Documentation

HiPath 2000, HiPath 3000, HiPath 5000, HiPath OpenOffice
OpenStage 15, OpenStage 20, OpenStage 40, OpenStage 60, OpenStage 80

Administration Manual

A31003-S2010-M100-13-76A9

Communication for the open minded

Siemens Enterprise Communications
www.siemens.com/open

SIEMENS

Content

1 Overview 1-1
1.1 Important Notes 1-1
1.2 Maintenance Notes 1-2
1.3 About the Manual 1-2
1.4 Conventions for this Document 1-2
1.5 The OpenStage Family 1-3
1.5.1 OpenStage 60/80 1-3
1.5.2 OpenStage 40 1-4
1.5.3 OpenStage 20 1-5
1.5.4 OpenStage 15 1-6
1.6 Administration Interfaces 1-6
1.6.1 Web-based Management (WBM) 1-6
1.6.2 Deployment Service (DLS) 1-7
1.6.3 Local Phone Menu 1-7

2 Startup 2-1
2.1 Prerequisites 2-1
2.2 Assembling and Installing the Phone 2-2
2.2.1 Shipment 2-2
2.2.2 Connectors at the bottom side 2-2
2.2.3 Assembly 2-4
2.2.4 Connecting the Phone 2-5
2.2.5 Key Module 2-7
2.3 Quick Start 2-8
2.3.1 Access the Web Interface (WBM) 2-9
2.3.2 Basic Network Configuration 2-9
2.3.3 Extended Network Configuration 2-10
2.3.4 VLAN Discovery 2-10
2.3.4.1 Using a Vendor Class 2-10
2.3.4.2 Using Option #43 "Vendor Specific" 2-16
2.3.5 DLS Server Address 2-18
2.3.5.1 Using Vendor Class 2-18
2.3.5.2 Using Option #43 "Vendor Specific" 2-25
2.3.6 HFA Gateway Settings 2-27
2.3.7 Using the Web Interface (WBM) 2-27
2.3.8 Using the Local Menu 2-27

3 Administration 3-1
3.1 Access via Local Phone 3-1
3.2 LAN Settings 3-5
3.2.1 LAN Port Settings 3-5
3.2.2 VLAN 3-7

3.2.2.1 Automatic VLAN discovery using DHCP . . . 3-8
3.2.2.2 Automatic VLAN discovery using LLDP-MED (V2) . . . 3-10
3.2.2.3 Manual configuration of a VLAN ID . . . 3-12
3.3 IP Network Parameters . . . 3-13
3.3.1 Quality of Service (QoS) . . . 3-13
3.3.1.1 Layer 2 / 802.1p . . . 3-13
3.3.1.2 Layer 3 / Diffserv . . . 3-14
3.3.2 Use DHCP . . . 3-16
3.3.3 IP Address - Manual Configuration . . . 3-18
3.3.4 Default Route/Gateway . . . 3-19
3.3.5 Specific IP Routing . . . 3-20
3.3.6 DNS . . . 3-21
3.3.6.1 DNS Domain Name . . . 3-21
3.3.6.2 DNS Servers . . . 3-22
3.3.6.3 Terminal Hostname (V2) . . . 3-23
3.3.7 Configuration & Update Service (DLS) . . . 3-24
3.3.8 SNMP . . . 3-25
3.4 HiPath Service Menu . . . 3-28
3.5 System Settings . . . 3-29
3.5.1 System Identity . . . 3-29
3.5.2 HFA Gateway Settings . . . 3-29
3.5.3 HFA Emergency Gateway Settings . . . 3-31
3.5.4 Server and Standby Server ports . . . 3-32
3.5.5 Redundancy . . . 3-33
3.5.6 Emergency number . . . 3-34
3.5.7 LIN . . . 3-34
3.5.8 Not Used Timeout . . . 3-36
3.5.9 Energy Saving (OpenStage 40/60/80) . . . 3-37
3.5.10 Date and Time . . . 3-38
3.5.10.1 SNTP is available, but no automatic configuration by DHCP server . . . 3-38
3.5.11 Security . . . 3-40
3.6 Dialing . . . 3-42
3.6.1 Canonical Dialing Configuration . . . 3-42
3.6.2 Canonical Dial Lookup . . . 3-46
3.7 Distinctive Ringing (V2) . . . 3-48
3.8 Mobility (OpenStage 60/80, V1R3 Onwards) . . . 3-49
3.8.1 Platform Specific Behaviour . . . 3-50
3.9 Transferring Phone Software, Application and Media Files . . . 3-51
3.9.1 FTP/HTTPS Server . . . 3-51
3.9.2 Common FTP Settings . . . 3-51
3.9.3 Phone Software . . . 3-53
3.9.3.1 FTP/HTTPS Access Data . . . 3-53
3.9.3.2 Download/Update Phone Software . . . 3-55

3.9.4 Picture Clips . . . 3-56
3.9.4.1 FTP/HTTPS Access Data . . . 3-56
3.9.4.2 Download Picture Clip . . . 3-58
3.9.5 LDAP Template . . . 3-59
3.9.5.1 FTP/HTTPS Access Data . . . 3-59
3.9.5.2 Download LDAP Template . . . 3-61
3.9.6 Logo . . . 3-62
3.9.6.1 FTP/HTTPS Access Data . . . 3-62
3.9.6.2 Download Logo . . . 3-64
3.9.7 Screensaver . . . 3-65
3.9.7.1 FTP/HTTPS Access Data . . . 3-65
3.9.7.2 Download Screensaver . . . 3-67
3.9.8 Ringer File . . . 3-68
3.9.8.1 FTP/HTTPS Access Data . . . 3-69
3.9.8.2 Download Ringer File . . . 3-71
3.9.9 ´HPT Dongle Key . . . 3-72
3.9.9.1 FTP/HTTPS Access Data . . . 3-72
3.9.9.2 Download Dongle Key File . . . 3-74
3.10 Corporate Phonebook: Directory Settings . . . 3-75
3.10.1 LDAP . . . 3-75
3.11 Speech . . . 3-77
3.11.1 RTP Base Port . . . 3-77
3.11.2 Codec Preferences . . . 3-78
3.11.3 Audio Settings . . . 3-80
3.12 Display General Phone Information . . . 3-81
3.13 Applications (V2 on OpenStage 60/80) . . . 3-82
3.13.1 XML Applications/Xpressions . . . 3-82
3.13.1.1 Setup/Configuration . . . 3-82
3.13.1.2 HTTP Proxy . . . 3-87
3.13.1.3 Modify an Existing Application . . . 3-89
3.13.1.4 Remove an Existing Application . . . 3-90
3.14 Password . . . 3-91
3.15 Troubleshooting: Lost Password . . . 3-92
3.16 Restart Phone . . . 3-93
3.17 Factory Reset . . . 3-94
3.18 SSH - Secure Shell Access (V2) . . . 3-95
3.19 Display License Information . . . 3-96
3.20 HPT Interface (For Service Staff) . . . 3-97
3.21 Diagnostics . . . 3-98
3.21.1 LLDP-MED (V2) . . . 3-98
3.21.2 Fault Trace Configuration . . . 3-100
3.21.3 Easy Trace Profiles . . . 3-107
3.21.3.1 No Tracing for All Services . . . 3-107
3.21.3.2 Bluetooth Handsfree . . . 3-108

3.21.3.3 Bluetooth Headset . . . 3-108
3.21.3.4 Call Connection . . . 3-108
3.21.3.5 Call Log . . . 3-109
3.21.3.6 LDAP Phonebook . . . 3-109
3.21.3.7 DAS Connection . . . 3-109
3.21.3.8 DLS Data Errors . . . 3-110
3.21.3.9 802.1x . . . 3-110
3.21.3.10 Help Application . . . 3-110
3.21.3.11 Sidecar . . . 3-111
3.21.3.12 Key Input . . . 3-111
3.21.3.13 LAN Connectivity . . . 3-111
3.21.3.14 Local Phonebook . . . 3-111
3.21.3.15 Messaging . . . 3-112
3.21.3.16 Mobility . . . 3-112
3.21.3.17 Phone administration . . . 3-112
3.21.3.18 Server based applications . . . 3-113
3.21.3.19 Speech . . . 3-113
3.21.3.20 Tone . . . 3-113
3.21.3.21 USB Backup/Restore . . . 3-113
3.21.3.22 Voice Dialling . . . 3-114
3.21.3.23 Web Based Management (OpenStage 15/20/40) . . . 3-114
3.21.3.24 Web Based Management (OpenStage 60/80) . . . 3-114
3.21.4 QoS Reports . . . 3-115
3.21.5 Ping . . . 3-118
3.21.6 Memory Status Information . . . 3-119
3.21.7 Core dump . . . 3-122
3.21.8 Remote Tracing - Syslog (V2) . . . 3-123
3.22 Bluetooth . . . 3-124

4 Examples and HowTos . . . 4-1
4.1 Canonical Dialing . . . 4-1
4.1.1 Canonical Dialing Settings . . . 4-1
4.1.2 Canonical Dial Lookup . . . 4-2
4.1.2.1 Conversion examples . . . 4-3
4.2 How to Create Logo Files for OpenStage Phones . . . 4-5
4.2.1 For OpenStage 40 . . . 4-5
4.2.2 For OpenStage 60/80 . . . 4-6
4.3 How to Set Up the Corporate Phonebook (LDAP) . . . 4-9
4.3.1 Prerequisites: . . . 4-9
4.3.2 Create an LDAP Template . . . 4-10
4.3.3 Load the LDAP Template into the Phone . . . 4-13
4.3.4 Configure LDAP Access . . . 4-14
4.3.5 Test . . . 4-14

5 Technical Reference . . . 5-1

5.1 Menus 5-1
5.1.1 Web Interface Menu 5-1
5.1.1.1 Menu Structure 5-1
5.1.1.2 Web Pages 5-4
5.1.2 Local Phone Menu 5-30
5.2 Troubleshooting: Error Messages 5-37
Glossary 6-1
Index 7-1

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 Siemens accessories!

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

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

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

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

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

This product is a UL Listed Accessory, I.T.E., in U.S.A. and Canada.
This equipment also complies with the Part 68 of the FCC Rules and the Industrie Canada CS-03.

1.2 Maintenance Notes

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

Use only original Siemens 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 OpenStage 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 OpenStage phone hand have a fundamental understanding of HFA/CorNet. 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.

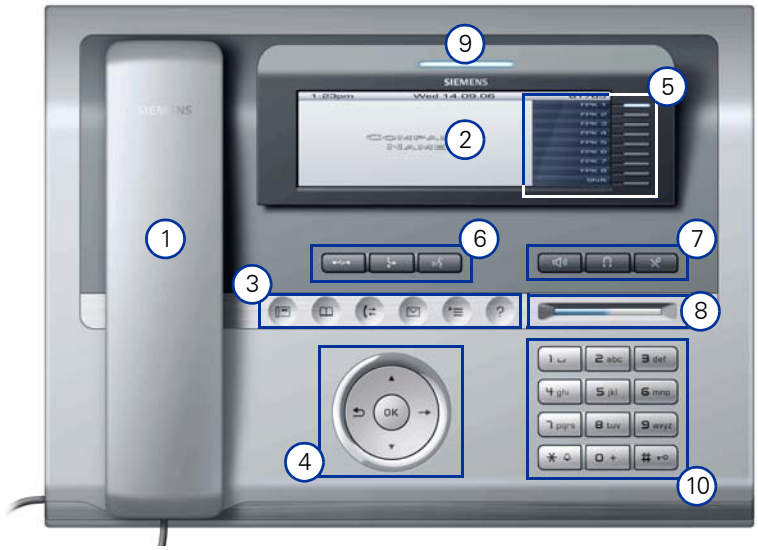
These instructions are laid out in a user-oriented manner, which means that you are led through the functions of the OpenStage phone step by step, wherever expedient. For the users, a separate manual is provided.

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 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 "/".

1.5 The OpenStage Family

1.5.1 OpenStage 60/80



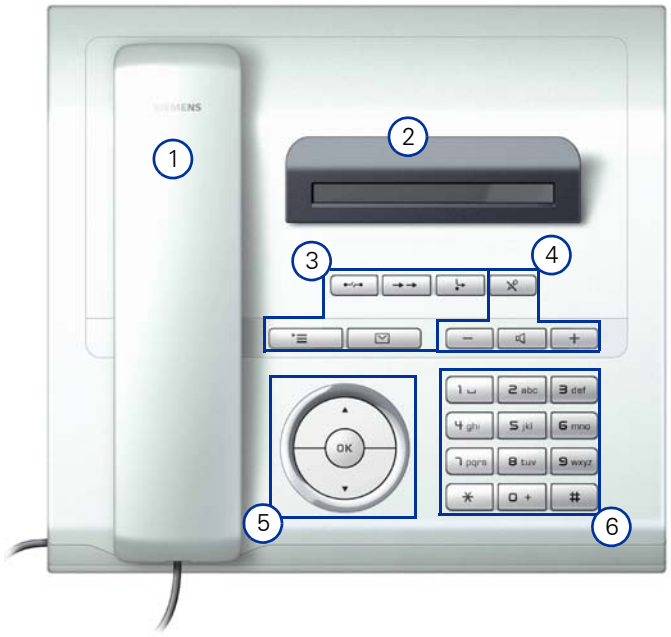
1	The **Handset** lets you pick up and dial calls in the usual manner.
2	The **Graphics Display** provides intuitive support for telephone operation.
3	The user-friendly **Application Keys** provide easy access to your telephone's applications.
4	With the **TouchGuide**, the user/administrator can navigate in the various phone functions, applications, and configuration menus.
5	You can customize your telephone in line with your personal needs by assigning individual phone numbers and functions to the **Program Keys**.
6	Press the **Function Keys** to access frequently used telephony functions.
7	The **Audio Keys** let you optimize the audio settings on your telephone.
8	With the **TouchSlider**, the user can adjust the volume, e.g. of ringtones.
9	Inbound calls are visually signaled on the **Call Display**.
10	The **keypad** is used for entering phone numbers and text.

[Feature-Übersicht]

1.5.2 OpenStage 40

1	The **Handset** lets you pick up and dial calls in the usual manner.
2	The **Graphics Display** provides intuitive support for telephone operation.
3	The user-friendly **Application Keys** provide easy access to your telephone's applications.
4	With the **Navigation Key**, the user/administrator can navigate in the various phone functions, applications, and configuration menus.
5	You can customize your telephone in line with your personal needs by assigning individual phone numbers and functions to the **Program Keys**.
6	Press the **Function Keys** to access frequently used telephony functions.
7	The **Audio Keys** let you optimize the audio settings on your telephone.
8	Inbound calls are visually signaled on the **Call Display**.
9	The **keypad** is used for entering phone numbers and text.

1.5.3 OpenStage 20



1	The **Handset** lets you pick up and dial calls in the usual manner.
2	The **Display** provides intuitive support for telephone operation.
3	The user-friendly **Application Keys** provide easy access to your telephone's applications.
4	Press the **Function Keys** to access frequently used telephony functions.
5	With the **Navigation Key**, the user/administrator can navigate in the various phone functions, applications, and configuration menus.
6	The **keypad** is used for entering phone numbers and text.

1.5.4 OpenStage 15

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.
3	With the **Audio Keys**, the user can optimize the audio settings.
4	Press the **Function Keys** to access frequently used telephony functions.
5	The **Keypad** is used for entering phone numbers and text.
6	With the **Navigation Keys**, the user/administrator can navigate in the various phone functions, applications, and configuration menus.
7	The **Program Keys** enable the user to customize the telephone in line with his/her personal needs by assigning individual phone numbers and functions.

1.6 Administration Interfaces

You can configure the OpenStage phone by using any of the following methods.

1.6.1 Web-based Management (WBM)

This method employs a web browser for communication with the phone via HTTP or 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.
The remote configuration is not applicable while the phone is not in idle mode.

1.6.2 Deployment Service (DLS)

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

1.6.3 Local Phone Menu

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

- An Ethernet connection to a LAN

> ⚠ Only use **switches** in the LAN to which the OpenStage phone is connected. An operation at hubs can cause serious malfunctions in the hub and in the whole network.

- A HiPath Communications System: HiPath 2000, HiPath 3000, HiPath 5000, or HiPath OpenOffice
- An FTP Server for file transfer, e. g. firmware, configuration data, application software
- A Dynamic Host Configuration Protocol (DHCP) server (recommended).

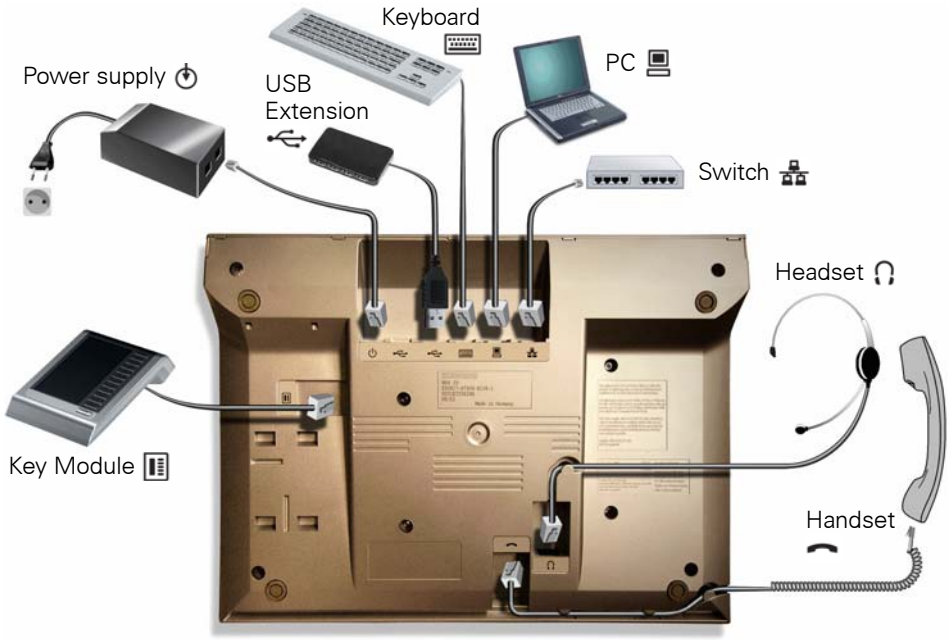
2.2 Assembling and Installing the Phone

2.2.1 Shipment

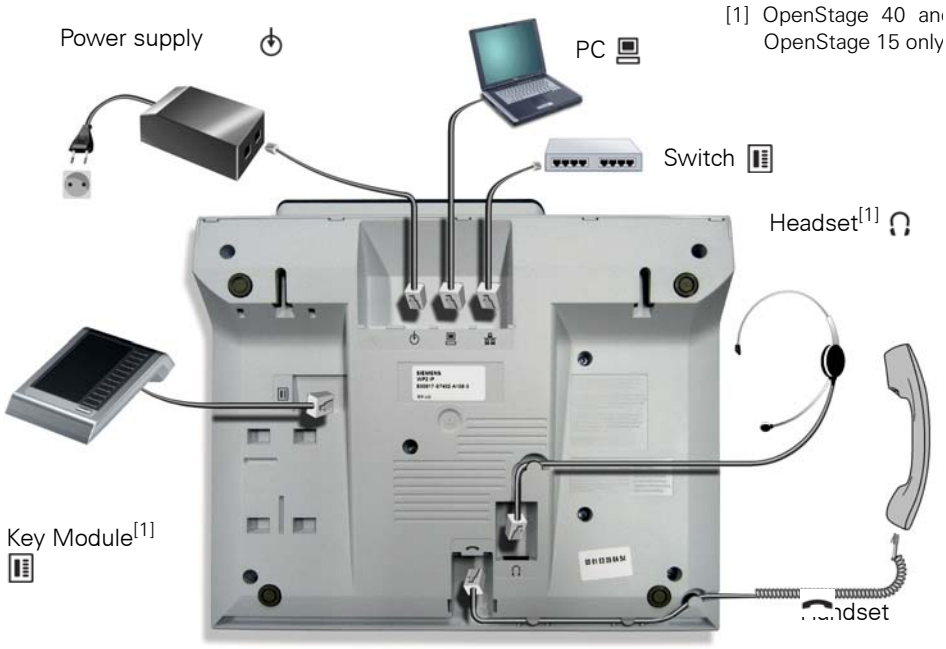
- **Phone**
- **Handset**
- **Handset cable**
- Subpackage:
  - **Document "Information and Important Operating Procedures"**
  - **Emergency number sticker**

2.2.2 Connectors at the bottom side

OpenStage 60



OpenStage 40 (OpenStage 15 and 20 similar, except [1])



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 Connecting the Phone

1. Plug the LAN cable into the connector at the bottom of the telephone and connect the cable to the LAN/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
OpenStage 15[1]	Power Class 1
OpenStage 20	Power Class 1
OpenStage 20 E	Power Class 1
OpenStage 20 G	Power Class 2
OpenStage 40[2]	Power Class 2
OpenStage 40 + 2nd Key Module	Power Class 3
OpenStage 40 G[2]	Power Class 3
OpenStage 40 G + 2nd Key Module	External power unit required
OpenStage 60/80[3]	Power Class 3
OpenStage 60/80 + 2nd Key Module	Power Class 3
OpenStage 60/80 G[3]	Power Class 3
OpenStage 60/80 G + 2nd Key Module	External power unit required

1 Includes 1 Key Module 15.
2 Includes 1 Key Module.
3 Includes 1 Key Module + USB-Extension with Acoustic Unit.

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

> Use only the plug-in power supply unit fitting the OpenStage phone:
> 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.

3. If applicable, connect the following optional jacks:
   - LAN connection to PC
   - Headset (accessory)
   - Connection to add-on device (accessory)
   - Connection to external keyboard (accessory)

- USB master for connection to a USB device (e. g. accessory USB Acoustic Adapter)

To prevent damage on the OpenStage 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 Key Module

A key module provides 12 additional program keys. Key modules are available for OpenStage 15/40/60/80 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	OpenStag Key Module 15	OpenStage Key Module
OpenStage 15	1	-
OpenStage 40	1	2
OpenStage 60/80	-	2

Please note that OpenStage Key Modules (self-labeling) and OpenStage Key Module 15 (paper label) can not be combined. For key labelling, a special tool is available; please refer to:
http://wiki.siemens-enterprise.com/index.php/Key_Labelling_Tool

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

2.3 Quick Start

This section describes a typical case: the setup of an OpenStage 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.

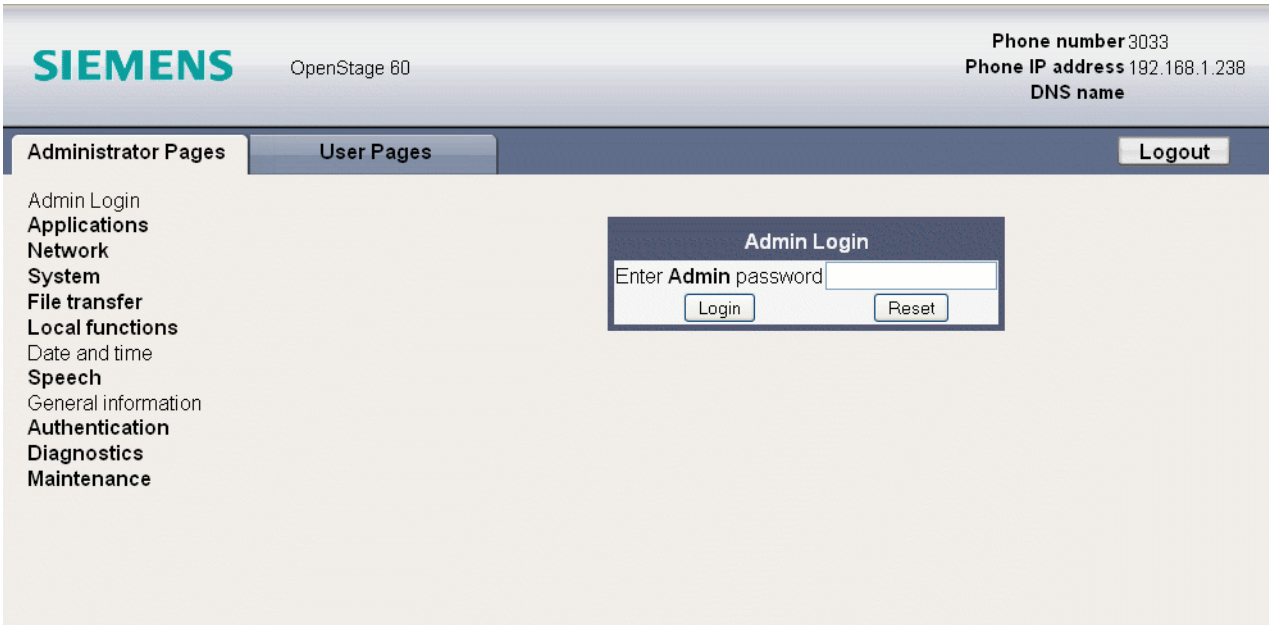
2.3.1 Access the Web Interface (WBM)

1. Open your web browser (MS Internet Explorer or Firefox) and enter the appropriate URL. Example: `https://192.168.1.15` or `https://myphone.phones` (firmware V2)

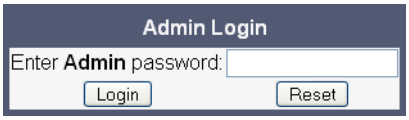
   Up to firmware V1R4, unencrypted HTTP can be used for web access. In this case, port 8085 must be added to the phone address or DNS name, for example `http://192.168.1.15:8085`

   For configuring the phone's DNS name, which is possible which firmware V2, please refer to section 3.3.6.3, "Terminal Hostname (V2)".

   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.



2. Click on the tab "Administrator Pages". In the dialog box, enter the admin password:



3. The administration menu is displayed in the left column. 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 in the right column.

2.3.2 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 default route.

2.3.3 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”.

2.3.4 VLAN Discovery

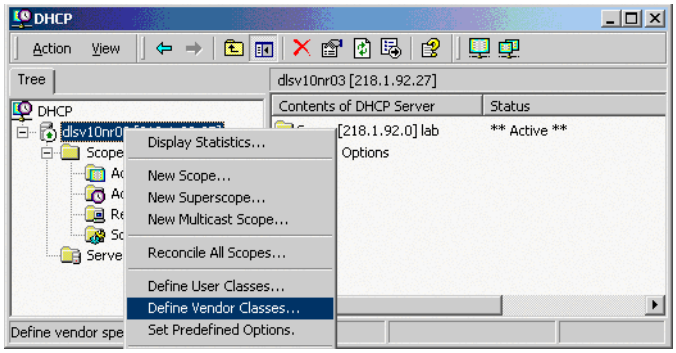
If the phone is to be located in a VLAN (Virtual LAN), a VLAN ID must be assigned. If the VLAN shall be provided by DHCP, **VLAN Discovery** must be set to "DHCP" (see section 3.2.2.1, “Automatic VLAN discovery using DHCP”). The corresponding DHCP option is vendor-specific, thus a specific procedure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

2.3.4.1 Using a Vendor Class

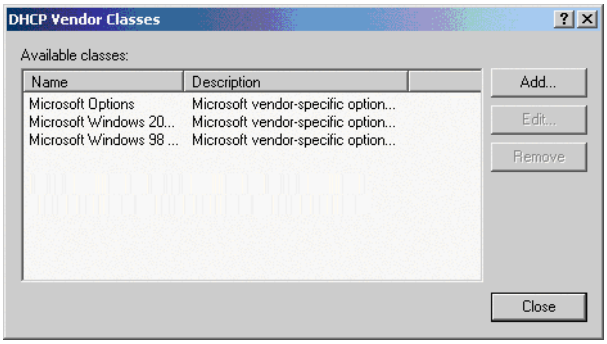
It is recommended to define a vendor class on the DHCP server, thus enabling server and phone to exchange vendor-specific data exclusively. The data is disclosed from other clients. The following steps are required for the configuration of the Windows DHCP server.

Setting up a new vendor class using the Windows DHCP Server

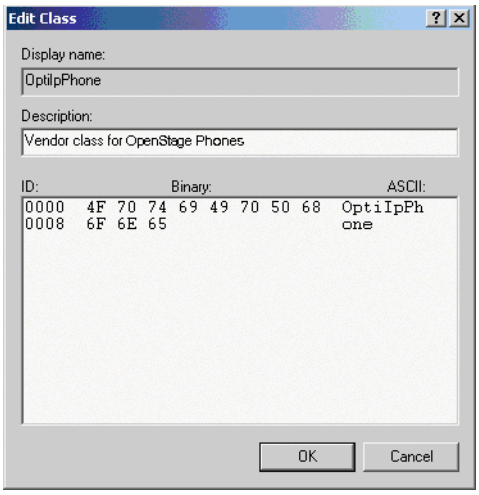
1. In the Windows Start menu, select **Start** > **Programs** > **Administrative Tools** > **DHCP**.
2. In the DHCP console menu, right-click the DHCP server in question and select **Define Vendor Classes...** in the context menu.



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



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



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

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

Add Options to the New Vendor Class

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

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

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

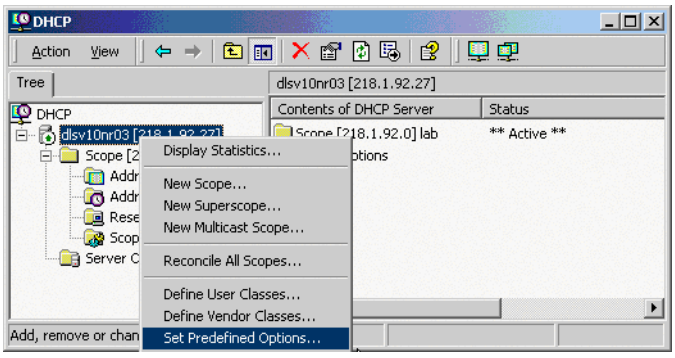
You can use the following command to configure the required option (without error message) so that it is also appears later in the DHCP console:

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

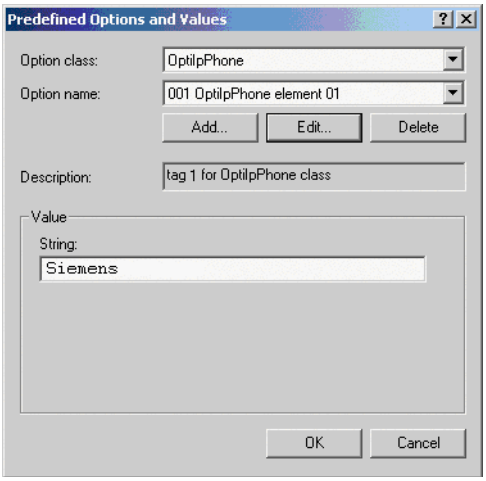
The value **SIEMENS** for optiPoint Element 1 can then be re-assigned over the DHCP console.

This error was corrected in Windows 2003 Server SP2.

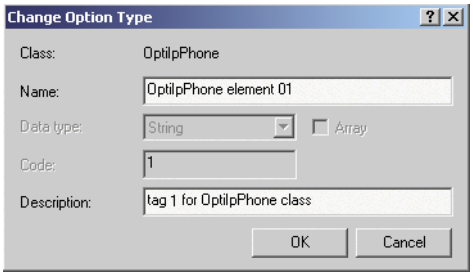
6. In the DHCP console menu, right-click the DHCP server in question and select Set Predefined Options from the context menu.



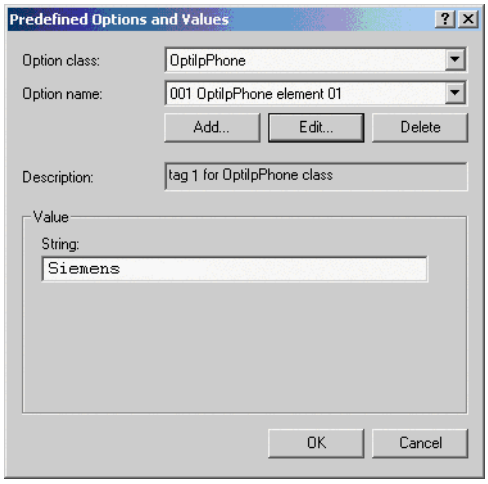
7. In the dialog, select the previously defined **OptiIpPhone** class and click on **Add...** to add a new option.



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



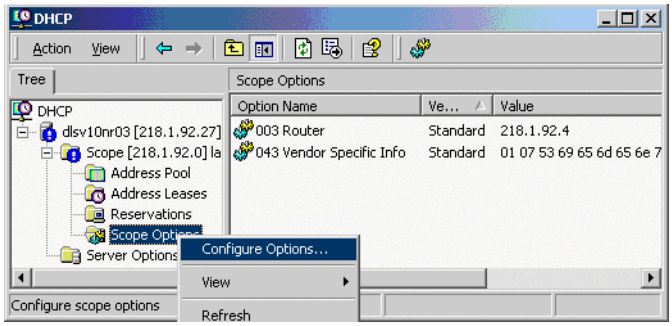
9. Enter the value for this option.
   1. First Pass: "Siemens"
   2. Second Pass: VLAN ID



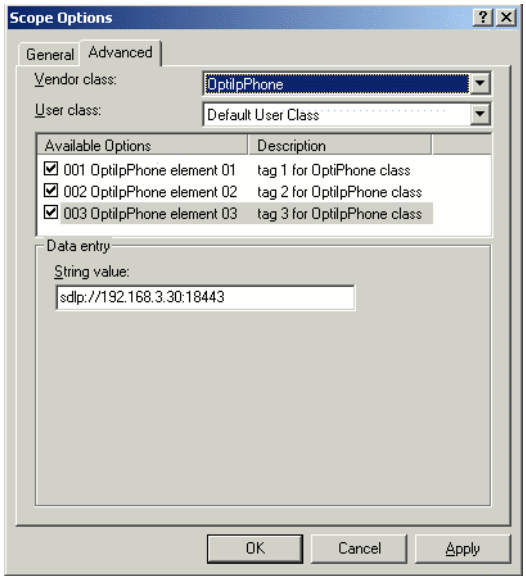
10. Press **OK**, repeat steps 7 to 9 for the second pass, and press **OK** again.

Defining the scope for the new vendor class

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



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



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

13. The DHCP console now shows the information that will be transmitted for the corresponding workpoints. Information from the **Standard** vendor is transmitted to all clients, whereas information from the **OptiIpPhone** vendor is transmitted only to the clients (workpoints) in this vendor class.

Setup using a DHCP server on Unix/Linux

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

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

2.3.4.2 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

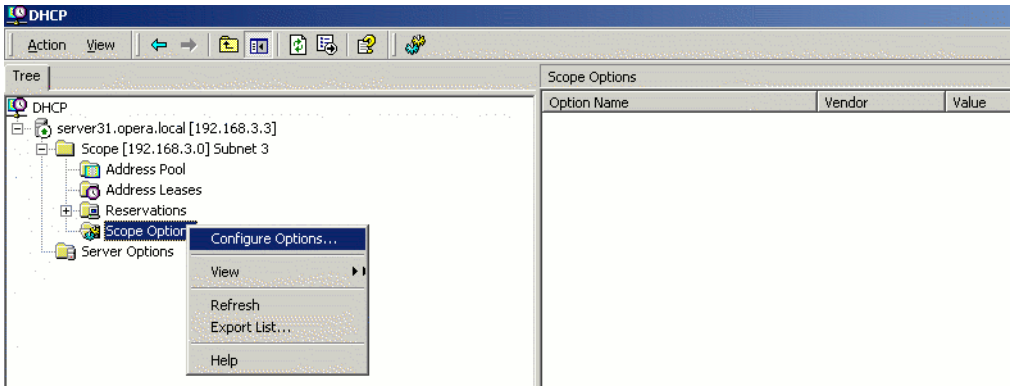
The following example shows a VLAN ID with the decimal value "10":

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

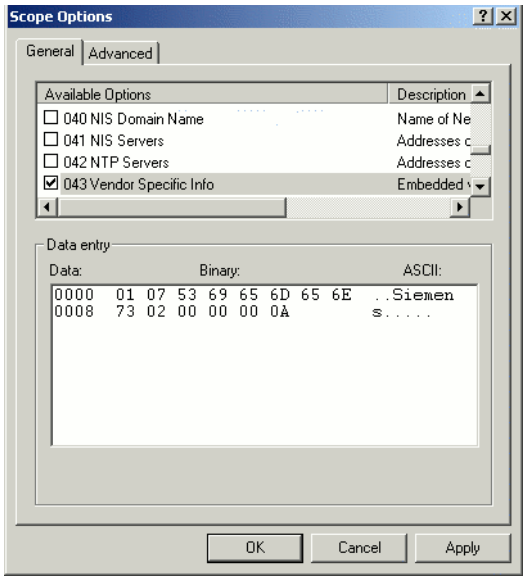
For manual configuration of the VLAN ID see section 3.2.2.3, “Manual configuration of a VLAN ID”.

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.



2.3.5 DLS Server Address

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

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

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

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

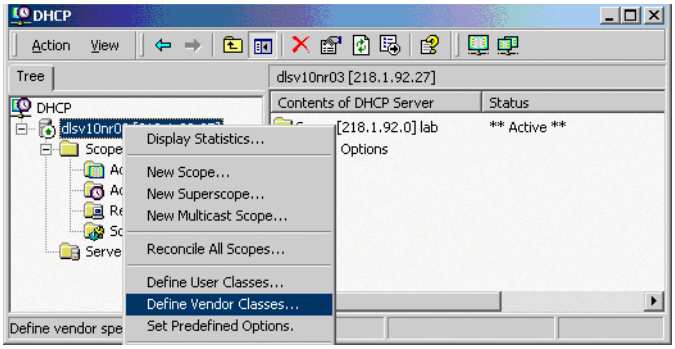
2.3.5.1 Using Vendor Class

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

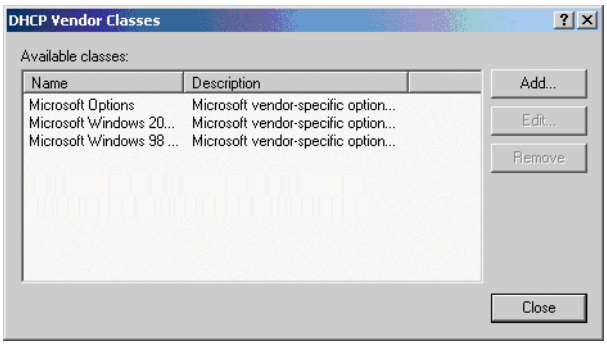
The following steps are required for the configuration of the Windows DHCP server.

Setting up a new vendor class using the Windows DHCP Server

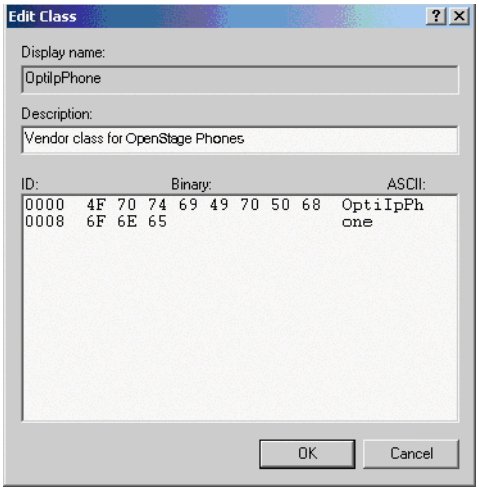
1. In the Windows Start menu, select **Start** > **Programs** > **Administrative Tools** > **DHCP**.
2. In the DHCP console menu, right-click the DHCP server in question and select **Define Vendor Classes...** in the context menu.



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



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



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

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

Add Options to the New Vendor Class

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

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

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

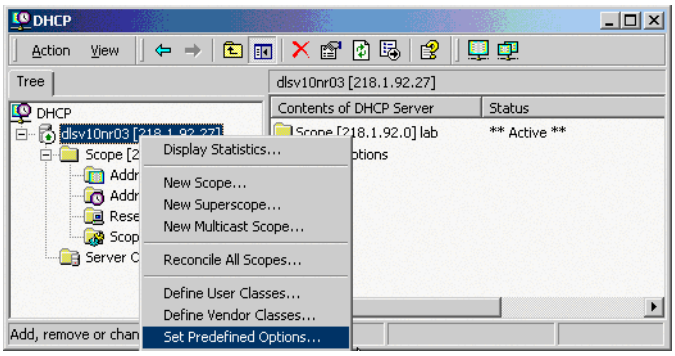
You can use the following command to configure the required option (without error message) so that it is also appears later in the DHCP console:

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

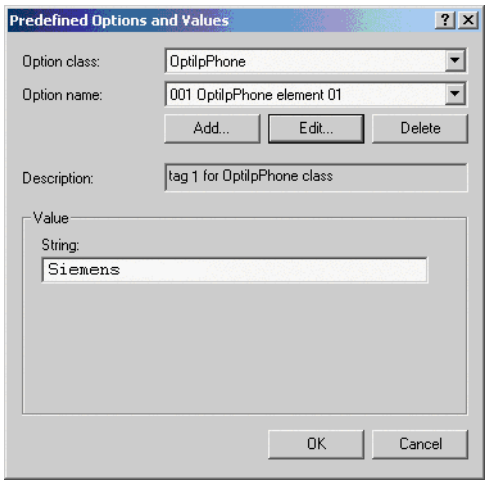
The value **SIEMENS** for optiPoint Element 1 can then be re-assigned over the DHCP console.

This error was corrected in Windows 2003 Server SP2.

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



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



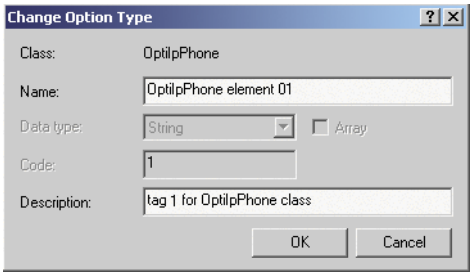
8. Enter the following data for the new option:

   1. First Pass: Option 1

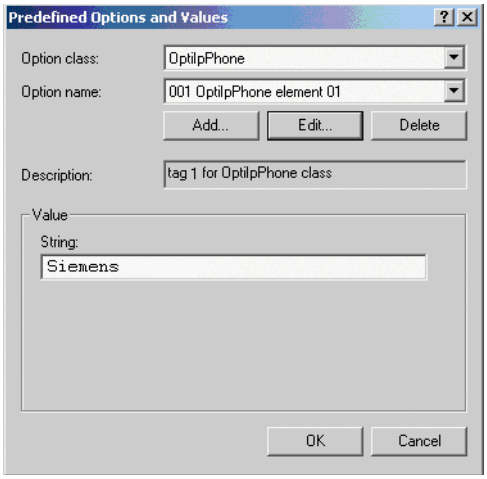
   - Name: Free text, e. g. "OptiIpPhone element 01"
   - Data type: "String"
   - Code: "1"
   - Description: Free text.

   2. Second Pass: Option 3

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



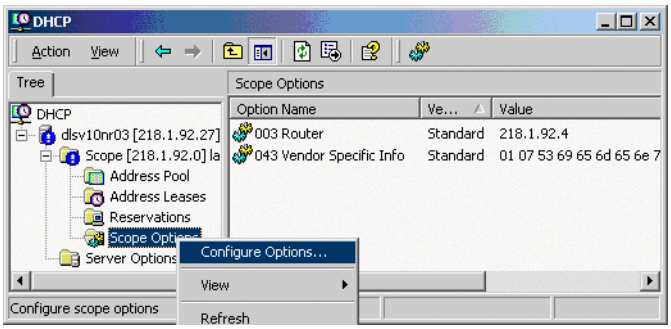
9. Enter the value for this option.
   1. First Pass: "Siemens"
   2. Second Pass: DLS address
      The DLS address has the following format:
      <PROTOCOL>:://<IP ADDRESS OF DLS SERVER>:<PORT NUMBER>
      Example: sdlp://192.168.3.30:18443



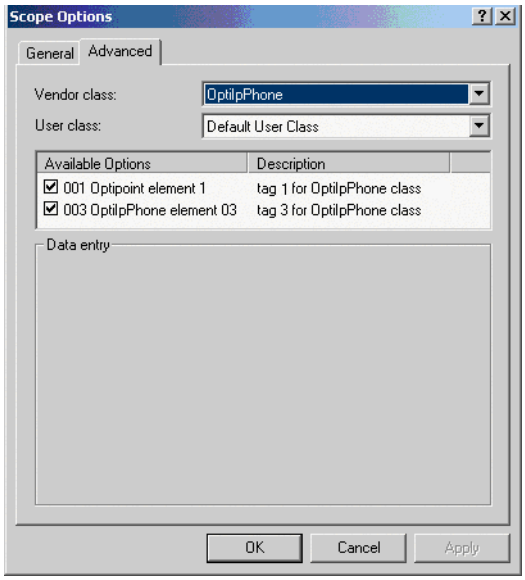
10. Press **OK**, repeat steps 7 to 9 for the second pass, and press **OK** again.

Defining the scope for the new vendor class

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



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



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

13. The DHCP console now shows the information that will be transmitted for the corresponding workpoints. Information from the **Standard** vendor is transmitted to all clients, whereas information from the **OptiIpPhone** vendor is transmitted only to the clients (workpoints) in this vendor class.

Setup using a DHCP server on Unix/Linux

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

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

2.3.5.2 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):

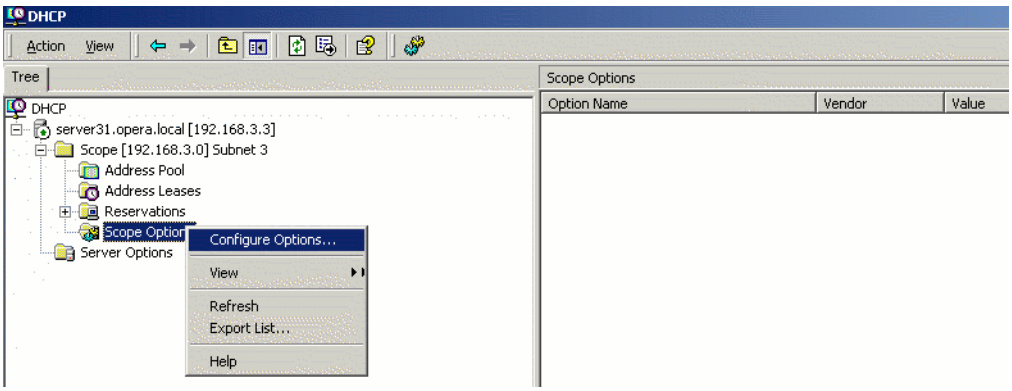
Code	**Length**	**Vendor name**						
1	7	S	i	e	m	e	n	s
01	07	53	69	65	6D	65	6E	73

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:

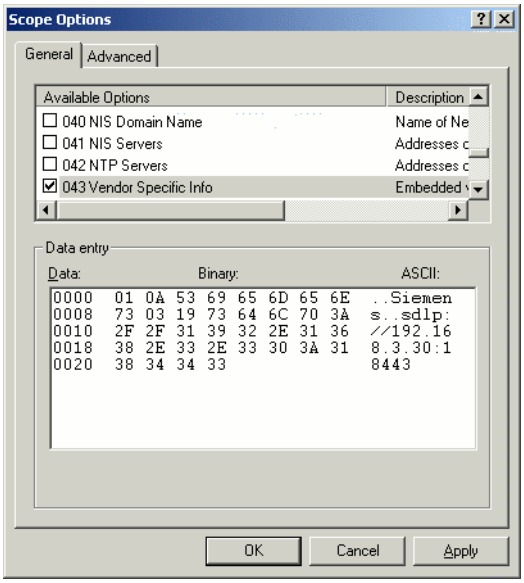
Code	**Length**	**DLS IP address**																						
3	25	s	d	l	p	:	/	/	1	9	2	.	1	6	8	.	2	.	1	9	:	1	8	4	4	3
03	19	73	64	6C	70	3A	2F	2F	31	39	32	2E	31	36	38	2E	32	2E	31	39	3A	31	38	34	34	33

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.



2.3.6 HFA Gateway Settings

To connect the OpenStage phone to the HiPath 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.

2.3.7 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, “Access the Web Interface (WBM)”.
2. In the menu at the lefthand side, go to **System** > Gateway.
3. Enter the IP address of the HiPath Communication System in the **Gateway 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 **New subscriber password** field.

2.3.8 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** > **HFA 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
             |--- HFA Gateway
                  |--- IP address
                  |--- Subscriber Number
                  |--- Password
   ```

4. Enter the IP address of the HFA gateway provided by your HiPath communication system.
5. Enter the phone’s subscriber number, which will also serve as internal phone number.
6. Enter the password associated with the subscriber number.
7. After the data has been entered, select **Save & exit** and press OK.

3 Administration

This chapter describes the configuration of every parameter available on the OpenStage phones. For access via the local phone menu, see the following; for access using the web interface, please refer to section 2.3.1, “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**

   OpenStage 60/80:

   Press the ☰ key once or twice to activate the administration menu (the ☰ key toggles between the user’s configuration menu and the administration menu).

   OpenStage 60/80 V2:

   The ☰ key toggles between the Settings menu, the Applications menu, and the applications currently running. Press the ☰ key repeatedly until the "Settings" tab is active. (The ☰ key toggles between the Settings menu, the Applications menu, and the applications currently running.)

   OpenStage 15/20/40:

   Press the number keys 1, 0, and 3 simultaneously to enter the admininstration menu.

   The key that is hit first will initiate the dialing process, and the first number will be interpreted as part of a call number. To exit the dialing dialog, press the 🔊 key. This will deactivate the loudspeaker and stop the dialing process.

   The ☰ key calls the HiPath configuration menu.

2. **Enter Password**

   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 3.14, “Password”) after your first login.

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

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

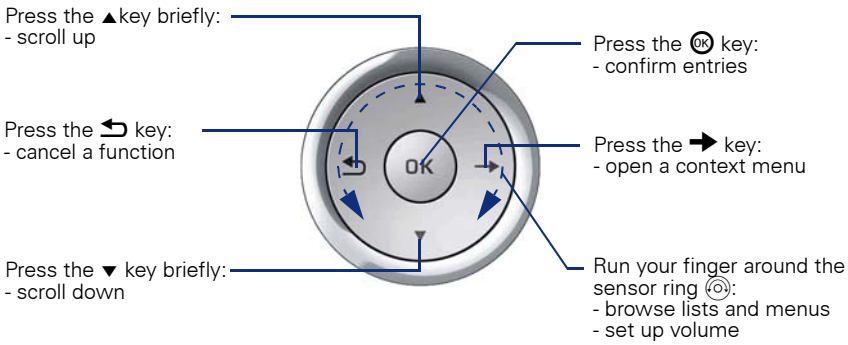
   (Abc) -> (abc) -> (123) -> (ABC) -> back to start.

3. Navigate within the Administration Menu

OpenStage 60/80

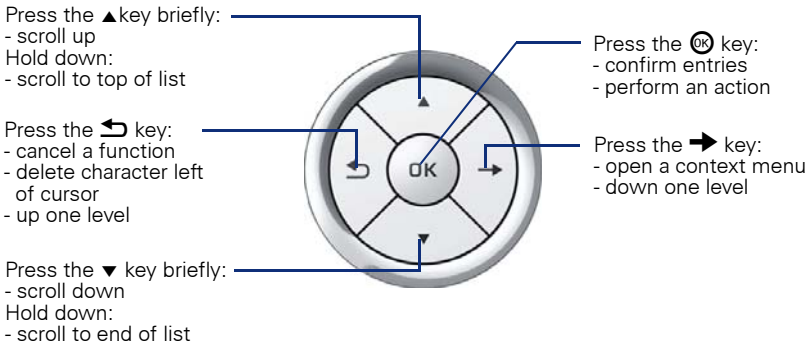
Use the TouchGuide to navigate and execute administrative actions in the administration menu.

For using the TouchGuide, see the following figure:



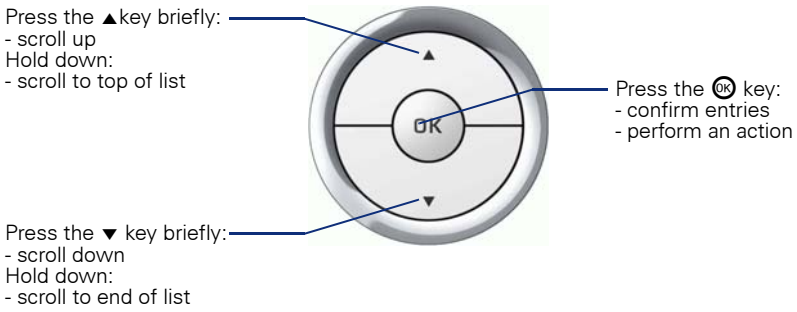
OpenStage 40

Use the 5-way Navigator to navigate and execute administrative actions in the administration menu.

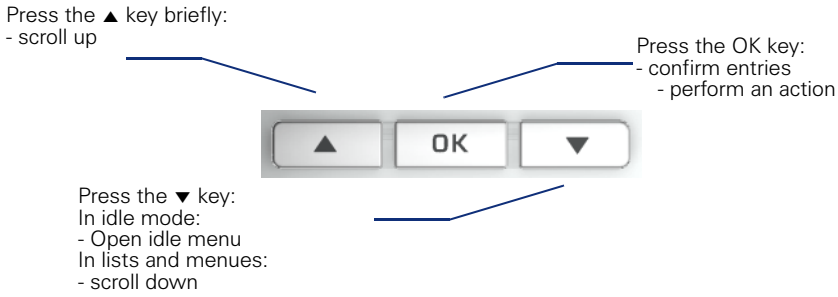


OpenStage 20

Use the 3-way Navigator to navigate and execute administrative actions in the administration menu.



OpenStage 15



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 key to enter the selective list. Use the Sensor Wheel resp. the ▲ and ▼ key to scroll up and down in the selective list. To select a list entry, press the OK key.

5. Enter the parameter value

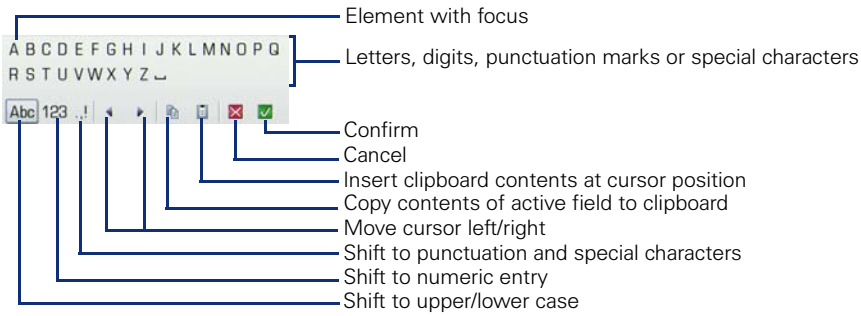
For selecting numbers and characters, you can use special keys. See the following table:

Key	Function
*🔔	Switch to punctuation and special characters.
#⊸	Toggle between lowercase characters, uppercase characters, and digits in the following order: (Abc) -> (abc) -> (123) -> (ABC) -> back to start.

OpenStage 60/80

If a parameter is set by entering a number or character data, the onscreen keypad is used. Press the OK key to enter the number editor. Within the number editor, solely use the key numbers or the Sensor Wheel for selecting numbers, characters, or groups of characters. The ⮌ key deletes one character in the input field, and the ➔ key moves the cursor to the OK field.

The following figure describes the elements of the onscreen keypad and their functions:



Additionally, you can use the following keys on the keypad as shortcuts for the selection of character groups:

Element	Function
*	Switch to punctuation and special characters.
#	Toggle between lowercase characters, uppercase characters, and digits.

OpenStage 15/20/40

With the OpenStage 20/40, use the keypad for entering parameters. With the 3 way/5 way-Navigator, you can enter, delete, copy and paste characters and numbers as well as navigate within an entry and toggle the input mode.Save and exit

6. Save end exit

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

3.2 LAN Settings

3.2.1 LAN Port Settings

The OpenStage 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 Mb/s, 1000 Mb/s with OpenStage 20/40/60/80 G) 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 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.

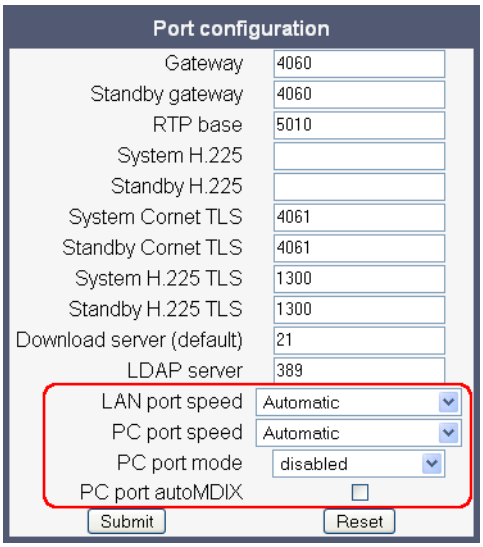
When **PC port autoMDIX** is enabled, the switch determines automatically whether a regular MDI connector or a MDI-X (crossover) connector is needed, and configures the connector accordingly.

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", and, additionally, for OpenStage 20/40/60/80 G, "1 Gbps full duplex"
  Default: "Automatic".
- **PC port speed** / **PC port type**: Settings for the ethernet port connected to a PC.
  Value range: "Automatic," "10 Mbps half duplex", "10 Mbps full duplex", "100 Mbps half duplex", "100 Mbps full duplex", and, additionally, for OpenStage 20/40/60/80 G, "1 Gbps full duplex"
  Default: "Automatic".
- **PC port mode** / **PC port status**: Controls the PC port.
  Value range: "Disabled", "Enabled", "Mirror".
  Default: "Disabled".
- **PC port autoMDIX**: Switches between MDI and MDI-X automatically.
  Value range: "On", "Off".
  Default: "Off".

Administration via WBM

Network > Port configuration



Administration via Local Phone

- Admin
  - Network
    - Port Configuration
      - Number
        - **LAN port speed**
        - **PC port status**
        - **PC port speed**
        - **PC port autoMDIX**

3.2.2 VLAN

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

Physically partitioning the LAN 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. It is possible to assign one device, i.e. one MAC address, to different VLANs.

It is important that every switch connected to a PC is VLAN-capable. This is also true for the integrated switch of the OpenStage. 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:

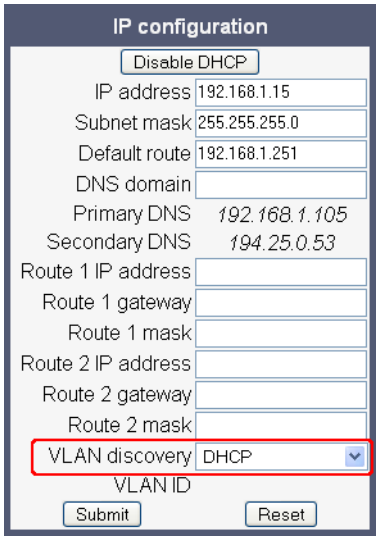
- Manually
- By DHCP
- By LLDP-MED

3.2.2.1 Automatic VLAN discovery using DHCP

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

Administration via WBM (up to V1R3)

Network > IP configuration



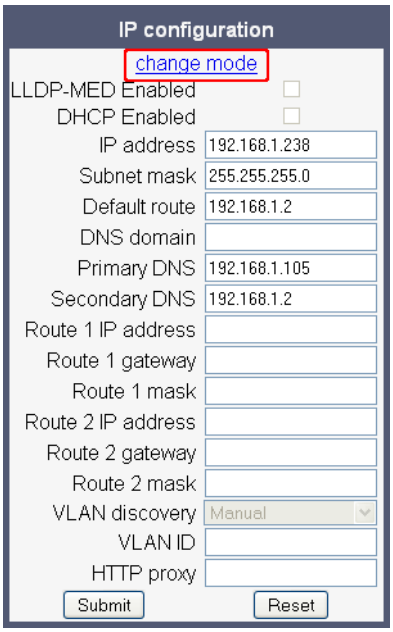
Administration via Local Phone (up to V1R3)

Admin
Network
IP Configuration
VLAN discovery

Administration via WBM (V2)

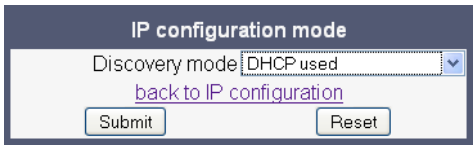
Network > IP configuration

With firmware V2, you must click on **change mode** first. Afterwards, the **IP configuration mode** dialog opens.



Network > IP configuration > **change mode**

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



Administration via Local Phone (up to V1R3)

└── Administration
  └── Network
    └── IP Configuration
      └── **VLAN discovery**

Administration via Local Phone (V2)

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

└--- Administration
└--- Network
└--- IP Configuration
└--- **Discovery mode**

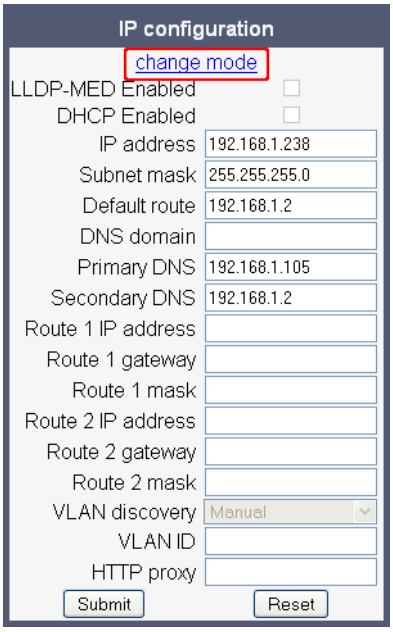
3.2.2.2 Automatic VLAN discovery using LLDP-MED (V2)

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

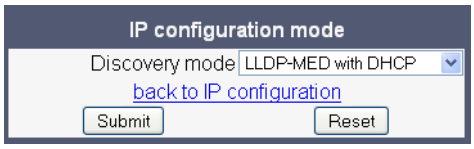
Network > IP configuration

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



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**.



Administration via Local Phone

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

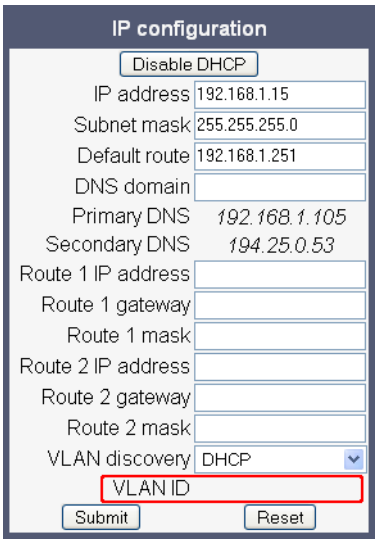
Administration
Network
IP Configuration
Discovery mode

3.2.2.3 Manual configuration of a VLAN ID

To configure layer 2 VLAN manually, first make sure that VLAN discovery is set to "Manual" (see section 3.2.2.1, “Automatic VLAN discovery using DHCP”). 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



Administration via Local Phone

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

3.3 IP Network Parameters

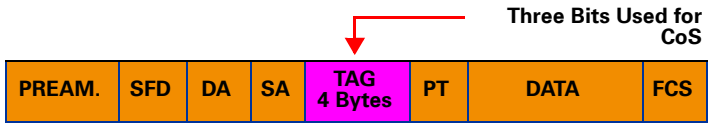
3.3.1 Quality of Service (QoS)

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.

3.3.1.1 Layer 2 / 802.1p

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

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

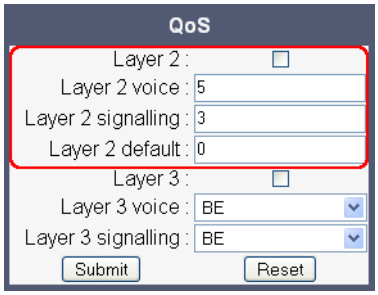


Data required

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

Administration via WBM

Network > QoS



Administration via Local Phone

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

3.3.1.2 Layer 3 / Diffserv

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

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

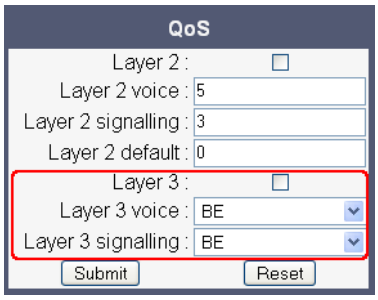
1. Default
   Any traffic that does not meet the requirements of any of the other defined classes is placed in the default per-hop behaviour group. Typically, the forwarding has best-effort forwarding characteristics. The DSCP (Diffserv Codepoint) value for Default is "0 0 0 0 0 0".
2. Expedited Forwarding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

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

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

Administration via WBM

Network > QoS



Administration via Local Phone

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

3.3.2 Use DHCP

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

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 following parameters can be obtained by DHCP:

Basic informations

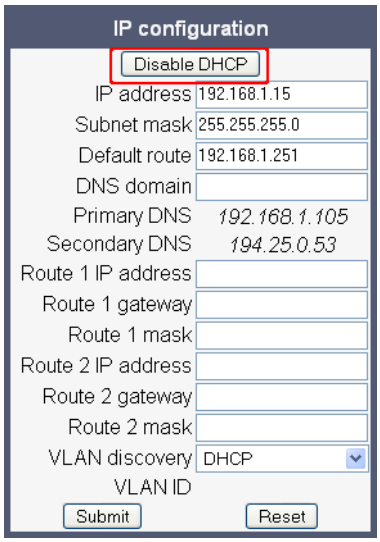
- IP Address
- Subnet Mask

Optional informations

- 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 IP Addresses (DNS Server option 6)
- DNS Domain Name (DNS Domain option 15)
- Vendor Unique (option 43)

Administration via WBM

Network > IP configuration



Administration via Local Phone

- Admin
  - Network
    - IP Configuration
      - **Use DHCP**

3.3.3 IP Address - Manual Configuration

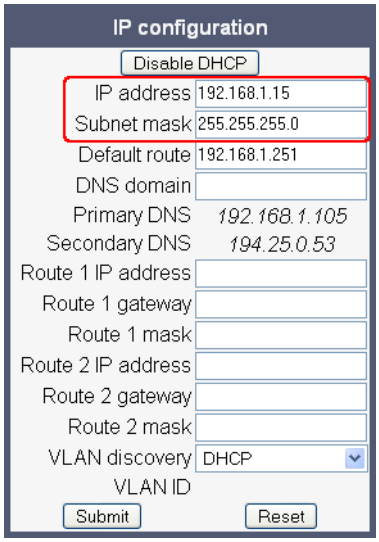
If not provided by DHCP dynamically, you must specify the phone's IP address and subnet mask manually.

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



Administration via Local Phone

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

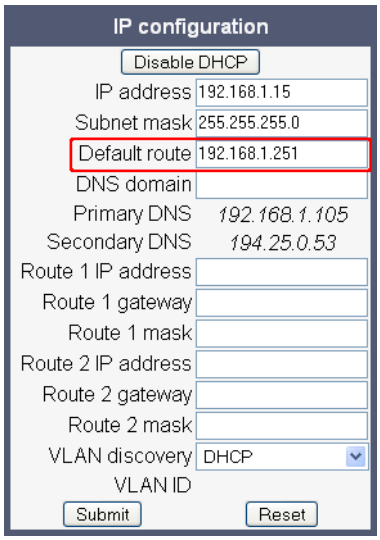
3.3.4 Default Route/Gateway

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



Administration via Local Phone

└── Admin
  └── Network
    └── IP Configuration
      └── **Default route (GW)**

3.3.5 Specific IP Routing

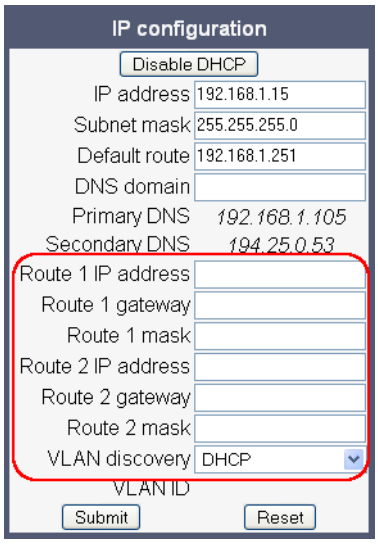
To have constant access to network subscribers of other domains, you can enter a total of two more network destinations, in addition to the default route/gateway. This is useful if the LAN has more than one router or if the LAN is divided into subnets.

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



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

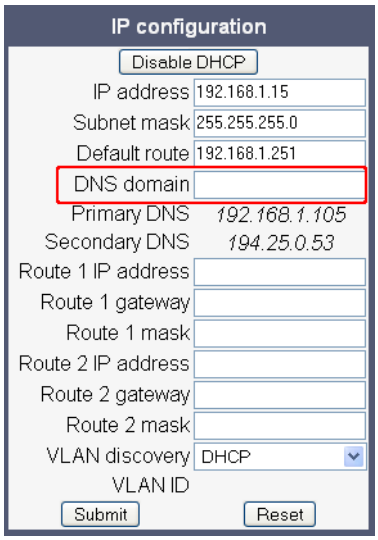
The main task of the domain name system (DNS) is to translate domain names to IP addresses. For some features and functions of the OpenStage phone, it is necessary to configure the DNS domain the phone belongs to, as well as the nameservers needed for DNS resolving.

3.3.6.1 DNS Domain Name

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

Administration via WBM

Network > IP configuration



Administration via Local Phone

Admin
Network
IP Configuration
DNS domain

3.3.6.2 DNS Servers

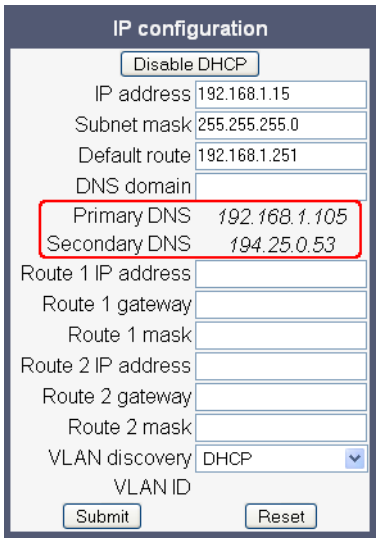
If not provided by DHCP automatically, a primary and a secondary DNS server can be configured.

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



Administration via Local Phone

```
└--- Admin
     └--- Network
          └--- IP Configuration
               |--- Primary DNS
               └--- Secondary DNS
```

3.3.6.3 Terminal Hostname (V2)

With OpenStage firmware V2, the phone's hostname for registration with the DNS server can be customised. The phone will send the specified hostname to the DNS server using DDNS. Therefore, the DNS server must support DDNS.

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.

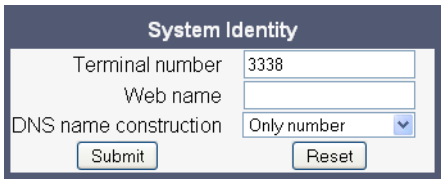
It is recommended to inform the user about the DNS name of his/her phone. The complete WBM address can be found under User menu > Network information > Web address.

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": The phone does not attempt to change its DNS name via DDNS.
- "MAC based": The DNS name is built from the prefix "OIP" followed by the phone's MAC address.
- "Web name": The DNS name is set to the the string entered in **Web name**.
- "Only number": The DNS name is set to the **Terminal number**, that is, the phone's call number (E.164).
- "Prefix number": The DNS name is constructed from the the string entered in **Web name**, followed by the **Terminal number**.

Administration via WBM

System > System Identity



Administration via Local Phone

└--- Administration
└--- Identity
├--- **Web name**
└--- **DDNS hostname**

3.3.7 Configuration & Update Service (DLS)

The Deployment Service (DLS) is a HiPath 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), software deployment, plug&play support, as well as error and activity logging.

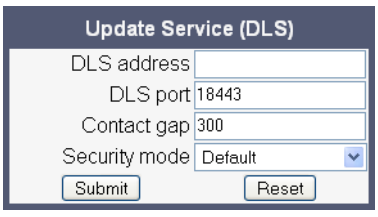
DLS address, i.e. the IP address or hostname of the DLS server, and **DLS port**, i.e. the port on which the DLS server is listening, are required to enable proper communication between phone and DLS. The **Contact gap** parameter controls a security function. It specifies a minimum time interval that must elapse between individual HTTP requests from the phone which are responding to a ContactMe request from the DLS. Any requests coming within that time will be ignored. The purpose is to prevent DoS (Denial of Service) attacks on the phone. 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.
- **DLS 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.
- **Security mode** / **Secured**: 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)



Administration via Local Phone

- Admin
  - Network
    - Update Service (DLS)
      - **DLS address**
      - **DLS port**
      - **Contact gap**
      - **Secured**

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.

OpenStage phones support SNMPv1.

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

Standard SNMP traps

OpenStage 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.

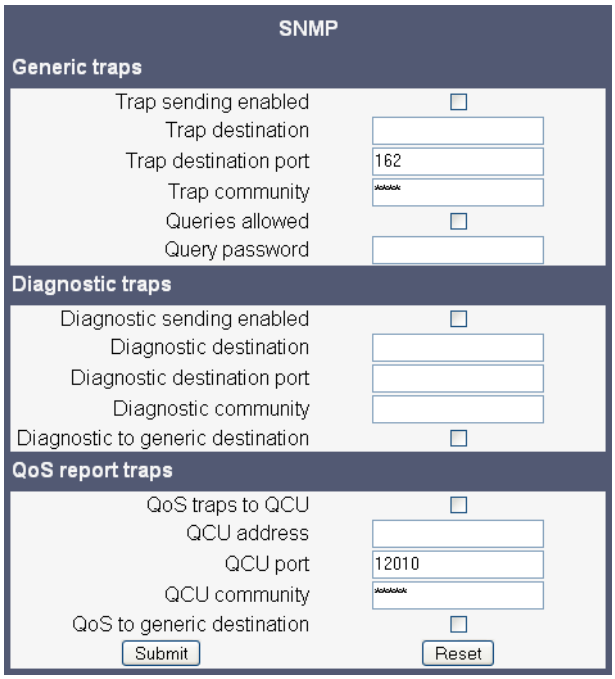
Data required

- **Trap sending enabled / Traps enabled**: Enables or disables the sending of a TRAP message to the SNMP manager.
  Value range: "Yes", "No".
  Default: "No".

- **Trap destination / Manager address**: IP address or hostname of the SNMP manager that receives traps.
- **Trap destination port / Manager port**: Port on which the SNMP manager is receiving TRAP messages.
  Default: 162.
- **Trap community / Community password**: SNMP community string for the SNMP manager receiving TRAP messages.
- **Queries allowed**: Allows or disallows queries by the SNMP manager.
  Value range: "Yes", "No".
  Default: "No".
- **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.
- **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 of the QCU server.
- **QCU port**: Port on which the QCU server is listening for messages.
  Default: 12010.
- **QCU community**: QCU community string.
- **QoS to generic destination / QoS to generic device**: Enables or disables the sending of QoS traps to a generic destination.
  Value range: "Yes", "No".
  Default: "No".

Administration via WBM

System > SNMP



Administration via Local Phone

- Admin
  - System
    - SNMP
      - **Traps enabled**
      - **Manager address**
      - **Manager port**
      - **Community password**

3.4 HiPath Service Menu

The phone's local menu allows for controlling functions provided the HiPath 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 OpenStage phone to the HiPath Communication System, the data described in the following is 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:

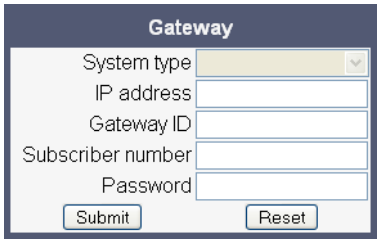
- **Gateway address**: IP address of the communication platform resp. HFA server.
- **Gateway port**: The HFA server's port for signaling.
  Default: "4060".
- **Subscriber number**: The phone's extension.
- **New subscriber password**: Password for logging on to the HFA server.

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 HiPath 4000 resp. the "H.323 ID" in the HiPath 3000.

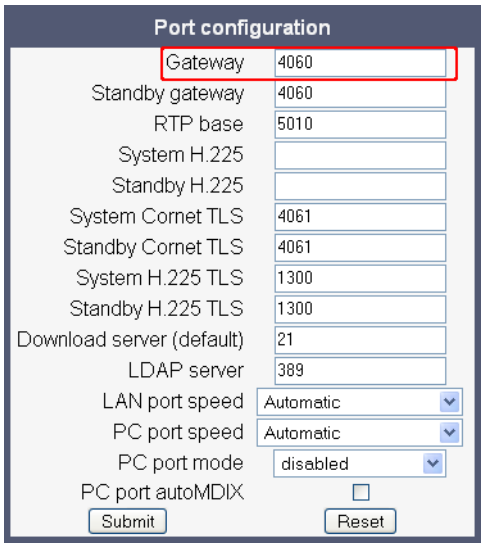
The **System type** is provided by the system the phone is connected to and therefore read-only.

Administration via WBM

System > Gateway



Network > Port configuration



Administration via Local Phone

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

- Admin
  - Network
    - Port configuration
      - Number
        - **Gatekeeper**

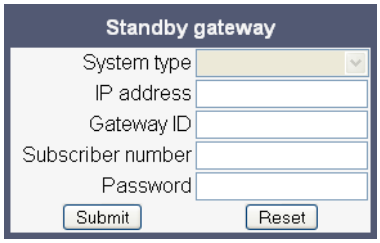
3.5.3 HFA Emergency Gateway Settings

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

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

Administration via WBM

System > Standby gateway



Administration via Local Phone

```
└── Admin
    └── System
        └── Standby gateway
            ├── System type
            ├── IP address
            ├── Gateway ID
            ├── Subscriber number
            └── Password
```

```
└── Admin
    └── Network
        └── Port configuration
            └── Number
                └── Backup
```

3.5.4 Server and Standby Server ports

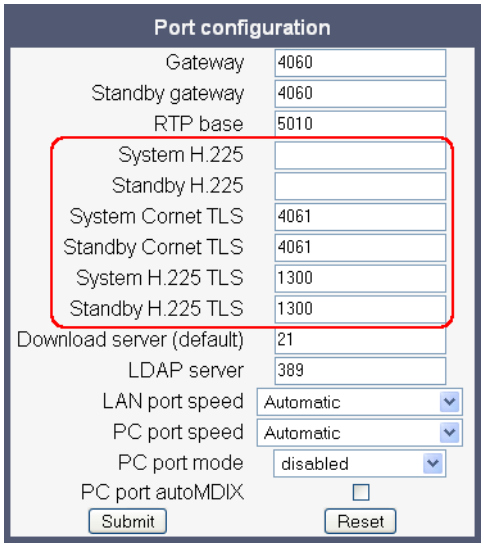
In this section, the server ports for signalisation and speech data transfer are determined.

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

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

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

Administration via WBM



Administration via Local Phone

- Admin
  - Network
    - Port configuration
      - Server port configuration
        - **H.225.0 port**
        - **CorNet-TC TLS port**
        - **H.225.0 TLS port**
      - Standby server port configuration
        - **H.225.0 port**
        - **CorNet-TC TLS port**
        - **H.225.0 TLS port**

3.5.5 Redundancy

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

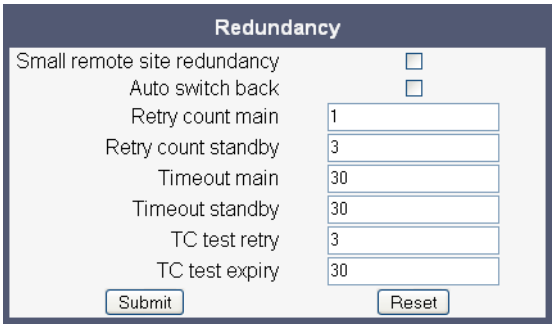
If **Small remote side redundancy** is activated, the phone willl switch over to the standby HFA server in case the connection to the main server ist lost. By default, this is disabled.

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

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

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

Administration via WBM



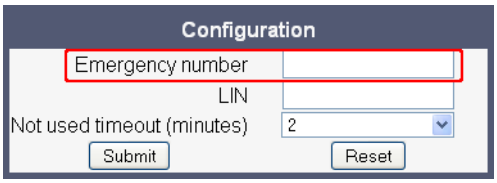
Administration via Local Phone

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

3.5.6 Emergency number

E911 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



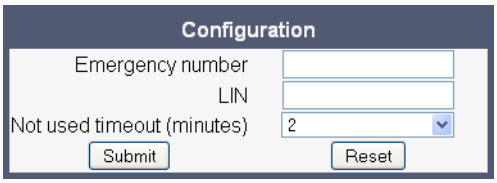
Administration via Local Phone

└--- Admin
└--- System
└--- Features
└--- Configuration
└--- General
└--- **Emergency number**

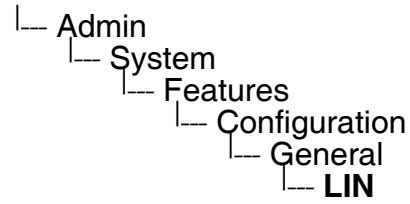
3.5.7 LIN

The **L**ocation **I**dentification **N**umber is a number code which provides detailed geographic information about the phone, including e. g. the office room. On issuing an emergency call using the E911 emergency number (see section 3.5.6, “Emergency number”), this code is transferred to an ALI (Automatic Location Information) system in the public network. When the ALI has looked up the location data in its database, it transmits the data along with the call to the PSAP. The emergency operator is presented with the location data in readable form, so he can dispatch help as appropriate.

Administration via WBM



Administration via Local Phone



3.5.8 Not Used Timeout

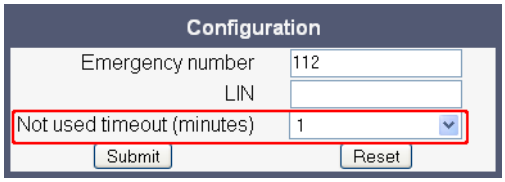
The timeout for the local user and admin menu is configurable. When the time interval is over, the menu is closed and the administrator/user is logged out.

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



Administration via Local Phone

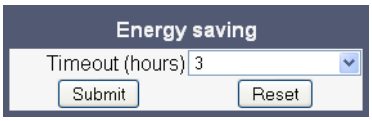
└--- Admin
└--- System
└--- Features
└--- Configuration
└--- General
└--- **Not used timeout**

3.5.9 Energy Saving (OpenStage 40/60/80)

After the phone has been inactive within the timespan specified in **Timeout (hours)** (V1R3) resp. **Backlight timeout (hours)** (V1R3), the display backlight is switched off. The length of this timespan ranges from 2 hours to 8 hours. The default value is 3.

Administration via WBM

Local functions > Energy saving



Administration via Local Phone

- Administration
  - Local Functions
    - Energy Saving
      - **Backlight Timeout (Hrs)**

3.5.10 Date and Time

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

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

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

3.5.10.1 SNTP is available, but no automatic configuration by DHCP server

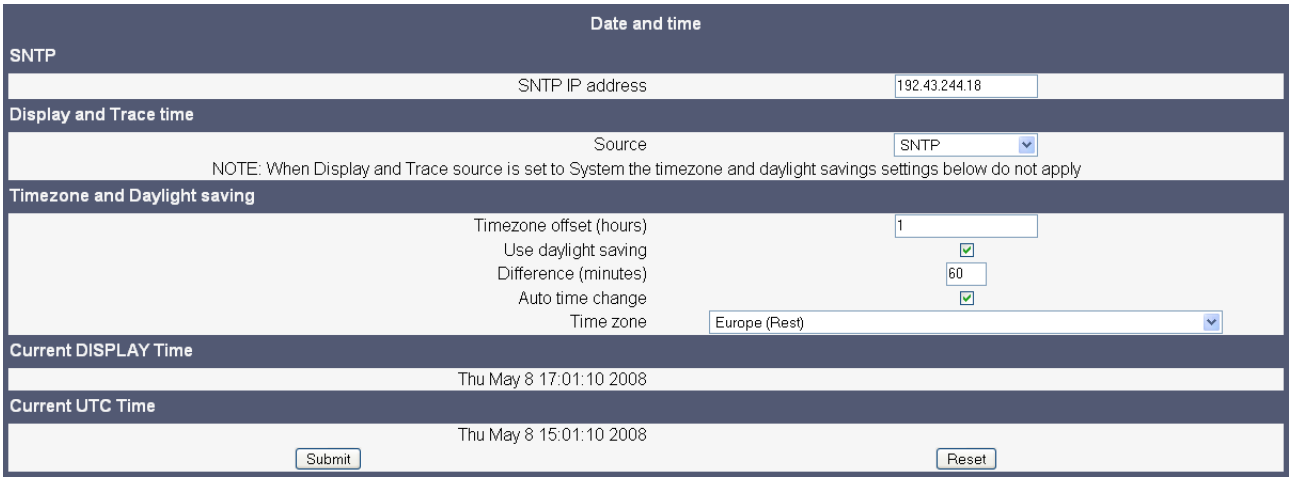
Data required

- **SNTP IP address**: IP address or hostname of the SNTP server.
- **Timezone offset (hours)**: Shift in hours corresponding to UTC.
- **Use 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 **Time zone**.
  Value range: "Yes", "No".

- **Time zone** / **DST zone**: Area with common start and end date for daylight saving time. Value range: "Australia 2007 (ACT, South Australia, Tasmania, Victoria)", "Australia 2007 (New South Wales)", "Australia (Western Australia)", "Australia 2008+ (ACT, New South Wales, South Australia, Tasmania, Victoria)", "Brazil", "Canada", "Canada (Newfoundland)", "Europe (Portugal, United Kingdom)", "Europe (Finland)", "Europe (Rest)", "Mexico", "United States".

Administration via WBM

Date and Time



Administration via Local Phone

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

3.5.11 Security

OpenStage 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 avaliable.

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

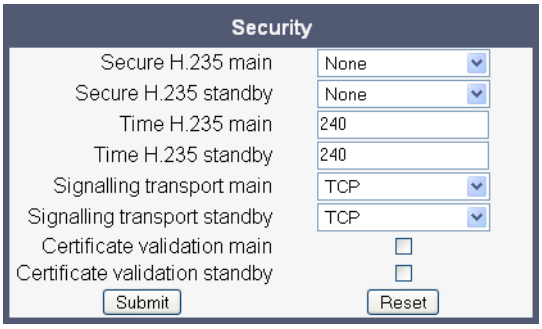
For further information on deploying SPE, please refer to the manual of the HiPath system in use, and to the Deployment Service Administration manual.

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



Administration via Local Phone

- Administration
  - System
    - **Secure H235 main**
    - **Secure H235 standby**
    - **Time H235 main**
    - **Time H235 standby**
    - **Signalling main**
    - **Signalling standby**
    - **Certificate main**
    - **Certificate standby**

3.6 Dialing

3.6.1 Canonical Dialing Configuration

Call numbers taken from a directory application, LDAP for instance, are mostly expressed in canonical format. Moreover, call numbers entered into the local phone book are automatically converted and stored in canonical format, thereby adding "+", **Local country code**, **Local national code**, and **Local enterprise number** as prefixes. If, for instance, the user enters the extension "1234", the local country code is "49", the local national code is "89", and the local enterprise number is "722", the resulting number in canonical format is "+49897221234".

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

To enable the number conversion, all parameters not marked as optional must be provided, and the canonical lookup settings must be configured (see section 3.6.2, “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 number**: 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 number**: 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 HiPath system, each number will start with 3, 4, or 5. Therefore, the digits to be entered are 3, 4, 5.
- **Internal numbers**

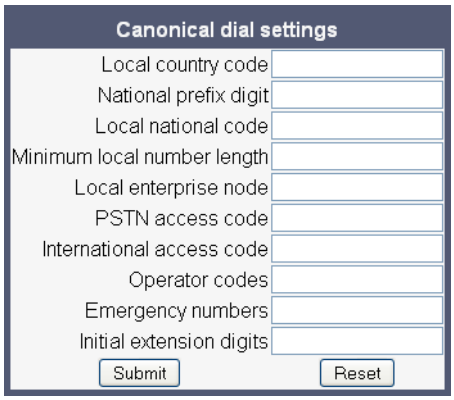
  To enable the phone to discern internal numbers from external numbers, it is crucial that a canonical lookup table is provided (section 3.6.2, “Canonical Dial Lookup”).

  - "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.

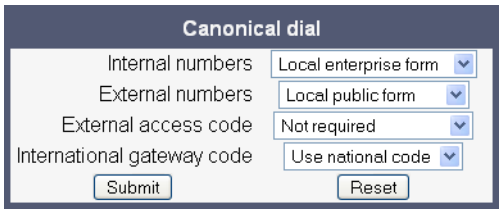
- **International gateway code**:
  - "Use national code": All international formatted numbers will be dialled explicitly by using the access code for the international gateway to replace the "+" prefix.
  - "Leave as +": All international formatted numbers will be prefixed with "+".

Administration via WBM

Locality > Canonical dial settings



Local functions > Locality > Canonical dial



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 gateway**

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)

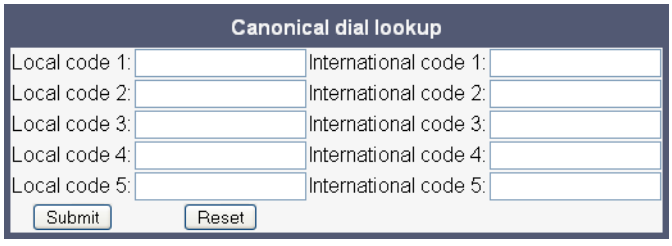
Up to 5 patterns can be defined. The **Local code 1 ... 5** parameters define up to 5 different local enterprise nodes, whilst **International code 1... 5** define up to 5 international codes, that is, fully qualified E.164 call numbers for use in a PSTN.

Data required

- **Local code 1 ... 5**: Local enterprise code for the node/PBX the phone is connected to. Example: "722" for Siemens Munich.
- **International code 1 ... 5**: Sequence of "+", local country code, local area code, and local enterprise node corresponding to to one or more phone book entries. Example: "+4989722" for Siemens Munich.

Administration via WBM

Locality > Canonical dial lookup



Administration via Local Phone

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

3.7 Distinctive Ringing (V2)

With firmware V2, the SIP server may provide information indicating a specific type of call within an incoming call.

The relevant information is carried within the signaling message. When the string matches a specific **Name**, the corresponding ringer is triggered.

The **Ringer sound** parameter determines whether a pattern, i. e. melody, or a specific sound file shall be used as ringer.

Pattern Melody selects the melody pattern that will be used if **Ringer sound** is set to "Pattern".

Pattern sequence determines the length for the melody pattern, and the interval between the repetitions of the pattern. There are 3 variants:

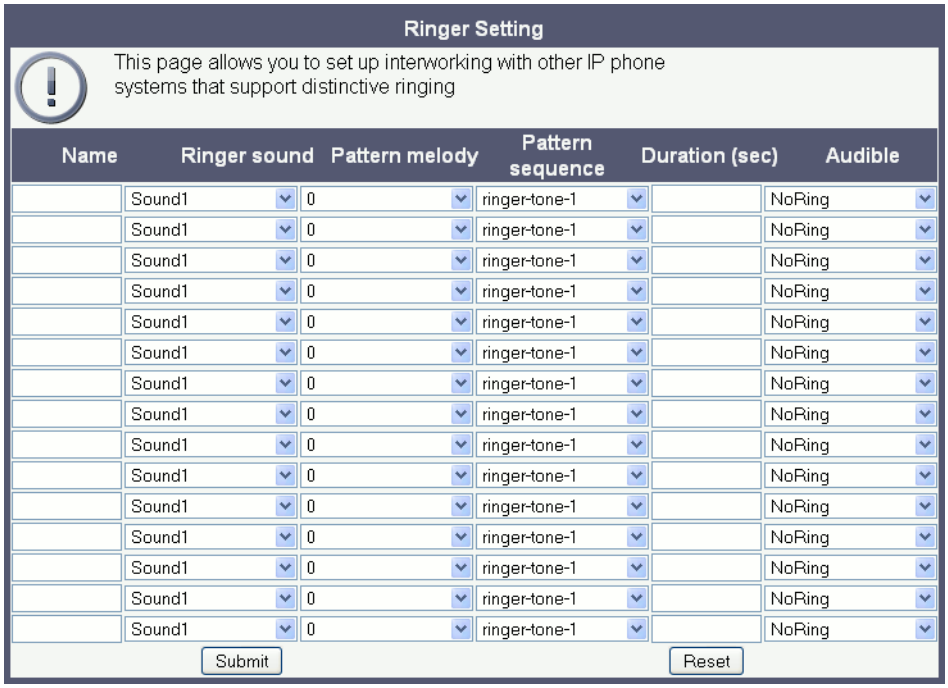
- "1": 1 sec ON, 4 sec OFF
- "2": 1 sec ON, 2 sec OFF
- "3": 0.7 sec ON, 0.7 sec OFF, 0.7 sec ON, 3 sec OFF

The **Duration** parameter determines how long the phone will ring on an incoming call. The range is 0-300 sec.

With the **Audible** parameter, the ringer can be muted. In this case, an incoming call will be indicated only visually.

Administration via WBM

Ringer setting



3.8 Mobility (OpenStage 60/80, V1R3 Onwards)

If data mobility is enabled, the user can log on at another phone and at the same time carry his user data with him. 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 3.6, "Dialing");
- the call log;
- the user password.

Mobility is applicable to OpenStage 60/80 only, as only these phone types have the relevant user data.

For 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, he will see all user data of the precedent user.
- **Data Privacy** (OpenStage 60/80 only): When a new user logs on at the phone, he will be provided with a pristine, empty phone book and call log. The user of the precedent user will be hidden to the new user.
- **Data Mobility** (OpenStage 60/80 only): 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 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 data mobility must be activated both on phone A and B.

In case a user wants to move from an OpenStage phone to an optiPoint phone, DLS-based data mobility ist not possible. However, when using an OpenStage 60/80 phone, the data can be saved on an USB stick. For details, please refer to the User Guide for OpenStage 60/80.

3.8.1 Platform Specific Behaviour

Regarding data mobility, there are some differences, dependent on whether a HiPath 3000 or HiPath 4000 is in use.

HiPath 4000

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.

HiPath 3000

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. The procedures are identical to those used for SIP mobility. For details, please refer to the Deployment Service Administration Manual.

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 ringtones 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:

- OpenStage 20/40: 4 MB
- OpenStage 60/80: 8 MB

3.9.1 FTP/HTTPS Server

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

3.9.2 Common FTP Settings

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**, **Server**, **Server port**, **Account**, **Username**, **FTP path**, and **HTTPS baser 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".

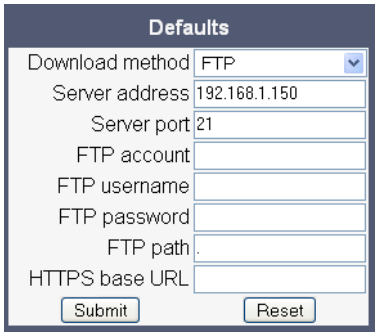
If **Use defaults** is activated for a specific file type, any specific settings for this file type are overridden by the defaults.

Data required

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS".
  Default: "FTP".
- **Server**: IP address or hostname of the FTP server in use.
- **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.
- **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. If no port number is specified here, port 443 is used. Only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > Defaults



Administration via Local Phone

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

3.9.3 Phone Software

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

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 Settings”) are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

Data required (in every case)

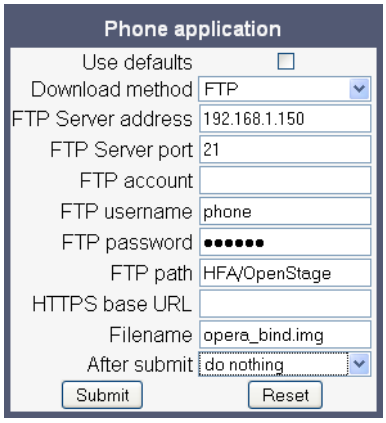
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No".
- **Filename**: Specifies the file name of the phone software.

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".

Administration via WBM

File transfer > Phone application



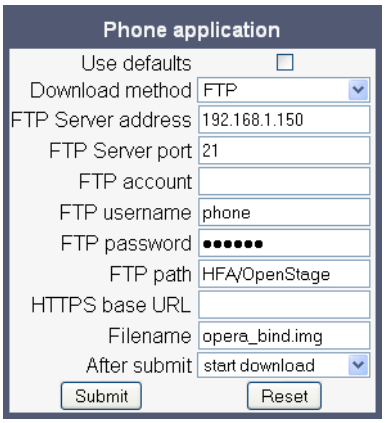
Administration via Local Phone

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

3.9.3.2 Download/Update Phone Software

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

Start Download via WBM



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

Start Download via Local Phone

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

```
└── Admin
    └── File Transfer
        └── Phone app
```

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.9.4 Picture Clips

Picture clips are available only on OpenStage 60/80 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

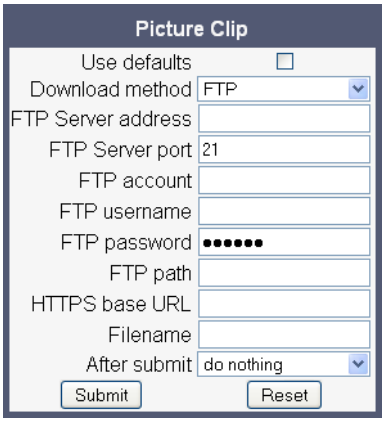
If the default FTP/HTTPS access settings (see section 3.9.2, “Common FTP Settings”) are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

Data required (in every 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".

Administration via WBM

File transfer > Picture clip



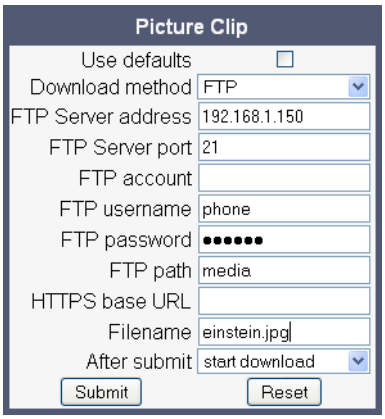
Administration via Local Phone

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

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



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

Start Download via Local Phone

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

└--- Admin
  └--- File Transfer
    └--- **Picture clip**

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.9.5 LDAP Template

LDAP is available only on OpenStage 60/80 phones.

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

The OpenStage phone supports LDAPv3.

3.9.5.1 FTP/HTTPS Access Data

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

Data required (in every case)

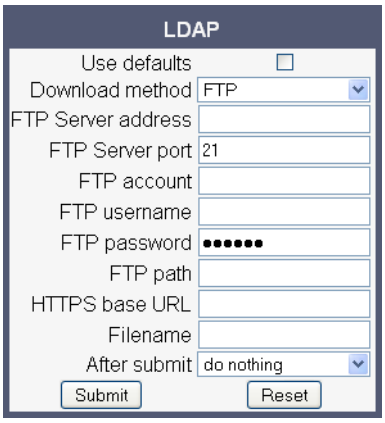
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No".
- **Filename**: Specifies the file name of the LDAP template file.

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".

Administration via WBM

File transfer > LDAP



Administration via Local Phone

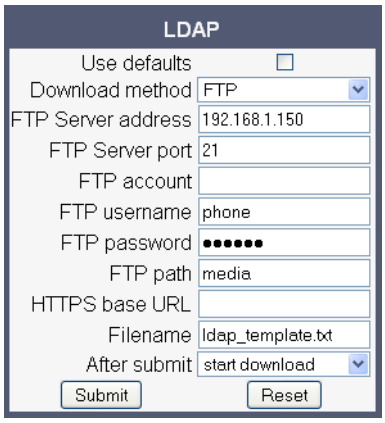
- Admin
  - File Transfer
    - LDAP
      - **Use default**
      - **Download method**
      - **Server**
      - **Port**
      - **Account**
      - **Username**
      - **Password**
      - **FTP path**
      - **HTTPS base URL**
      - **Filename**

3.9.5.2 Download LDAP Template

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

The OpenStage phone supports LDAPv3.

Start Download via WBM



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

Start Download via Local Phone

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

```
└── Admin
    └── File Transfer
        └── LDAP
```

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.9.6 Logo

On OpenStage 40/60/80, a custom background image for the telephony interface can be supplied. In most cases, this will be the company logo.

On OpenStage 40, monochrome bitmap files (BMP) are supported. The ideal size is as follows:
- Width: 144 px
- Height: 32 px

On OpenStage 60/80, the supported file formats are JPEG and PNG. The ideal size values are is as follows:

OpenStage 60:
- Width: 240 px
- Height: 70 px

OpenStage 80:
- Width: 480 px
- Height: 142 px

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

For creating a logo file, see section 4.2, “How to Create Logo Files for OpenStage Phones”.

3.9.6.1 FTP/HTTPS Access Data

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

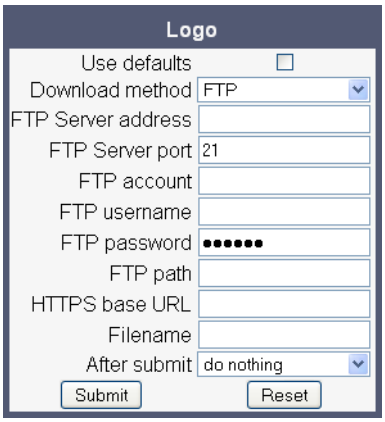
Data required (in every case)

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

Administration via WBM

File transfer > Logo



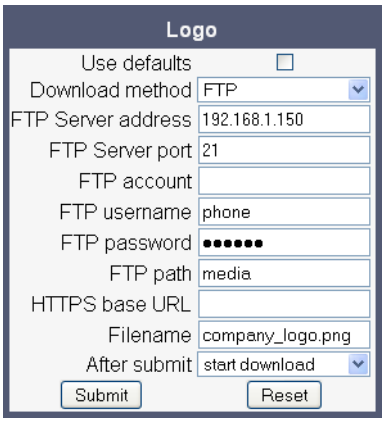
Administration via Local Phone

- 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 Deployment Service (DLS) . 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

1. In the administration menu, set the focus to **Logo**.

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

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

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 OpenStage 60/80 phones.

The file size for a screensaver image is limited to 300 KB.

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:
  - OpenStage 60: 320x240
  - OpenStage 80: 640x480

3.9.7.1 FTP/HTTPS Access Data

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

Data required (in every 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.

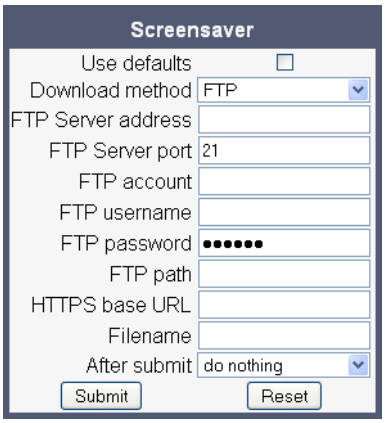
Data required (if not derived from Defaults)

- **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".

Administration via WBM

File transfer > Screensaver



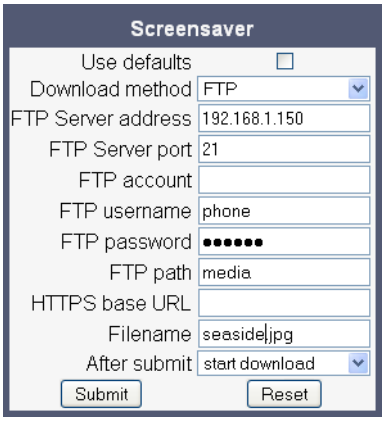
Administration via Local Phone

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

3.9.7.2 Download Screensaver

If applicable, screensavers 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



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

Start Download via Local Phone

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

```
└── Admin
    └── File Transfer
        └── Screensaver
```

2. Press the ➔ key. A context menu opens. In the context menu, select **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 OpenStage 60/80.

Custom Ringtones can be uploaded to the phone.

The file size for a ringer file is limited to 1 MB. If the contents of the file are not valid, the file transfer will be cancelled.

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 (OpenStage 60/80 only). The OpenStage 60/80 phones are able to play MP3 files from 32 kbit/s up to 320 kbit/s. As the memory for user data is limited to 8 MB, a constant bitrate of 48 kbit/sec to 112 kbit/s and a length of max. 1 minute is recommended. Although the phone software can play stereo files, mono files are recommended, as the phone has only 1 loudspeaker.
  See the following table for estimated file size (mono files):

Length	64 kbit/s	80 kbit/s	96 kbit/s	112 kbit/s
0:15 min	0,12 MB	0,15 MB	0,18 MB	0,21 MB
0:30 min	0,23 MB	0,29 MB	0,35 MB	0,41 MB
0:45 min	0,35 MB	0,44 MB	0,53 MB	0,62 MB
1:00 min	0,47 MB	0,59 MB	0,70 MB	0,82 MB

3.9.8.1 FTP/HTTPS Access Data

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

Data required (in every case)

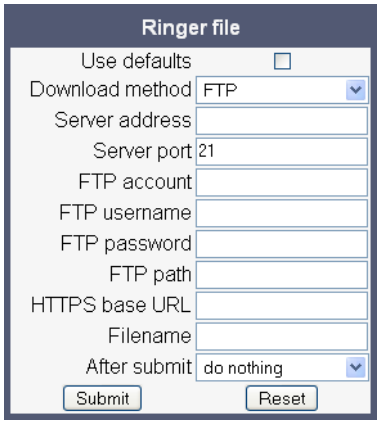
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No".
- **Filename**: Specifies the file name of the ringtone file.

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".

Administration via WBM

File transfer > Ringer file



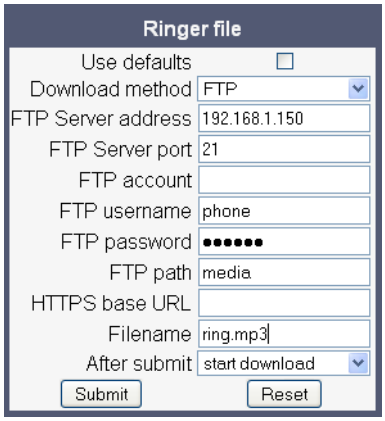
Administration via Local Phone

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

3.9.8.2 Download Ringer File

If applicable, ringtone files 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



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

Start Download via Local Phone

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

```
└── Admin
    └── File Transfer
        └── Ringer
```

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.9.9 ´HPT 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) are to be used, **Use default** must be set to „Yes“, and only the **Filename** must be specified.

Data required (in every case)

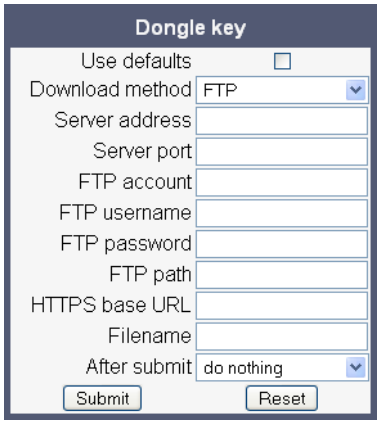
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used. Value range: „Yes“, „No“.
  Default: „No“.
- **Filename**: Specifies the file name of the phone software.

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.
- **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; only applicable if **Download method** is switched to „HTTPS“.

Administration via WBM

File transfer > Dongle key



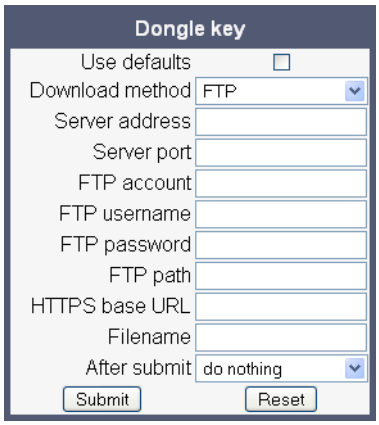
Administration via Local Phone

- Administration
  - 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 Deployment Service (DLS). 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

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

└--- Administration
  └--- File Transfer
    └--- **Dongle key**

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.10 Corporate Phonebook: Directory Settings

3.10.1 LDAP

LDAP is available only on OpenStage 60/80 phones.

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, organisation and contact data of persons working in an organisation. 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 OpenStage phone supports LDAPv3.

For connecting the phone's LDAP client to a LDAP server, the required access data must be configured. The parameters **Server address** and **Server port** specify the IP address and hostname as well as the port used by 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 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)".

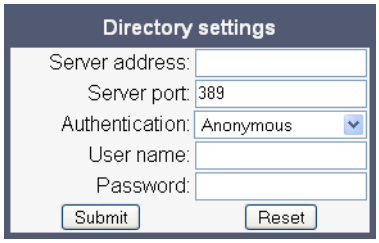
With firmware V2, the OpenStage 60/80 GUI features a new search field for LDAP requests. The search string is submitted to the LDAP server as soon as the OK key is pressed, or when the **Search trigger timeout** expires.

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** (V2 on OpenStage 60/80): Timespan between entering the last character and search string submission to the LDAP server.

Administration via WBM

Local Functions > Directory settings



Administration via Local Phone

- Administration
  - Local Functions
    - Directory Settings
      - **LDAP server address**
      - **LDAP server port**
      - **LDAP authentication**
      - **LDAP user name**
      - **LDAP password**

3.11 Speech

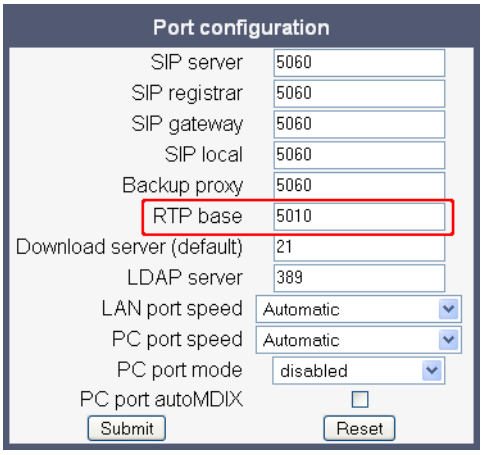
3.11.1 RTP Base Port

The port used for RTP is negotiated during the establishment of a connection. The RTP base port number defines the starting point from which the phone will count up when negotiating. The default value is 5010.

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

Administration via WBM

Network > Port Configuration



Administration via Local Phone

- Admin
  - Network
    - Port Configuration
      - Number
        - **RTP base**

3.11.2 Codec Preferences

If **Silence suppression** is activated, the transmission of data packets is suppressed on no conversation.

The OpenStage phone provides the codecs G.711, G.722, and G.729. When an 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.

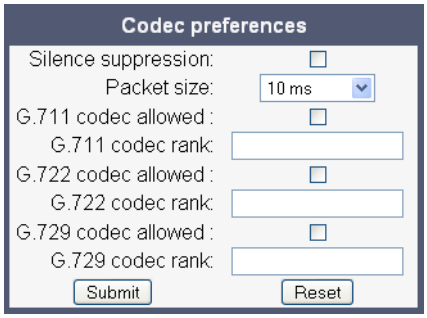
The **Packet size**, i. e. length in milliseconds, of the RTP packets for speech data, can be set to 10ms or 20ms or to automatic detection.

Data required

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

Administration via WBM

Speech > Codec preferences



Administration via Local Phone

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

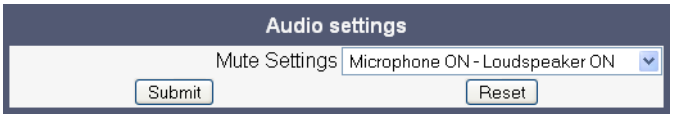
3.11.3 Audio Settings

The usage of microphone and speaker for speakerphone mode can be controlled by the administrator.

Both microphone and loudspeaker can be switched on or off separately.

Administration via WBM

Speech > Audio Settings



Administration via Local Phone

```
└--- Admin
     └--- Speech
          └--- Audio Settings
               |--- Disable microphone
               └--- Disable loudspeech
```

3.12 Display General Phone Information

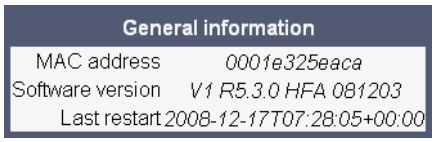
General information about the status of the phone can be displayed if desired.

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



Display on the Local Phone

└── Admin
  └── General Information
    ├── **MAC address**
    ├── **Software version**
    └── **Last restart**

3.13 Applications (V2 on OpenStage 60/80)

3.13.1 XML Applications/Xpressions

3.13.1.1 Setup/Configuration

With firmware V2, an XML interface is available that 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 OpenStage 60/80 phones.

An XML application can be started by using the ☰ 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 ✉ 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 🕮 will invoke this application, in place of the personal (local) or corporate (LDAP) phonebook.

For detailed information about the OpenStage XML application interface, please see the OpenStage 60/80 XML Applications Developer's Guide.

To set up a new XML application, enter the access data for the application on the server:

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

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

Program name 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. The program name cannot be longer than 100 characters.

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.

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

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: If checked, a running XML application is automatically restarted after it has been modified. Please note that a restart will take place even if no changes have been made for the application selected for modification in the Modify application mask, and Submit has been pressed. After the XML application has restarted, this option is automatically unchecked. If Auto restart is checked whilst the XML application is not running, there will be no restart, and the option is automatically unchecked.

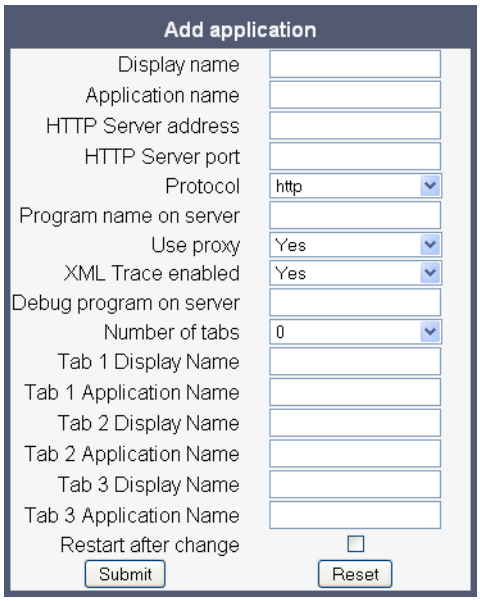
Data required

- **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".

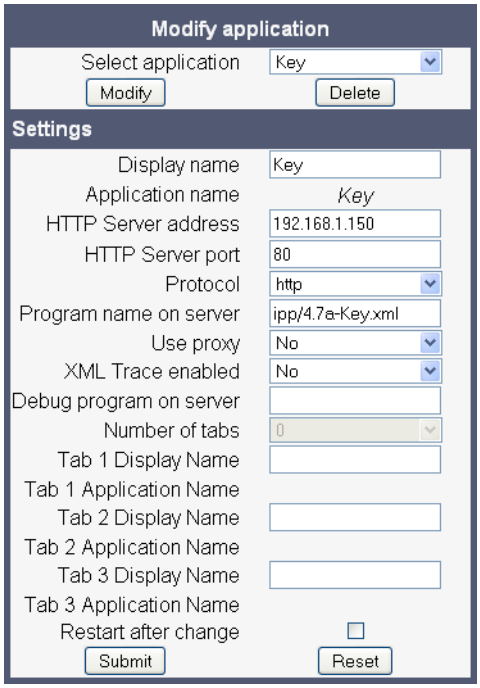
- **HTTP Server address**: IP address or domain/host name of the server that provides the application or the XML document.
- **Server port number**: Number of the port that the server uses to provide the application or XML document.
- **Program name**: Relative path to the servlet or to the first XML page of the application on the server.
- **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 via WBM

Applications > XML Applications > Add application



Applications > XML Applications > Modify application



Administration via Local Phone

- Administration
  - Applications
    - XML
      - Add application
        - **Display name**
        - **Application name**
        - **Server address**
        - **Server port**
        - **Protocol**
        - **Program name**
        - **XML trace enabled**
        - **Debug program name**
        - **Number of tabs**
        - **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**

3.13.1.2 HTTP Proxy

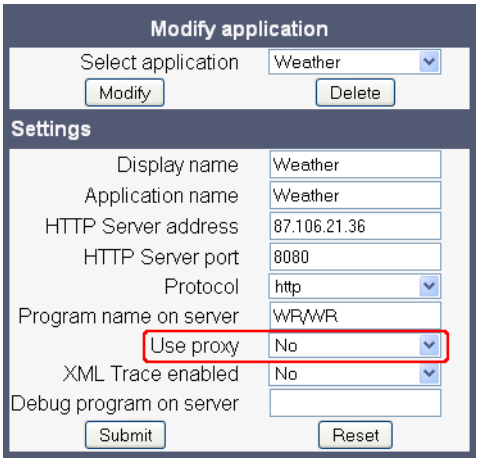
The HTTP data transfer between the phone and the server on which the remote program is running can be handled be an HTTP proxy, if desired.

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.

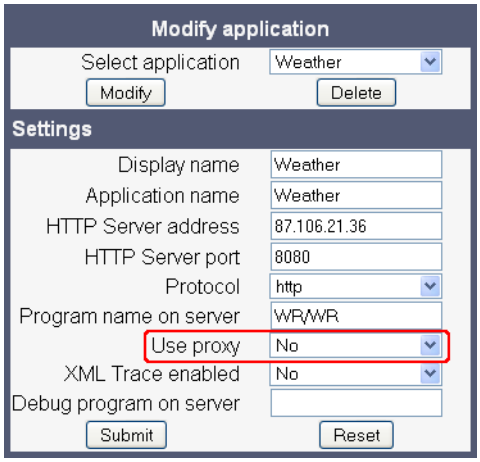
Use proxy enables or disables the use of the proxy. If disabled, the phones connects directly to the server. By default, the use of a proxy is disabled.

Administration via WBM

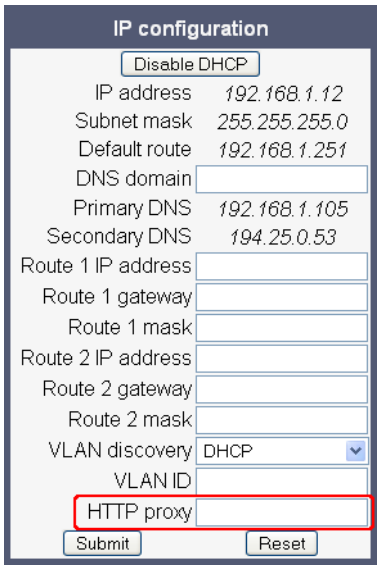
Applications > XML Applications > Add application



Applications > XML Applications > Modify application



Network > IP Configuration



Administration via Local Phone

- Administration
  - Applications
    - XML
      - Add application
        - **Use proxy**
      - Add Xpressions
        - **Use proxy**

- Administration
  - Network
    - IP Configuration
      - **HTTP proxy**

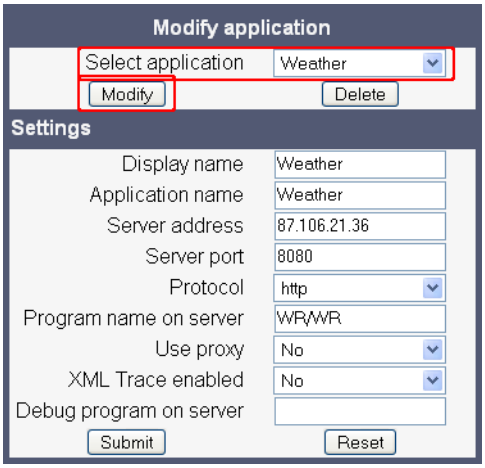
- Administration
  - Network
    - Port configuration
      - **HTTP proxy**

3.13.1.3 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 application



Administration via Local Phone

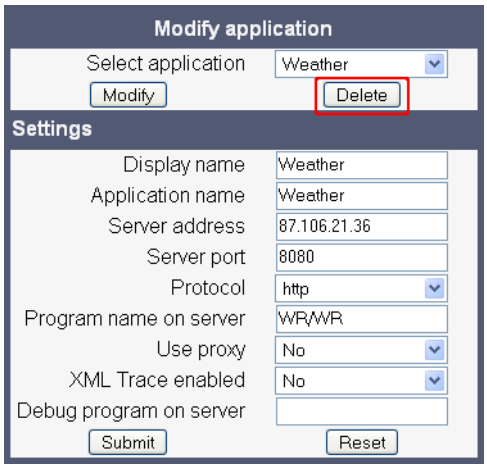
- Administration
  - Applications
    - XML
      - <Application to be modified>
        - **Display name**
        - **Application name**
        - **Server address**
        - **Server port**
        - **Protocol**
        - **Program name**
        - **XML trace enabled**
        - **Debug program name**

3.13.1.4 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 application



Administration via Local Phone

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

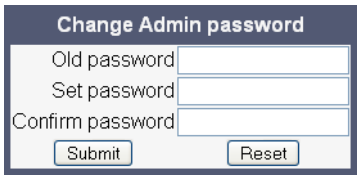
```
└── Administration
    └── Applications
        └── XML
            └── <Application to be deleted>
```

3.14 Password

The passwords for user and administrator can be set here. They have to be confirmed after entering. The factory setting is "123456"; it should be changed after the first login.

Administration via WBM

Security > Change Admin password



Security > Change User password

Administration via Local Phone

- Admin
  - Password
    - **Admin**
    - **Confirm admin**
    - **User**
    - **Confirm user**

3.15 Troubleshooting: Lost Password

If the administration and/or user password is lost, and there is no DLS available, new passwords must be provided. For this purpose, a factory reset is necessary. Take the following steps to initiate a factory reset:

1. On the phone, press the ☰ key to activate the administration menu (the ☰ 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.
3. In the input field, enter the special password for factory reset: "124816".
4. Confirm by pressing OK.

3.16 Restart Phone

If necessary, the phone can be restarted from the administration menu.

Administration via WBM

Administration via Local Phone

└── Admin
    └── **Restart**

3.17 Factory Reset

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

Administration via WBM

Maintenance > Factory reset

Administration via Local Phone

└── Admin
    └── **Factory reset**

3.18 SSH - Secure Shell Access (V2)

With firmware V2, the phone's operating system can be accessed via SSH for special trouble-shooting 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.

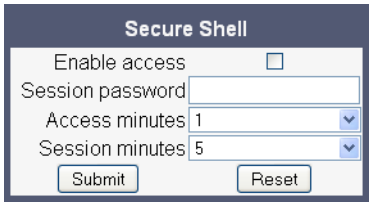
When **Enable access** is enabled, and the parameters described underneath are specified, SSH access is activated. By default, SSH access is disabled.

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 minuts within which the SSH connection must be established. After it has expired, a logon via SSH is not possible. The possible values are 1, 3, 5, 10, 15.

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



3.19 Display License Information

The license information for the OpenStage phone software currently loaded can be viewed via the local menu.

└─ Administration
  └─ **Licence information**

3.20 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, "´HPT Dongle Key"). This key is accessable to the service staff only. It is specific for a particular HFA firmware version, but it will also be valid for previous versions.

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

A control session allows for activating phone functions remotely. When a control session is established, the following changes will occur:

- The display shows a message indicating that remote service is active.
- Handset, microphone, speaker, headset, and microphone are disabled.

An observation session allows for supervising events on the phone, like, for instance, pressing a key, incoming calls or navigating in the menus. Before an observation session is started, the user is prompted for allowing the observation. During an observation session, the phone operates normally, including loudspeaker, microphone and ringer. Thus, the local user can demonstrate an error towards the service staff that is connected via HPT.

The HPT interface is enabled by downloading the dongle key file to the phone (see section 3.9.9, "´HPT 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 3.21.2, "Fault Trace Configuration").

Administration via WBM

Maintenance > Test interface

Administration via Local Phone (Disable)

Administration
Maintenance
Disable HPT / Enable HTP

3.21 Diagnostics

3.21.1 LLDP-MED (V2)

With formware V2, the phone can receive a VLAN ID and QoS parameters and advertise its own network-related properties when connected to a switch with LLDP-MED capabilities. 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.
- **LLDEP-MED capabilities**: The LLDP-MED TLVs supported by the phone and the switch as well as the specific device class they belong to.
- **MAC_Phy configuration**: Identifies the possible duplex and bit-rate capability of the sending device, its current duplex and bit-rate capability, and whether theses settings are the result of auto-negotiation during the initialization of the link, or of manual set override actions.
- **System capabilities**: The devices advertise their potential and currently enabled functions, e. g. "Bridge", "Telephone".
- **TTL**: **T**ime **T**o **L**ive. This parameter determines how long the TLVs are valid. When expired, the device will send a new set of TLVs.

View Data From WBM

Diagnostics > LLDEP-MED TLVs

LLDP-MED TLVs

Sent	Received
Sent: Mon Oct 27 10:51:14 2008	Received: Mon Oct 27 10:51:14 2008
Chassis ID TLV Data .Subtype = Network address .IANA_TYPE = IPv4 Address .ID = 192.168.6.109	Chassis ID TLV Data .Subtype = MAC address .ID = C0:1E:F7:05:2D:C4
Port ID TLV Data .Subtype = MAC address .ID = D0:01:E3:2D:66:38	Port ID TLV Data .Subtype = Locally assigned .ID = Fa0/2
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, Bridge, Router, .Enabled = Other, Repeater,
MAC_Phy config TLV data .Auto-net supported = Yes .Auto-net enabled = Yes .PMD = 0x6c00 .PMD1 = 10BASE-T half duplex mode .PMD2 = 10BASE-T full duplex mode .PMD3 = 100BASE-TX half duplex mode .PMD4 = 100BASE-TX full duplex mode .MAU = 100BaseTXFD : 0x10	MAC_Phy config TLV data .Auto-net supported = Yes .Auto-net enabled = Yes .PMD = 0x36 .PMD1 = Symmetric PAUSE for full-duplex .PMD2 = Asy and Sym PAUSE for full-duplex links .PMD3 = 1000BASE-X, -LX, -SX, -CX full duplex .PMD4 = 1000BASE-T half duplex mode .MAU = 100BaseTXFD : 0x10
LLDP-MED Caps TLV Data .Caps - LLDP-MED = Yes .Caps - Network Policy = Yes .Caps - Location ID = No .Caps - Extended Power Mdi PD = Yes .Caps - Extended Power Mdi Pse = No	LLDP-MED Caps TLV Data .Caps - LLDP-MED = Yes .Caps - Network Policy = Yes .Caps - Location ID = Yes .Caps - Extended Power Mdi PD = Yes .Caps - Extended Power Mdi Pse = Yes .Caps - Inventory = Yes .Type = Network Connectivity

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.

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

3.21.2 Fault Trace Configuration

Error tracing and logging can be configured separately for all components, i. e. the services and applications running on the OpenStage phone. 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 the maximum size is reached, the file is deleted, and a new file is generated. The trace data is then written to the new file. The default value is 65536.

The **Trace timeout (minutes)** determines when to stop tracing, i. e. writing to the trace file. When the value is 0, no trace file will be written.

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.

The log files can be downloaded by clicking on the following hyperlinks:

- **Download trace file**
  This file contains the trace data according to the settings specified for the services.
- **Download boot file** (not present with V2)
  The system messages of the booting process. With firmware version V2, these messages will be incorparated in the syslog file (see **Download syslog file** underneath).
- **Download old/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 old/saved boot file** (not present with V2)
  Normally, the boot file is saved only in the phone RAM. When the phone restarts in a controlled manner, the boot file will be saved in permanent memory. With firmware version V2, these messages will be incorparated in the syslog file (see **Download syslog file** underneath).
- **Download sci trace file**

- **Download upgrade trace file**
  The trace log created during a software upgrade.
- **Download upgrade error file** (not present with V2)
  The error log created during a software upgrade.
- **Download exception file** (not present with V2)

- **Download old exception file** (not present with V2)
  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 old trace file**

The trace file is stored 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 error file** (not present with V2)
  The error log, written by the phone's services.
- **Download old error file** (not present with V2)
  The error file is stored permanent memory. When the file has reached its size limit, it will be saved as old error file, and the current exception file is emptied for future messages. The old error file can be viewed here.
- **Download syslog file** (V2)
  Messages from the phone's operating system.
- **Download old syslog file** (V2)
  Old messages from the phone's operating system.
- **Download saved syslog file** (V2)
  Old messages from the phone's operating system.
- **Download Database file** (V2)
  Configuration parameters of the phone in SQLite format.
- **Download upgrade error file** (V2)
  The trace log created during a software upgrade.
- **Download HPT remote service log file** (V2)
  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**: Only errors messages are stored.
- **DEBUG**: All 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.
- **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**
  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.
- **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. OpenStage 20/40 HFA/SIP, OpenStage 60/80 HFA/SIP.
- **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.
- **HFA service agent** (up to V1R3)

- **HFA messages** (V2)

- **H.323 messages**

- **H.323 security**

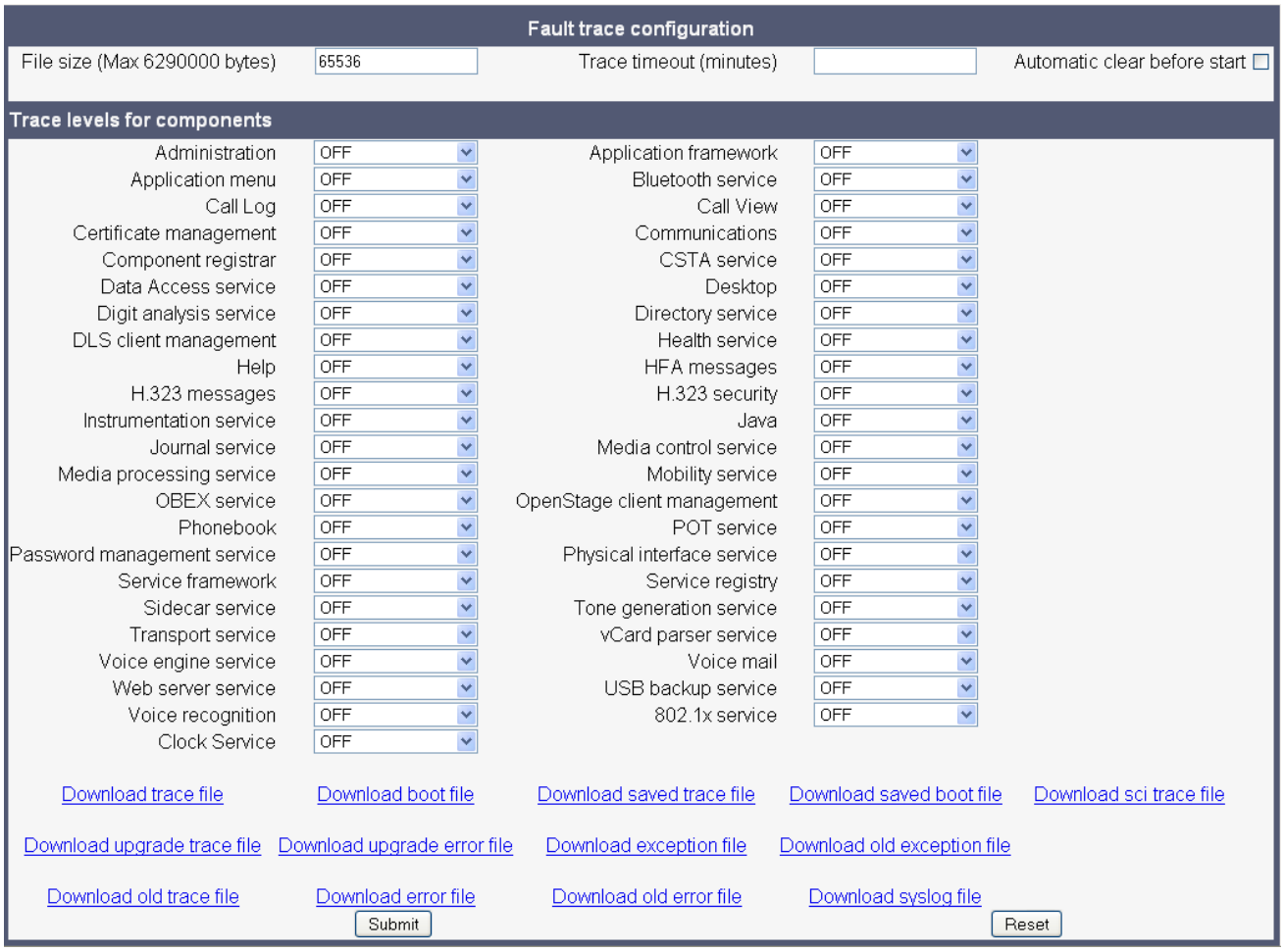
- **Instrumentation service**
  Used by the Husim phone tester to exchange data with the phone for remote control, testing and monitoring purposes.
- **Java**
  Any Java applications running on the phone will be run in the Java sandbox controlled by the Java service.
- **Journal service**
  Responsible 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**
  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.
- **Phonebook**
  Responsible for the phonebook application.
- **POT service** (not present with V2)
  Takes over control of basic telephony if the callview application fails.
- **Performance Marks** (V2)
  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".

- **Password management service**
  Verifies passwords used in the phone.
- **Physical interface service**
  Handles any interactions with the phone via the keypad, mode keys, fixed feature buttons, clickwheel and slider.
- **Service framework**
  This is the environment within which other phone services operate. It is involved in the starting and stopping of services.
- **Service registry**
  Keeps a record of all services currently running inside the phone.
- **Sidecar service**
  Handles interactions between the phone and any attached sidecars.
- **Tone generation service**
  Handles the generation of the tones and ringers on the phone.
- **Transport service**
  Provides the IP (LAN) interface between the phone and the outside world.
- **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.
- **Web server service**
  Provides access to the phone via web browser.
- **USB backup service**
  Used to make backup/restore to/from USB stick by using password. This item is available in the phone GUI.
- **Voice recognition**
  Used by the voice dial facility for recognizing spoken dialing commands.
- **802.1x service** (V1R3 onwards)
  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.
- **Clock service**
  Handles the phone's time and date, including daylight saving and NTP functionality.

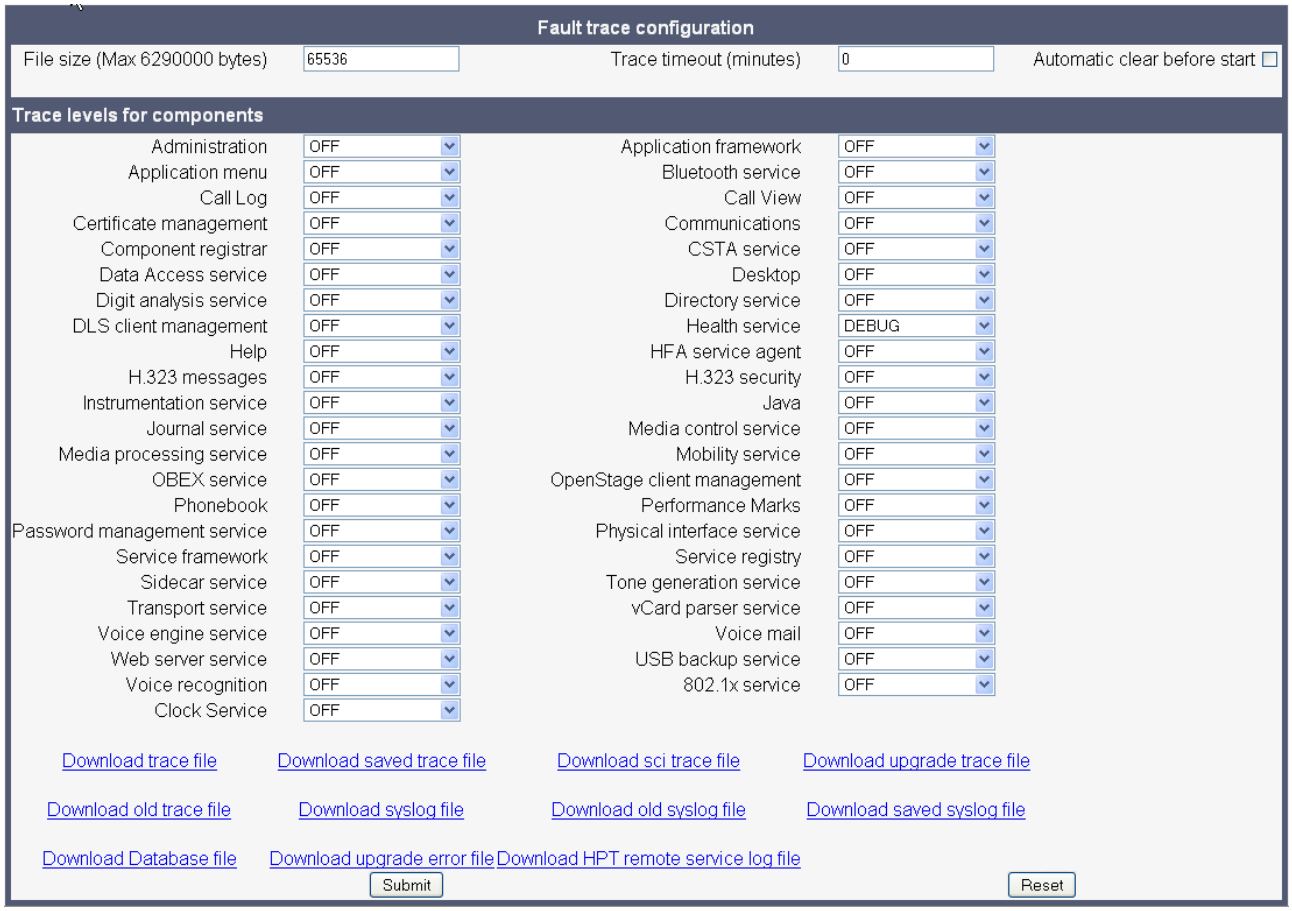
Administration via WBM (V1R3)

Diagnostics > Fault Trace Configuration



Administration via WBM (V2)

Diagnostics > Fault Trace Configuration



3.21.3 Easy Trace Profiles

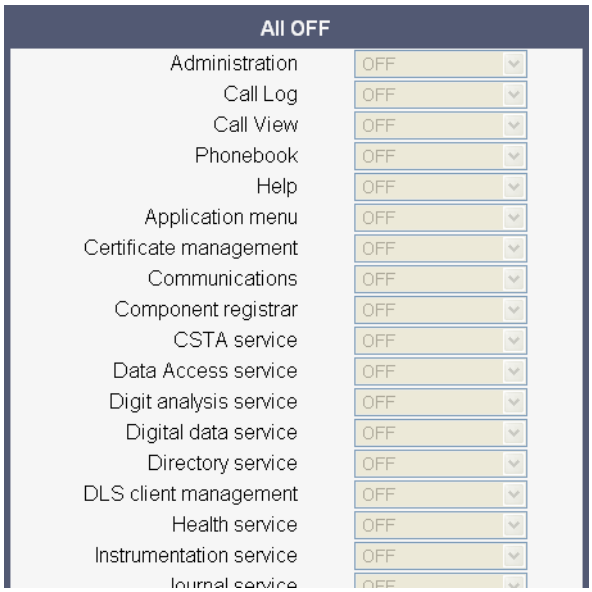
In order to simplify tracing for a specific problem, the tracing levels can be adjusted using pre-defined settings. The Easy Trace profiles provide settings for all services, or for a specific area, e. g. call connection. On pressing **Submit**, those pre-defined settings are sent to the phone. If desired, the settings can be modified anytime using the general mask for trace configuration under Diagnostics > Fault Trace Configuration (see section 3.21.2, “Fault Trace Configuration”).

Special EasyTrace profiles enable setting one level for all parameters with just one click (see section 3.21.3.1, “No Tracing for All Services”).

The following sections describe the Easy Trace profiles available for the phone.

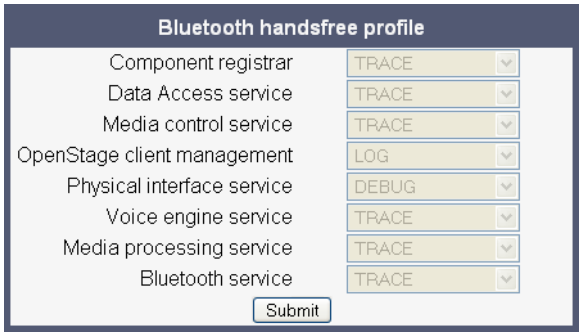
3.21.3.1 No Tracing for All Services

Diagnostics > Easy Trace Profiles > All OFF



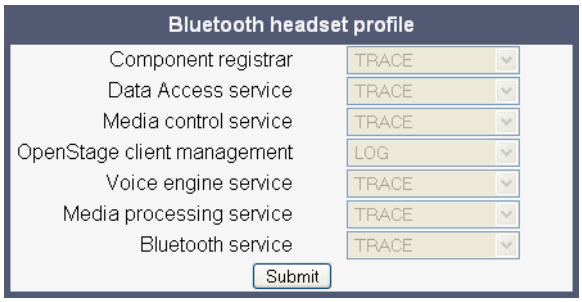
3.21.3.2 Bluetooth Handsfree

Diagnostics > Easy Trace Profiles > Bluetooth handsfree profile



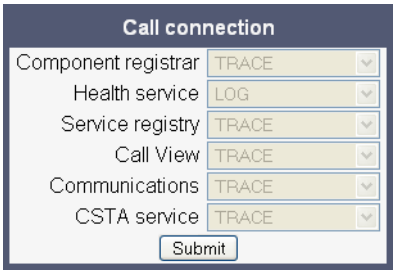
3.21.3.3 Bluetooth Headset

Diagnostics > Easy Trace Profiles > Bluetooth headset profile



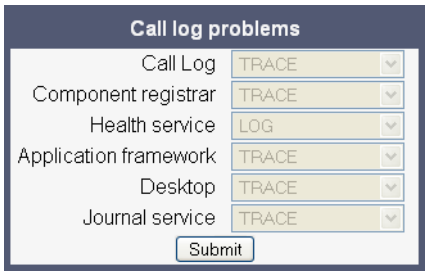
3.21.3.4 Call Connection

Diagnostics > Easy Trace Profiles > Call connection



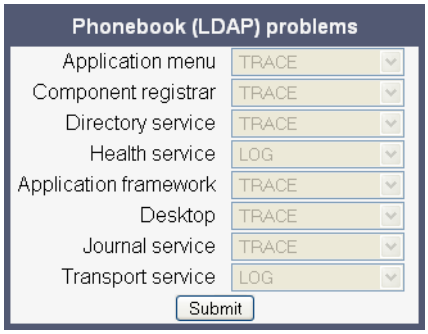
3.21.3.5 Call Log

Diagnostics > Easy Trace Profiles > Call log problems



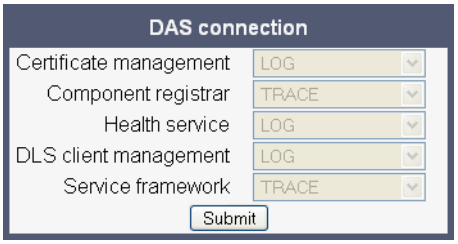
3.21.3.6 LDAP Phonebook

Diagnostics > Easy Trace Profiles > Phonebook (LDAP) problems



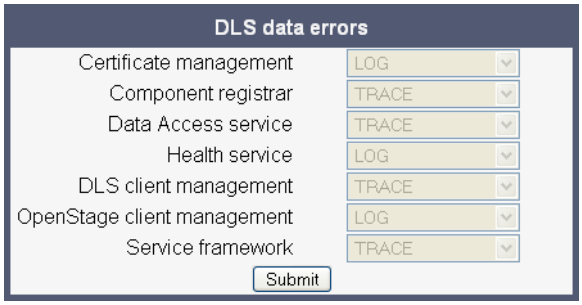
3.21.3.7 DAS Connection

Diagnostics > Easy Trace Profiles > DAS connection



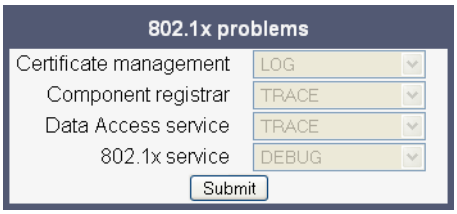
3.21.3.8 DLS Data Errors

Diagnostics > Easy Trace Profiles > DLS data errors



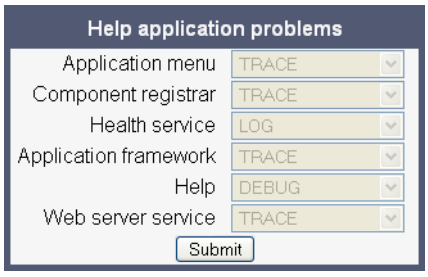
3.21.3.9 802.1x

Diagnostics > Easy Trace Profiles > 802.1x problems



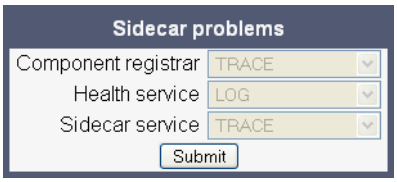
3.21.3.10 Help Application

Diagnostics > Easy Trace Profiles > Help application problems



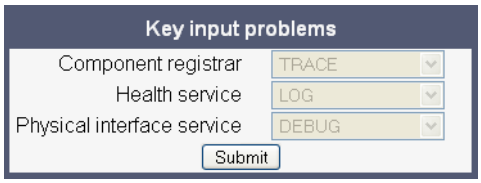
3.21.3.11 Sidecar

Diagnostics > Easy Trace Profiles > Sidecar problems



3.21.3.12 Key Input

Diagnostics > Easy Trace Profiles > Key input problems

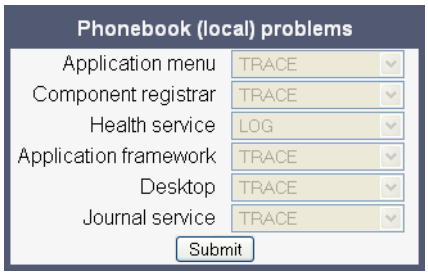


3.21.3.13 LAN Connectivity

Diagnostics > Easy Trace Profiles > LAN connectivity problems

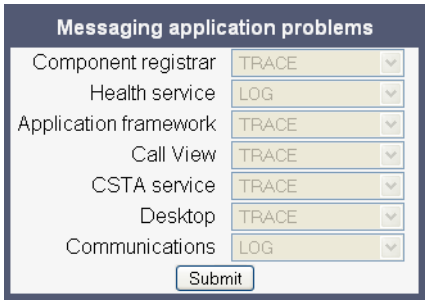
3.21.3.14 Local Phonebook

Diagnostics > Easy Trace Profiles > Phonebook (local) problems



3.21.3.15 Messaging

Diagnostics > Easy Trace Profiles > Messaging application problems



3.21.3.16 Mobility

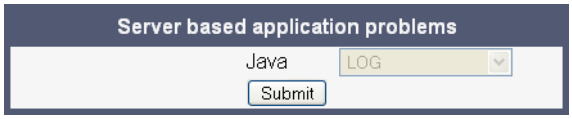
Diagnostics > Easy Trace Profiles > Mobility problems

3.21.3.17 Phone administration

Diagnostics > Easy Trace Profiles > Phone administration problems

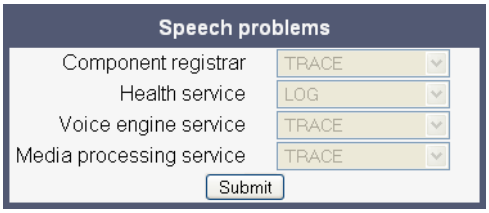
3.21.3.18 Server based applications

Diagnostics > Easy Trace Profiles > Server based application problems



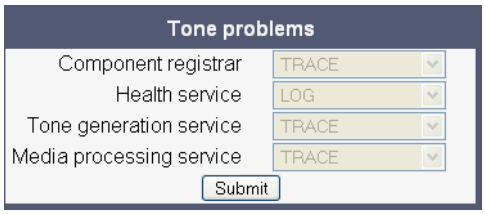
3.21.3.19 Speech

Diagnostics > Easy Trace Profiles > Speech problems



3.21.3.20 Tone

Diagnostics > Easy Trace Profiles > Tone problems

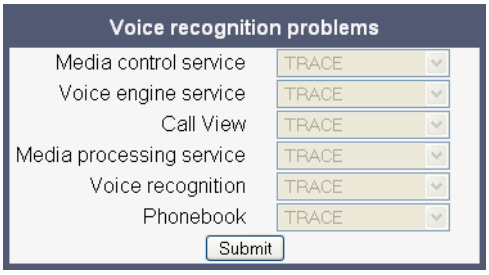


3.21.3.21 USB Backup/Restore

Diagnostics > Easy Trace Profiles > USB backup/restore

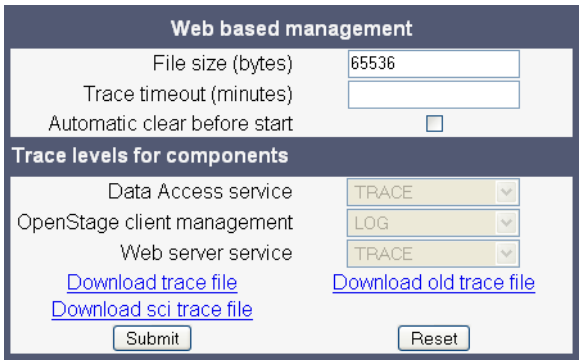
3.21.3.22 Voice Dialling

Diagnostics > Easy Trace Profiles > Voice recognition problems



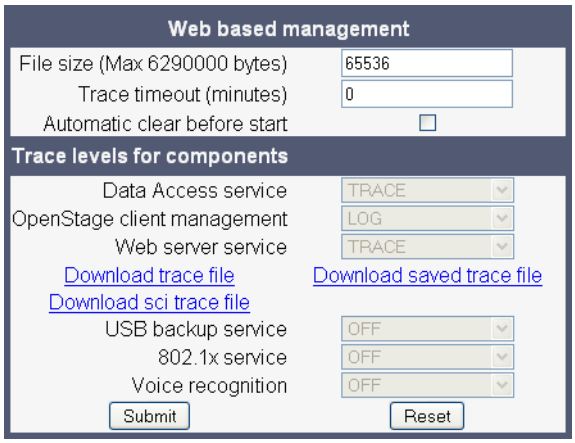
3.21.3.23 Web Based Management (OpenStage 15/20/40)

Diagnostics > Easy Trace Profiles > EasyTrace: Web based management



3.21.3.24 Web Based Management (OpenStage 60/80)

Diagnostics > Easy Trace Profiles > EasyTrace: Web based management



3.21.4 QoS Reports

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.

Settings

- **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. The fixed value is 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.

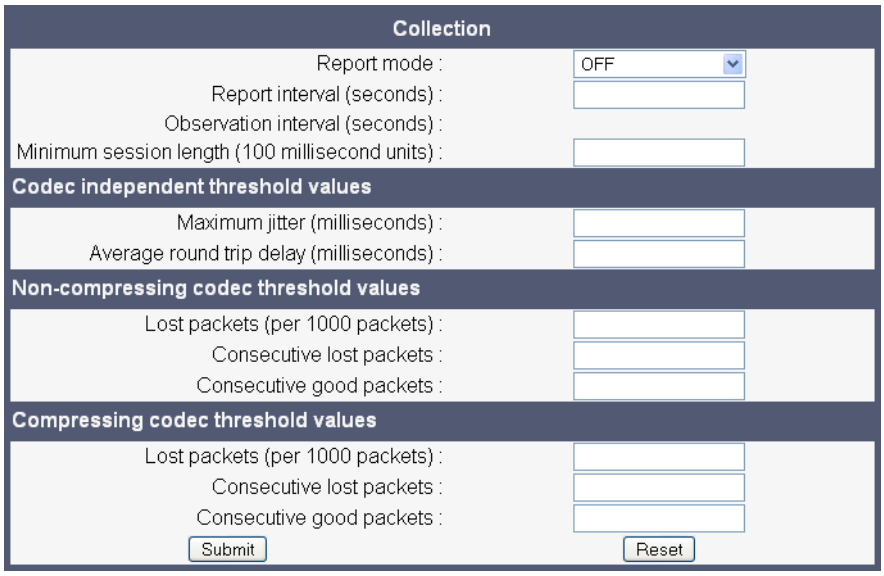
- **Lost packets (per 1000 packets)**: When the number of lost packets exceeds this maximum value during the observation interval, a report is created.
  Default: 10.
- **Consecutive lost packets**: When the number of lost packets following one another exceeds this maximum value during the observation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

Administration via WBM

Diagnostics > QoS Reports > Generation



Administration via Local Phone

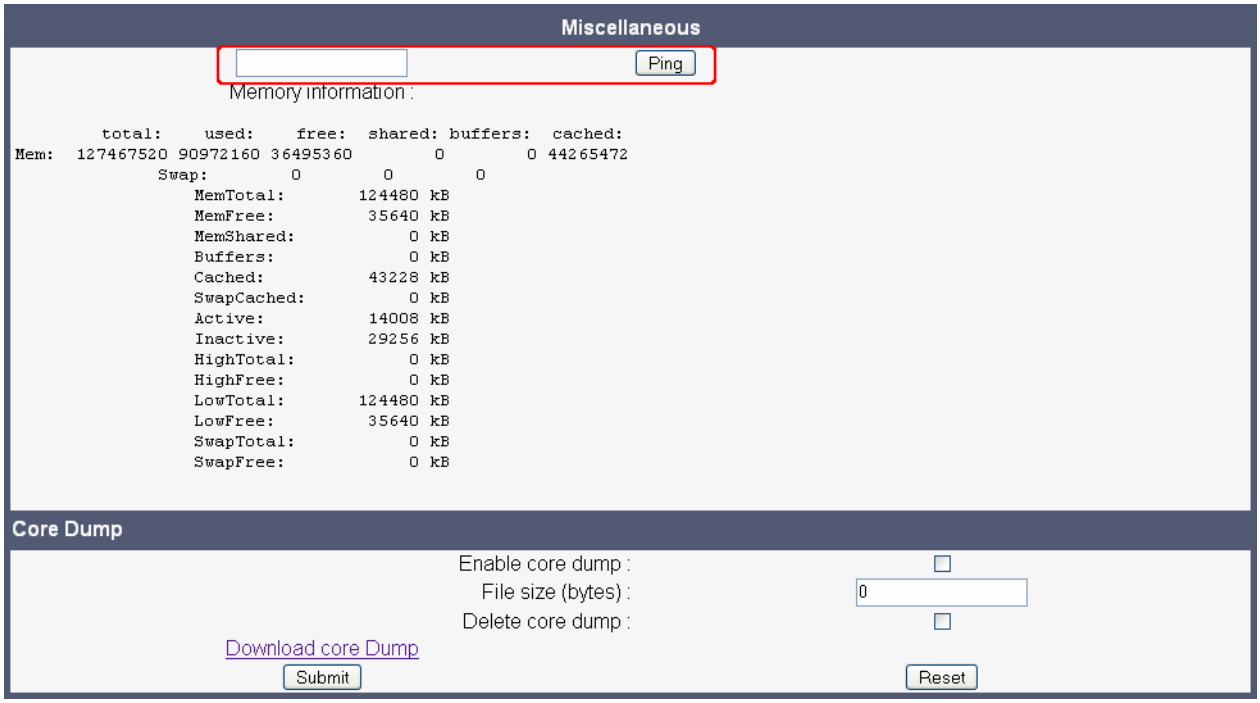
- Admin
  - Network
    - QoS
      - Reports
        - Generation
          - **Mode**
          - **Report interval**
          - **Observe interval**
          - **Minimum session length**
        - **Send now**
        - Thresholds
          - **Max jitter**
          - **Round-trip delay**
    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

3.21.5 Ping

For network diagnostics, the OpenStage phone can ping any host or network device to determine whether it is reachable.

Administration via WBM

In the Diagnostics > Miscellaneous dialog, enter the host's IP address or hostname into the input field and press **Ping**. The result will be reported underneath the input field.



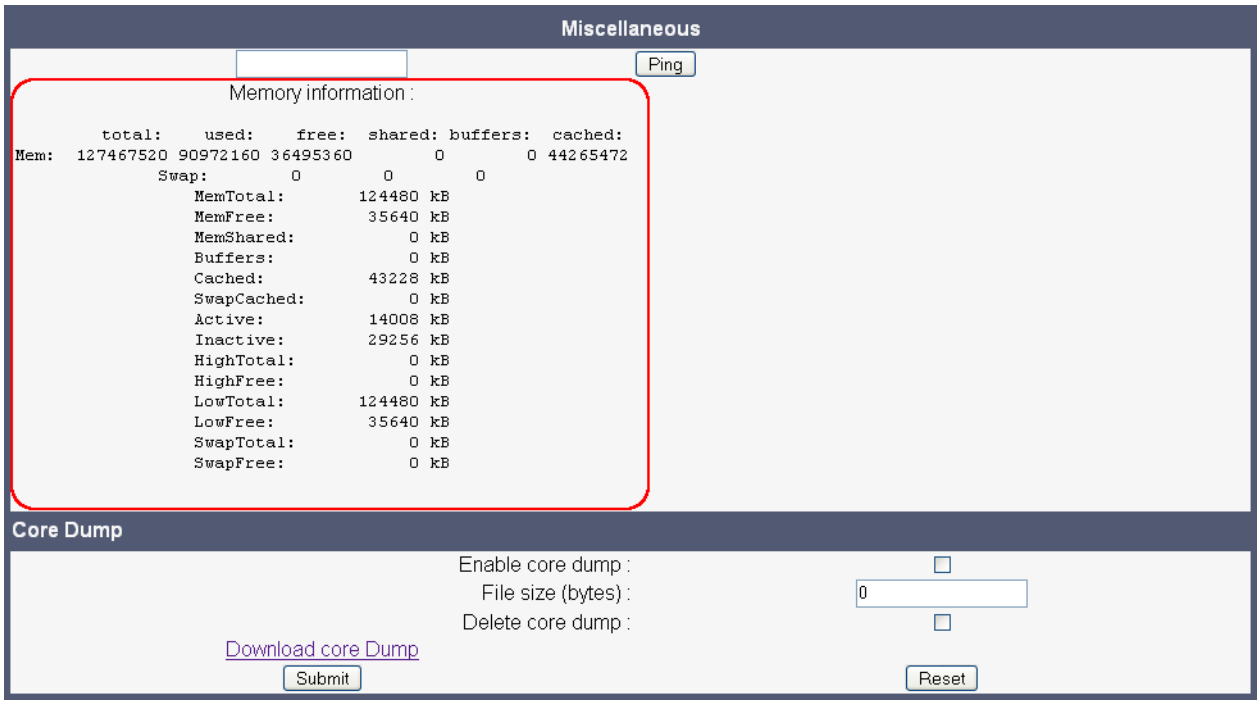
3.21.6 Memory Status Information

Firmware Version up to V1R5

The OpenStage phone offers detailed information on the current consumption of memory.

Display on the WBM (up to V1R5)

Diagnostics > Miscellaneous



Firmware Version V2

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.

With firmware version V2, 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 OpenStage 15/20/40, the default value is 10 MB, and for OpenStage 60/80, it is 30 MB. With **Low Threshold (MBs)**, the threshold for off-time is defined. For OpenStage 15/20/40, the default value is 8 MB, and for OpenStage 60/80, it is 20 MB.

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

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

Display on the WBM (V2)

Diagnostics > Miscellaneous > Memory information

3.21.7 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.

When **File size unlimited** is checked, there is no size limit for the core dump file. By default, it is not checked.

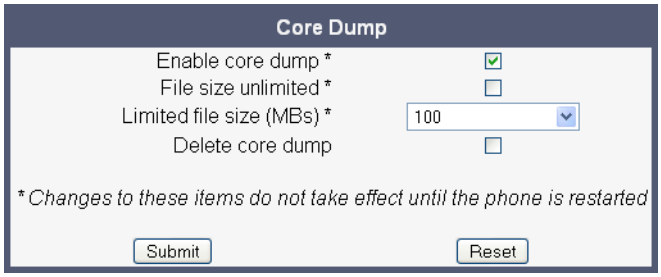
The maximum size for core dump files in MBytes can be chosen in the **Limited file size (MBs)** field. The possible values are 1, 5, 10, 25, 50, 75, and 100. The default value is 100.

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

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

Administration via WBM

Diagnostics > Miscellaneous > Core dump



3.21.8 Remote Tracing - Syslog (V2)

With firmware V2, 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
  - Maintenance
    - Remote trace
      - **Remote trace status**
      - **Remote ip**
      - **Remote port**

3.22 Bluetooth

The Bluetooth interface can be enabled or disabled here. By default, it is enabled.

With firmware V2 onwards, the Bluetooth address is displayed, and the sending of vcards is supported.

Bluetooth is available only on OpenStage 60/80 phones.

Administration via WBM

Administration via Local Phone

- Admin
  - Bluetooth
    - **Enable**

Administration via Local Phone (V2)

- Admin
  - Bluetooth
    - **Bluetooth enable**
    - **Local device address**

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 Siemens network.
PSTN access code	9	Prefix to make an international call in the UK.
Operator codes	0, 7800	Set of numbers to access the local operators.
Emergency numbers	999, 555	Set of numbers to access emergency services.
Initial extension digits	2, 3, 4, 5, 6, 8	1st digits of numbers that are used for extension numbers on the local node.

4.1.2 Canonical Dial Lookup

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

Parameter	Example value	Explanation
Local code <1>	780	Enterprise node prefix (here: Nottingham).
International code <1>	+44115943	Equivalent prefix to access numbers on this node from the PSTN. Here, the prefix used by the PSTN (DID/DDI: direct inward dialing) is 943, which differs from the enterprise node prefix used within the enterprise network.
Local code <2>	722	Enterprise node prefix (here: Munich).
International code <2>	+4989722	Equivalent prefix to access numbers on this node from the PSTN. Here, the prefix used by the PSTN for direct inward dialing is identical to the enterprise node prefix.

4.1.2.1 Conversion examples

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

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

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

Example 2: Internal number, different node

User entry		7222345
External numbers		Local public form
External access code		Not required
International gateway code		Use national code
Number stored in the phone book		+49897222345
Dial string sent when dialing from the phone book	Internal numbers = Local enterprise form	2345
	Internal numbers = Always add node	7802345
	Internal numbers = Use external numbers	9432345

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

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

4.2 How to Create Logo Files for OpenStage Phones

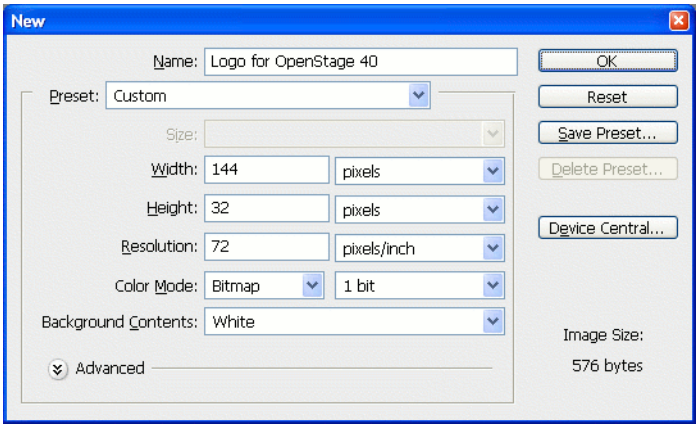
4.2.1 For OpenStage 40

1. Create a New Image

Create an image with the following specifications:

- Width: 144 px
- Height: 32 px
- Color Mode: 1 bit (monochrome)

Adobe Photoshop:



2. Insert the Logo

Place the logo image on the background, e.g. by copying it from a source file. Due to the size and color specifications, some adaptations may be necessary.

Adobe Photoshop Example:

3. Save the Image

Finally, save the image in BMP format. You can now upload the logo file to the phone as described in section 3.9.6, “Logo”.

4.2.2 For OpenStage 60/80

In the following, the creation of a transparent image suitable for use as a logo in OpenStage 60/80 is described. This description is based on Adobe Photoshop, but any similar graphics software can be used as well.

Because of performance issues, half transparency in the alpha channel of the PNG files is not allowed on OpenStage 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
OpenStage 60	Silver Blue	#BDBDBD
OpenStage 60	Anthracite Orange	#424242[1]
OpenStage 80	Silver Blue	#E6EBEF
OpenStage 80	Anthracite Orange	#3A3D3A

1 The background color on WP4 - skin 1 is a gradient; the colour listed here is an average value.

Adobe Photoshop:

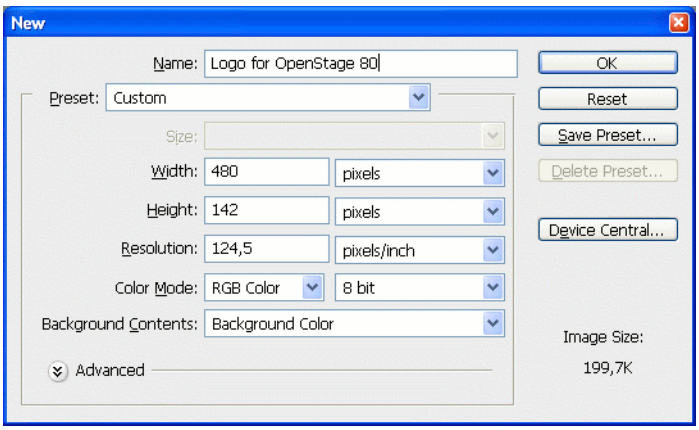
Click on the Background Color icon on the Color palette group, then type the color code without leading "#" into the **#** field)

2. Create a New Image

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

Phone Type	Size (px)
OpenStage 60	240 x 70
OpenStage 80	480 x 142

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”

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.

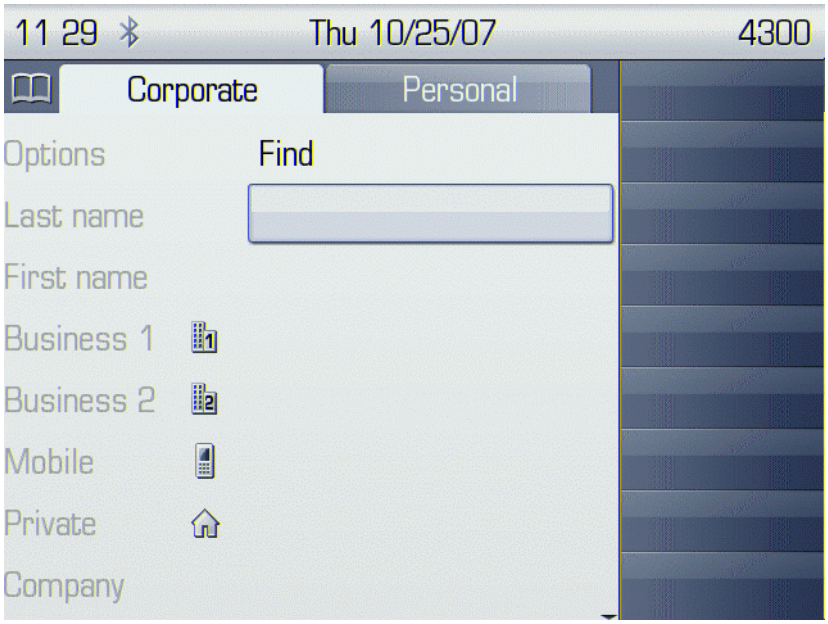
The Corporate Phonebook is available only on OpenStage 60/80.

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 passwort must be provided. It might be feasible to use a single login/password for all OpenStage 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.

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.

Generic Example (Standard Attributes)

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

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

```
OpenStage LDAP TEMPLATE (v.1)
SEARCHBASE="dc=example,dc=com"
ATTRIB01="sn"
ATTRIB02="givenname"
ATTRIB03="telephoneNumber"
ATTRIB04="facsimileTelephoneNumber"
ATTRIB05="mobile"
ATTRIB06="homePhone"
ATTRIB07="o"
ATTRIB08="departmentNumber"
ATTRIB09=""
ATTRIB10="title"
ATTRIB11="mail"
EOF
```

Microsoft Active Directory Specific Example

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

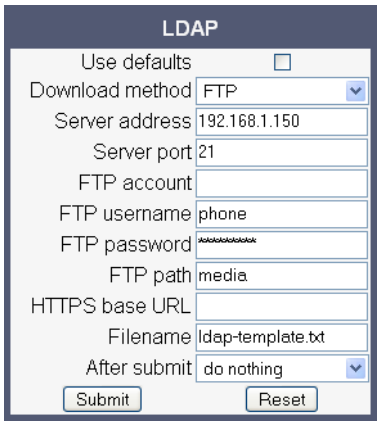
Given "example.com" as the LDAP subtree to be searched, the LDAP template file would look like this:

```
OpenStage LDAP TEMPLATE (v.1)
SEARCHBASE="dc=example,dc=com"
ATTRIB01="sn"
ATTRIB02="givenname"
ATTRIB03="ipPhone"
ATTRIB04="otherTelephone"
ATTRIB05="mobile"
ATTRIB06="homePhone"
ATTRIB07="company"
ATTRIB08="department"
ATTRIB09=""
ATTRIB10="title"
ATTRIB11="mail"
EOF
```

4.3.3 Load the LDAP Template into the Phone

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

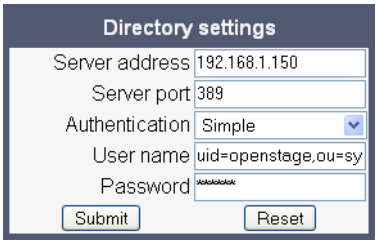
1. Save the template under a suitable name, for example, `ldap-template.txt`.
2. Copy the template file to the FTP server designated for deploying LDAP templates.
3. Upload the file using the WBM (see section 3.9.5, “LDAP Template”), or, alternatively, the Local menu, or the DLS (see the Deployment Service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



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).



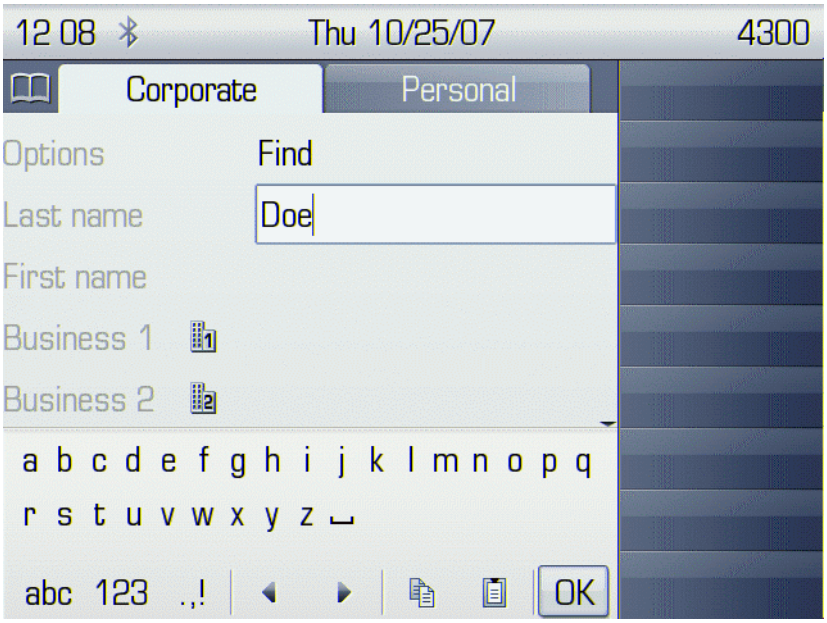
3. Press **Submit**.

4.3.5 Test

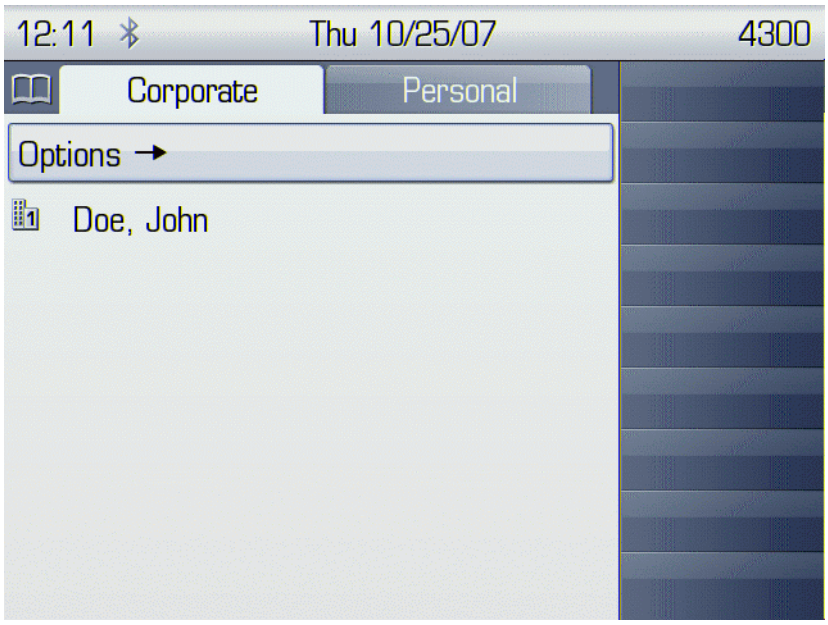
If everything went well, you can run a test query on your OpenStage phone.

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

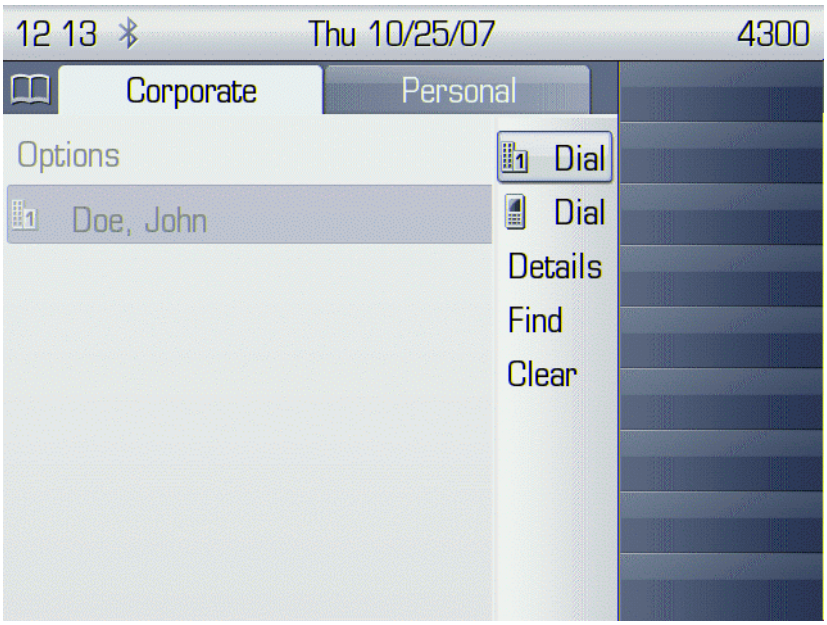
4. Enter the text to be searched. For information on using the onscreen keypad, see section 3.1, “Access via Local Phone”, step 5.



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



6. Navigate to the desired entry and press ➔ on the TouchGuide 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.



5 Technical Reference

5.1 Menus

This section describes the structure of the aministration menus of the OpenStage phone. For information on user menus, please refer to the user manual.

5.1.1 Web Interface Menu

5.1.1.1 Menu Structure

Admin Login

Applications

- **XML applications** (OpenStage 60/80)
  - Add application
  - Modify application
  - Xpressions
  - XML Phonebook

Bluetooth[1]

Network

- IP configuration / IP configuration (V2 on OpenStage 15/20/40) / IP configuration (V2 on OpenStage 60/80)
- Update Service (DLS)
- QoS
- Port configuration / Port configuration (V2 on OpenStage 15/20/40) / Port configuration (V2 on OpenStage 60/80)
- LLDP-MED operation (V2)

System

- Gateway
- Standby gateway
- Redundancy
- SNMP

Features

- Configuration

1. OpenStage 60/80 only.

Security

File transfer
- Defaults
- Phone application
- Picture Clip (OpenStage 60/80)[1]
- LDAP (OpenStage 60/80)[1]
- Logo[1]
- Screensaver (OpenStage 60/80)[1]
- Ringer file
- Dongle Key

Local functions
- Directory settings (OpenStage 60/80) / Directory settings (V2 on OpenStage 60/80)
- **Locality**
  - Canonical dial settings
  - Canonical dial lookup
  - Canonical dial
- Energy saving

Date and Time

Speech
- Codec preferences

General information

Authentication
- Change Admin password
- Change User password

User mobility (OpenStage 60/80, V1R3 Onwards)
- Set Mobility Mode
- Cancel mobility password

Diagnostics
- LLDP-MED TLVs (V2)
- Fault trace configuration / Fault trace configuration (V2 on OpenStage 15/20/40) / Fault trace configuration (V2 on OpenStage 60/80)
- **EasyTrace Profiles**
  - Bluetooth handsfree profile (OpenStage 60/80)
  - Bluetooth headset profile (OpenStage 60/80)

1. OpenStage 40/60/80 only.

- Call connection
- Call log problems
- DAS connection
- DLS data errors
- Help application problems (OpenStage 60/80)
- Key input problems
- LAN connectivity problems
- Messaging application issues
- Mobility problems
- Phone administration problems
- Phonebook (LDAP) problems (OpenStage 60/80)
- Phonebook (local) problems (OpenStage 60/80)
- Server based application problems (OpenStage 60/80)
- Sidecar problems
- Speech problems
- Tone problems
- USB backup/restore (OpenStage 60/80)
- Voice recognition problems (OpenStage 60/80)
- Web based management (OpenStage 15/20/40)
- 802.1x problems
- Clear all profiles

QoS reports

- Generation
- View Session Data

Miscellaneous

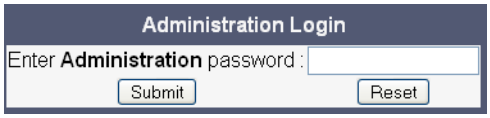
- IP tests
- Memory information / Memory information (V2)
- Core dump

Maintenance

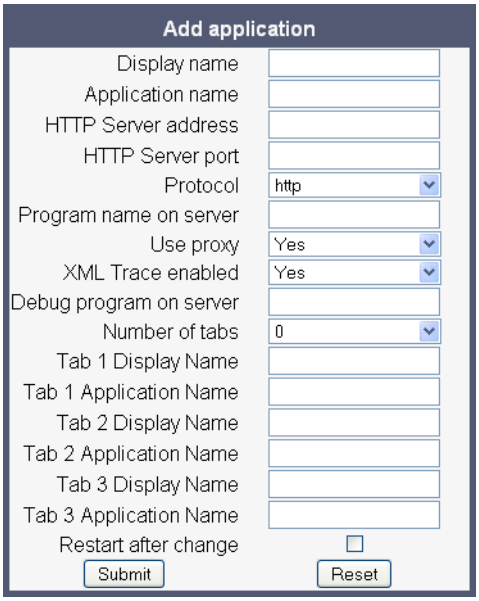
- Remote trace
- Restart Phone
- Factory reset
- HPT interface
- Secure shell
- Secure shell

5.1.1.2 Web Pages

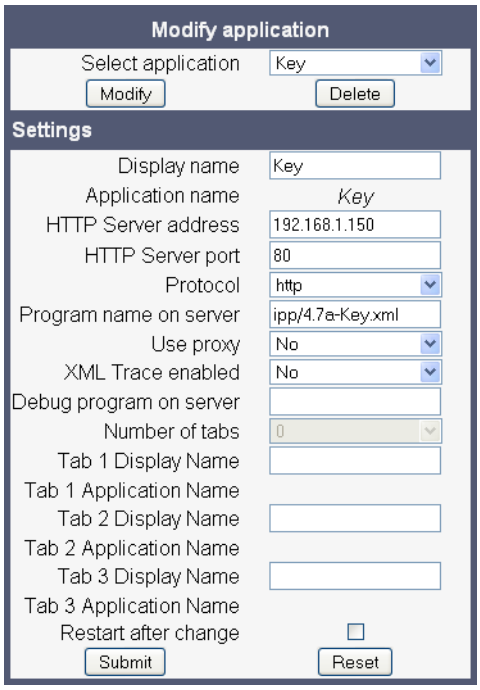
Admin Login



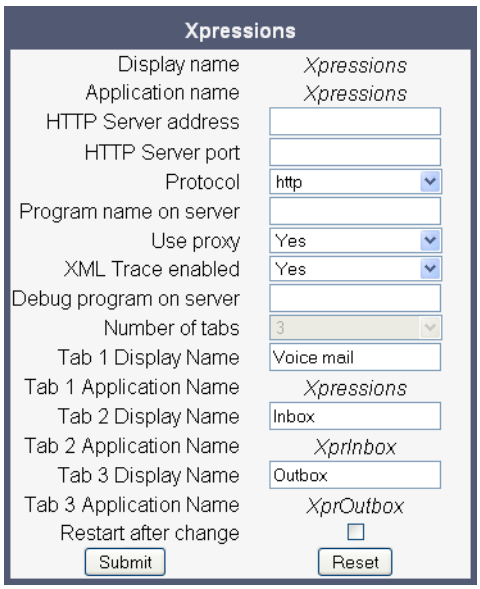
Add application



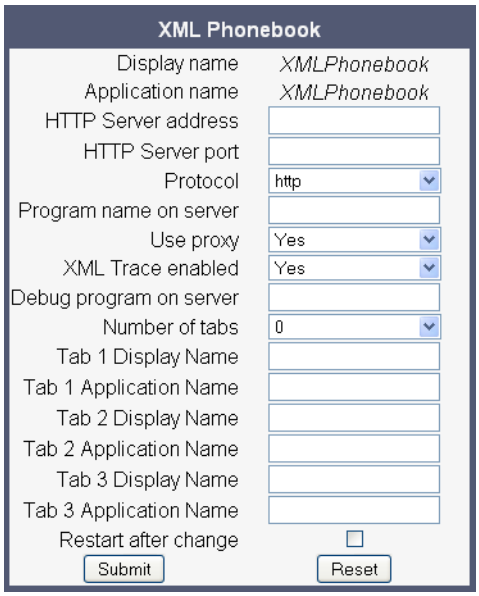
Modify application



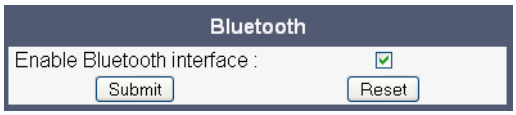
Xpressions



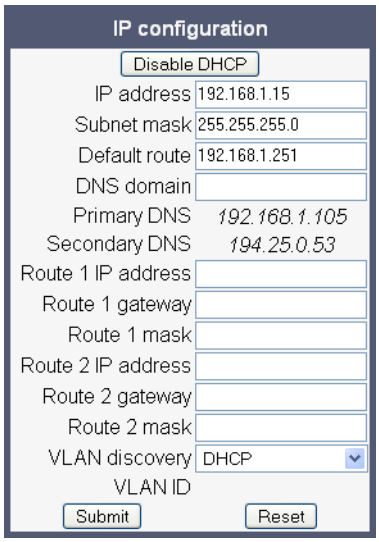
XML Phonebook



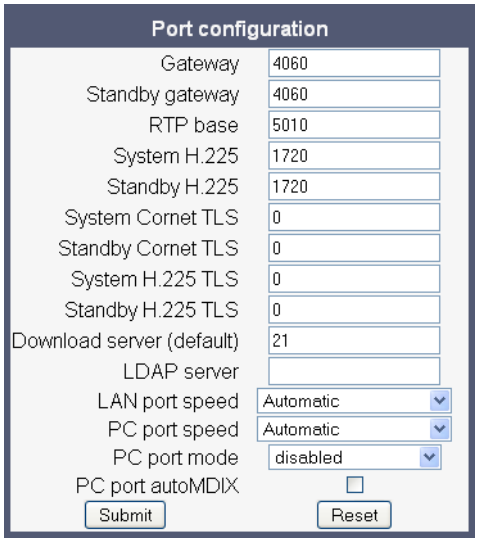
Bluetooth



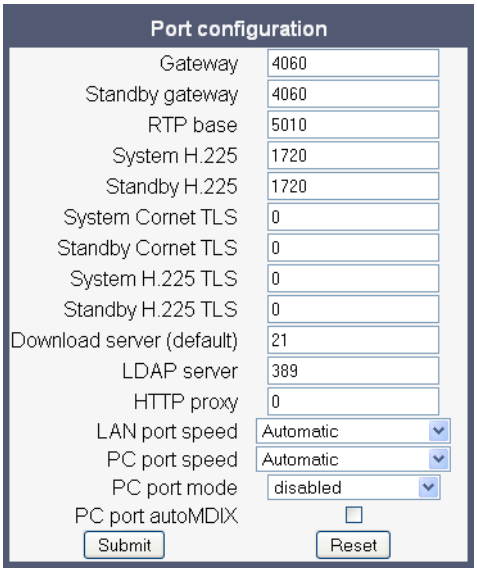
IP configuration



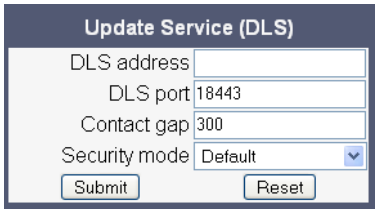
IP configuration (V2 on OpenStage 15/20/40)



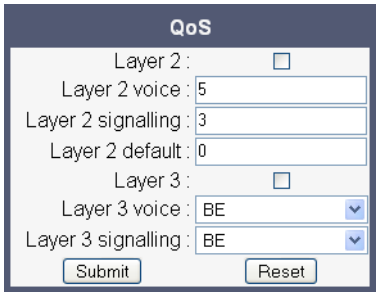
IP configuration (V2 on OpenStage 60/80)



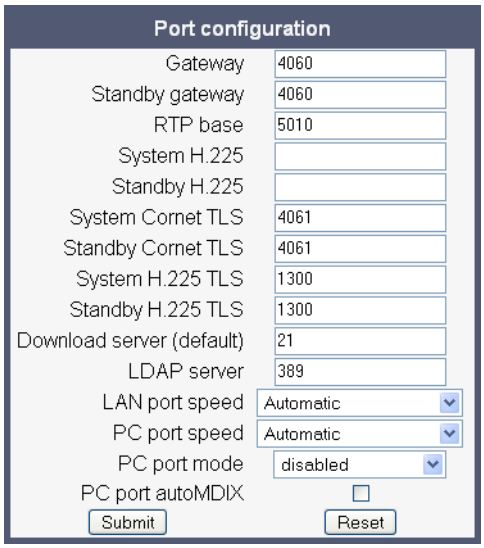
Update Service (DLS)



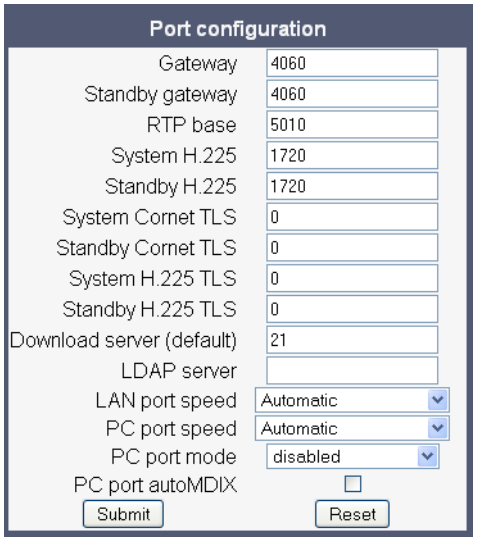
QoS



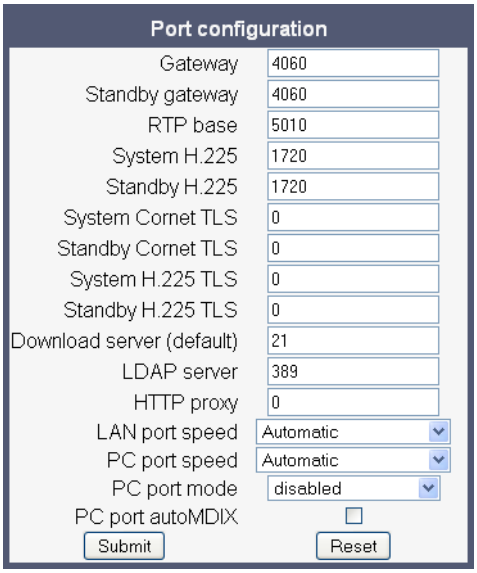
Port configuration



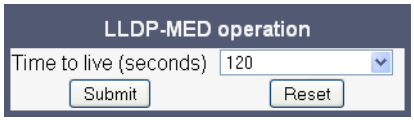
Port configuration (V2 on OpenStage 15/20/40)



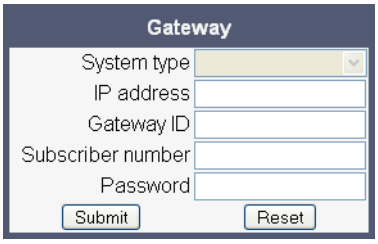
Port configuration (V2 on OpenStage 60/80)



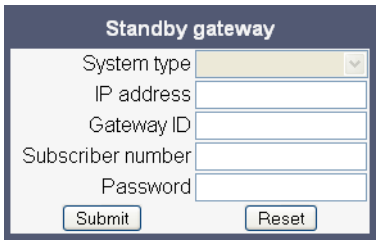
LLDP-MED operation (V2)



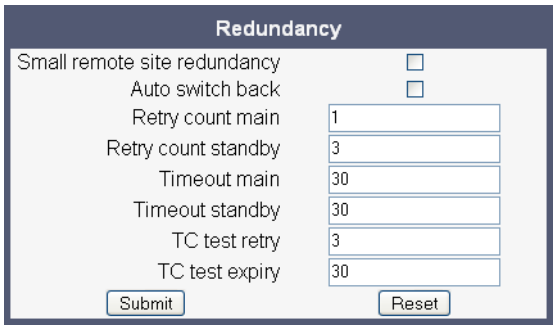
Gateway



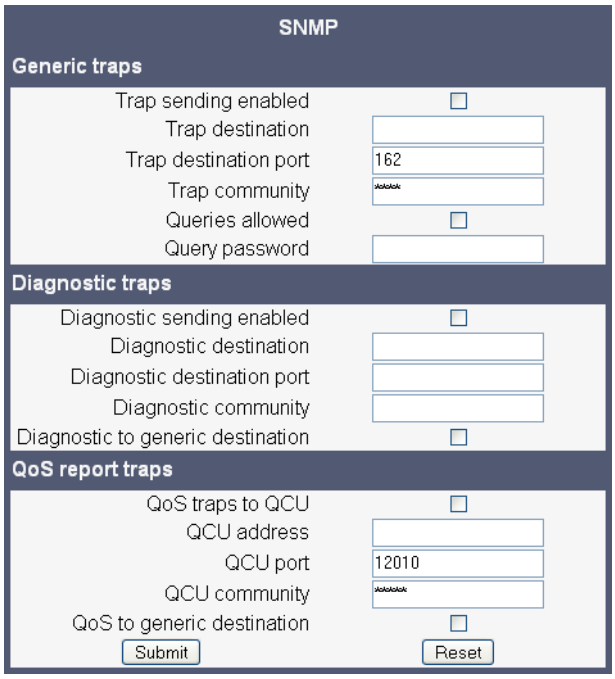
Standby gateway



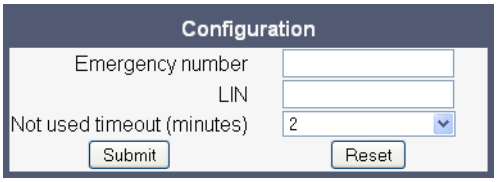
Redundancy



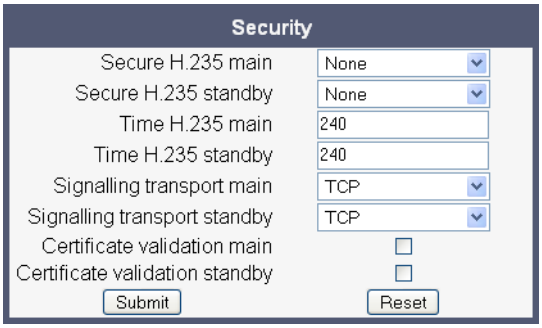
SNMP



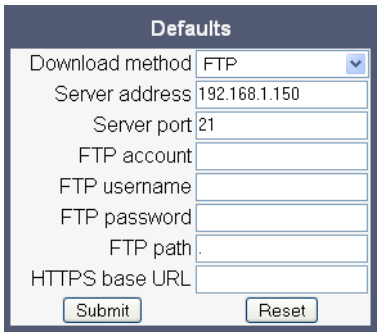
Configuration



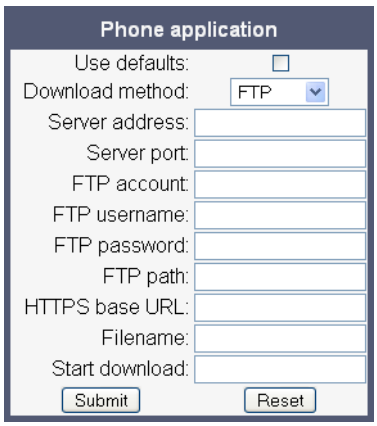
Security



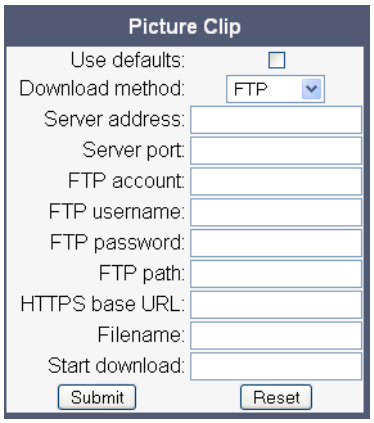
Defaults



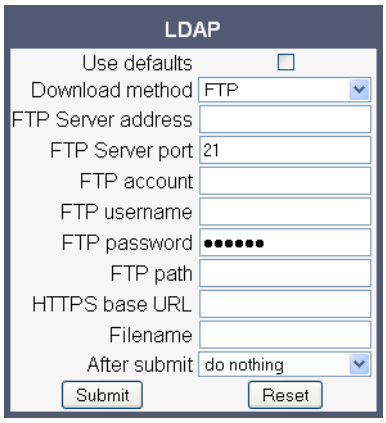
Phone application



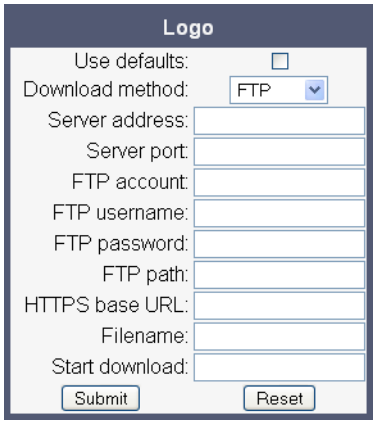
Picture Clip (OpenStage 60/80)



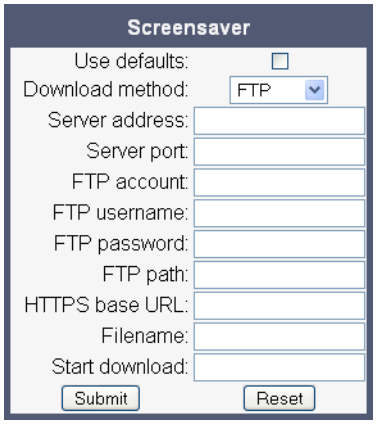
LDAP (OpenStage 60/80)



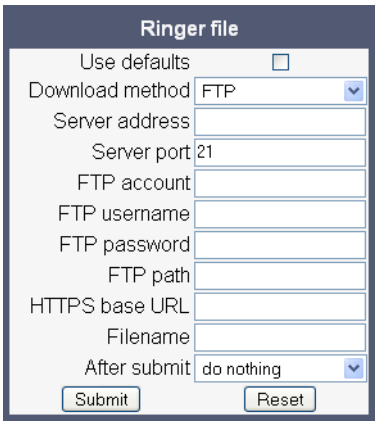
Logo



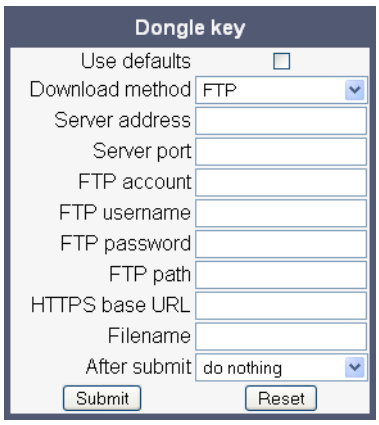
Screensaver (OpenStage 60/80)



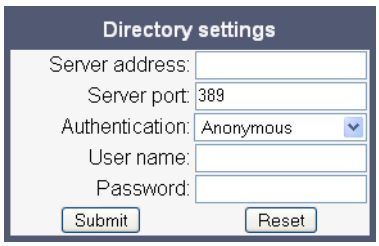
Ringer file



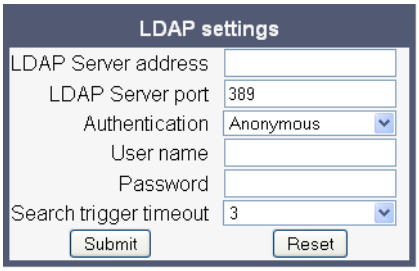
Dongle Key



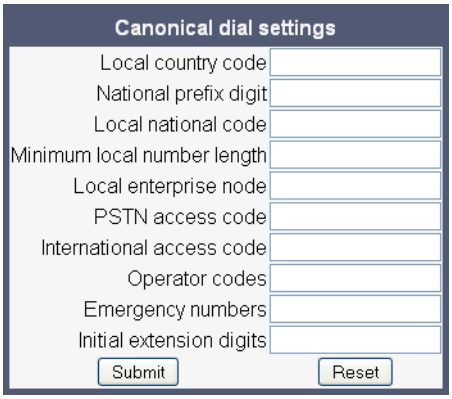
Directory settings (OpenStage 60/80)



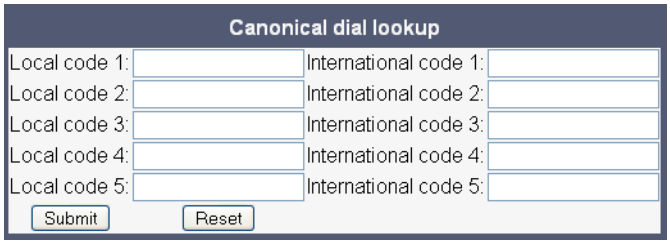
Directory settings (V2 on OpenStage 60/80)



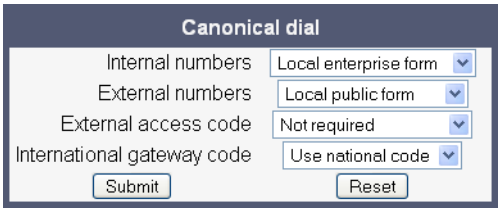
Canonical dial settings



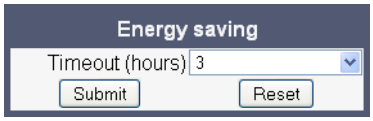
Canonical dial lookup



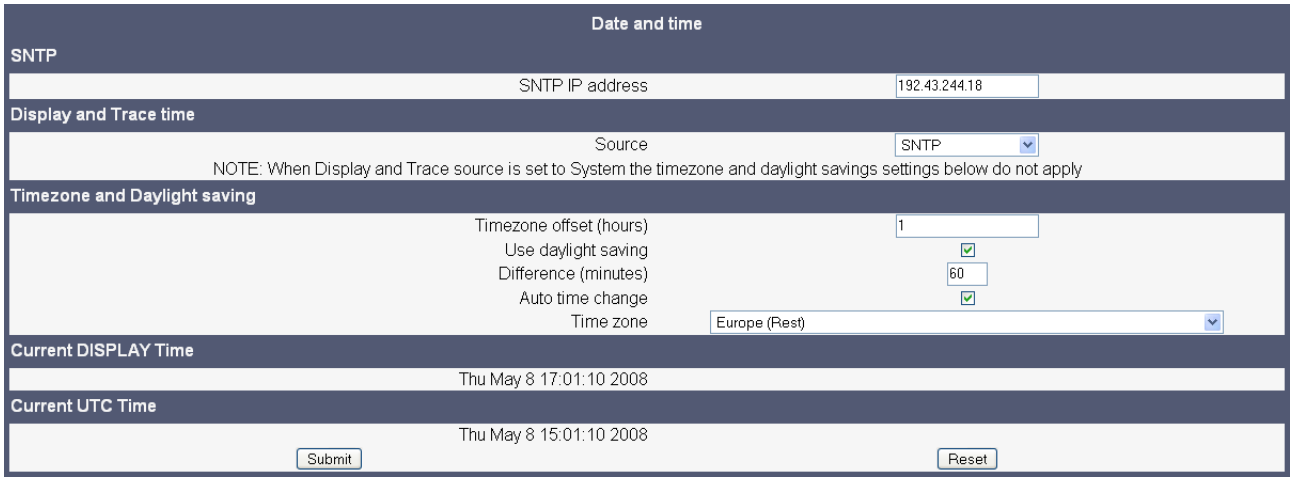
Canonical dial



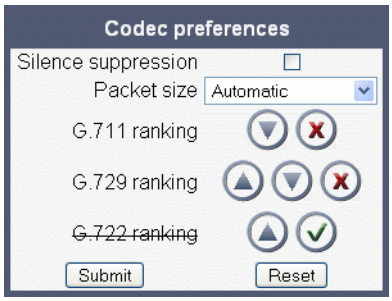
Energy saving



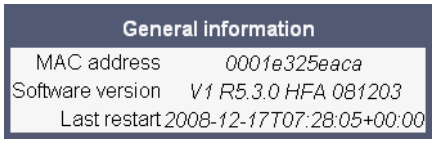
Date and Time



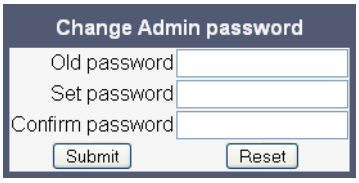
Codec preferences



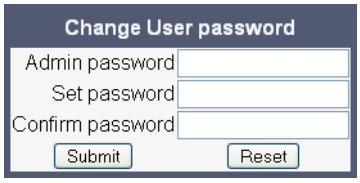
General information



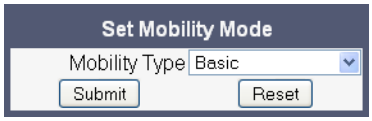
Change Admin password



Change User password

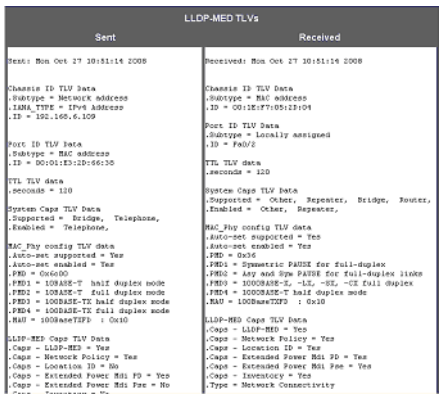


Set Mobility Mode

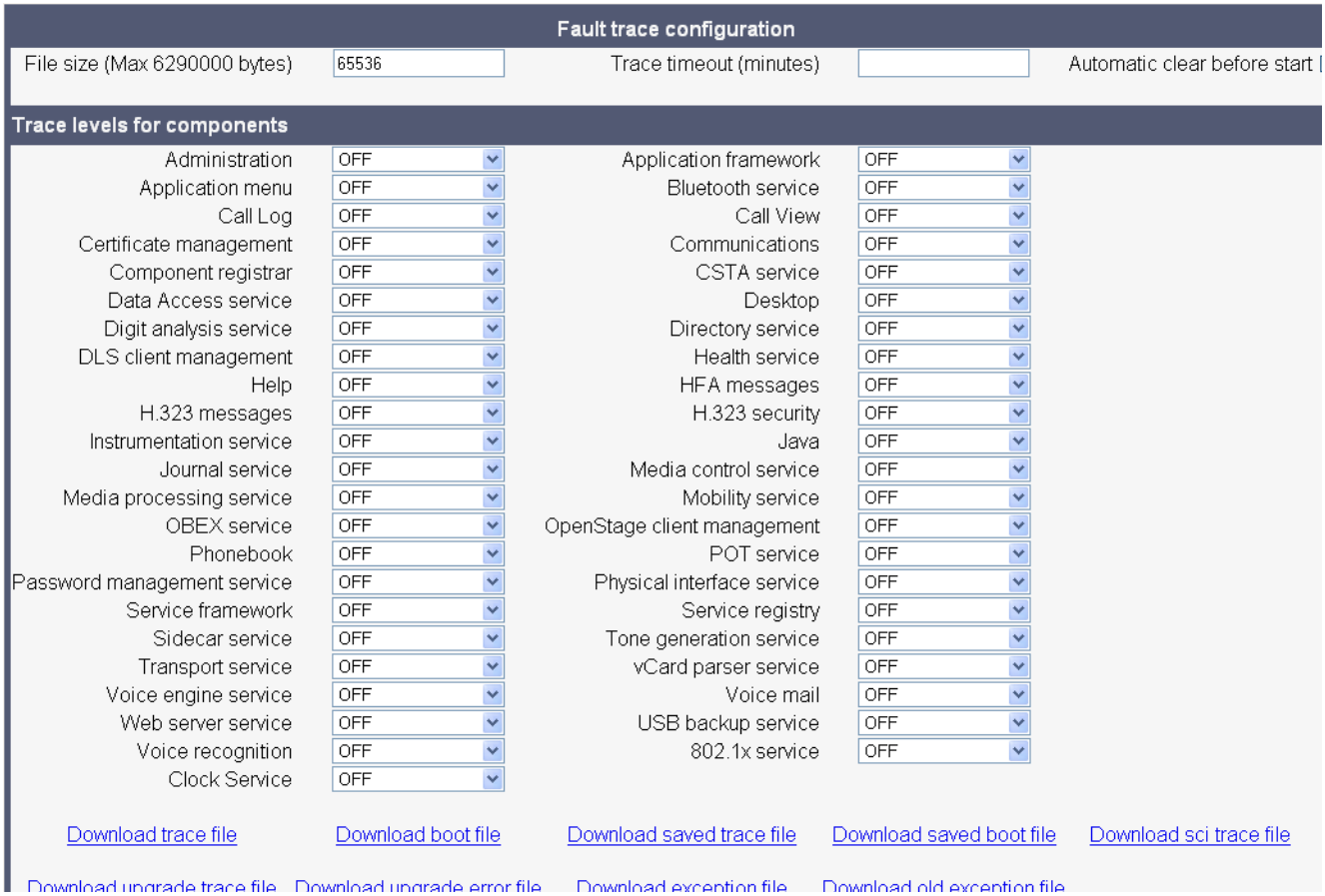


Cancel mobility password

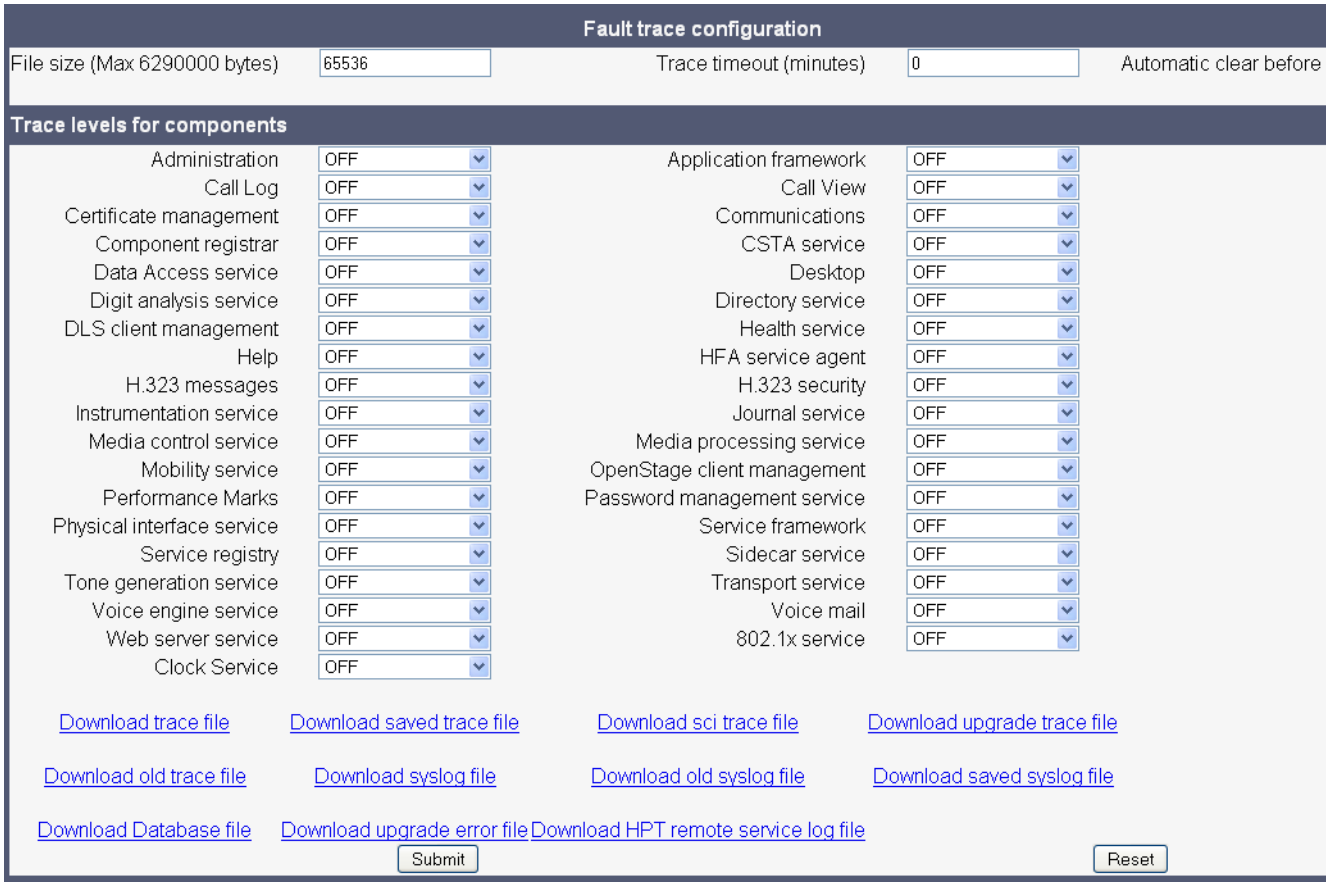
LLDP-MED TLVs (V2)



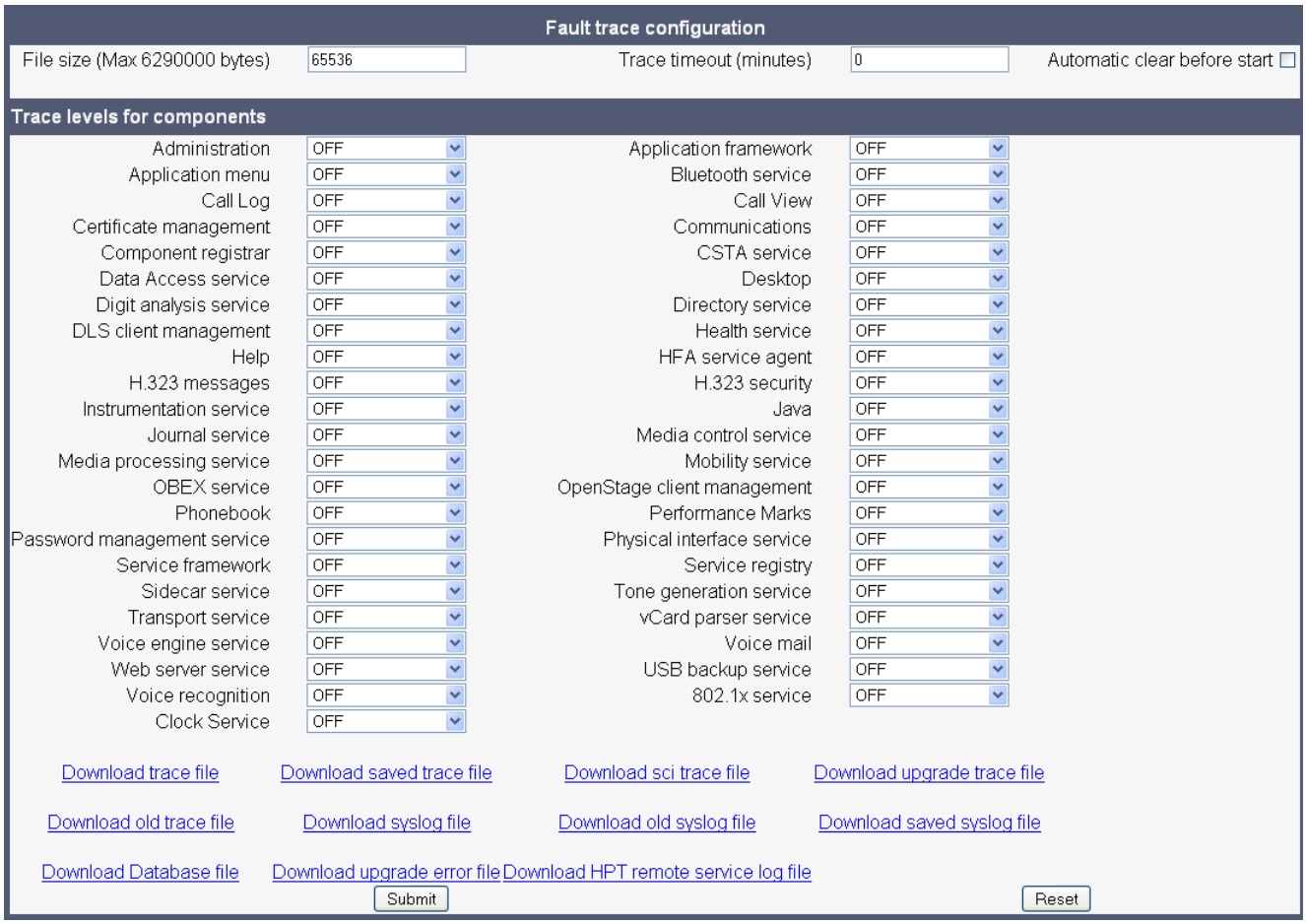
Fault trace configuration



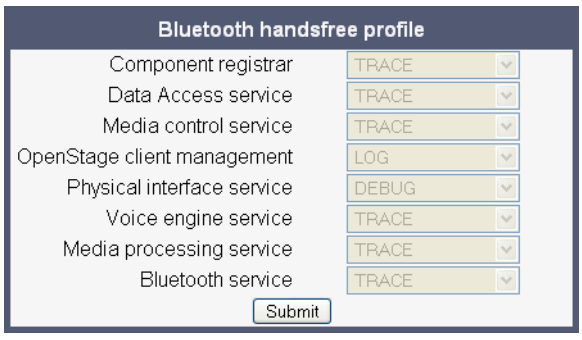
Fault trace configuration (V2 on OpenStage 15/20/40)



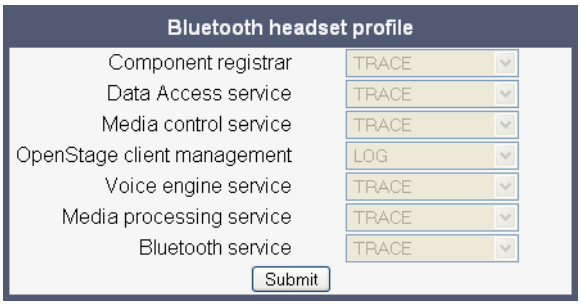
Fault trace configuration (V2 on OpenStage 60/80)



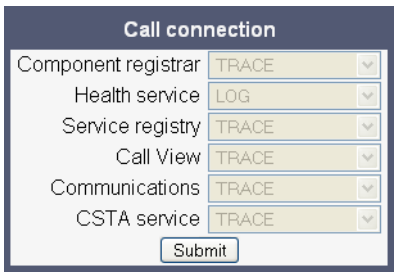
Bluetooth handsfree profile (OpenStage 60/80)



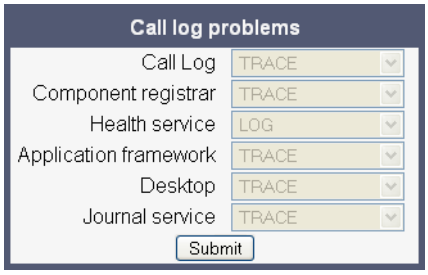
Bluetooth headset profile (OpenStage 60/80)



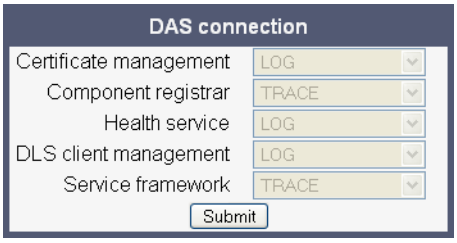
Call connection



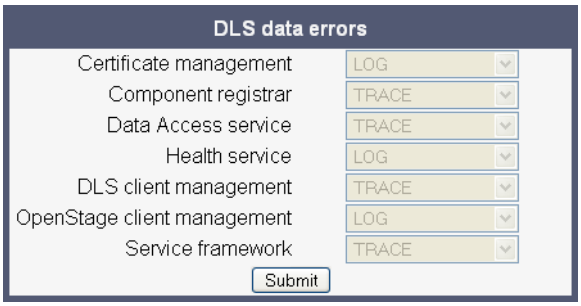
Call log problems



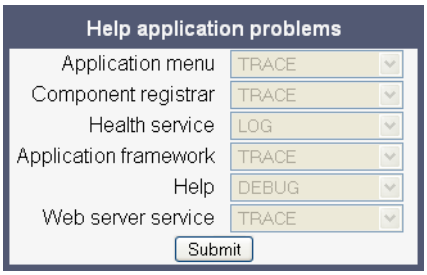
DAS connection



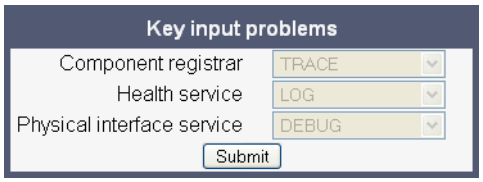
DLS data errors



Help application problems (OpenStage 60/80)

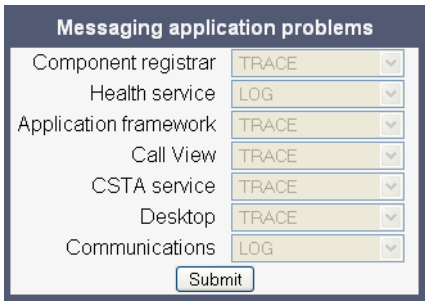


Key input problems



LAN connectivity problems

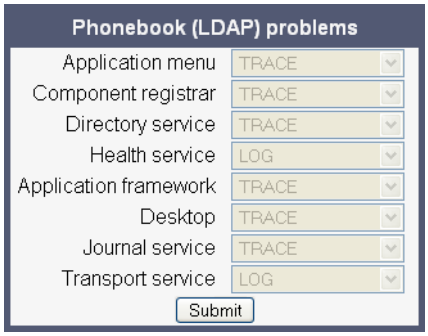
Messaging application issues



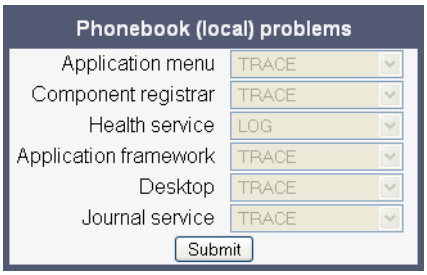
Mobility problems

Phone administration problems

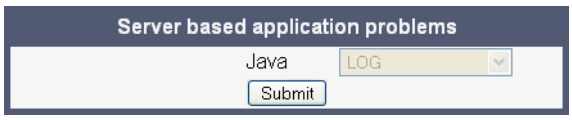
Phonebook (LDAP) problems (OpenStage 60/80)



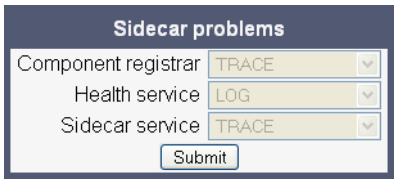
Phonebook (local) problems (OpenStage 60/80)



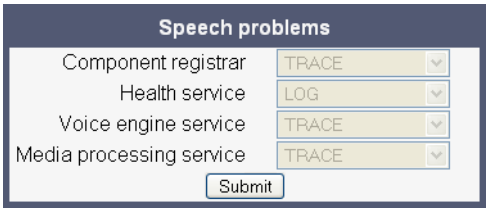
Server based application problems (OpenStage 60/80)



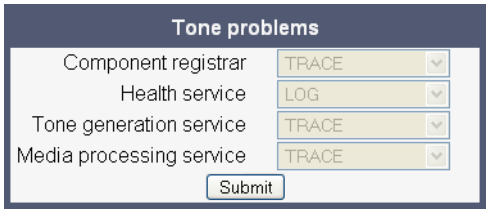
Sidecar problems



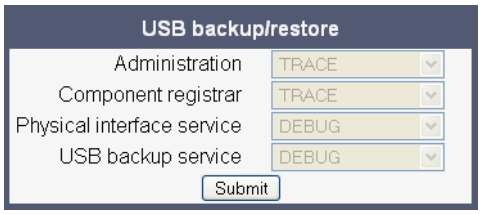
Speech problems



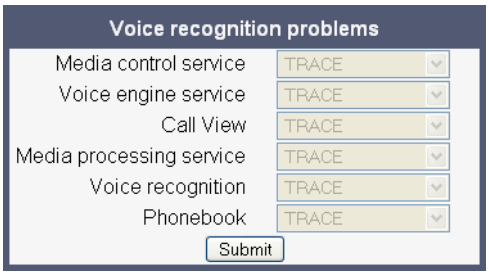
Tone problems



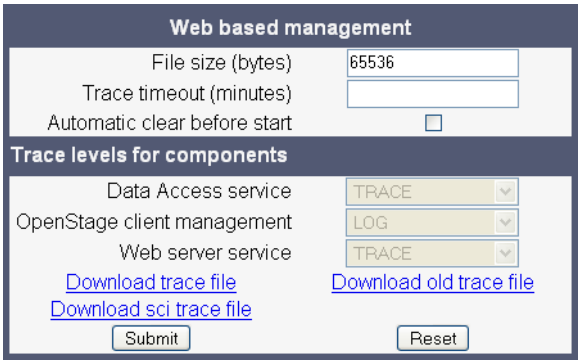
USB backup/restore (OpenStage 60/80)



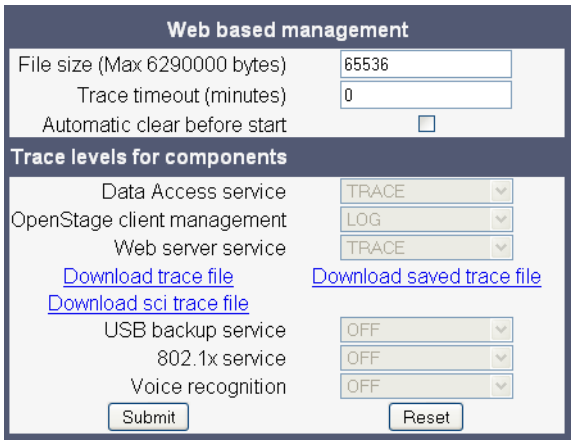
Voice recognition problems (OpenStage 60/80)



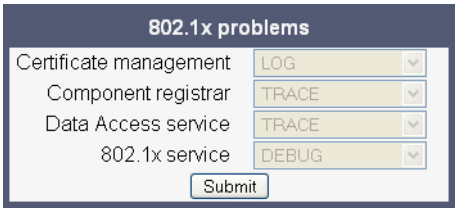
Web based management (OpenStage 15/20/40)



Web based management (OpenStage 60/80)

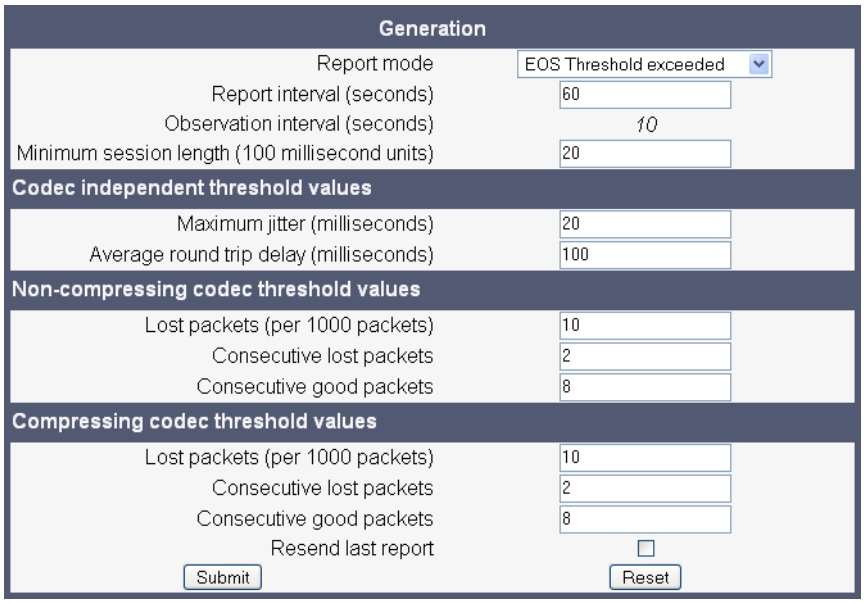


802.1x problems

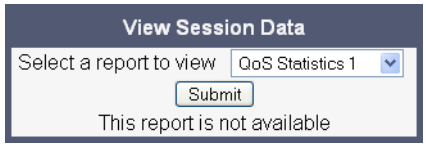


Clear all profiles

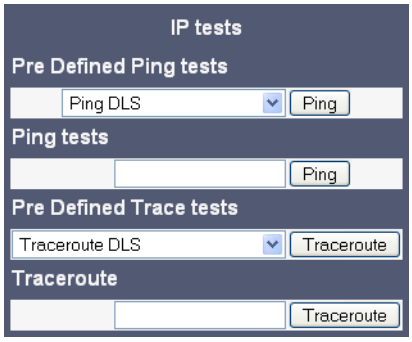
Generation



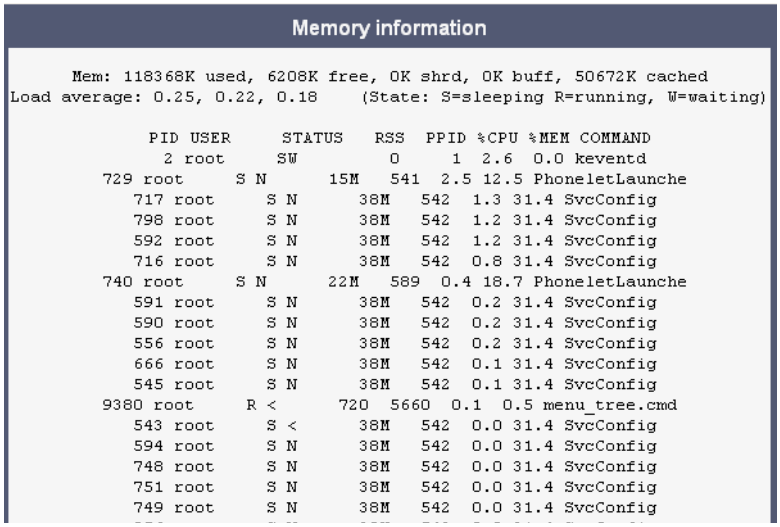
View Session Data



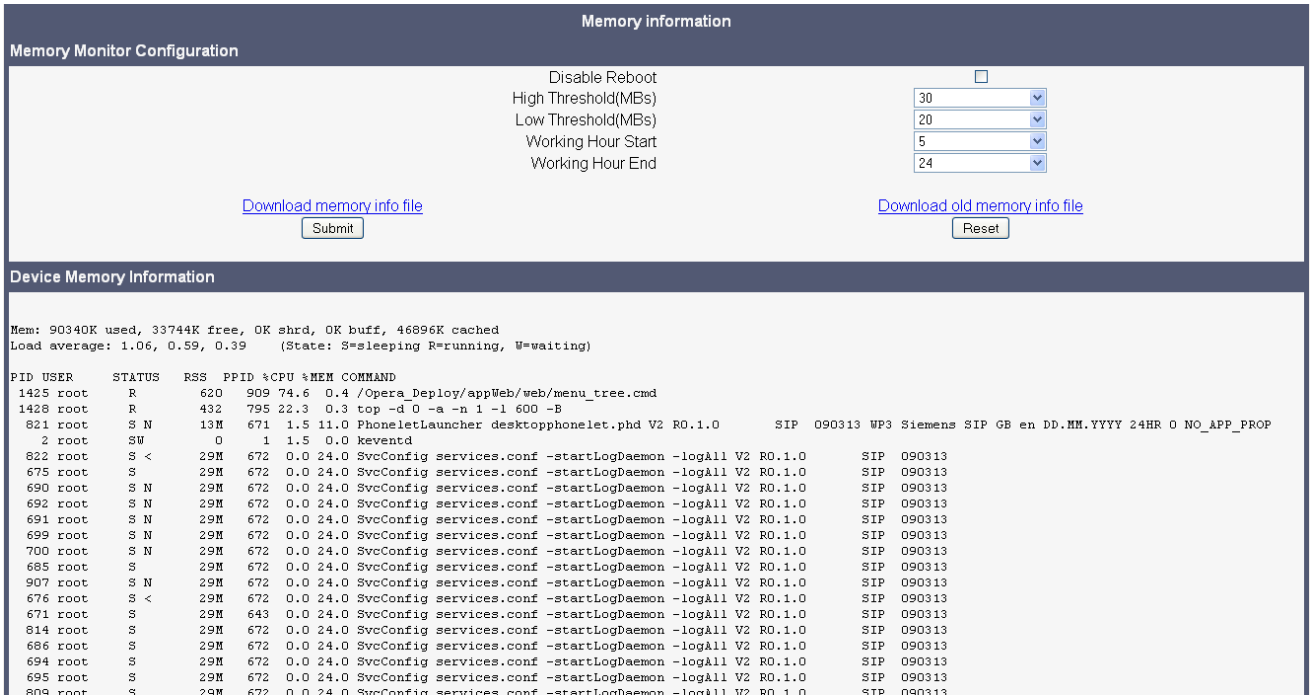
IP tests



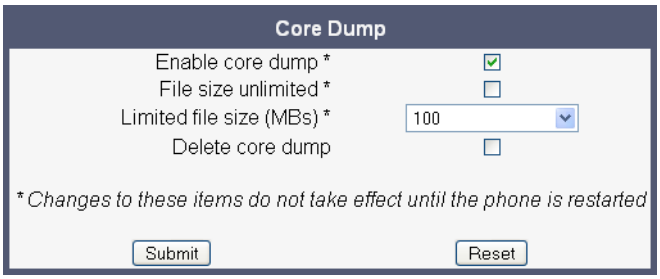
Memory information



Memory information (V2)



Core dump



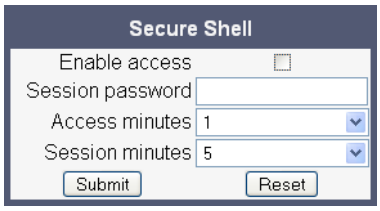
Remote trace

Restart Phone

Factory reset

HPT interface

Secure shell



5.1.2 Local Phone Menu

Menu	Further information ...
Admin	
XML	
Add application[1]	
Display name	-> Section 3.13.1.1
Application name	-> Section 3.13.1.1
Server address	-> Section 3.13.1.1
Server port	-> Section 3.13.1.1
Protocol	-> Section 3.13.1.1
Program name	-> Section 3.13.1.1
Use proxy	-> Section 3.13.1.1
XML trace enabled	-> Section 3.13.1.1
Debug program name	-> Section 3.13.1.1
Number of tabs	-> Section 3.13.1.1
Tab 1 display name	-> Section 3.13.1.1
Tab 1 application name	-> Section 3.13.1.1
Tab 2 display name	-> Section 3.13.1.1
Tab 2 application name	-> Section 3.13.1.1
Tab 3 display name	-> Section 3.13.1.1
Tab 3 application name	-> Section 3.13.1.1
Auto restart / Restart after change	-> Section 3.13.1.1
Add Xpressions[1]	
Display name	-> Section 3.13.1.1
Application name	-> Section 3.13.1.1
Server address	-> Section 3.13.1.1
Server port	-> Section 3.13.1.1
Protocol	-> Section 3.13.1.1
Program name	-> Section 3.13.1.1
Use proxy	-> Section 3.13.1.1
XML trace enabled	-> Section 3.13.1.1
Debug program name	-> Section 3.13.1.1
Number of tabs	-> Section 3.13.1.1
Tab 1 display name	-> Section 3.13.1.1
Tab 1 application name	-> Section 3.13.1.1
Tab 2 display name	-> Section 3.13.1.1
Tab 2 application name	-> Section 3.13.1.1
Tab 3 display name	-> Section 3.13.1.1
Tab 3 application name	-> Section 3.13.1.1
Auto restart	-> Section 3.13.1.1
Add phonebook[1]	
Display name	-> Section 3.13.1.1
Application name	-> Section 3.13.1.1
Server address	-> Section 3.13.1.1
Server port	-> Section 3.13.1.1
Protocol	-> Section 3.13.1.1
Program name	-> Section 3.13.1.1
Use proxy	-> Section 3.13.1.1
XML trace enabled	-> Section 3.13.1.1

Menu	**Further information ...**
Debug program name	-> Section 3.13.1.1
Number of tabs	-> Section 3.13.1.1
Tab 1 display name	-> Section 3.13.1.1
Tab 1 application name	-> Section 3.13.1.1
Tab 2 display name	-> Section 3.13.1.1
Tab 2 application name	-> Section 3.13.1.1
Tab 3 display name	-> Section 3.13.1.1
Tab 3 application name	-> Section 3.13.1.1
Auto restart	-> Section 3.13.1.1
Bluetooth[2]	
Enable	-> Section 3.22
Network	
IP Configuration	
Use DHCP / Discovery mode	-> Section 3.2.2.1
Use LLDP-Med[3]	-> Section 3.2.2.2
Use DHCP	-> Section 3.2.2.1
IP address	-> Section 3.3.3
Subnet mask	-> Section 3.3.3
Default route (GW)	-> Section 3.3.4
DNS domain	-> Section 3.3.6.1
Primary DNS	-> Section 3.3.6.2
Secondary DNS	-> Section 3.3.6.2
Route 1 IP	-> Section 3.3.6
Route 1 gateway	-> Section 3.3.6
Route 1 mask	-> Section 3.3.6
Route 2 IP	-> Section 3.3.6
Route 2 gateway	-> Section 3.3.6
Route 2 mask	-> Section 3.3.6
VLAN discovery	-> Section 3.2.2.1
VLAN ID	-> Section 3.2.2.3
HTTP Proxy	
Update Service (DLS)	
DLS address	-> Section 3.3.7
DLS port	-> Section 3.3.7
Contact gap	-> Section 3.3.7
Secured / Securidity status	-> Section 3.3.7
QoS	
Service	
Layer 2	-> Section 3.3.1.1
Layer 2 voice	-> Section 3.3.1.1
Layer 2 signalling	-> Section 3.3.1.1
Layer 2 default	-> Section 3.3.1.1
Layer 3	-> Section 3.3.1.2
Layer 3 voice	-> Section 3.3.1.2
Layer 3 signalling	-> Section 3.3.1.2
Reports	
Generation	
Mode	-> Section 3.21.4
Report interval	-> Section 3.21.4
Observation interval	-> Section 3.21.4
Minimum session	-> Section 3.21.4

Menu	Further information ...
Send Now	-> Section 3.21.4
Thresholds	
Maximum jitter	-> Section 3.21.4
Round-trip delay	-> Section 3.21.4
Non-compressing	-> Section 3.21.4
...Lost packets (K)	-> Section 3.21.4
...Lost consecutive	-> Section 3.21.4
...Good consecutive	-> Section 3.21.4
Compressing:	-> Section 3.21.4
...Lost packets (K)	-> Section 3.21.4
...Lost consecutive	-> Section 3.21.4
...Good consecutive	-> Section 3.21.4
Port configuration	
Number	-> Section 3.5.2
Gatekeeper	-> Section 3.5.3
Backup	-> Section 3.5.3
RTP base	-> Section 3.11.1
Server port	
LAN port speed	-> Section 3.2.1
PC port status	-> Section 3.2.1
PC port speed	-> Section 3.2.1
PC port autoMDIX	-> Section 3.2.1
Server port configuration	
H.225.0 port	-> Section 3.5.4
CorNet-TC TLS port	-> Section 3.5.4
H.225.0 TLS port	-> Section 3.5.4
Standby server port configuration	
H.225.0 port	-> Section 3.5.4
CorNet-TC port	-> Section 3.5.4
H.225.0 TLS port	-> Section 3.5.4
System	
Gateway	
System type	-> Section 3.5.2
IP address	-> Section 3.5.2
Gateway ID	-> Section 3.5.2
Subscriber number	-> Section 3.5.2
Password	-> Section 3.5.2
Standby gateway	
System type	-> Section 3.5.2
IP address	-> Section 3.5.2
Gateway ID	-> Section 3.5.2
Subscriber number	-> Section 3.5.2
Password	-> Section 3.5.2
Redundancy	
Small remote site	-> Section 3.5.5
Auto switch back	-> Section 3.5.5
Retry count main	-> Section 3.5.5
Timeout main	-> Section 3.5.5
Retry count standby	
Timeout standby	
TC TEST retry	

Menu	Further information ...
TC TEST expiry	
Identity	
Terminal number	-> Section 3.3.6.3
Web name	-> Section 3.3.6.3
DDNS hostname	-> Section 3.3.6.3
SNMP	
Traps enabled	-> Section 3.3.8
Manager address	-> Section 3.3.8
Manager port	-> Section 3.3.8
Community password	-> Section 3.3.8
Features	
Configuration	
General	
Emergency number	-> Section 3.5.6
Not used timeout	-> Section 3.5.8
LIN	-> Section 3.5.7
Bluetooth	
Bluetooth enable	-> Section 3.22
Local device address[1]	-> Section 3.22
Security	
Secure H235 main	-> Section 3.5.11
Secure H235 standby	-> Section 3.5.11
Time H235 main	-> Section 3.5.11
Time H235 standby	-> Section 3.5.11
Signalling main	-> Section 3.5.11
Signalling standby	-> Section 3.5.11
Certificate main	-> Section 3.5.11
Certificate standby	-> Section 3.5.11
File Transfer	
Defaults	
Download method	-> Section 3.9.2
Server	-> Section 3.9.2
Port	-> Section 3.9.2
Account	-> Section 3.9.2
Username	-> Section 3.9.2
Password	-> Section 3.9.2
FTP path	-> Section 3.9.2
HTTPS base URL	-> Section 3.9.2
Phone app	
Use default	-> Section 3.9.3.1
Download method	-> Section 3.9.3.1
Server	-> Section 3.9.3.1
Port	-> Section 3.9.3.1
Account	-> Section 3.9.3.1
Username	-> Section 3.9.3.1
Password	-> Section 3.9.3.1
FTP path	-> Section 3.9.3.1
HTTPS base URL	-> Section 3.9.3.1
Filename	-> Section 3.9.3.1
Picture Clip[4]	
Use default	-> Section 3.9.4.1

Menu	Further information ...
--- Download method	-> Section 3.9.4.1
--- Server	-> Section 3.9.4.1
--- Port	-> Section 3.9.4.1
--- Account	-> Section 3.9.4.1
--- Username	-> Section 3.9.4.1
--- Password	-> Section 3.9.4.1
--- FTP path	-> Section 3.9.4.1
--- HTTPS base URL	-> Section 3.9.4.1
--- Filename	-> Section 3.9.4.1
--- LDAP[1]	
--- Use default	-> Section 3.9.5.1
--- Download method	-> Section 3.9.5.1
--- Server	-> Section 3.9.5.1
--- Port	-> Section 3.9.5.1
--- Account	-> Section 3.9.5.1
--- Username	-> Section 3.9.5.1
--- Password	-> Section 3.9.5.1
--- FTP path	-> Section 3.9.5.1
--- HTTPS base URL	-> Section 3.9.5.1
--- Filename	-> Section 3.9.5.1
--- Ringer	
--- Use default	-> Section 3.9.8.1
--- Download method	-> Section 3.9.8.1
--- Server	-> Section 3.9.8.1
--- Port	-> Section 3.9.8.1
--- Account	-> Section 3.9.8.1
--- Username	-> Section 3.9.8.1
--- Password	-> Section 3.9.8.1
--- FTP path	-> Section 3.9.8.1
--- HTTPS base URL	-> Section 3.9.8.1
--- Filename	-> Section 3.9.8.1
--- Logo[5]	
--- Use default	-> Section 3.9.6.1
--- Download method	-> Section 3.9.6.1
--- Server	-> Section 3.9.6.1
--- Port	-> Section 3.9.6.1
--- Account	-> Section 3.9.6.1
--- Username	-> Section 3.9.6.1
--- Password	-> Section 3.9.6.1
--- FTP path	-> Section 3.9.6.1
--- HTTPS base URL	-> Section 3.9.6.1
--- Filename	-> Section 3.9.6.1
--- Screensaver[4]	
--- Use default	-> Section 3.9.7.1
--- Download method	-> Section 3.9.7.1
--- Server	-> Section 3.9.7.1
--- Port	-> Section 3.9.7.1
--- Account	-> Section 3.9.7.1
--- Username	-> Section 3.9.7.1
--- Password	-> Section 3.9.7.1
--- FTP path	-> Section 3.9.7.1

Menu	Further information ...
--- HTTPS base URL	-> Section 3.9.7.1
--- Filename	-> Section 3.9.7.1
--- HPT dongle	
--- Use default	-> Section 3.9.9.1
--- Download method	-> Section 3.9.9.1
--- Server	-> Section 3.9.9.1
--- Port	-> Section 3.9.9.1
--- Account	-> Section 3.9.9.1
--- Username	-> Section 3.9.9.1
--- Password	-> Section 3.9.9.1
--- FTP path	-> Section 3.9.9.1
--- HTTPS base URL	-> Section 3.9.9.1
--- Filename	-> Section 3.9.9.1
--- Local Functions	
--- Directory settings / Directories[4]	
--- LDAP	
--- Server address	-> Section 3.10.1
--- Server port	-> Section 3.10.1
--- Timeout (sec)[1]	-> Section 3.10.1
--- Authentication	-> Section 3.10.1
--- User name	-> Section 3.10.1
--- Password	-> Section 3.10.1
--- Locality	
--- Canonical settings	
--- Local country code	-> Section 3.6.1
--- National prefix digit	-> Section 3.6.1
--- Local national code	-> Section 3.6.1
--- Minimum local number length	-> Section 3.6.1
--- Local enterprise node	-> Section 3.6.1
--- PSTN access code	-> Section 3.6.1
--- International access code	-> Section 3.6.1
--- Operator code	-> Section 3.6.1
--- Emergency number	-> Section 3.6.1
--- Initial extension digits	-> Section 3.6.1
--- Canonical lookup	
--- Local code 1	-> Section 3.6.2
--- International code 1	-> Section 3.6.2
--- Local code 2	-> Section 3.6.2
--- International code 2	-> Section 3.6.2
--- Local code 3	-> Section 3.6.2
--- International code 3	-> Section 3.6.2
--- Local code 4	-> Section 3.6.2
--- International code 4	-> Section 3.6.2
--- Local code 5	-> Section 3.6.2
--- International code 5	-> Section 3.6.2
--- Canonical dial	
--- Internal numbers	-> Section 3.6.1
--- External numbers	-> Section 3.6.1
--- External access code	-> Section 3.6.1
--- International gateway / International access	-> Section 3.6.1
--- Energy saving	

Menu	Further information ...
Timeout (Hrs)	-> Section 3.5.9
Date and time	
Time source[6]	
SNTP IP address	-> Section 3.5.10
Timezone offset	-> Section 3.5.10
Time source	-> Section 3.5.10
Daylight saving	
Speech	
Codec Preferences	
Silence suppression	-> Section 3.11.2
Packet size	-> Section 3.11.2
G.711	-> Section 3.11.2
G.729	-> Section 3.11.2
G.722	-> Section 3.11.2
Audio Settings	
Disable microphone	-> Section 3.11.3
Disable loudspeech	-> Section 3.11.3
General Information	
MAC address	-> Section 3.12
Software version	-> Section 3.12
Last restart	-> Section 3.12
Password	
Admin	-> Section 3.14
Confirm admin	-> Section 3.14
User	-> Section 3.14
Confirm user	-> Section 3.14
Mobility	-> Section 3.8.1
Confirm mobility	-> Section 3.8.1
Mobility	
Mobility mode	-> Section 3.8
Maintenance	
Restart	-> Section 3.16
Factory reset	-> Section 3.17
Disable HPT[3]	-> Section 3.20
Remote trace[3]	-> Section 3.21.8
Memory monitor[3]	

1 OpenStage 60/80 V2 only.
2 The parameter is paced here in OpenStage 60/80 V1R3 only. In V2, please refer to Features > Configuration > Bluetooth.
3 V2 only.
4 OpenStage 60/80 only.
5 OpenStage 40/60/80 only.
6 V1R3 only.

5.2 Troubleshooting: Error Messages

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

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

Table 5-1 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 5-1 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 5-1 Error Messages

Glossary

A

ADPCM

Adaptive **D**ifferential **P**ulse **C**ode **M**odulation. A compressed encoding method for audio signals which are to be transmitted by a low bandwidth. As opposed to regular -> PCM, a sample is coded as the difference between its predicted value and its real value. As this difference is usually smaller than the real, absolute value itself, a lesser number of bits can be used to encode it.

C

CSTA

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

CTI

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

D

DFT

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

DHCP

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

DiffServ

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

DLS

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

DNS

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

DTMF

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

E

EAP

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

F

FTP

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

G

G.711

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

G.722

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

G.729

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

Gateway

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

H

HTTP

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

I

IP

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

IP address

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

J

Jitter

Latency fluctuations in the data transmission resulting in distorted sound.

L

LAN

Local **A**rea **N**etwork. A computer network covering a local area, like an office, or group of buildings.

Layer 2

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

Layer 3

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

LCD

Liquid **C**rystal **D**isplay. Display of numbers, text or graphics with the help of liquid crystal technology.

LDAP

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

LED

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

M

MAC Address

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

MDI-X

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

MIB

Management **I**nformation **B**ase. A type of database used to manage the devices in a communications network.

MWI

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

P

PBX

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

PCM

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

PING

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

PoE

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

Port

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

PSTN

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

Q

QoS

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

R

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

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

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

RTP
Realtime **T**ransport **P**rotocol. This application layer protocol has been designed for audio and video communication. Typically, the underlying protocol is -> UDP.

S

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

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

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

Subnet Mask
To discern the network part from the host part of an -> IP address, a device performs an AND operation on the IP address and the network mask. The network classes A, B, and C each have a subnet mask that demasks the relevant bits: 255.0.0.0 for Class A, 255.255.0.0 for Class B and 255.255.255.0 for Class C. In a Class C network, for instance, 254 IP addresses are available.

Switch
Network device that connects multiple network segments and terminal devices. The forwarding of data packets is based on -> MAC Addresses: data targeted to a specific device is directed to the switch port that device is attached to.

T

TCP
Transfer **C**ontrol **P**rotocol. The protocol belongs to the transport layer and establishes a connection between two entities on the application layer. It guarantees reliable and in-order delivery of data from sender to receiver, as opposed to -> UDP.

TLS
Transport **L**ayer **S**ecurity. Ensures privacy between communicating applications. Typically, the server is authenticated, but mutual authentication is also possible.

U

UDP
User **D**atagram **P**rotocol. A minimal message-oriented transport layer protocol used especially in streaming media applications such as -> VoIP. Reliability and order of packet delivery are not guaranteed, as opposed to -> TCP, but -> UDP is faster and more efficient.

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

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

V

VLAN
Virtual **L**ocal **A**rea **N**etwork. A method of creating several independent logical networks within a physical network. For example, an existing network can be separated into a data and a voice VLAN.

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

W

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

WBM

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

WML

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

WSP

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

Index

A

Administration Menu (Local Menu) 3-1, 3-2
Application Keys 1-3, 1-4, 1-5
Audio Keys 1-3, 1-4, 1-6

B

Bluetooth 3-124

C

Call Display 1-3, 1-4
Canonical Dial Lookup 3-46
Canonical Dialing 3-42
CSTA 6-1
CTI 6-1

D

Date and Time (SNTP) 3-38
Daylight Saving 3-38
Default Route 3-19
DFT 6-1
DHCP 3-16, 6-1
Diffserv 3-14
DLS (Deployment Service) 1-7, 2-18, 3-24, 6-1
DNS 2-10, 3-21, 3-22, 6-1
DNS Domain Name 3-21
DST Zone (Daylight Saving Time Zone) 3-39

E

Emergency Number 3-42
External Access Code 3-43
External Numbers 3-43

F

FTP Settings 3-51
Function Keys 1-3, 1-4, 1-5, 1-6

G

Graphics Display 1-3, 1-4

H

Handset 1-3, 1-4, 1-5, 1-6

I

Initial Digits 3-43
Internal Numbers 3-43
International Code (Local Country Code) 3-42
International Gateway Code 3-44
International Prefix (International Access Code) 3-42
IP
- Address 2-10
- Address (Manual configuration) 3-18
- IP 6-3
- Specific Routing 3-20

K

Keypad 1-3, 1-4, 1-5, 1-6

L

LAN 6-3
LAN Port 3-5
LDAP 6-3
LDAP Template (Download) 3-59
Local Country Code (International Code) 3-42
Local Enterprise Number 3-42
Local National Code (Local Area Code) 3-42
Logo (Create) 4-5
Logo (Download) 3-62

M

MAC Address 6-3
MDI-X 3-5, 6-4
MIB 6-4
MWI (Message Waiting Indicator) 6-4

N

National Prefix (Trunk Prefix) 3-42

O

Operator Code 3-42

P

Password, enter 2-27
PBX 6-4
Phone software (Download) 3-53
Picture Clips (Download) 3-56
Ping 3-118
PoE (Power over Ethernet) 2-5, 6-4
Program Keys 1-3, 1-4, 1-6
PSTN 6-4
PSTN Access Code 3-42

Q

QCU 3-26
QoS 3-13

R

RTP 6-5

S

Screensaver (Download) 3-65
SNMP 3-25, 6-5
Subnet Mask 2-10
Subnet Mask (Manual configuration) 3-18

T

TCP 6-6
Timezone Offset 3-38
TLS 6-6
TouchGuide 1-3, 1-4, 1-5, 1-6
TouchSlider 1-3

U

UDP 6-6

V

Vendor Class (DHCP) 2-10, 2-18
VLAN 2-10, 3-7

W

WBM (Web Based Management) 1-6, 2-9, 6-7

Communication for the open minded

Siemens Enterprise Communications
www.siemens.com/open

Copyright © Siemens Enterprise Communications GmbH & Co. KG 07/08/2009
Hofmannstr. 51, D-81359 München

Reference No.: A31003-S2010-M100-12-7619

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. Subject to availability. Right of modification reserved. The trademarks used are owned by Siemens Enterprise Communications GmbH & Co. KG or their respective owners.