local Phone

```
├─ Admin
│   └─ File Transfer
│       └─ Defaults
│           └─ Download method
│           └─ Server
│           └─ Port
│           └─ Account
│           └─ Username
│           └─ Password
│           └─ FTP path
│           └─ HTTPS base URL
```

Administration

Transferring Phone Software, Application, and Media Files

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 its own hardware level (from the part number and/or by a dynamical check of its HW level).

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

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



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 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)

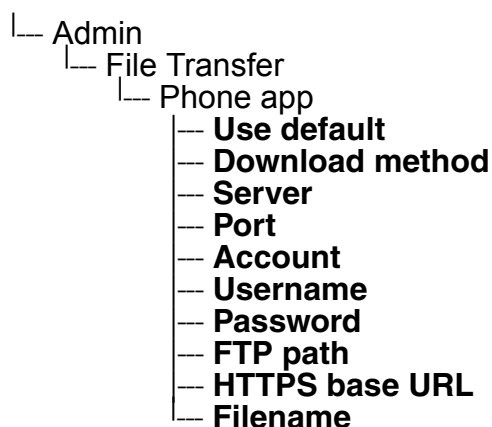
- **Download method:** Selects the protocol to be used.
Value range: "FTP", "HTTPS".
Default: "FTP".

- **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



Administration

Transferring Phone Software, Application, and Media Files

3.9.3.2 Download/Update Phone Application

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



When Phone Application was upgraded to HFA V3R0 there may be displayed a downgrade protection message.

Downgrade of DPIP phones is protected to avoid download of software lower than HFA V3R0 due to License Restrictions.

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 IP 35G:
Press the **OK** key. A context menu opens. In the context menu, select **Download**. The download will start immediately.
- On Desk Phone IP 55G:
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 IP 55G 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

Transferring Phone Software, Application, and Media Files

Administration via WBM

File transfer > Picture clip

Picture clip

Use defaults

☐

Download method

FTP

FTP Server address

FTP Server port

21

FTP account

FTP username

FTP password

•••••

FTP path

HTTPS base URL

Filename

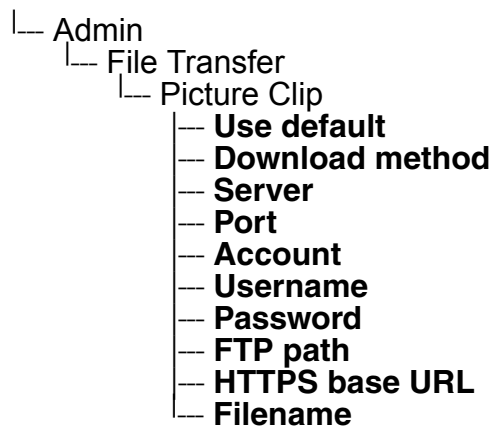
After submit

do nothing

Submit

Reset

Administration via Local Phone



- On Desk Phone IP 55G:
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 IP 55G:
Press the Soft Key labeled **Download**. The download will start immediately.

Administration

Transferring Phone Software, Application, and Media Files

3.9.5 LDAP Template

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



The OpenScape Desk Phone IP 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)

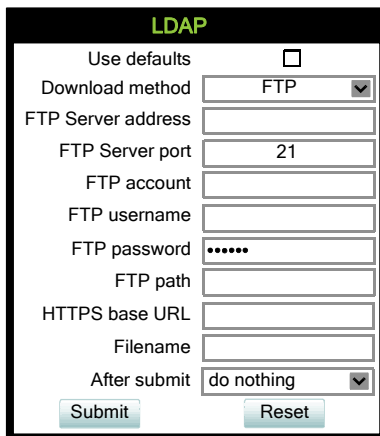
- **Use default:** Specifies whether the default FTP/HTTPS access settings shall be used.
Value range: "Yes", "No"
Default: "No"
- **Filename:** Specifies the file name of the phone software.
- **After submit:** Specifies actions after submit button is pressed.
Value range: "do nothing", "start download".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



The screenshot shows a web-based configuration form titled "LDAP" in green text. The form contains the following fields and controls:

- Use defaults:** A checkbox that is currently unchecked.
- Download method:** A dropdown menu with "FTP" selected.
- FTP Server address:** An empty text input field.
- FTP Server port:** A text input field containing the value "21".
- FTP account:** An empty text input field.
- FTP username:** An empty text input field.
- FTP password:** A text input field with masked characters (dots).
- FTP path:** An empty text input field.
- HTTPS base URL:** An empty text input field.
- Filename:** An empty text input field.
- After submit:** A dropdown menu with "do nothing" selected.
- Buttons:** "Submit" and "Reset" buttons at the bottom.

Administration via Local Phone

```


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

Administration

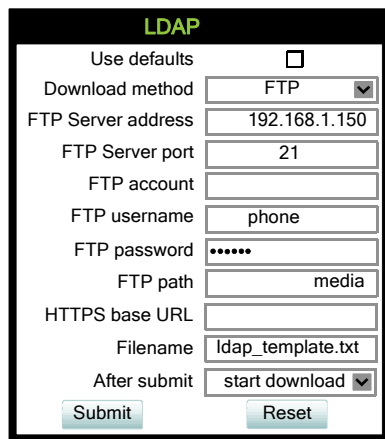
Transferring Phone Software, Application, and Media Files

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 IP phone supports LDAPv3.

Start Download via WBM



The image shows a web-based configuration dialog titled "LDAP". It contains several fields and controls:

- Use defaults:** A checkbox that is currently unchecked.
- Download method:** A dropdown menu set to "FTP".
- FTP Server address:** A text field containing "192.168.1.150".
- FTP Server port:** A text field containing "21".
- FTP account:** An empty text field.
- FTP username:** A text field containing "phone".
- FTP password:** A text field with masked characters "*****".
- FTP path:** A text field containing "media".
- HTTPS base URL:** An empty text field.
- Filename:** A text field containing "ldap_template.txt".
- After submit:** A dropdown menu set to "start download".
- Buttons:** "Submit" and "Reset" buttons at the bottom.

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 IP 35G:
Press the OK key. A context menu opens. In the context menu, select Download. The download will start immediately.
- On Desk Phone IP 55G:
Press the Soft Key labeled Download. The download will start immediately.

3.9.6 Logo

On OpenScape Desk Phone IP 55G, a custom background image for the telephony interface can be supplied. In most cases, this will be the company logo.

On OpenScape Desk Phone IP 55G, the supported file formats are JPEG and PNG. The ideal size values are as follows:

- Width: 240 px
- Height: 70 px

If the size should deviate from these values, the image will appear skewed.

For guidance on creating a logo file for OpenScape Desk Phone IP 55G, see Section 4.2, “How to Create Logo Files for OpenScape Desk Phone”.

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".

Administration

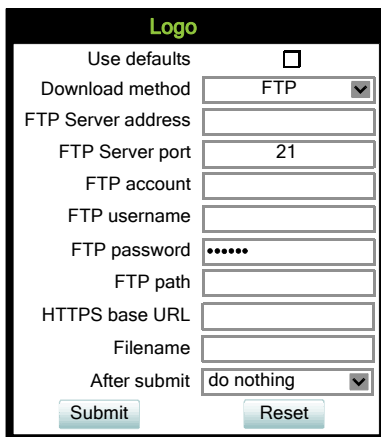
Transferring Phone Software, Application, and Media Files

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 > Logo



Administration via Local Phone

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


3.9.6.2 Download Logo

If applicable, logos 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** > Logo 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 **Logo**.

```

└─ Admin
    └─ File Transfer
        └─ Logo
  
```

- On Desk Phone IP 55G:
Press the Soft Key labeled Download. The download will start immediately.

Administration

Transferring Phone Software, Application, and Media Files

3.9.7 Screensaver

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



Screensavers are available only on OpenScape Desk Phone IP 55G.



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 IP 55G: 320x240

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 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
  
```

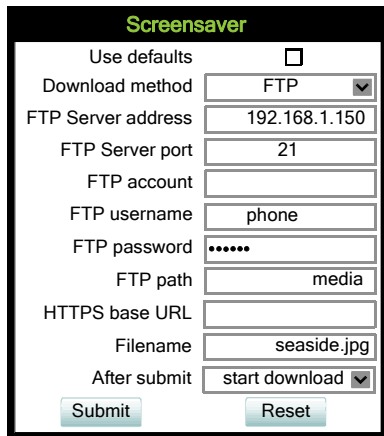
Administration

Transferring Phone Software, Application, and Media Files

3.9.7.2 Download Screensaver

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

Start Download via WBM



The screenshot shows a web interface titled "Screensaver". It contains several configuration fields: "Use defaults" with an unchecked checkbox, "Download method" set to "FTP", "FTP Server address" set to "192.168.1.150", "FTP Server port" set to "21", "FTP account" (empty), "FTP username" set to "phone", "FTP password" masked with dots, "FTP path" set to "media", "HTTPS base URL" (empty), "Filename" set to "seaside.jpg", and "After submit" set to "start download". At the bottom are "Submit" and "Reset" buttons.

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 IP 55G:
Press the Soft Key labeled **Download**. The download will start immediately.

3.9.8 Ringer File



The download of ringer files via WBM or local menu is possible only for OpenScape Desk Phone IP 55G.

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. If a ringer file is downloaded via OpenStage Manager, this restriction does not apply.

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 IP 55G only). The OpenScape Desk Phone IP 55G 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

Administration

Transferring Phone Software, Application, and Media Files

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 action after submit button is pressed.
Value range: "do nothing", "start download".
Default: "do nothing".

Data required (if not derived from Defaults)

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

Administration via WBM

File transfer > Ringer file

Ringer file

Use defaults ☐

Download method FTP

FTP Server address

FTP Server port 21

FTP account

FTP username

FTP password

FTP path

HTTPS base URL

Filename

After submit do nothing

Administration via Local Phone

```

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

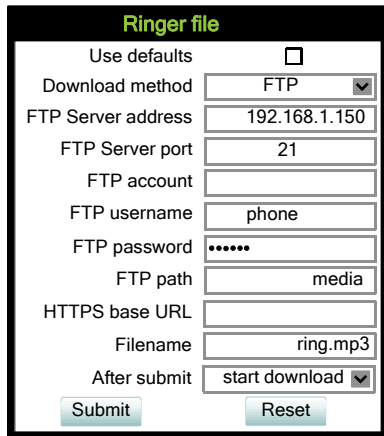
Administration

Transferring Phone Software, Application, and Media Files

3.9.8.2 Download Ringer File

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

Start Download via WBM



The screenshot shows a web interface titled "Ringer file" in green text. It contains several configuration fields: "Use defaults" with an unchecked checkbox, "Download method" with a dropdown menu set to "FTP", "FTP Server address" with the value "192.168.1.150", "FTP Server port" with the value "21", "FTP account" (empty), "FTP username" with the value "phone", "FTP password" with masked characters "*****", "FTP path" with the value "media", "HTTPS base URL" (empty), "Filename" with the value "ring.mp3", and "After submit" with a dropdown menu set to "start download". At the bottom are "Submit" and "Reset" buttons.

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 IP 55G:
Press the Soft Key labeled **Download**. The download will start immediately.

3.9.9 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.

3.9.9.1 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

Transferring Phone Software, Application, and Media Files

Administration via WBM

File transfer > Dongle key

Dongle key

Use defaults☐

Download method

FTP

FTP Server address

FTP Server port

21

FTP account

FTP username

FTP password

FTP path

HTTPS base URL

Filename

After submit

do nothing

SubmitReset

Administration via Local Phone

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

3.9.9.2 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 IP 35G:
Press the **OK** key. A context menu opens. In the context menu, select **Download**. The download will start immediately.
- On Desk Phone IP 55G:
Press the Soft Key labeled **Download**. The download will start immediately.

3.10 Corporate Phonebook: Directory Settings

3.10.1 LDAP

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



The OpenScape Desk Phone IP 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 OpenStage phone, please refer to Section 4.3, "How to Set Up the Corporate Phonebook (LDAP)".

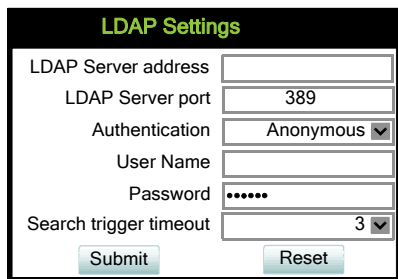
A search field for LDAP requests is supported. The search string is submitted to the LDAP server as soon as the OK key is pressed or when the **Search trigger timeout** expires.

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 > LDAP Settings



The image shows a web-based form titled "LDAP Settings". It contains the following fields and controls:

- LDAP Server address: A text input field.
- LDAP Server port: A text input field with the value "389".
- Authentication: A dropdown menu with "Anonymous" selected.
- User Name: A text input field.
- Password: A text input field with masked characters (dots).
- Search trigger timeout: A text input field with the value "3" and a small dropdown arrow.
- Submit: A button.
- Reset: A button.

Administration via Local Phone

```
├── Admin
│   ├── Local Functions
│   │   └── LDAP
│   │       ├── Server address
│   │       ├── LDAP server port
│   │       ├── Authenticate
│   │       ├── User name
│   │       ├── Password
│   │       └── Search trigger (s)
```

Administration

Corporate Phonebook: Directory Settings

3.10.2 Picture via LDAP

In order to display centrally stored contact data the OpenScape Desk Phone IP 55G will request and retrieve the data from a server.

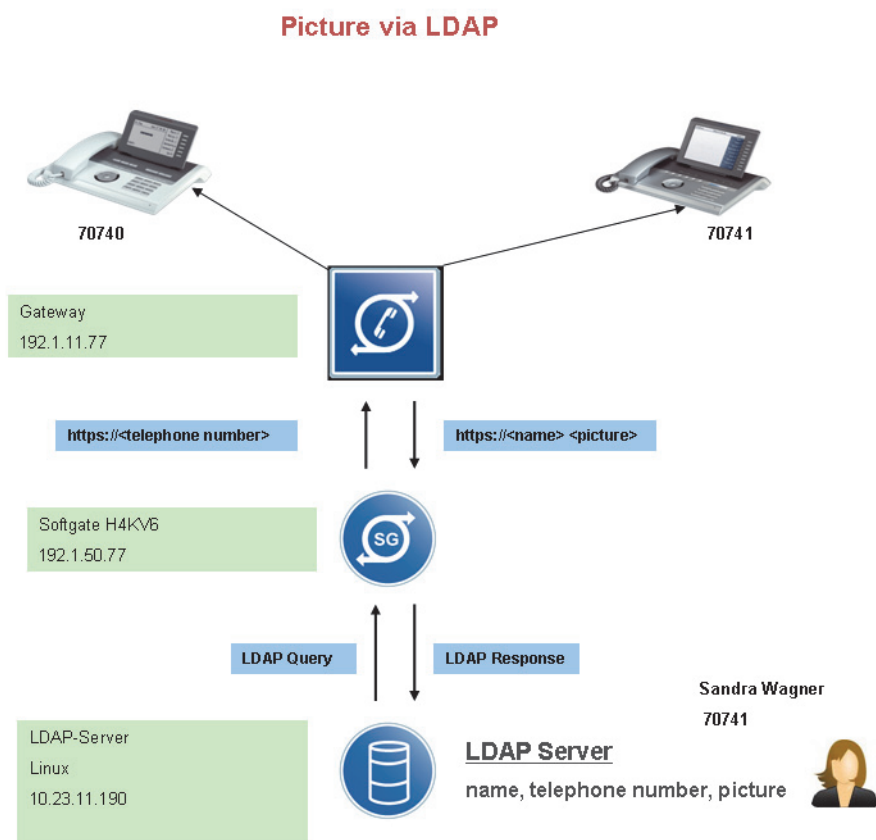
The OpenScape Desk Phone IP 55G HFA uses the services of an intermediate service located on OpenScape 4000 V7 Softgate via https messages. The Softgate lookup service then contacts the directory server via LDAP and queries for the name and picture corresponding to the requested phone number.

The OpenScape Desk Phone IP 55G 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.



3.10.2.1 "Softgate V6" settings for central access to subscriber pictures

Required input

- The url (including protocol and port) to reach the directory server LDAP account
- Password
- Node under which to search for contact data
- Key under which the mobile number is stored
- Key under which the regular telephone number is stored
- Key under which a further telephone number is stored
- Key under which the picture is stored
- Url prefix of location to fetch picture from (indirect mode, may be empty in case of direct mode)
- Key under which the first name(s) is/are stored
- Key under which the last name is stored
- Url suffix of location to fetch picture from (indirect mode, may be empty in case of direct mode)

For further information please refer to "Softgate V6" documentation

3.10.2.2 Local Phone Configuration

Feature configuration data is provided via xml settings (see also Section 3.12.1, "XML Applications/Xpressions(OpenScape Desk Phone IP 55G)").

Administration via WBM

Applications > XML Applications > Add application

Administration
Corporate Phonebook: Directory Settings

Add application

Display name	<input type="text" value="ldap"/>
Application name	<input type="text" value="ldap"/>
HTTP Server address	<input type="text" value="172.29.136.224"/>
HTTP Server port	<input type="text" value="443"/>
Protocol	<input type="text" value="https"/>
Program name on server	<input type="text" value="ldap"/>
Use proxy	<input checked="" type="checkbox"/> Yes
XML Trace enabled	<input checked="" type="checkbox"/> Yes
Debug program on server	<input type="text"/>
Number of tabs	<input type="text" value="0"/>
All tabs Start	<input type="checkbox"/>
Tab 1 Display Name	<input type="text"/>
Tab 1 Application name	<input type="text"/>
Tab 2 Display Name	<input type="text"/>
Tab 2 Application name	<input type="text"/>
Tab 3 Display Name	<input type="text"/>
Tab 3 Application name	<input type="text"/>
Restart after change	<input type="checkbox"/>

Submit

Reset

- Administration
 - Applications
 - XML
 - Add application
 - Display name
 - Application name
 - Server address
 - Server port
 - Protocol
 - Program name
 - Auto start
 - Use Proxy
 - XML trace
 - Debug name
 - Number of tabs
 - All tabs start
 - Tab 1 display name
 - Tab 1 application name
 - Tab 2 display name
 - Tab 2 application name
 - Tab 3 display name
 - Tab 3 application name
 - Restart after change

Variable parts of the configuration:

- Server address – the ip address of the server hosting the feature servlet (Softgate)
- Server port – the http port (varies according to the Protocol configured, but Softgate only allows 443)
- Protocol – https (Softgate only allows https).
- Use proxy – **Yes** means the ldap server only provides a reference to the picture for indirect retrieval, **No** means the ldap server provides the picture itself (direct retrieval)

Display name, Application name, Program name must be configured as shown. None of the other configuration items are currently evaluated for the feature.

Administration

Corporate Phonebook: Directory Settings

3.10.2.3 Phone Canonical 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 3.6.1, “Canonical Dialing Configuration”). The format of the resulting number should match the format the numbers are stored in the directory server. It is recommended to convert the numbers to fully qualified format, i.e. adding country and area code to the subscriber number. This way it is ensured that the number used for lookup is unique.

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

Administration via WBM

Local functions > Locality > Canonical dial settings

Canonical dial settings

Local country code	49
National prefix digit	0
Local national code	89
Minimum local number length	5
Local enterprise node	8008
PSTN access code	0
International access code	00
Operator codes	
Emergency numbers	
Initial extension digits	1,2,3,4,5,6,7,8,9

Submit

Reset

- Administration
 - Local Functions
 - Locality
 - Canonical dial settings
 - Local country code
 - National prefix digit
 - Local national code
 - Minimum local number length
 - Local enterprise node
 - PSTN access code
 - International code
 - Operator code
 - Emergency number
 - Initial extension digits

3.11 Speech

3.11.1 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

Port configuration	
Gateway	4060
Standby gateway	4060
RTP base	5004
System H.225	1720
Standby H.225	1720
System Cornet TLS	4061
Standby Cornet TLS	4061
System H.225 TLS	1300
Standby H.225 TLS	1300
Download server (default)	21
LDAP server	389
HTTP Proxy	0
LAN port speed	Automatic
PC port speed	Automatic
PC port mode	disabled
PC port autoMDIX	<input type="checkbox"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Administration via Local Phone

```

├─ Admin
│   └─ Network
│       └─ Port configuration
│           └─ RTP base
    
```

3.11.2 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 IP 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"
- **Allow "HD" icon:** If "On" an additional icon is shown when codec G.722 is used.
Value range: "On", "Off"
Default: "On"
- **Packet size:** Size of RTP packets in milliseconds.
Value range: "10 ms", "20ms", "30ms", "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"

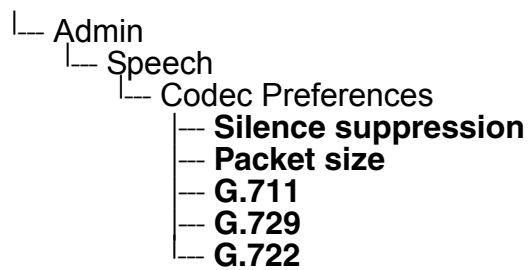
Administration via WBM

Speech > Codec preferences

The screenshot shows a web interface titled "Codec preferences". It contains the following elements:

- Silence suppression:** A checkbox that is currently unchecked.
- Packet size:** A dropdown menu with "Automatic" selected.
- G.711 ranking:** Two circular buttons: a green one with a downward arrow and a red one with an "X".
- G.729 ranking:** Three circular buttons: a green one with an upward arrow, a green one with a downward arrow, and a red one with an "X".
- G.722 ranking:** Two circular buttons: a green one with an upward arrow and a green one with a checkmark.
- Submit and Reset buttons:** Located at the bottom of the form.

Administration via Local Phone



3.11.3 Display General Phone Information

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

Displayed Data

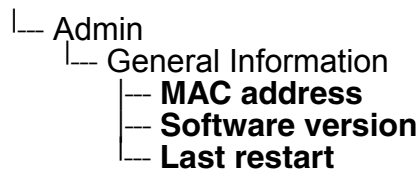
- **MAC address:** Shows the phone’s MAC address.
- **Software version:** Displays the version of the phone’s firmware.
- **Last restart:** Shows date and time of the last reboot.

Display on the WBM

General information

General information	
MAC address:	0001e323f9a1
Software version:	0.7.5.0004-061027
Last restart:	2014-02-18T13:30

Display on the Local Phone



3.12 Applications

3.12.1 XML Applications/Xpressions(OpenScape Desk Phone IP 55G)

3.12.1.1 Setup/Configuration

The XML interface enables server-based applications with a set of GUI elements. The technologies commonly used in web applications can be used: Java Servlets, JSP, PHP, CGI etc., delivered by servers such as Tomcat, Apache, Microsoft IIS.



A maximum number of 20 XML applications can be configured on OpenScape Desk Phone IP 55G.

An XML application can be started by using the Menu key to navigate to the **Applications** tab and then selecting an application, or by assigning it to a program key (System > Features > Program keys).



Xpressions is a special Unified Communications application which also uses the XML interface. Thus, the configuration is just the same as with other XML applications, except a few parameters, which are pre-configured. For details, please refer to the relevant Xpressions documentation. When configured on the phone, a press on Message will invoke this application.



XML Phonebook is a preconfiguration intended for a regular XML application with phonebook functionality. When configured on the phone, a press on Directory key will invoke this application, in place of the personal (local) or corporate (LDAP) phonebook.

For detailed information about the XML application interface, please see the OpenScape Desk Phone IP 55G - XML Applications Developer's Guide. You can find the current version under http://wiki.unify.com/index.php/OpenStage_XML_Applications.

To set up a new XML application, enter the access data for the application on the server, which is described in the following.

The **Display name** can be defined freely. This name will appear in the applications tab once the application is configured, and it will appear in a newly created tab when the application is running. With Xpressions, this value is predefined as "Xpressions".

The **Application name** is used by the phone software to identify the XML application running on the phone. With Xpressions, this value is predefined as "Xpressions".

The **HTTP Server address** is the IP address or domain name of the server which hosts the remote program. **HTTP Server port** specifies the corresponding port.

The **Protocol** for exchanging XML data with the server-side program can be set to "HTTP" or "HTTPS".

Program name on server specifies the relative path to the servlet or to the first XML page of the application on the server. The relative path refers to the root directory for documents on the web server. For instance, if an XML document is saved in:

`C:\Program Files\Apache Group\Apache\htdocs\ipp\ippTest.xml`

the entry is:

`ipp/ippTest.xml`.

The program name cannot be longer than 100 characters.

Auto start determines whether the application is started automatically on phone startup or on mobile user logon. Please note that, for being started on logon, the application must be part of the mobile user's profile. When activated, the application will be ready without delay as soon as the user presses the corresponding start key or navigates to the application in the application menu.

XML trace enabled determines whether debugging information is sent to a special debugging program on the remote server. The relative path for the debugging program is given by the **Debug program name** parameter. When enabled, trace information about the XML elements and key internal objects is sent to the remote debug program.

Debug program name specifies the relative path to a special program on the same server as the program specified by **Program name**. This program must be able to receive the debug information sent by the phone as HTTP/HTTPS POST requests with **Content-Type** set to `application/x-www-form-urlencoded`.

XML applications can have internal tabs, if desired. The number of these tabs is specified in **Number of tabs**.



For an XML application with a number of tabs > 0, one of the entries between **Tab 1 Application Name** and **Tab 3 Application Name** must be set to the same value as the **Application name** that it is associated with. When the XML application is started, the tab which has the same name as the XML application is the tab that initially gets focus.

All tabs start determines whether all tabs of the application are started automatically when the application is started.

Tab 1...3 Display Name provides the label text for the corresponding tab.

Tab 1...3 Application Name is required if the application has internal tabs. This is a unique name for the specified tab. The remote program will use this name to provide the tab with specific content.

Auto restart / Restart after change : If checked, a running XML application is automatically restarted after it has been modified. This might be especially useful for special XML applications, like messages applications, or phonebook applications, as these cannot be stopped or

restarted by the user. Please note that a restart will take place even if no changes have been made for the application selected in the **Modify/Delete application** mask, and **Submit** has been pressed. After the XML application has restarted, this option is automatically unchecked. If the option is checked whilst the XML application is not running, there will be no restart, and the option is automatically unchecked.

Data required

- **Display name:** Program name to be displayed on the phone.
Value specifications:
 - It must be unique on the phone.
 - It cannot contain the '^' character.
 - It cannot not be empty.
 - Its length cannot not exceed 20 characters.
- **Application name:** Used internally to identify the XML application running on the phone.
Value specifications:
 - It must be unique on the phone.
 - It cannot contain non-alphanumeric characters, spaces for instance.
 - The first character must be a letter.
 - It must not be empty.
 - Its length must not exceed 20 characters.
- **Protocol:** Communication protocol for the data exchange with the server.
Value range: "HTTP", "HTTPS"
Default: "HTTPS"
- **HTTP Server address:** IP address or domain/host name of the server that provides the application or the XML document.
Examples: 192.168.1.133, backoffice.intranet
- **Server port number:** Number of the port that the server uses to provide the application or XML document.
Examples: 80 (Apache default port), 8080 (Tomcat default port).
- **Program name:** Relative path to the servlet or to the first XML page of the application on the server. For instance, if an XML document is saved in:
C:\Program Files\Apache Group\Apache\htdocs\ipp\ippTest.xml
the entry is:
ipp/ippTest.xml
The program name cannot be longer than 100 characters.
- **XML trace enabled:** Enables or disables the debugging of the XML application.
Value range: "Yes", "No"
Default: "No"
- **Debug program name:** The relative path to a special servlet that receives the debug information.

Administration

Applications

Administration via WBM

A fixed function key can be defined as a start key for an XML application, in addition to the previously available start methods. Since the parameters are the same for those types of application, only the screenshot for a regular XML application is shown underneath.

Applications > XML applications > Add application

Applications > XML applications > Add messages application

Applications > XML applications > Xpressions

Applications > XML applications > Add directory application

Applications > XML applications > Add call log application

Add application

Display name	<input type="text"/>
Application name	<input type="text"/>
HTTP Server address	<input type="text"/>
HTTP Server port	<input type="text"/>
Protocol	<input type="text" value="http"/>
Program name on server	<input type="text"/>
Auto start	<input type="checkbox"/>
Use proxy	<input type="text" value="Yes"/>
XML Trace enabled	<input type="text" value="Yes"/>
Debug program on server	<input type="text"/>
Number of tabs	<input type="text" value="0"/>
All tabs Start	<input type="checkbox"/>
Tab 1 Display Name	<input type="text"/>
Tab 1 Application Name	<input type="text"/>
Tab 2 Display Name	<input type="text"/>
Tab 2 Application Name	<input type="text"/>
Tab 3 Display Name	<input type="text"/>
Tab 3 Application Name	<input type="text"/>
Restart after change	<input type="checkbox"/>

Applications > XML Applications > Modify/Delete application

Modify/Delete application

Select application
testxml
Modify
Delete

Settings

Display name
testxml
Application name
testxml
HTTP Server address
192.168.1.150
HTTP Server port
8080
Protocol
http
Program name on server
testxml/servlet
Auto start
☒
Use proxy
No
XML Trace enabled
No
Debug program on server
Number of tabs
0
All tabs start
☐
Tab 1 Display Name
Tab 1 Application Name
Tab 2 Display Name
Tab 2 Application Name
Tab 3 Display Name
Tab 3 Application Name
Restart after change
☐
Mode key
0
Submit
Reset

Administration via Local Phone

- └─ Admin
 - └─ Applications
 - └─ XML
 - └─ Add application
 - Display name
 - Application name
 - Server address
 - Server port
 - Protocol
 - Program name
 - Auto start
 - Use Proxy
 - XML trace
 - Debug name
 - Number of tabs
 - All tabs start
 - Tab 1 display name
 - Tab 1 application name
 - Tab 2 display name
 - Tab 2 application name
 - Tab 3 display name

Administration

Applications

- |— **Tab 3 application name**
- |— **Restart after change**

3.12.1.2 HTTP Proxy

For the HTTP data transfer between the phone and the server hosting the remote program, an HTTP proxy can be used.

First, the proxy itself must be configured. Enter the IP address of the proxy it in the Network > IP configuration > HTTP proxy parameter, and the corresponding port in the Network > Port configuration > HTTP proxy parameter.

Use proxy enables or disables the use of the proxy. If disabled, the phone connects directly to the server. By default, the use of a proxy is disabled.

Administration via WBM

Applications > XML Applications > Add application

Add application

Display name	<input type="text"/>
Application name	<input type="text"/>
HTTP Server address	<input type="text"/>
HTTP Server port	<input type="text"/>
Protocol	http
Program name on server	<input type="text"/>
Use proxy	Yes
XML Trace enabled	Yes
Debug program on server	<input type="text"/>

Submit Reset

Applications > XML Applications > Modify/Delete application

Modify/Delete application

Select application: Weather

Modify Delete

Settings

Display name	Weather
Application name	Weather
HTTP Server address	87.106.21.36
HTTP Server port	8080
Protocol	http
Program name on server	WR/WR
Use proxy	No
XML Trace enabled	No
Debug program on server	<input type="text"/>

Submit Reset

Administration
Applications

Network > IP configuration

IP configuration

[Disable DHCP](#)

LLDP-MED Enabled

☐

DHCP Enabled

☐

IP address

192.168.1.105

Subnet mask

255.255.255.0

Default route

192.168.1.2

DNS domain

Primary DNS

192.168.1.105

Secondary DNS

192.168.1.2

Route 1 IP address

Route 1 gateway

Route 1 mask

Route 2 IP address

Route 2 gateway

Route 2 mask

VLAN discovery

DHCP

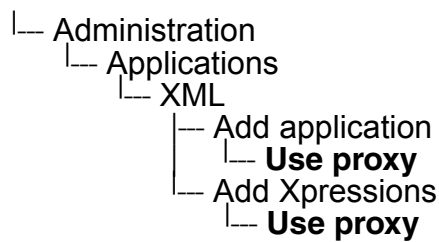
VLAN ID

HTTP proxy

Submit

Reset

Administration via Local Phone



3.12.1.3 Modify an Existing Application

An existing application can be modified by changing its parameters. Please ensure to select the desired application before changing the parameters.

Administration via WBM

Applications > XML applications > Modify/Delete application

Administration via Local Phone

```

├─ Admin
│   └─ Applications
│       └─ XML
│           └─ <Application to be modified>
│               └─ Display name
│               └─ Application name
│               └─ Server address
│               └─ Server port
│               └─ Protocol
│               └─ Program name
│               └─ XML trace enabled
│               └─ Debug program name

```

Administration

Applications

3.12.1.4 Remove an Existing Application

An existing application can be removed. Please ensure to select the desired application before changing the parameters.

Administration via WBM

Applications > XML applications > Modify/Delete application

Modify/Delete application

Select application: Weather

Modify Delete

Settings

Display name	Weather
Application name	Weather
HTTP Server address	87.106.21.36
HTTP Server port	8080
Protocol	http
Program name on server	WR/WR
Use proxy	No
XML Trace enabled	No
Debug program on server	

Submit Reset

Administration via Local Phone

Select the application to be deleted, and, in the context menu, select **Remove & exit**.

```
|__ Admin
    |__ Applications
        |__ XML
            |__ <Application to be deleted>
```


3.13 Password

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

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

Administration via WBM

Security and Policies > Password > Change Admin password

Security and Policies > Password > Change User password

Administration via Local Phone

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

Administration

Troubleshooting: Lost Password

3.14 Troubleshooting: Lost Password

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

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

3.15 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**

3.16 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**

3.17 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.

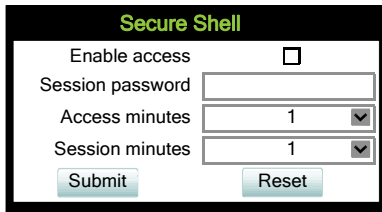
Session minutes defines the maximum length in minutes for an SSH connection. After it has expired, the "admin" user is logged out. The possible values are 5, 10, 20, 30, 60.

Administration via WBM

Maintenance > Secure Shell

Administration

Display License Information

A screenshot of a 'Secure Shell' configuration window. It has a title bar with the text 'Secure Shell' in green. Inside the window, there is a checkbox labeled 'Enable access' which is currently unchecked. Below this is a text input field labeled 'Session password'. Underneath the password field are two dropdown menus: 'Access minutes' and 'Session minutes', both of which are set to '1'. At the bottom of the window are two buttons: 'Submit' and 'Reset'.

3.18 Display License Information

The license information for the OpenStage 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**

3.19 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 OpenStage phone remotely. For security reasons, this tool can only be used when a dongle key file is uploaded to the phone (see Section 3.9.9, “Dongle Key”). This key is accessible 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 3.9.9, “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 4.4, “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 these settings are the result of auto-negotiation during the initialization of the link, or of manual set override actions.
- **System capabilities:** The devices advertise their potential and currently enabled functions, e. g. "Bridge", "Telephone".
- **TTL: Time To Live.** This parameter determines how long the TLVs are valid. When expired, the device will send a new set of TLVs.

Administration via WBM

Admin > Network > LLDP-MED operation

LLDP-MED operation

Time to live (seconds)

View Data From WBM

Diagnostics > LLDP-MED TLVs

LLDP-MED TLV's	
Sent	Received
Sent: Mon Oct 27 10:41:14 2013	Received: Mon Oct 27 10:41:14 2013
Chassis ID TLV Data .ID = 163.165.2.105	Chassis ID TLV Data .ID = 00:3E:37:01:20:01
TTL TLV Data .seconds = 120	TTL TLV Data .seconds = 120
System Caps TLV Data .Supported = Bridge, Telephone .Enabled = Telephone	System Caps TLV Data .Supported = Other, Repeater .Enabled = Other, Repeater

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 IP. 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 IP 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

- **Administration**
Deals with the changing and setting of parameters within the phone database, from both the User and Admin menus.
- **AGP Phonelet**
- **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.
- **Bluetooth service (not applicable for OpenScape Desk Phone IP 33G/55G)**

Handles the Bluetooth interactions between external Bluetooth devices and the phone. Bluetooth is available only on OpenStage 60/80 phones.

- **Call Log**

The Call log application displays the call history of the phone.

- **Call View**

Handles the representation of telephony calls on the phone screen.

- **Certificate management**

Handles the verification and exchange of certificates for security and verification purposes.

- **Clock Service**

Handles the phone's time and date, including daylight saving and NTP functionality.

- **Communications**

Involved in the passing of call related information and signaling to and from the CSTA service.

- **Component registrar**

Handles data relating to the type of phone, e.g. OpenScape Desk Phone IP 33G/55G 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).

- **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.

- **H.323 messages**

- **HFA service agent**

- **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 IP 33G/55G)**
Involved with Bluetooth accesses to the phone.
Bluetooth is available only on OpenStage 60/80 phones.
- **OpenStage client management**
Provides a means by which other services within the phone can interact with the database.
- **Password management service**
Verifies passwords used in the phone.
- **Phonebook**
Responsible for the phonebook application.
- **Performance Marks**
Aid for measuring the performance of the phone. For events triggered by the user, a performance mark is written to the trace file, together with a timestamp in the format hh:mm:ss yyyy.milliseconds, and information about the event. The timespan between two performance marks is an indicator for the performance of the phone.



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

- **Physical interface service**
Handles any interactions with the phone via the keypad, mode keys, fixed feature buttons, clickwheel and slider.
- **Service framework**

Administration

Diagnostics

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.
- **Security Log Service**
- **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.
- **vCard parser service**
Handles parsing and identification of VCard information while sending or getting VCards via Bluetooth.
- **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.
- **802.1x service**
Provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. The service is used for certain closed wireless access points.

Administration via WBM

Diagnostics > Fault trace configuration

Fault trace configuration

File size (bytes)

Trace timeout (minutes)

Automatic clear before start ☐

Trace levels for components

Administration	<input type="text" value="OFF"/>	Application framework	<input type="text" value="OFF"/>
Application menu	<input type="text" value="OFF"/>	Bluetooth service	<input type="text" value="OFF"/>
Call Log	<input type="text" value="OFF"/>	Call View	<input type="text" value="OFF"/>
Certificate management	<input type="text" value="OFF"/>	Communications	<input type="text" value="OFF"/>
Component registrar	<input type="text" value="OFF"/>	CSTA service	<input type="text" value="OFF"/>
Data Access service	<input type="text" value="OFF"/>	Desktop	<input type="text" value="OFF"/>
Digit analysis service	<input type="text" value="OFF"/>	Directory service	<input type="text" value="OFF"/>
DLS client management	<input type="text" value="OFF"/>	Health service	<input type="text" value="OFF"/>
Help	<input type="text" value="OFF"/>	HFA service agent	<input type="text" value="OFF"/>
H.323 messages	<input type="text" value="OFF"/>	AGP Phonelet	<input type="text" value="OFF"/>
Media procession service	<input type="text" value="OFF"/>	Media control service	<input type="text" value="OFF"/>
Instrumentation service	<input type="text" value="OFF"/>	OpenStage client management	<input type="text" value="OFF"/>
OBEX service	<input type="text" value="OFF"/>	Performance Marks	<input type="text" value="OFF"/>
Phonebook	<input type="text" value="OFF"/>	Physical interface service	<input type="text" value="OFF"/>
Password management service	<input type="text" value="OFF"/>	Service registry	<input type="text" value="OFF"/>
Service framework	<input type="text" value="OFF"/>	Tone generation service	<input type="text" value="OFF"/>
Sidecar service	<input type="text" value="OFF"/>	vCard parser service	<input type="text" value="OFF"/>
Transport service	<input type="text" value="OFF"/>	Voice mail	<input type="text" value="OFF"/>
Voice generation service	<input type="text" value="OFF"/>	Transport service	<input type="text" value="OFF"/>
vCard parser service	<input type="text" value="OFF"/>	USB backup service	<input type="text" value="OFF"/>
Web server service	<input type="text" value="OFF"/>	802.1 x service	<input type="text" value="OFF"/>
Voice recognition	<input type="text" value="OFF"/>	Security Log Service	<input type="text" value="OFF"/>
Clock Service	<input type="text" value="OFF"/>	HTTP Service	<input type="text" value="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](#)

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

Call connection

File size (Max 6290000 bytes)

1048576

Trace timeout (minutes)

0

Automatic clear before start

☐

Trace levels for components

Component registrar	TRACE	▼
Health service	LOG	▼
Service registry	TRACE	▼
Call View	TRACE	▼
Communications	TRACE	▼
CSTA service	TRACE	▼
H.323 messages	DEBUG	▼


[Download trace file](#)

[Download saved trace file](#)

[Download H.323 trace file](#)

Submit

Reset



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

Call log problems

File size (Max 6290000 bytes)

Trace timeout (minutes)

Automatic clear before start
☐

Trace levels for components

Call Log	TRACE	▼
Component registrar	TRACE	▼
Health service	LOG	▼
Application framework	TRACE	▼
Desktop	TRACE	▼
Journal service	TRACE	▼

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

[Download H.323 trace file](#)

3.20.3.3 DAS Connection

Diagnostics > EasyTrace Profiles > DAS connection

DAS connection

File size (Max 6290000 bytes)

Trace timeout (minutes)

Automatic clear before start
☐

Trace levels for components

Certificate management	LOG	▼
Component registrar	TRACE	▼
Health service	LOG	▼
DLS client management	TRACE	▼
Service framework	TRACE	▼

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

[Download H.323 trace file](#)

3.20.3.4 DLS Data Errors

Diagnostics > EasyTrace Profiles > DLS data errors

DLS data errors

File size (Max 6290000 bytes)

1048576

Trace timeout (minutes)

0

Automatic clear before start

☐

Trace levels for components

Certificate management	LOG
Component registrar	TRACE
Data Access service	TRACE
Health service	LOG
DLS client management	TRACE
OpenStage client management	LOG
Service framework	TRACE

[Download trace file](#)

[Download saved trace file](#)

[Download H.323 trace file](#)

Submit

Reset

3.20.3.5 HFA registration and security

Diagnostics > EasyTrace Profiles > HFA registration and security

HFA registration and security problems

File size (Max 6290000 bytes)

1048576

Trace timeout (minutes)

0

Automatic clear before start

☐

Trace levels for components

Communications	TRACE
H.323 messages	TRACE

[Download trace file](#)

[Download saved trace file](#)

[Download H.323 trace file](#)

Submit

Reset

3.20.3.6 Help Application

Diagnostics > EasyTrace Profiles > Help application problems

Help application problems

File size (Max 6290000 bytes)

Trace timeout (minutes)

Automatic clear before start
☐

Trace levels for components

Application menu	LOG	▼
Component registrar	TRACE	▼
Health service	LOG	▼
Application framework	TRACE	▼
Help	DEBUG	▼
Web server service	TRACE	▼

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

[Download H.323 trace file](#)

3.20.3.7 Key Input

Diagnostics > EasyTrace Profiles > Key input problems

Key input problems

File size (Max 6290000 bytes)

Trace timeout (minutes)

Automatic clear before start
☐

Trace levels for components

Component registrar	TRACE	▼
Health service	LOG	▼
Physical interface service	DEBUG	▼

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

[Download H.323 trace file](#)

3.20.3.8 LAN Connectivity

Diagnostics > EasyTrace Profiles > LAN connectivity problems

LAN connectivity problems

File size (Max 6290000 bytes)

1048576

Trace timeout (minutes)

0

Automatic clear before start

☐

Trace levels for components

Component registrar

TRACE

Health service

LOG

Transport service

TRACE

HTTP service

TRACE

[Download trace file](#)

[Download saved trace file](#)

[Download H.323 trace file](#)

Submit

Reset

3.20.3.9 Messaging

Diagnostics > EasyTrace Profiles > Messaging application problems

Messaging application problems

File size (Max 6290000 bytes)

1048576

Trace timeout (minutes)

0

Automatic clear before start

☐

Trace levels for components

Component registrar

TRACE

Health service

LOG

Application framework

TRACE

Call View

TRACE

CSTA service

TRACE

Desktop

TRACE

Communications

TRACE

[Download trace file](#)

[Download saved trace file](#)

[Download H.323 trace file](#)

Submit

Reset

3.20.3.10 Mobility

Diagnostics > EasyTrace Profiles > Mobility problems

Mobility problems

File size (Max 6290000 bytes)
Trace timeout (minutes)
Automatic clear before start ☐

Trace levels for components

Administration	TRACE	▼
Data Access service	TRACE	▼
DLS client management	LOG	▼
Mobility service	TRACE	▼

[Download trace file](#)
[Download saved trace file](#)
[Download H.323 trace file](#)

3.20.3.11 Phone administration

Diagnostics > EasyTrace Profiles > Phone administration problems

Phone administration problems

File size (Max 6290000 bytes)
Trace timeout (minutes)
Automatic clear before start ☐

Trace levels for components

Administration	TRACE	▼
Health service	WARNING	▼
OpenStage client management	LOG	▼
Application framework	TRACE	▼
Communications	TRACE	▼
CSTA service	TRACE	▼
Desktop	TRACE	▼

[Download trace file](#)
[Download saved trace file](#)
[Download H.323 trace file](#)

3.20.3.12 Local Phonebook

Diagnostics > EasyTrace Profiles > Phonebook (local) problems

Phonebook (local) problems

File size (Max 6290000 bytes)

1048576

Trace timeout (minutes)

0

Automatic clear before start

☐

Trace levels for components

Application menu	LOG	▼
Component registrar	TRACE	▼
Health service	LOG	▼
Application framework	TRACE	▼
Desktop	TRACE	▼
Journal service	TRACE	▼

[Download trace file](#)

[Download saved trace file](#)

[Download H.323 trace file](#)

Submit

Reset

3.20.3.13 LDAP Phonebook

Diagnostics > EasyTrace Profiles > Phonebook (LDAP) problems

Phonebook (LDAP) problems

File size (Max 6290000 bytes)

1048576

Trace timeout (minutes)

0

Automatic clear before start

☐

Trace levels for components

Application menu	LOG	▼
Component registrar	TRACE	▼
Directory service	LOG	▼
Health service	TRACE	▼
Application framework	TRACE	▼
Desktop	TRACE	▼
Journal service	TRACE	▼
Transport service	TRACE	▼

[Download trace file](#)

[Download saved trace file](#)

[Download H.323 trace file](#)

Submit

Reset

3.20.3.14 Server based applications

Diagnostics > EasyTrace Profiles > Server based application problems

Server based application problems	
File size (Max 6290000 bytes)	<input type="text" value="1048576"/>
Trace timeout (minutes)	<input type="text" value="0"/>
Automatic clear before start	<input type="checkbox"/>
Trace levels for components	
AGP Phonelet	LOG <input type="button" value="v"/>
Download trace file	Download saved trace file
Download H.323 trace file	
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

3.20.3.15 Sidecar

Diagnostics > Easy Trace Profiles > Sidecar problems

Sidecar problems	
File size (Max 6290000 bytes)	<input type="text" value="1048576"/>
Trace timeout (minutes)	<input type="text" value="0"/>
Automatic clear before start	<input type="checkbox"/>
Trace levels for components	
Component registrar	TRACE <input type="button" value="v"/>
Health service	LOG <input type="button" value="v"/>
Sidecar service	DEBUG <input type="button" value="v"/>
Download trace file	Download saved trace file
Download H.323 trace file	
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

3.20.3.16 Speech

Diagnostics > EasyTrace Profiles > Speech problems

Speech problems	
File size (Max 6290000 bytes)	<input type="text" value="1048576"/>
Trace timeout (minutes)	<input type="text" value="0"/>
Automatic clear before start	<input type="checkbox"/>
Trace levels for components	
Component registrar	TRACE <input type="button" value="v"/>
Health service	LOG <input type="button" value="v"/>
Voice engine service	TRACE <input type="button" value="v"/>
Media processing service	TRACE <input type="button" value="v"/>
Download trace file	Download saved trace file
Download H.323 trace file	
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

3.20.3.17 **Tone**

Diagnostics > EasyTrace Profiles > Tone problems

Tone problems

File size (Max 6290000 bytes)

1048576

Trace timeout (minutes)

0

Automatic clear before start

☐

Trace levels for components

Component registrar

TRACE

▼

Health service

LOG

▼

Tone generation service

TRACE

▼

Media processing service

TRACE

▼

[Download trace file](#)

[Download saved trace file](#)

[Download H.323 trace file](#)

Submit

Reset

3.20.3.18 **USB Backup/Restore**

Diagnostics > EasyTrace Profiles > USB backup/restore

USB backup/restore

File size (Max 6290000 bytes)

1048576

Trace timeout (minutes)

0

Automatic clear before start

☐

Trace levels for components

Administration

TRACE

▼

Component registrar

TRACE

▼

Physical interface service

DEBUG

▼

USB backup service

DEBUG

▼

[Download trace file](#)

[Download saved trace file](#)

[Download H.323 trace file](#)

Submit

Reset

3.20.3.19 Web Based Management

Diagnostics > EasyTrace Profiles > Web based management

Web based management

File size (Max 6290000 bytes)

Trace timeout (minutes)

Automatic clear before start ☐

Trace levels for components

Data Access service	TRACE	<input type="button" value="v"/>
OpenStage client management	TRACE	<input type="button" value="v"/>
Web server service	TRACE	<input type="button" value="v"/>
USB backup service	TRACE	<input type="button" value="v"/>
802.1x service	TRACE	<input type="button" value="v"/>
Voice recognition	TRACE	<input type="button" value="v"/>

[Download trace file](#)
[Download saved trace file](#)
[Download H.323 trace file](#)

3.20.3.20 802.1x problems

Diagnostics > EasyTrace Profiles > 802.1x problems

802.1x problems

File size (Max 6290000 bytes)

Trace timeout (minutes)

Automatic clear before start ☐

Trace levels for components

Certificate management	LOG	<input type="button" value="v"/>
Component registrar	TRACE	<input type="button" value="v"/>
Data Access service	TRACE	<input type="button" value="v"/>

[Download trace file](#)
[Download saved trace file](#)
[Download H.323 trace file](#)

3.20.3.21 No Tracing for All Services

Diagnostics > EasyTrace Profiles > Clear all profiles

Clear all profiles

File size (Max 6290000 bytes)

1048576

Trace timeout (minutes)

0

Automatic clear before start

☐

Trace levels for components

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

[Download trace file](#)

[Download saved trace file](#)

[Download H.323 trace file](#)

Submit

Reset

3.20.4 QoS Reports

3.20.4.1 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

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

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 Miscellaneous

3.20.5.1 IP tests

For network diagnostics, the OpenScape Desk Phone IP 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 Hi-Path gatekeeper"
- **Traceroute:** Pings the entered host's IP address or hostname.

Administration via WBM

IP tests

Pre Defined Ping tests

Ping DLS

Ping

Ping tests

Ping

Pre Defined Trace tests

Traceroute DLS

Traceroute

Traceroute

Traceroute

3.20.5.2 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 IP 35G, the default value is 10 MB, and for OpenScape Desk Phone IP 55G, it is 30 MB. With **Low Threshold (MBs)**, the threshold for off-time is defined. For OpenScape Desk Phone IP 35G, the default value is 8 MB, and for OpenScape Desk Phone IP 55G, it is 20 MB.

The beginning and end of the working hours are defined in 24 hours format with **Working Hour Start** (Default: 5) and **Working Hour End** (Default: 24).

When memory shortage has occurred, information about the incident is written to a log file which can be viewed via the **Download memory info file** link. If there has been a previous case of memory shortage, the corresponding log file can be viewed via **Download memory info file**.

Administration via WBM

Diagnostics > Miscellaneous > Memory information

Memory information

Memory Monitor Configuration

Disable Reboot

High Threshold(MBs)

Low Threshold(MBs)

Working Hour Start

Working Hour End

☐

10

8

5

24

[Download memory info file](#)

[Download old memory info file](#)

Submit

Reset

Mem: 111336K used, 12380K free, 0K shrd, 0K buff, 55084K cached

CPU: 5% usr 15% sys 5% nic 25% idle 0% io 0% irq 50% sirq

Load average: 0.14 0.13 0.09 1/196 6098

PID	PPID	USER	STAT	VSZ	%MEM	%CPU	COMMAND
6098	1908	root	R	1420	1%	40%	/bin/busybox top -d 0 -a -n 1 -l 600 -b
1929	1877	root	S	44712	36%	0%	SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 HFA 110924
2515	1877	root	S	44712	36%	0%	SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 HFA 110924
1902	1877	root	S	44712	36%	0%	SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 HFA 110924
2992	1877	root	S	44712	36%	0%	SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 HFA 110924
1876	1855	root	S	44712	36%	0%	SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 HFA 110924
1880	1877	root	S	44712	36%	0%	SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 HFA 110924
2057	1877	root	S	44712	36%	0%	SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 HFA 110924
1881	1877	root	S	44712	36%	0%	SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 HFA 110924
2064	1877	root	S <	44712	36%	0%	SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 HFA 110924
2058	1877	root	S	44712	36%	0%	SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 HFA 110924
5400	1877	root	S	44712	36%	0%	SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 HFA 110924
1886	1877	root	S	44712	36%	0%	SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 HFA 110924
1885	1877	root	S	44712	36%	0%	SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 HFA 110924

3.20.5.3 Core dump

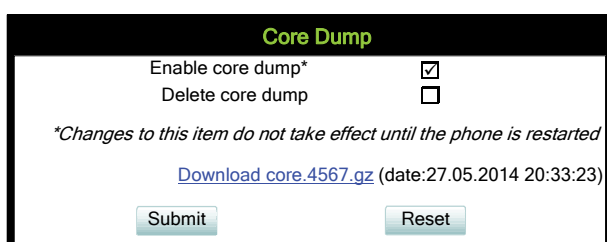
If **Enable core dump** is checked, a core dump will be initiated in case of a severe error. The core dump will be saved to a file. By default, this function is activated.

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



The screenshot shows a web-based management interface titled "Core Dump". It contains two configuration options: "Enable core dump*" with a checked checkbox and "Delete core dump" with an unchecked checkbox. Below these options is a note: "*Changes to this item do not take effect until the phone is restarted". A link "Download core.4567.gz (date:27.05.2014 20:33:23)" is displayed. At the bottom, there are "Submit" and "Reset" buttons.

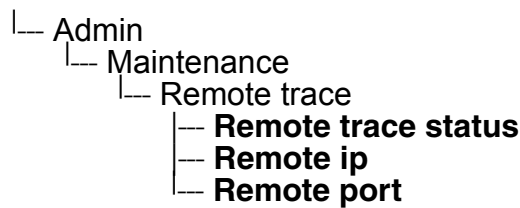
Core Dump	
Enable core dump*	<input checked="" type="checkbox"/>
Delete core dump	<input type="checkbox"/>
<i>*Changes to this item do not take effect until the phone is restarted</i>	
Download core.4567.gz (date:27.05.2014 20:33:23)	
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

3.20.6 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 Local Phone



Administration via WBM

The screenshot shows a configuration window titled "Remote trace" with a black border. It contains the following fields and controls:

- Remote Trace Status:** A dropdown menu currently set to "Disabled".
- Use Notification:** A dropdown menu currently set to "Enabled".
- Remote Server:** An empty text input field.
- Remote Server Port:** A text input field containing the value "514".
- Buttons:** "Submit" and "Reset" buttons at the bottom.

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	1 st 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 gate-way 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 gate-way 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

Examples and HowTos

Canonical Dialing

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 gate-way 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 Create Logo Files for OpenScape Desk Phone

4.2.1 For OpenScape Desk Phone IP 55G

In the following, the creation of a transparent image suitable for use as a logo in OpenScape Desk Phone IP 55G is described. This description is based on Adobe Photoshop, but any similar graphics software can be used as well.

**INFO:**

Because of performance issues, half transparency in the alpha channel of the PNG files is not allowed on OpenScape phones. Therefore only 100% transparency or no transparency is used in the phone's UI elements.

1. Select the Background Color

For production purposes, we set the background color to the background color of the skin currently selected on the phone. Later, the background color will be replaced by transparency, which facilitates placing a logo on a gradient background. The following table lists the hexadecimal values, as used in HTML:

Phone Type	Skin	Color Code
OpenScape Desk Phone IP 55G	Silver Blue	#E7E7E7
OpenScape Desk Phone IP 55G	Anthracite Orange	#424242 ¹

¹ The background color on OpenScape Desk Phone IP 55G - skin 1 is a gradient; the colour listed here is an average value.

Adobe Photoshop:

Click on the Background Color icon on the Color palette group, then type the color code without leading "#" into the # field)

Examples and HowTos

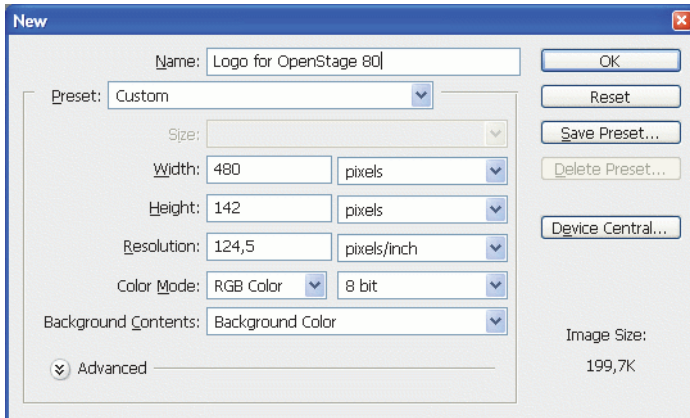
How to Create Logo Files for OpenScape Desk Phone

2. Create a New Image

Create an image with the size according to the phone type:

Phone Type	Size (px)
OpenScape Desk Phone IP 55G	240 x 70

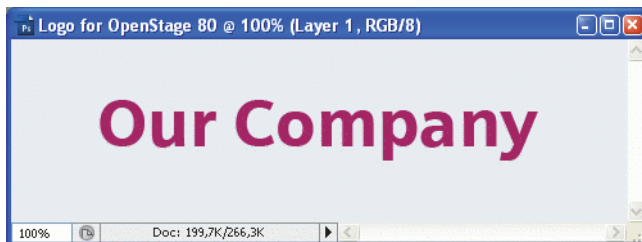
Adobe Photoshop:



3. Insert the Logo

Place the logo image on the background, e.g. by copying it from a source file.

Adobe Photoshop Example:



4. Merge Layers

Merge the two layers to one.

Adobe Photoshop:

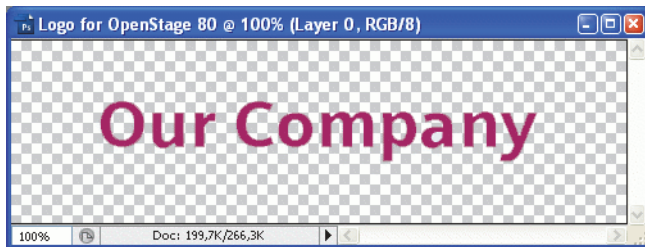
In the Panel, select both the background layer and the new layer containing the inserted logo. Afterwards, go to **Layer** in the Menu bar, and select **Merge Layers**.

5. Background Transparency

Delete the background colour so that only the exact former background colour is 100% transparent.

Adobe Photoshop:

Make sure that the background color is selected by clicking on the Background Color icon. In the Tool palette, click on the Eraser symbol with the right Mouse button and select the **Magic Eraser Tool**. After this, got to the Menu bar and set the **Tolerance** field to "0".



6. Save the Image

Finally, save the image in PNG format. You can now upload the logo file to the phone as described in Section 3.9.6, "Logo"

Examples and HowTos

How to Set Up the Corporate Phonebook (LDAP)

4.3 How to Set Up the Corporate Phonebook (LDAP)

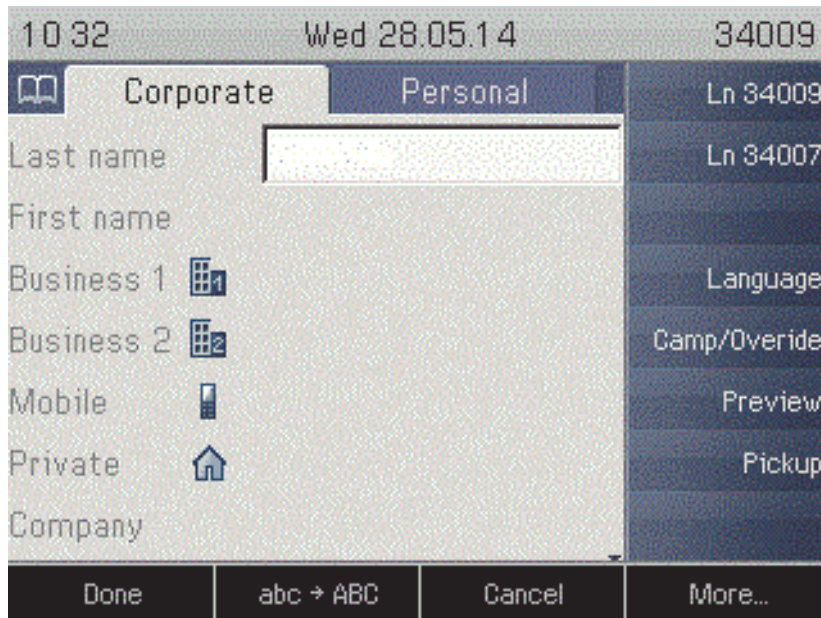
The Corporate Phonebook function is based on an LDAP client that can be connected to the company's LDAP service. A variety of LDAP servers can be used, for instance Microsoft Active Directory, OpenLDAP, or Apache Directory Server.

4.3.1 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 OpenStage 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.

4.3.2 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

Examples and HowTos

How to Set Up the Corporate Phonebook (LDAP)

OpenStage Field	LDAP Template Lables	LDAP Attribute	Example Value
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

OpenStage Field	LDAP Template Attribute	LDAP Attribute	Example Value
Business 1	ATTRIB03	ipPhone	9991234
Business 2	ATTRIB04	otherTelephoneNumber	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="otherTelephoneNumber"
ATTRIB05="mobile"
ATTRIB06="homePhone"
ATTRIB07="company"
ATTRIB08="department"
ATTRIB09=""
ATTRIB10="title"
ATTRIB11="mail"
EOF
```

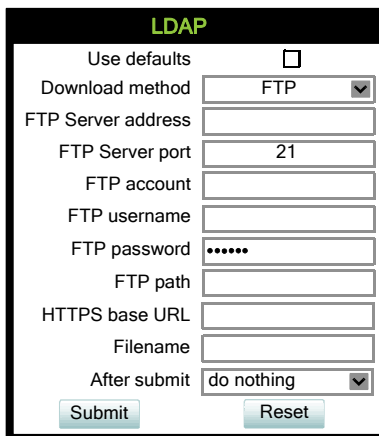
Examples and HowTos

How to Set Up the Corporate Phonebook (LDAP)

4.3.3 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):



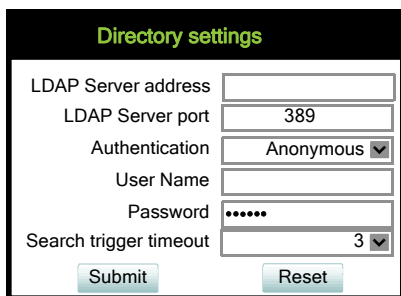
The screenshot shows a web form titled "LDAP" in green text. The form contains the following fields and controls:

- Use defaults:** A checkbox that is currently unchecked.
- Download method:** A dropdown menu with "FTP" selected.
- FTP Server address:** An empty text input field.
- FTP Server port:** A text input field containing the number "21".
- FTP account:** An empty text input field.
- FTP username:** An empty text input field.
- FTP password:** A text input field with masked characters (dots).
- FTP path:** An empty text input field.
- HTTPS base URL:** An empty text input field.
- Filename:** An empty text input field.
- After submit:** A dropdown menu with "do nothing" selected.
- Buttons:** "Submit" and "Reset" buttons at the bottom.

4.3.4 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).



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

- LDAP Server address: A text input field.
- LDAP Server port: A text input field containing the value "389".
- Authentication: A dropdown menu with "Anonymous" selected.
- User Name: A text input field.
- Password: A text input field with masked characters (dots).
- Search trigger timeout: A dropdown menu with "3" selected.
- At the bottom, there are two buttons: "Submit" and "Reset".

3. Press **Submit**.

4.3.5 Test

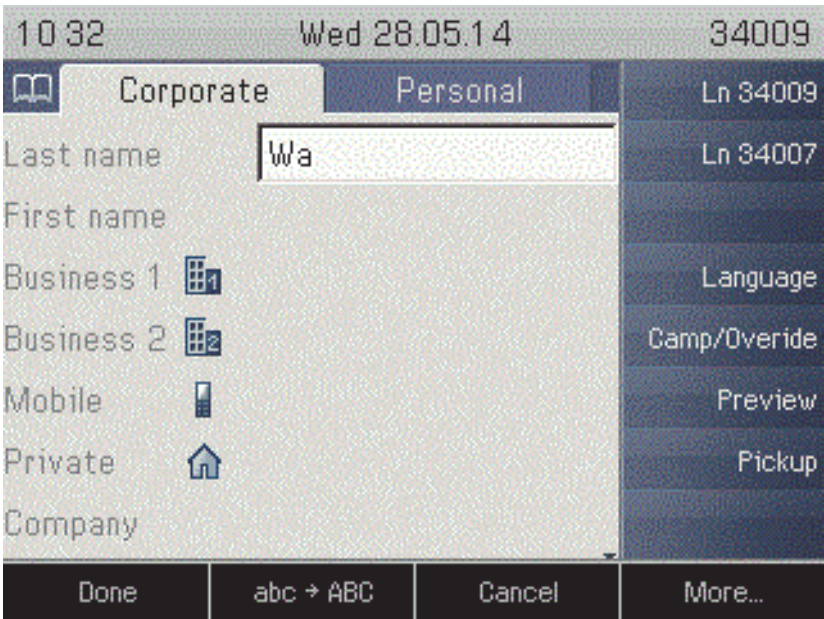
If everything went well, you can run a test query on your OpenStage Desk Phone.

1. To navigate to the phone's corporate phonebook, press the Directory button twice.
2. Press Directory key. In the context menu, select Find by pressing >.
3. In the query mask, select the entry to be searched, for instance **Last Name**. Press > to open the onscreen keypad for text input.

Examples and HowTos

How to Set Up the Corporate Phonebook (LDAP)

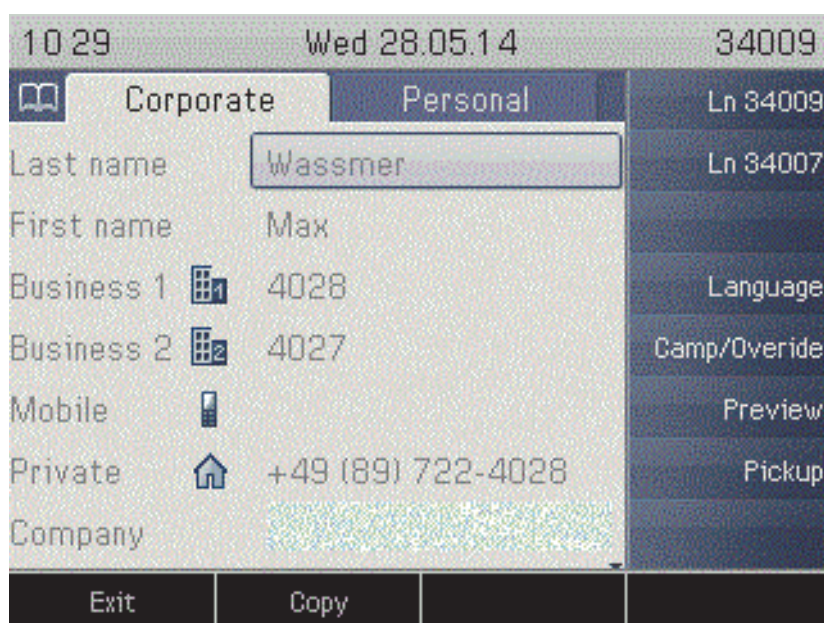
- 4. Enter the text to be searched. For information on using the onscreen keypad, see Section 3.1, “Access via Local Phone”, step 5.



- 5. Navigate to the Find option and press >. If the query was successful, at least one entry will be listed in the following manner:



6. Navigate to the desired entry and press > to open the context menu. You can select one of the following options:
- Dial the **Business 1** number.
 - Dial the **Mobile** number.
 - Have the entry's details, that is, all attributes displayed.
 - Start a new search.
 - Clear the list of search results.



Examples and HowTos

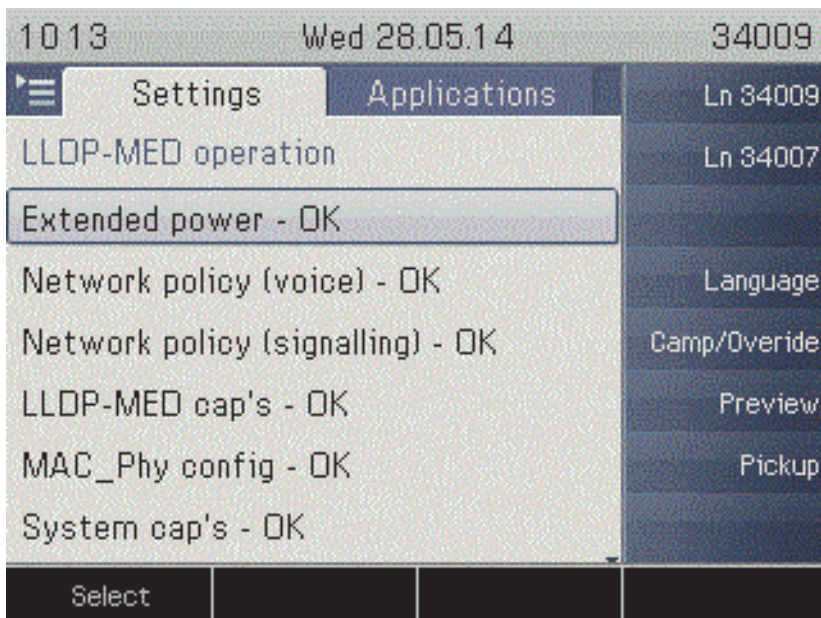
An LLDP-Med Example

4.4 An LLDP-Med Example

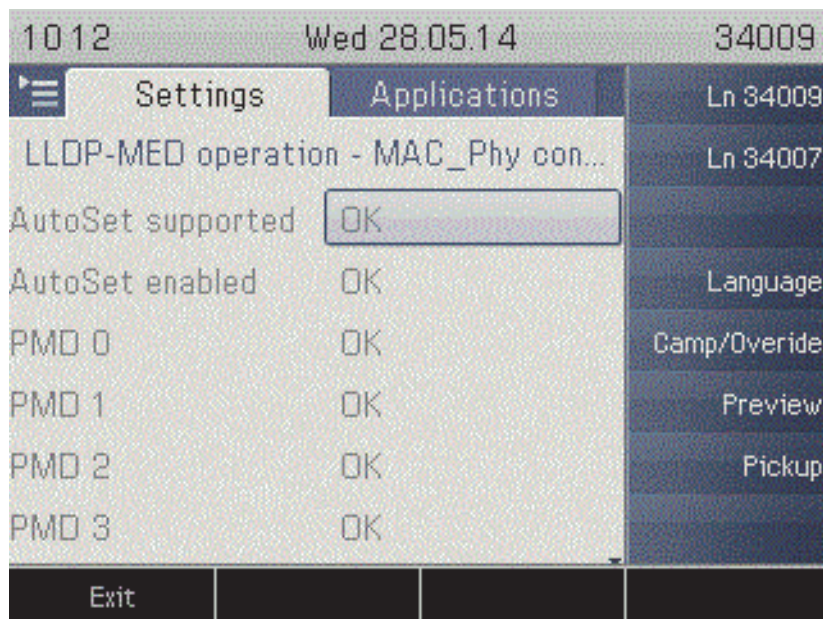
The following example illustrates the mode of operation of LLDP-MED. In order to evoke a reaction from LLDP-MED, the LAN switch has been set to auto-negotiation, whereas the phone's LAN port (see Section 3.2.1, "LAN Port Settings") is set to 100Mbit/s, hence a fixed value. This configuration error is 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:

MAC_Phy config - Error



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
OpenStage Phone Manager	65532	---	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/OpenStage_SIP_FAQ#Error_codes

Technical Reference

Troubleshooting: Error Codes

5.3 Troubleshooting: Error Messages

The following table lists the possible error messages for OpenScope 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 blocked

Table 5-2 Error Messages

Technical Reference

Troubleshooting: 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 Differential Pulse Code Modulation. 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 Supported Telecommunications Applications. An abstraction layer for telecommunications applications allowing for the interaction of -> CTI computer applications with telephony devices and networks.

CTI

Computer Telephony Integration. This term denotes the interaction of computer applications with telephony devices and networks.

D

DFT

Digital Feature Telephone. A phone with no line keys.

DHCP

Dynamic Host Configuration Protocol. Allows for the automatic configuration of network endpoints, like IP Phones and IP Clients.

DiffServ

Differentiated Services. Specifies a layer 3 mechanism for classifying and managing network traffic and providing quality of service (-> QoS) guarantees on -> IP networks. Diff-Serv 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.

Glossary

DNS

Domain Name System. Performs the translation of network domain names and computer hostnames to -> IP addresses.

DPIP55G or DPIP35G

Stands for OpenScape Desk Phone IP 55G or OpenScape Desk Phone IP 35G

DTMF

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

E

EAP

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

F

FTP

File Transfer Protocol. 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**

Hypertext **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.

Glossary

M

MAC Address

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

MDI-X

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

MIB

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

MWI

Message Waiting Indicator. A signal, typically a LED, to notify the user that new mailbox messages have arrived.

P

PBX

Private Branch Exchange. Private telephone system that connects the internal devices to each other and to the ISDN network.

PCM

Pulse Code Modulation. A digital representation of an analog signal, e. g. audio data, which consists of quantized samples taken in regular time intervals.

PING

Packet Internet Gro(u)per. A program to test whether a connection can be made to a defined IP target. Data is sent to the target and returned from there during the test.

PoE

Power over Ethernet. The IEEE 802.3af standard specifies how to supply power to compliant devices over Ethernet cabling (10/100Base-T).

Port

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

PSTN

Public Switched Telephone Network. The network of the world's public circuit-switched telephone networks.

Q**QoS**

Quality of Service. The term refers to control mechanisms that can provide different priority to different users or data flows, or guarantee a certain level of performance to a data flow in accordance with requests from the application program. The OpenScape Desk Phone phone allows for the setting of QoS parameters on layer 2 and layer 3 (DiffServ).

R**RAM**

Random Access Memory. Memory with read / write access.

ROM

Read Only Memory. Memory with read only access.

RTCP

Realtime Transport Control Protocol. Controls the -> RTP stream and provides information about the status of the transmission, like QoS parameters.

RTP

Realtime Transport Protocol. This application layer protocol has been designed for audio communication.

S**SDP**

Session Description Protocol. Describes and initiates multimedia sessions, like web conferences. The informations provided by SDP can be processed by -> SNMP.

SNMP

Simple Network Management Protocol. Used for monitoring, controlling, and administration of network and network devices.

SNTP

Simple Network Time Protocol. Used to synchronize the time of a terminal device with a timeserver.

Subnet Mask

To discern the network part from the host part of an -> 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.

Glossary

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 Control Protocol. The protocol belongs to the transport layer and establishes a connection between two entities on the application layer. It guarantees reliable and in-order delivery of data from sender to receiver.

TLS

Transport Layer Security. Ensures privacy between communicating applications. Typically, the server is authenticated, but mutual authentication is also possible.

U

URI

Uniform Resource Identifier. A compact string of characters used to identify or name a resource.

URL

Uniform Resource Locator. 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 Local Area Network. A method of creating several independent logical networks within a physical network. For example, an existing network can be separated into a data and a voice VLAN.

VoIP

Voice over IP. A term for the protocols and technologies enabling the routing of voice conversations over the internet or through any other -> IP-based network

W

WAP

Wireless Application Protocol. 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 phone.

WBM

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

WML

Wireless Markup Language. An XML-based markup language which supports text, graphics, hyperlinks and forms on a -> WAP-browser.

WSP

Wireless Session Protocol. 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) 3-42
- Application
 - Modify 3-141
 - Remove 3-142

C

- Canonical Dial Lookup 3-89
- Canonical Dialing 3-85
- Codec Preferences 3-130
- Connectors 2-15
- Core dump 3-173
- Corporate Phonebook 3-122
- CSTA 6-199
- CTI 6-199

D

- Date and Time (SNTP) 3-79
- Daylight Saving 3-79
- Default Route 3-58
- DFT 6-199
- DHCP 3-55, 6-199
- Diffserv 3-53
- Directory Settings 3-122
- DLS (Deployment Service) 1-13, 2-31, 3-64, 6-199
- DNS 3-60, 6-200
 - Domain Name 3-60
 - Primary/Secondary 3-61
 - Servers 3-61
- Dongle Key (Download) 3-119
- DST Zone (Daylight Saving Time Zone) 3-80

E

- Easy Trace Profiles 3-156
 - 802.1x 3-165
 - Call Connection 3-156
 - Call Log 3-157
 - DAS Connection 3-157
 - DLS Data Errors 3-158

- Help Application 3-159
- Key Input 3-159
- LAN Connectivity 3-160
- Local Phonebook 3-162
- Mobility 3-161
- No Tracing for All Services 3-166
- Phone administration 3-161
- Server based applications 3-163
- Speech 3-163
- Tone 3-164
- USB Backup/Restore 3-164
- Web Based Management 3-165

- Emergency Number 3-85

- Energy Saving 3-79

- Error Codes 5-193

- External Access Code 3-86

- External Numbers 3-86

F

- Factory Reset 3-144
- Fault Trace Configuration 3-150
- FTP Settings 3-98

G

- G.711 3-130
- G.722 3-130
- G.729 3-130
- Gateway 3-58
- General Information 3-132

H

- Handset 1-12
- HTTP Proxy 3-139

I

- Initial Digits 3-86
- Internal Numbers 3-86
- International Code (Local Country Code) 3-85
- International Gateway Code 3-87
- International Prefix (International Access Code) 3-85

IP

- Address 2-22, 3-57
- Address (Manual configuration) 3-57

IP 6-201
Specific Routing 3-59

L

LAN 6-201
Monitoring 3-148
Port 3-45
Layer 2 3-52
Layer 3 3-53
LDAP 3-122, 6-201
LDAP Template (Download) 3-106
License Information 3-146
LLDP-MED 3-148
Local Country Code (International Code) 3-85
Local National Code (Local Area Code) 3-85
Logo (Create) 4-179
Logo (Download) 3-109

M

MAC Address 6-202
MDI-X 3-45, 6-202
MIB 6-202
Monitoring 3-148
MWI (Message Waiting Indicator) 6-202

N

National Prefix (Trunk Prefix) 3-85
Network port configuration 3-46

O

Operator Code 3-85

P

Password
Change 3-143
Lost 3-144
Password, enter 2-40
PBX 6-202
PC port 3-45
Phone
Restart 3-144
Phone software (Download) 3-100
Phonebook 3-122
Picture Clips (Download) 3-103

PoE (Power over Ethernet) 2-17, 6-202
Port configuration 3-46
Port List 5-192
Power Consumption/Supply 2-17
PSTN 6-202
PSTN Access Code 3-85

Q

QCU 3-67
QoS 3-52
QoS Reports 3-167
Quick Start 2-20

R

Remote Tracing – Syslog 3-174
Reset Factory 3-144
Restart Phone 3-144
Ringer File 3-115
RTP 6-203
Base Port 3-129

S

Screensaver (Download) 3-112
Shipment 2-14
Silence suppression 3-130
SNMP 3-66, 6-203
SSH – Secure Shell Access 3-145
Subnet Mask 2-22
Subnet Mask (Manual configuration) 3-57

T

TCP 6-204
Timezone Offset 3-79
TLS 6-204
TouchGuide 3-43
Trace Configuration 3-150
Trace Profiles 3-156
Traps 3-66

U

UDP 6-204
Update Service 3-64

V

Vendor Class (DHCP) 2-23, 2-31

Index

VLAN 2-23, 3-47

W

WBM (Web Based Management) 1-13, 2-20,
6-205

X

XML ApplicationsApplications

XML 3-133

Xpressions 3-133