A MITEL PRODUCT GUIDE

Unify OpenScape 4000 V11

vHG 3575 for OpenScape 4000 SoftGate

Administrator Documentation

07/2024

P31003-H31B0-M105-02-7620

Mitel

Notices

Trademarks

Contents

1 Introduction and Important Notes

OpenScape 4000 SoftGate and Enterprise Gateway

OpenScape 4000 SoftGate is an IP telephony application for connecting HFA and SIP telephones, e. g. the OpenStage HFA and OpenStage SIP phone families. The product enables IP-based communication across the entire company, including small branch offices. Connection to the public phone network is via SIP trunking (SIP-Q or native SIP).

OpenScape Enterprise Gateway is based on hardware and software of OpenScape 4000. It is successor of AP 3700-9 shelves with HG3575.

The vHG 3575 (Enterprise Gateway) (virtual HG 3575 = virtual NCUI) is the central controller for IPDA (IP Distributed Architecture) in the OpenScape 4000 SoftGate or Enterprise Gateway.

Topics in this Chapter

Section 1.1, "Target Audience for this Manual"

Section 1.2, "Contents of this Manual"

Section 1.3, "Note for Internet Explorer"

Section 1.4, "Conventions Used"

1.1 Target Audience for this Manual

This manual is aimed at employees who are responsible for managing OpenScape 4000 SoftGate. They should have experience in LAN administration and be familiar with the following areas:

- Hardware for data communication
- OpenScape 4000 V10
- WAN (Wide Area Network) concepts and terms
- LAN (Local Area Network) concepts and terms
- Internet concepts and terms

They should have received instruction on the following for vHG 3575 (Enterprise Gateway) and OpenScape 4000 SoftGate:

- Installation and start-up
- Configuring VoIP functions
- Setting up and configuring data communication parameters

1.2 Contents of this Manual

This manual describes vHG 3575 SoftGate and Enterprise Gateway WBM (Web-Based Management). This includes general operation of the WBM, descriptions of individual modules for administering SoftGate and also how administration should be performed.

1.3 Note for Internet Explorer

IMPORTANT: After changing any Internet Explorer security settings for a WBM page (like adding the page in Trusted Sites), it is recommended to restart the browser in order to work correctly with the new settings.

1.4 Conventions Used

The following typographical conventions are used in this book:

Convention	Example
`Courier`	Input and output Example: Enter `LOCAL` as the file name. `Command not found`
Italic	Variable Example: *Name* can contain up to eight characters.
Italic	User interface elements Example: Click *OK*.
Section 1.4, "Conventions Used"	Cross-reference
Configuration	User interface elements as cross references
Bold	Special emphasis Example: This name must **not** be deleted.
`<Courier>`	Keyboard shortcuts Example: `<CTRL>+<ALT>+<ESC>`
>	Menu sequence Example: *WBM* **>** Configuration
NOTICE:	Designates situations that may result in property damage or loss of data.
IMPORTANT:	Designates useful information.

2 OpenScape 4000 WBM

WBM

WBM is the administration interface of the vHG 3575 SoftGate and Enterprise Gateway (virtual HG 3575 = virtual NCUI). As long as the Root administrator has enabled WBM, it is available via any TCP/IP connection, as well as via LAN and WAN.

All PCs with TCP/IP-supported network connections running a compatible Web browser can access the vHG 3575 WBM after login. WBM has an integrated Web server, and can thus be accessed via a HTTPS URL.

The WBM user interface is available only in English.

Topics in this Chapter

Section 2.1, "Hardware and Software Requirements"

Section 2.2, "Starting and Finishing WBM"

Section 2.3, "WBM User Interface"

2.1 Hardware and Software Requirements

2.1.1 Hardware

Please, refer to requirements for the Internet browser.

2.1.2 Software

The vHG 3575 WBM consists of HTML/XSL pages with frames. The requirements for using it are:

- Windows 7 and higher.
- Internet Explorer version 10 and higher, Firefox and Google Chrome.

Other browsers which support frames and JavaScript may also be compatible with WBM. Browsers which do not support frames cannot be used with WBM.

IMPORTANT: If a DNS server is configured on the administration PC, but cannot be reached, this causes significant delays on the WBM interface. If this is the case, check the network settings for the installed DNS server on the administration PC. Remove any DNS servers that cannot be reached, or enter reachable Click *Close*.

2.1.3 Setting Internet Explorer

Make the following settings in Internet Explorer:

Deleting temporary Internet files

Tools > Internet Options > Advanced > Security > activate Empty Temporary Internet Files folder when browser is closed

Bypassing the proxy server

The connection from the administration PC to the vHG 3575 must not be routed over a proxy server.

Tools > Internet Options > Connections > LAN Settings > LAN Settings... button > Proxy server > activate Bypass proxy server for local address

Enable download from files

- Either for all URLs:

  Tools > Internet Options > Security tab > Local intranet Web content zone > click Custom Level... > Download > File download > Enable
- Or only for the vHG 3575 WBM URL:

  1) Tools > Internet Options > Security tab > Trusted sites Web content zone > click Sites > enter the WBM URL in Add this website to the zone > click Add, enable the check box Require server verification (https:) for all sites in this zone

  2) Tools > Internet Options > Security tab > Trusted sites Web content zone > click Custom Level... > Download > File download > Enable

When you have made all these settings, close Internet Explorer and restart it.

2.2 Starting and Finishing WBM

Access options

There are two options for starting the vHG 3575 WBM. It can be started via OpenScape 4000 Assistant, or directly from a Web browser using the WBM URL. Access via OpenScape 4000 Assistant is the most common method used.

Topics in this chapter

Section 2.2.1, "Starting via OpenScape 4000 Assistant"

Section 2.2.2, "Starting via Web Browser"

Section 2.2.3, "Finishing a WBM Session"

2.2.1 Starting via OpenScape 4000 Assistant

To start the WBM session, follow these steps:

1) Log in to OpenScape 4000 Assistant using your user name and password.

2) In the hierarchy, select *OpenScape 4000 Assistant* **>** *Expert Mode* **>** *Gateway Dashboard*. The *Gateway Dashboard* window is displayed with the existing boards.

3) Click *[WBM] [N/A]* in the line for the required Enterprise Gateway (e.g. SoftGate) in the *Remote access* column. You need to know the IP address of the relevant board.

   The WBM Web server is contacted. Since the server only works with HTTPS (secure data transmission), it sends a certificate.

   > **NOTICE:** You may see a message in Explorer to the effect that there is a problem with the security certificate for the website. In this case, click *Continue to this website*.

4) Confirm the browser dialog with the certificate information. The WBM homepage is displayed:
5) Check whether you are in the Enterpise Gateway WBM (e.g. SoftGate).
6) You can now use the Configuration and Maintenance modules to administer vHG 3575 (Enterprise Gateway).

2.2.2 Starting via Web Browser

User Account

The user account "Administrator" is available for WBM. This account provides access to configuration settings.

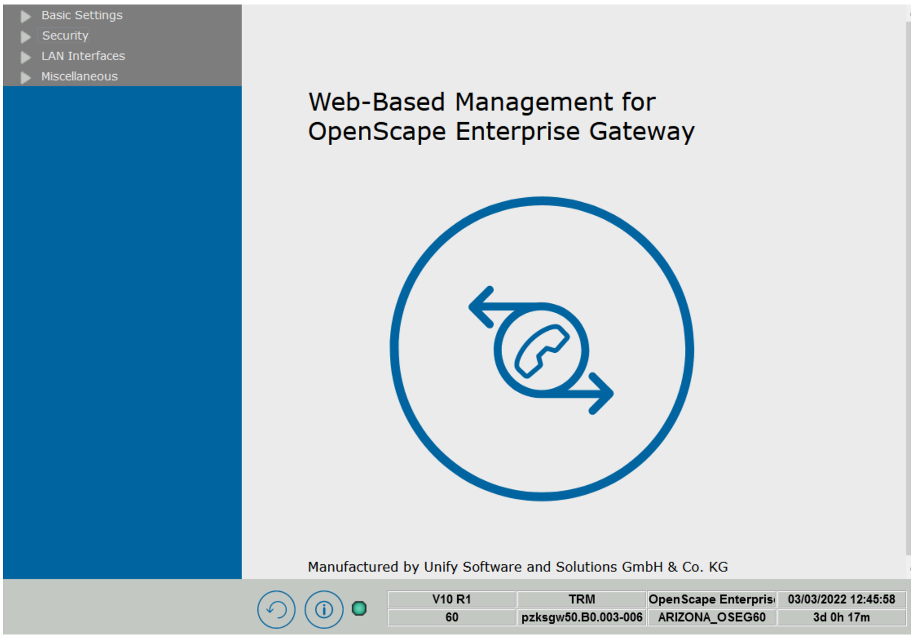
The default user name is **TRM** and the default password is **HICOM** (as configured in AMO STMIB). You can modify these defaults in AMO STMIB.

Starting a WBM session

To start the WBM session, follow these steps:

1) Open your Web browser.
2) In the address bar of your browser, enter the desired (Enterpise Gateway or SoftGate) WBM URL, in the format: *https://999.999.999.999*. The WBM Web server is contacted. Since the server only works with HTTPS (secure data transmission), it sends a certificate.
3) Confirm the browser dialog with the certificate information. The vHG 3575 (Enterprise Gateway)WBM login dialog is displayed.

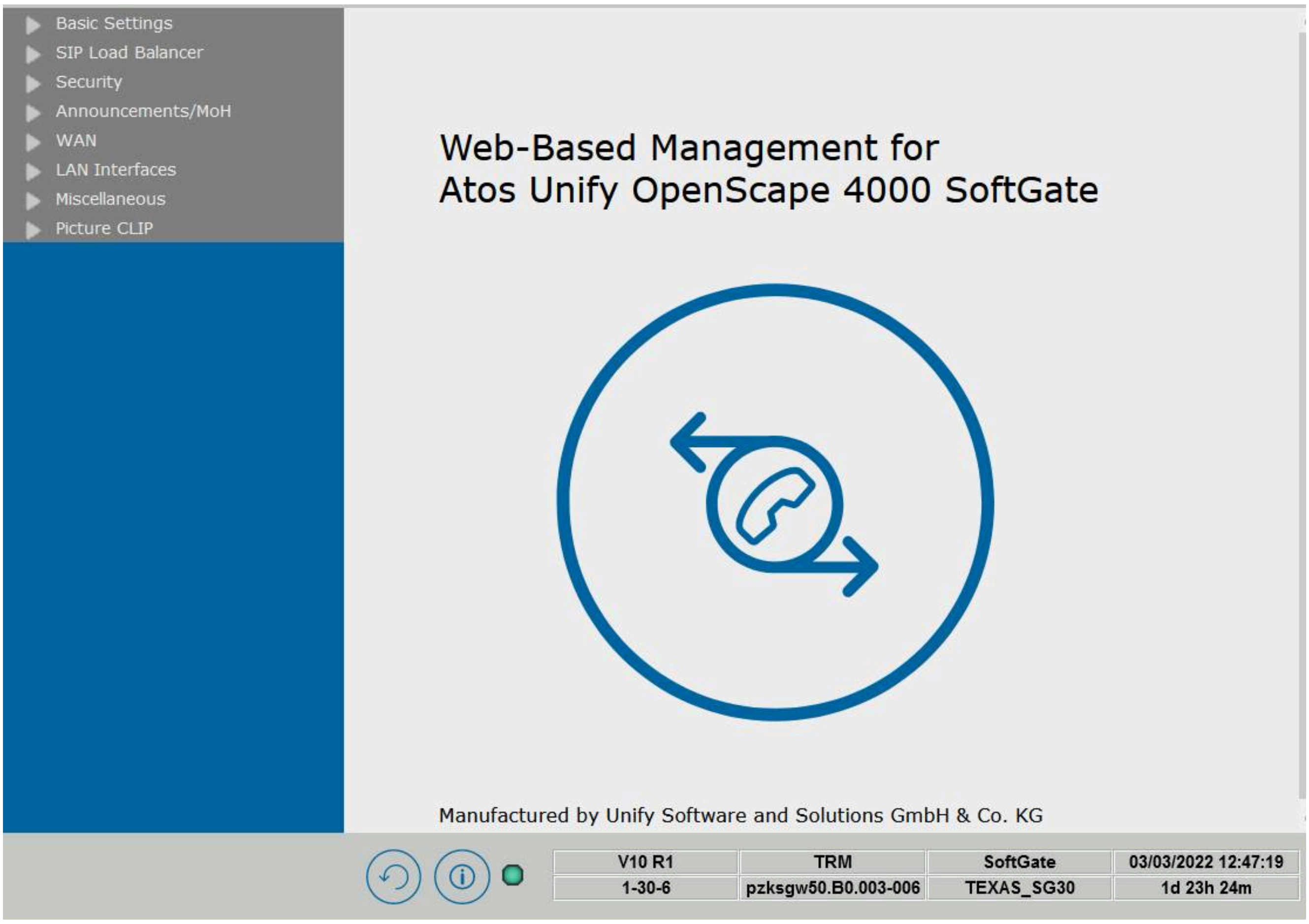
4) Enter the user name and password. Click *Login*. The WBM homepage is displayed.



Web-Based Management for
OpenScape Enterprise Gateway

Manufactured by Unify Software and Solutions GmbH & Co. KG

V10 R1	TRM	OpenScape Enterpris	03/03/2022 12:45:58
60	pzksgw50.B0.003-006	ARIZONA_OSEG60	3d 0h 17m



Web-Based Management for
Atos Unify OpenScape 4000 SoftGate

Manufactured by Unify Software and Solutions GmbH & Co. KG

V10 R1	TRM	SoftGate	03/03/2022 12:47:19
1-30-6	pzksgw50.B0.003-006	TEXAS_SG30	1d 23h 24m

5) You can now use the Configuration and Maintenance modules.

2.2.3 Finishing a WBM Session

To finish the WBM session, follow these steps:

1) Click the *Logoff* module. The connection to WBM is ended and the WBM session is closed.

For more information on closing the WBM session, refer to Section 6, "Logoff".

2.3 WBM User Interface

This chapter outlines the basic structure of the user interface, names the individual control elements, and describes their use.

Topics in this chapter

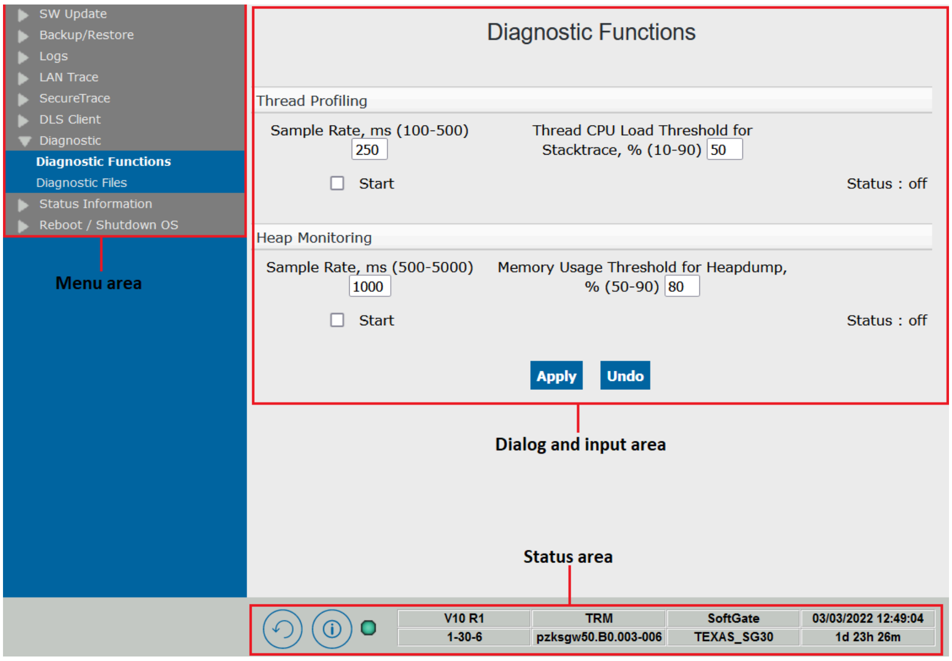
Section 2.3.1, "User Interface Division"

Section 2.3.2, "Icons in the WBM Window's Status Area"

Section 2.3.3, "Dialog Elements"

2.3.1 User Interface Division

The WBM user interface can be divided into the following areas:



Diagnostic Functions

Thread Profiling

Sample Rate, ms (100-500) 250

Thread CPU Load Threshold for Stacktrace, % (10-90) 50

□ Start

Status : off

Heap Monitoring

Sample Rate, ms (500-5000) 1000

Memory Usage Threshold for Heapdump, % (50-90) 80

□ Start

Status : off

V10 R1	TRM	SoftGate	03/03/2022 12:49:04
1-30-6	pzksgw50.B0.003-006	TEXAS_SG30	1d 23h 26m

Menu area

This area is used to navigate within a module. The menus that are displayed here vary depending on the module selected.

Module area

This area shows the modules available. These modules are: Configuration, Maintenance, Help and Logoff. Click the module name to display the corresponding menu entries in the menu area.

Dialog and input area

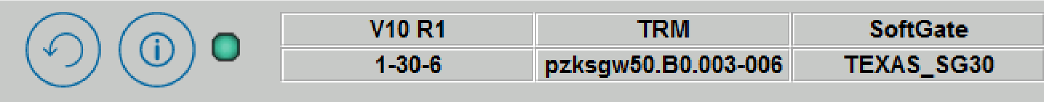
Once you have selected a module and a menu entry, this area shows the settings dialogs.

Status area

Status information is constantly displayed at the lower edge of your screen. For information on the meaning of the icons, see Section 2.3.2, "Icons in the WBM Window's Status Area".

2.3.2 Icons in the WBM Window's Status Area

The status area constantly provides control and status information. The figure below shows an example:



V10 R1	TRM	SoftGate
1-30-6	pzksgw50.B0.003-006	TEXAS_SG30

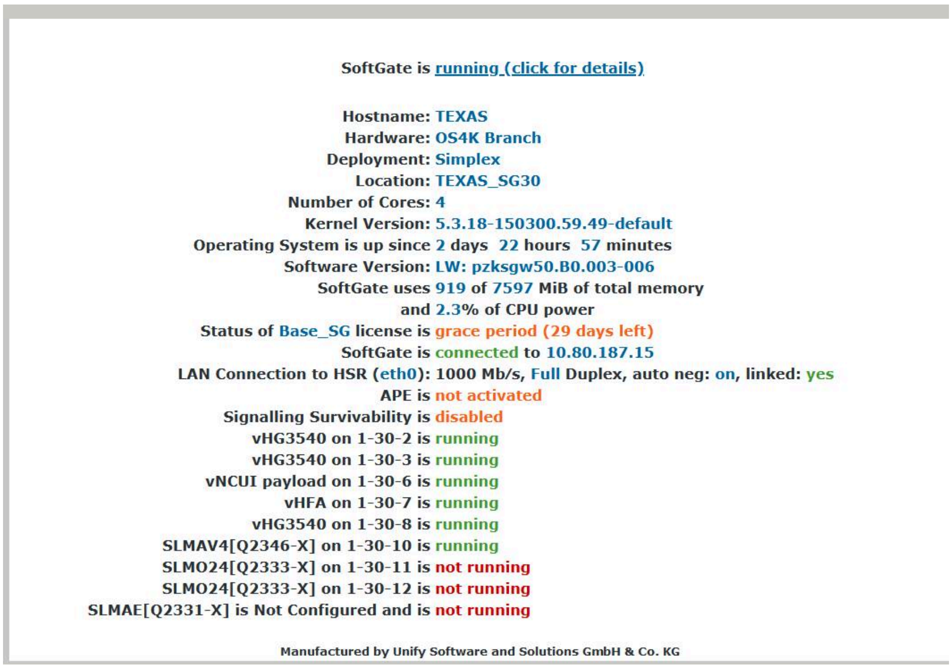
The following control icons are used:

Reset icon (1)

↺	**White/black:** Click this icon to restart vHG 3575.

Information icon (2)

ⓘ	Click this icon to display information on the OpenScape 4000 SoftGate or Enterprise Gateway operating status, e. g. running/ not running, host name, location, software version.



```
SoftGate is running (click for details)

Hostname: TEXAS
Hardware: OS4K Branch
Deployment: Simplex
Location: TEXAS_SG30
Number of Cores: 4
Kernel Version: 5.3.18-150300.59.49-default
Operating System is up since 2 days  22 hours  57 minutes
Software Version: LW: pzksgw50.B0.003-006
SoftGate uses 919 of 7597 MiB of total memory
and 2.3% of CPU power
Status of Base_SG license is grace period (29 days left)
SoftGate is connected to 10.80.187.15
LAN Connection to HSR (eth0): 1000 Mb/s, Full Duplex, auto neg: on, linked: yes
APE is not activated
Signalling Survivability is disabled
vHG3540 on 1-30-2 is running
vHG3540 on 1-30-3 is running
vNCUI payload on 1-30-6 is running
vHFA on 1-30-7 is running
vHG3540 on 1-30-8 is running
SLMAV4[Q2346-X] on 1-30-10 is running
SLMO24[Q2333-X] on 1-30-11 is not running
SLMO24[Q2333-X] on 1-30-12 is not running
SLMAE[Q2331-X] is Not Configured and is not running

Manufactured by Unify Software and Solutions GmbH & Co. KG
```

Action icon (3)

The icon turns green to indicate a connection to the WBM Web server. The icon flashes red when there is no connection set up.

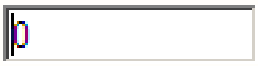
The following status information is also displayed:

- Status information for the ITIL version (4),
- Access category of the user and system version (5),
- Name of the board and installation location (6),
- System date and time and how long since the last restart (7).

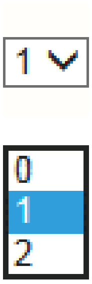
2.3.3 Dialog Elements

The following dialog elements appear in WBM:

Input fields

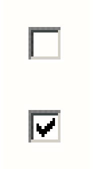
	For entering numeric or alphanumeric values. The relevant field label is displayed before, after or over the field. For security purposes, characters are exclusively displayed as unambiguous symbols, such as stars, in password fields. Characters unavailable on the keyboard can be inserted using the "Charmap" character table, for example, under Microsoft Windows.

Dropdown lists



(in the figure to the left: left = closed; right = open) Click the arrow to open or close the list. Click to select the required entry.

Check boxes

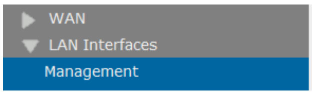


(Here, the upper check box is disabled while the lower one is enabled): The relevant field label is displayed before, after or over the field. Click to enable or disable the relevant option. Multiple check boxes can be enabled.

Radio buttons

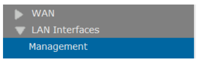
(Here, the upper check box is disabled while the lower one is enabled): Radio buttons are combined in groups where one element is always selected and all others deselected. The relevant field label is displayed before, after or over the field. Click to enable the corresponding function.

Arrows



(in the figures to the left: top figure = menu closed; bottom figure = menu open): In the menu area, you can click these arrows to open or close a menu. Multiple menus can be opened.

Menu items

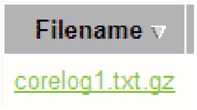


(in the figure to the left: top figure = menu item inactive; bottom figure = menu item active): Click a menu item to display the corresponding dialog. Inactive menu items are green; active menu items are white.

Buttons

Click to perform the action described by the button's label text. The texts are self-explanatory, for example *Undo* or *Apply*.

Sort sequence



The sort sequence of a column can be changed, for example in ascending or descending alphabetical order, by clicking the triangle next to the title in a table header.

3 Configuration

WBM path

WBM **>** Configuration

The Configuration module is displayed

Before starting the configuration, the gateway must have been installed according to the descriptions in the installation manual.

The Configuration module is used for defining the basic setup and for configuring the following settings of the gateway vHG 3575 or global settings of the complete SoftGate:

Options in the Configuration**module**

Basic Settings

SIP Load Balancer

Security

Announcements/MoH

WAN

LAN Interfaces

Miscellaneous

Picture CLIP

3.1 Basic Settings

In the Basic Settings menu, you can enter fundamental data about vHG 3575.

WBM path

WBM **>** Configuration **>** Basic Settings

The Basic Settings menu is displayed.

Basic Settings **menu**

The following options are shown in this menu:

Gateway

License Information

3.1.1 Gateway

WBM path

WBM **>** Configuration **>** Basic Settings **>** Gateway

The *Gateway Properties* dialog is displayed. You can enter basic data in this dialog.

Input fields

The following input fields are shown in this dialog:

- *System Name*: Enter the vHG 3575 (Enterprise Gateway) name in this field
- *Gateway Location*: The SoftGate location is displayed. Read-only. The value is taken from AMO UCSU.

3.1.2 License Information

- *Advanced Locking ID (ALI):* The ALI string is displayed.
- When the ALI cannot be calculated the missing parameter is displayed: (e.g *Missing ALI parameter:* Primary DNS IP Address). ALI is needed for ordering SoftGate or Enterprise Gateway license files.
- *License Type*
- License Type is either SoftGate or Enterprise Gateway Base license.
- *License Version*
- The version of the requested SoftGate or Enterprise Gateway Base license is shown.
- *License Status: (e.g.* 30 day grace period)
- *License Expiration:* (e.g. 15 days)
- SIEL-ID
- Here the SIEL-ID of the currently used SoftGate or Enterprise Gateway Base license is shown. SIEL-ID can only be shown if a valid license session could be established. When the SoftGate or Enterprise Gateway does not have a valid license file or are still in the Grace period, no SIEL-ID is shown.

3.1.3 License Import

WBM path

WBM > Configuration > Basic Settings > License Import

The License Import dialog box is displayed. Here you can import the SoftGate license.

Input field

This dialog box contains the following input field:

- Filename: In this field you can enter the name of the license file that you wish to import, along with the path to where it is stored. You can also click Browse to select the file.

Buttons:

The following buttons are displayed in this dialog box:

- Load: The specific license file is loaded.
- Undo: The path and the file name entered are deleted.

Procedure

To import the license file proceed as follows:

1) Enter the path and name of the license file, or select the file using the Browse button.

2) Click the Load button. The license file is now loaded.

3.2 SIP Load Balancer

WBM path

WBM **>** Configuration **>** SIP Load Balancer

The SIP Load Balancer menu opens.

Menu SIP Load Balancer

The following selection options are offered in this menu:

SettingsStatus

SPE (SIP Load Balancer)

Feature Description

SIP Load Balancing is deployed to distribute load in SIP-related data traffic in the IP network. With SIP Load Balancing, the system is able to scale the performance of participating SIP servers in order to avoid overloading of the server and to achieve high availability of the SIP services.

Load Balancing distributes calls from a provider connection, an OpenScape UC or OpenScape Xpression to a number of gateways, for example if the connection has more than the maximum number of gateway channels. Only one target IP address can be configured in the case of a provider connection, which means that one provider connection would have to be available without Load Balancing for each gateway.

Calls can also be sent selectively by means of their phone number from one connection to a number of even geographically distributed gateway groups or OpenScape 4000 systems with the help of a routing number (e.g. local area code) which can be configured for each gateway. Within a group, the calls are sent to the gateway with the most free channels.

SIP Load Balancing can be activated for every SIP gateway (HG 3500, vHG 3500 SIP, STMIX or STMIY) in the network. If the feature is activated correctly, the participating gateways can only be registered to the SIP Load Balancer via OpenScape 4000 SoftGate WBM.

SIP Load Balancing is also released for multiple OpenScape UC Media Server. These cannot register automatically to the SIP Load Balance server. Therefore, they must be configured manually in the OpenScape 4000 SoftGate WBM.

Service Information for OpenSIPS Load Balancer

The OpenSIPS Load Balancer is part of the OpenScape 4000 SoftGate software package and will be installed with each OpenScape 4000 SoftGate. It runs on a OpenScape 4000 SoftGate but has its own IP address (different from the IP address of the OpenScape 4000 SoftGate). The IP address is configured during installation.

Using its configured IP addresses, the Load Balancer automatically fetches its available DNS server names from the DNS server.

The "Load Balancing" feature is deactivated by default and must be activated with the WBM of the OpenScape 4000 SoftGate and the WBM of every participating gateway.

Features

- "Load Balancing" for inbound native SIP trunks towards virtual HG 3500 gateways (OpenScape 4000 SoftGate) and vxWorks based HG 3500 gateways (IPDA) (e.g. SIP Provider or OpenScape UC connectivity).
- Native SIP trunks without registration.
- Virtual HG 3500s of several OpenScape 4000 SoftGates and HG 3500 gateways of several access points can participate in Load Balancing.
- Error logging / tracing with OpenSIPS.
- Failover mechanism for inbound calls, which have been rejected by the gateway with an error response.
- Status monitoring of configured gateways by the Open SIPS Load Balancer.
- Load Balancing for several gateway groups.

Requirements

- A OpenScape 4000 SoftGate must be available within the network.
- SIP Load Balancing can only be activated if the use of SIP trunking profiles is activated in the WBM.
- For SIP Load Balancing to function, you must ensure that the (outbound) proxy settings in the SIP trunking profile are correctly configured.

Restrictions

- The "SIP Load Balancing" feature can be used only in a "SoftGate Standalone" deployment. This means, it is not available for e.g. "Survivable SoftGate".

Generation:

IMPORTANT: Generation with AMOs is not possible.

3.2.1 Settings

The SIP Load Balance server is activated via the WBM of the OpenScape 4000 SoftGate. The IP address of the Load Balancer and the network mask have to be entered for this purpose.

The OpenScape 4000 SoftGate has to be restarted every time the Load Balancer is activated/deactivated or every time the IP address is changed.

WBM path

WBM **>** Configuration **>** SIP Load Balancer **>** Settings

The *SIP Load Balancer Properties* dialog opens.

Input fields/check boxes

Make the following settings in the *SIP Load Balancer* dialog:

- *IP Address [IPv4]*: The IP address of the SIP Load Balance Server should be entered in IPv4 format in this input field.
- *Netmask [IPv4]*: The subnet mask where the SIP Load Balance Server is located should be entered in IPv4 format in this input field.
- *Default Gateway [IPv4]*: The IP address of the default gateway should be entered in IPv4 format in this input field.

- *Use VLAN Tagging*: Can be activated/deactivated. It is possible with IEEE802.1p/q for several virtual LANs to share a common physical network. The virtual LAN is packet-based in contrast to older port-based LANs. A tag is contained in the data area of the Ethernet packet that defines the VLAN to which the Ethernet packet belongs as well as the priority of the data packet.
- *VLAN ID*: Every VLAN is assigned a unique number, referred to as the VLAN ID. All devices that have the same VLAN ID can communicate with one another.
- *Activate*: Can be activated/deactivated. Activate the modified settings in this dialog.

IMPORTANT: OpenScape 4000 SoftGate must be restarted in order to activate all configuration changes.

Buttons

The following buttons are shown in this dialog:

- *Apply:* The input is saved. OpenScape 4000 SoftGate must be restarted to activate the changes.
- *Undo:* The input is rejected and the default value restored.

3.2.2 Status

The configured gateways for SIP Load Balancing are displayed.

WBM path

WBM **>** Configuration **>** SIP Load Balancer **>** Status

The *SIP Load Balancer Status* table opens.

Columns

The *SIP Load Balancer Status* table contains the following columns:

- *LTU*: Line Trunk Unit. Shelves 17 - 99 are connected to the processor via IPDA. This option is configurable in the WBM.
- *Slot*: Mounting slot for OpenScape 4000 gateway. This option is configurable in the WBM.
- *Gateway IPv4 Address*: IP address of gateway in IPv4 format
- *IPv4 Port*: SIP Port 5060 is used for unencrypted signaling data.
- *IPv4 TLS Port*: SIP Port 5061 is used for signaling data encrypted with TLS (Transport Layer Security).
- *Gateway IPv6 Address*: IP address of gateway in IPv6 format
- *IPv6 Port*: SIP Port 5060 is used for unencrypted signaling data.
- *IPv6 TLS Port*: SIP Port 5061 is used for signaling data encrypted with TLS (Transport Layer Security).
- *Routing Number*: Dial-in numbers (e.g. +4982700332200 for "1" and +4982700332201 for "11")
- *Max Number of B-Channels*: The maximum possible number of parallel B channels should be used.
- *Load*: Load on gateway
- *Enabled*: Indicates whether the gateway is accessible.

Buttons

The *SIP Load Balancer Status* table contains the following buttons:

- *Delete Rule*: Delete rule for gateway.
- Add Rule: Create rule for gateway.

3.2.3 SPE (SIP Load Balancer)

SPE (Signaling & Payload Encryption) encrypts VoIP payload and signaling data streams to and from the Load Balancer. This feature is based on an asymmetric encryption process. Public and private keys are used for this type of process.

The individual VoIP gateways and Load Balancer must be identifiable in the communication system. This is achieved using certificates containing private or public keys.

According to requirement, security settings for evaluating the certificates and encrypting data streams can be activated or deactivated. This increases or decreases the encryption security.

WBM path

WBM **>** Configuration **>** SIP Load Balancer**>** SPE (SIP Load Balancer)

The SPE (SIP Load Balancer) menu is displayed.

SPE (SIP Load Balancer)

The following options are shown in this menu:

Import Keycert

Show Keycert

Delete Keycert

SPE Security Setup for HFA

3.2.4 Import Keycert

> **NOTICE:** When you import a certificate for the first time with active SPE, a reset is automatically performed.

WBM path

WBM **>** Configuration **>** SIP Load Balancer**>** SPE (SIP Load Balancer)**>** Import Keycert

The *Load a SPE Key Certificate via HTTP* dialog is displayed. In this dialog, you can import an SPE key certificate by entering the decryption password and the file name. The file containing the certificate originates from a customer PKI certification authority (RA/CA) or the internal DLS server certification authority (CA) and must be available in PEM or PKCS#12 format.

Input fields

The following input fields are shown in this dialog:

- *Passphrase for decryption*: Enter the password used when creating the PEM or PKCS#12 file in this field.
- *File with certificate and private Key (PEM or PKCS#12 format)*: Enter the path and name of the file containing the certificate in this input field. You can also click *Browse* to select the file.

Buttons

The following buttons are shown in this dialog:

- *View Fingerprint of Certificate*: You can check the fingerprint to determine whether an unchanged certificate is available or whether it has been modified.
- *Import Certificate from File*: The certificate is imported from the file specified in the above input field.

Procedure

To load an SPE certificate, perform the following steps:

1) Select: *WBM* **>** Configuration **>** SIP Load Balancer **>** SPE (SIP Load Balancer) **>** Import Keycert. The *Load a SPE Key Certificate via HTTP* is displayed. You can edit the following fields:

  - *Passphrase for decryption*: Enter the password used when creating the PEM or PKCS#12 file in this field.
  - *File with certificate and private Key (PEM or PKCS#12 format)*: Enter the path and file name of the file containing the certificate data you wish to import. Click *Browse* to open a dialog to search for the file.

2) Click *View Fingerprint of Certificate*. A window appears showing the fingerprint of the certificate you wish to import:

  a) Check the fingerprint (hexadecimal figure). When the certificate is changed, the fingerprint always changes. Only an unchanged fingerprint guarantees an unchanged certificate. If the two fingerprints are not identical, an attack was probably attempted. In this case, the key should no longer be used and the specified measures should be taken.

  b) Click *OK* to close the fingerprint window.

3) Click *Import Certificate from File* if you are satisfied with your examination of the fingerprint. Do not import the certificate if the fingerprint does not satisfy your expectations.

3.2.5 Show Keycert

WBM path

WBM **>** Configuration **>** SIP Load Balancer **>** SPE (SIP Load Balancer) **>** Show Keycert

The *Certificate Information* dialog is displayed. In this dialog, you can see the SPE certificate, e. g. to test it.

Displayed data

The following certificate data is displayed:

- *General data:* Certificate Name, Certificate Type, Serial Number of Certificate, Serial Number of Certificate (hex), Type of Signature Algorithm, Start

Time of Validity Period (GMT), End Time of Validity Period (GMT), CRL Distribution Point

- *Issued by CA:* Country (C), Organization (O), Organization Unit (OU), Common Name: (CN)
- *Subject Name:* Country (C), Organization (O), Organization Unit (OU), Common Name: (CN)
- *Subject Alternative Name*
- *Public Key Encryption Data:* Public Key Length, Public Key, Fingerprint

3.2.6 Delete Keycert

WBM path

WBM **>** Configuration **>** SIP Load Balancer **>** SPE (SIP Load Balancer) **>** Delete Keycert

The *Remove SPE Certificate* dialog is displayed. In this dialog, you can remove the SPE certificate, e. g. if a new certificate is required.

Buttons

The following buttons are shown in this dialog:

- *Delete*: The SPE certificate is removed after a warning appears.
- *Cancel*: The removal procedure is canceled.

Procedure

To remove an SPE certificate, perform the following steps:

1) Select: *WBM* **>** Configuration **>** SIP Load Balancer **>** SPE (SIP Load Balancer) **>** Delete Keycert. A warning is displayed. The name of the certificate is specified for inspection purposes.

2) Click *Delete* and then click *OK* in the confirmation dialog.

3.2.7 SPE Security Setup for HFA

WBM path

WBM **>** Configuration **>** SIP Load Balancer **>** SPE (SIP Load Balancer) **>** SPE Security Setup for HFA

The *SPE Security Setup for HFA* dialog is displayed. In this dialog, the security settings for Signaling and Payload Encryption (SPE) can be adapted to the customerâs security requirements. This affects the encryption of signaling and payload data in communication between the vHG 3575 and the VoIP clients, or between two vHG 3575 systems.

Dropdown lists, input fields, check boxes

The following settings are shown in this dialog:

- *Activate TLS for LoadBalancer:* This option is used for the SPE feature for Load Balancer.
- *Maximum Re-Keying interval [hours]*: This value specifies the length of time a specific key should be used for encrypting signaling and payload data. When this time has elapsed, a new key is defined.

- *Salt Key Usage*: This process allows passwords to be strongly encrypted. This makes decryption considerably more difficult or even impossible. For example, after encryption it is no longer possible to detect if two users have the same password.
- *SRTP authentication required* (SRTP: Secure Real-time Transport Protocol): SRTP authentication prevents payload falsification and replay attacks. It also checks:
  - that a VoIP client payload message is not counterfeit.
  - if a payload message has already been received.
- *SRTCP encryption required* (SRTCP: Secure Real-time Transport Control Protocol): SRTCP encryption prevents signaling data falsification and replay attacks. It also checks:
  - that a VoIP client signaling data message is not counterfeit.
  - if a signaling data message has already been received.

Buttons

The following buttons are shown in this dialog:

- *Apply:* Save your entries.
- *Undo:* The entries made are deleted and replaced by default values.

Procedure

To modify SPE security settings, perform the following steps:

1) Select: *WBM* **>** Configuration **>** SIP Load Balancer**>** SPE (SIP Load Balancer) **>** SPE Security Setup for HFA. The *Edit SPE Security Setup* dialog is displayed.

2) Make the required settings, see section "Dropdown lists, input fields, check boxes".

Click *Apply* and then click *OK* in the confirmation dialog. The modified data is accepted into the configuration.

3.3 Security

In the Security menu you can manage the Master Encryption Keys (MEKs), Security Options and the TLS Configuration for HTTPS.

WBM path

WBM **>** Configuration **>** Security

The Security menu is displayed.

Security **menu**

The following selection options are offered in this menu:

Manage MEKs

Security Options

TLS Config for HTTPS

3.3.1 Manage MEKs

WBM path

WBM **>** Configuration **>** Security **>** Manage MEKs

The *Master Encryption Key (MEK) Management* dialog is displayed: In this dialog, you can add or remove MEKs for vHG 3575. An MEK is a special symmetrical key required for establishing an IP connection between OpenScape 4000 SoftGate and the OpenScape 4000 Host System. It consists of precisely 16 alphanumeric characters.

Input field

This dialog contains the following input field:

- *MEK [16 characters]:* You must enter the same MEK here as you entered previously in OpenScape 4000 Assistant. You can enter multiple MEKs.

Buttons

The following buttons are shown in this dialog:

- *Add MEK:* The MEKs entered in the *MEK* input field are added to OpenScape 4000 SoftGate.
- *Remove all MEKs:* All previously added MEKs are removed.
- *Undo:* The entries in this window are reset.

Procedure

To add an MEK, follow these steps:

1) In the *MEK* input field, enter the 16 alphanumeric characters of the MEK that you wish to add.

2) Click *Add MEK*. The MEK is added to the local MEK administration. If one of the MEKs matches the MEK in the OpenScape 4000 system, the connection can be established between vHG 3575 (Enterprise Gateway) and the OpenScape 4000 system.

3.3.2 Security Options

WBM path

WBM **>** Configuration **>** Security **>** Security Options

The *Security Options* dialog is displayed.

Checkboxes

The following check box are shown in this dialog:

- *Enforce Secure TLS Renegotiation (RFC 5746)*: Only applies for HFA. TLS is vulnerable to situations where a malicious server establishes a connection to a target server, injects it with its own rogue data and then splices in the new TLS connection from a client. The target server treats the client's initial TLS handshake as a renegotiation of an existing connection that the malicious server has previously established and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. This problem can be avoided with secure renegotiation based on RFC 5746.

NOTICE: A SoftGate restart is required to make changes effective.

NOTICE: This option applies to all configured HFA boards of the complete SoftGate.

Buttons

The following buttons are shown in this dialog:

- *Apply:* The input is saved. OpenScape 4000 SoftGate must be restarted to activate the changes.
- *Undo:* The input is rejected and reset to the default value.

3.3.3 TLS Config for HTTPS

WBM path

WBM **>** Configuration **>** Security **>** TLS Config for HTTPS **>** *TLS Configuration for HTTPS*

In Openscape 4000 V10, TLSv1.0 is not offered anymore.

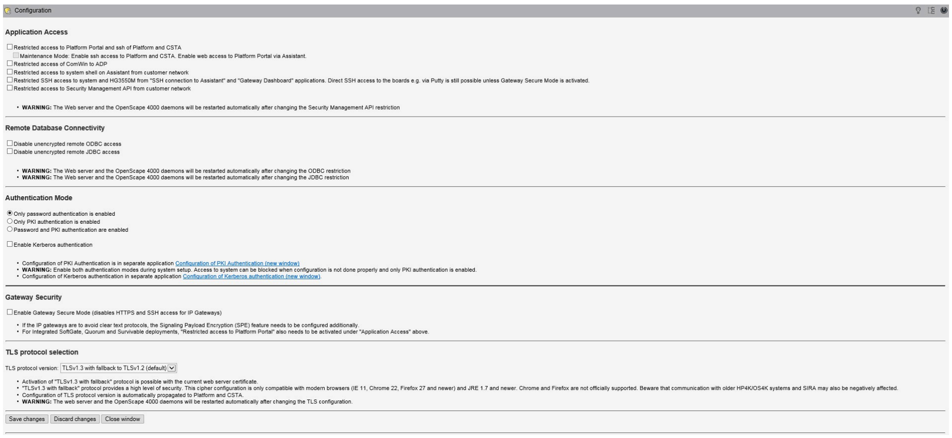
The only option available in Assistant will be TLSv1.3 with fallback to TLSv1.2.

SSLv2 and SSLv3 are not permitted due to security issues.

NOTICE: For integrated or survivable SoftGates the configuration of TLS protocol version is done at Assistant SecM

The TLS version can be configured in WBM for StandAlone SoftGates. It is offered and supported by the web server of the SoftGate. The configured TLS versions apply to all boards of SoftGate.

The default configuration of the web server in V10 enables communication in TLSv1.3 with fallback to TLSv1.2.



Configuration

Application Access

□ Restricted access to Platform Portal and ssh of Platform and CSTA
□ Maintenance Mode: Enable ssh access to Platform and CSTA. Enable web access to Platform Portal via Assistant.
□ Restricted access of ComWin to ADP
□ Restricted access to system shell on Assistant from customer network
□ Restricted SSH access to system and HG3550M from "SSH connection to Assistant" and "Gateway Dashboard" applications. Direct SSH access to the boards e.g. via Putty is still possible unless Gateway Secure Mode is activated.
□ Restricted access to Security Management API from customer network

- **WARNING:** The Web server and the OpenScape 4000 daemons will be restarted automatically after changing the Security Management API restriction

Remote Database Connectivity

□ Disable unencrypted remote ODBC access
□ Disable unencrypted remote JDBC access

- **WARNING:** The Web server and the OpenScape 4000 daemons will be restarted automatically after changing the ODBC restriction
- **WARNING:** The Web server and the OpenScape 4000 daemons will be restarted automatically after changing the JDBC restriction

Authentication Mode

● Only password authentication is enabled
○ Only PKI authentication is enabled
○ Password and PKI authentication are enabled

□ Enable Kerberos authentication

- Configuration of PKI Authentication is in separate application Configuration of PKI Authentication (new window)
- **WARNING:** Enable both authentication modes during system setup. Access to system can be blocked when configuration is not done properly and only PKI authentication is enabled.
- Configuration of Kerberos authentication in separate application Configuration of Kerberos authentication (new window).

Gateway Security

□ Enable Gateway Secure Mode (disables HTTPS and SSH access for IP Gateways)

- If the IP gateways are to avoid clear text protocols, the Signaling Payload Encryption (SPE) feature needs to be configured additionally.
- For Integrated SoftGate, Quorum and Survivable deployments, "Restricted access to Platform Portal" also needs to be activated under "Application Access" above.

TLS protocol selection

TLS protocol version: TLSv1.3 with fallback to TLSv1.2 (default)

- Activation of "TLSv1.3 with fallback" protocol is possible with the current web server certificate.
- "TLSv1.3 with fallback" protocol provides a high level of security. This cipher configuration is only compatible with modern browsers (IE 11, Chrome 22, Firefox 27 and newer) and JRE 1.7 and newer. Chrome and Firefox are not officially supported. Beware that communication with older HP4K/OS4K systems and SIRA may also be negatively affected.
- Configuration of TLS protocol version is automatically propagated to Platform and CSTA.
- **WARNING:** The web server and the OpenScape 4000 daemons will be restarted automatically after changing the TLS configuration.

3.4 Announcements/MoH

The Announcements/MoH menu allows you to manage the external and internal announcements and the settings for Music on Hold (MoH).

WBM path

WBM **>** Configuration **>** Announcements/MoH

The *Announcements/MoH*dialog is displayed.

Announcements/MoH**menu**

The following selection options are shown in this menu:

External Announcements

Internal Announcements

3.4.1 External Announcements

WBM path

WBM **>** Configuration **>** External Announcements

The *Manage External Announcements* dialog is displayed

In this dialog you can make modifications to the settings for the announcement board where announcements are saved.

Input fields

The following input fields are shown in this dialog:

- *Slot Circuit:* Only slots with configured vSLAM and vTMOM are displayed in the dropdown list.
- *Filename:* Enter the path and file name containing the announcement in this field (wav file in the format "PCM16, 8 kHz, mono"). You can also click *Browse* to select the file.

NOTICE: When loading the wav file it is checked if it has a valid format and fulfills all restrictions (PCM16, 8 kHz, mono).

Buttons

The following buttons are shown in this dialog:

- *Load:* The specified file is loaded.
- *Undo:* The path and file name entered are deleted.
- *Delete:* The relevant announcement in the *Filename* / *Action* table is deleted.

***Filename / Action* table**

The loaded announcements are displayed in this table.

Procedure

To load an announcement, proceed as follows:

1) Enter the required value into the *Circuit (0-255)* input field.

2) Enter the path and file name where the announcement is stored or click *Browse* to select the file.

3) Click *Load*. The file is loaded and displayed in the *Filename / Action* table.

With V10, SoftGate allows the download of configured external announcement files.

The download is offered via a hyperlink on the filename (right click on the filename).

3.4.2 Internal Announcements

WBM **>** Configuration **>** Announcements/MoH > Internal Announcements

The *Internal MoH Settings*dialog is displayed.

Buttons and check boxes

The following buttons and check boxes are shown in this dialog:

- *Use classic internal MoH*: Use this check box to enable/disable the *Use classic internal MoH* feature.
- *Apply:* The input is saved. OpenScape 4000 SoftGate must be restarted to activate the changes.
- *Undo:* The input is rejected and reset to the default value.

3.5 WAN

In the *WAN* menu you can configure the settings for the WAN interface and for the SPE certificates. The WAN interface is used for features HFA@Home, SIP@Home and SIP Trunking (e. g. SIP Service Provider).

WBM-Pfad

WBM **>** Configuration **>** WAN

The WAN menu is displayed.

WAN **menu**

The following selection options are shown in this menu:

SettingsSPE (WAN)

3.5.1 Settings

WBM path

WBM **>** Configuration **>** WAN **>** Settings

The *WAN Settings*dialog is displayed:

In this dialog you can configure the settings for the WAN Interface and enable/ disable the retrieval of telephone pictures via WAN.

Selection and Input Fields, Checkboxes

The following input fields are shown in this dialog:

- *WAN Redundancy - on/off:*Activate/deactivate redundancy for the Management LAN. Select the required setting from the dropdown list. Default setting: off (deactivated).
- *WAN Interface:*The required Ethernet interface can be selected from the drop down list. The default is "Deactivated"

Check boxes

The following check box is shown in this dialog:

- *Activate Telephone Picture Retrieval for WAN (Picture CLIP):* By enabling/ disabling this checkbox you can define whether the retrieval of telephone pictures saved on external servers shall be enabled or blocked. Choose the Picture CLIP menu option from the navigation bar in order to configure the paramaters for this feature. For details, refer to Picture CLIP.

NOTICE: A SoftGate restart is required to make changes effective.

Buttons

The following buttons are shown in this dialog:

- *Apply:* The input is saved. OpenScape 4000 SoftGate must be restarted to activate the changes.
- *Undo:* The input is rejected and reset to the default value.

3.5.2 SPE (WAN)

SPE (Signaling & Payload Encryption) encrypts VoIP payload and signaling data streams to and from vHG 3575. This feature is based on an asymmetric encryption process. Public and private keys are used for this type of process.

The individual VoIP clients and gateways, e. g. vHG 3575, must be identifiable in the communication system. This is achieved using certificates containing private or public keys. Certificates are created either by a customer PKI certification authority (RA/CA) or by the DLS serverâs internal certification authority (CA). The DLS server sends the files containing these certificates to the gateway DLS client.

According to requirement, security settings for evaluating the certificates and encrypting data streams can be activated or deactivated. This increases or decreases the encryption security.

WBM path

WBM **>** Configuration **>** WAN **>** SPE (WAN)

The SPE (WAN) menu is displayed.

SPE (WAN) *menu*

The following options are shown in this menu:

Import Keycert

Show Keycert

Delete Keycert

SPE Security Setup

3.5.3 Import Keycert

NOTICE: When you import a certificate for the first time with active SPE, a reset is automatically performed.

WBM path

WBM **>** Configuration **>** WAN**>** SPE (WAN)**>** Import Keycert

The *Load a SPE Key Certificate via HTTP* dialog is displayed. In this dialog, you can import an SPE key certificate by entering the decryption password and the file name. The file containing the certificate originates from a customer PKI certification authority (RA/CA) or the internal DLS server certification authority (CA) and must be available in PEM or PKCS#12 format.

Input fields

The following input fields are shown in this dialog:

- *Passphrase for decryption*: Enter the password used when creating the PEM or PKCS#12 file in this field.
- *File with certificate and private Key (PEM or PKCS#12 format)*: Enter the path and name of the file containing the certificate in this input field. You can also click *Browse* to select the file.

Buttons

The following buttons are shown in this dialog:

- *View Fingerprint of Certificate*: You can check the fingerprint to determine whether an unchanged certificate is available or whether it has been modified.
- *Import Certificate from File*: The certificate is imported from the file specified in the above input field.

Procedure

To load an SPE certificate, perform the following steps:

1) Select: *WBM* **>** Configuration **>** WAN **>**SPE (WAN)**>** Import Keycert*.* The *Load a SPE Key Certificate via HTTP* is displayed. You can edit the following fields:

   - *Passphrase for decryption*: Enter the password used when creating the PEM or PKCS#12 file in this field.
   - *File with certificate and private Key (PEM or PKCS#12 format)*: Enter the path and file name of the file containing the certificate data you wish to import. Click *Browse* to open a dialog to search for the file.

2) Click *View Fingerprint of Certificate*. A window appears showing the fingerprint of the certificate you wish to import:

   a) Check the fingerprint (hexadecimal figure). When the certificate is changed, the fingerprint always changes. Only an unchanged fingerprint guarantees an unchanged certificate. If the two fingerprints are not identical, an attack was probably attempted. In this case, the key should no longer be used and the specified measures should be taken.

   b) Click *OK* to close the fingerprint window.

3) Click *Import Certificate from File* if you are satisfied with your examination of the fingerprint. Do not import the certificate if the fingerprint does not satisfy your expectations.

3.5.4 Show Keycert

WBM path

WBM **>** Configuration **>** WAN **>**SPE (WAN) **>** Show Keycert

The *Certificate Information* dialog is displayed. In this dialog, you can see the SPE certificate, e. g. to test it.

Displayed data

The following certificate data is displayed:

- *General data:* Certificate Name, Certificate Type, Serial Number of Certificate, Serial Number of Certificate (hex), Type of Signature Algorithm, Start Time of Validity Period (GMT), End Time of Validity Period (GMT), CRL Distribution Point
- *Issued by CA:* Country (C), Organization (O), Organization Unit (OU), Common Name: (CN)
- *Subject Name:* Country (C), Organization (O), Organization Unit (OU), Common Name: (CN)
- *Subject Alternative Name*
- *Public Key Encryption Data:* Public Key Length, Public Key, Fingerprint

3.5.5 Delete Keycert

WBM path

WBM **>** Configuration **>** WAN **>** SPE (WAN) **>** Delete Keycert

The *Remove SPE Certificate* dialog is displayed. In this dialog, you can remove the SPE certificate, e. g. if a new certificate is required.

Buttons

The following buttons are shown in this dialog:

- *Delete*: The SPE certificate is removed after a warning appears.
- *Cancel*: The removal procedure is canceled.

Procedure

To remove an SPE certificate, perform the following steps:

1) Select: *WBM* **>** Configuration **>** WAN **>** SPE (WAN) **>** Delete Keycert. A warning is displayed. The name of the certificate is specified for inspection purposes.

2) Click *Delete* and then click *OK* in the confirmation dialog.

3.5.6 SPE Security Setup

WBM path

WBM **>** Configuration **>** WAN **>** SPE (WAN)**>** SPE Security Setup

The *Edit SPE Security Setup* dialog is displayed. In this dialog, the security settings for Signaling and Payload Encryption (SPE) can be adapted to the customerâs security requirements. This affects the encryption of signaling and payload data in communication between the vHG 3575 and the VoIP clients, or between two vHG 3575 systems.

Dropdown lists, input fields, check boxes

The following settings are shown in this dialog:

- *Minimum length of RSA keys:* Define the minimum length of RSA key in the certificate received from the remote entity. The greater the value, the more secure the key.The minimum is 512 bits and the maximum is 2048 bits.
- *Maximum Re-Keying interval [hours]*: This value specifies the length of time a specific key should be used for encrypting signaling and payload data. When this time has elapsed, a new key is defined.
- *Enforce Secure Renegotiation (RFC 5746):* Activate by checkbox.
- *TLS Protocol Version:* You can select TLS 1.2 with fallback to TLS 1.0 (Default), TLS 1.0 only, or TLS 1.2 only.

TLS 1.2 Cipher Selection

- *Key Agreement*: Select with Perfect Foward Secrecy or without.
- *Encryption*: Select AES-128 with fallback to AES-256 or AES-256 only.
- *AES Operation Mode*: Select GCM preferred with fallback to CBC, GCM only, or CBC only.

TLS Parameters

- *Certificate Verification Level:* None, Trusted or Full
- *Certificate validation with CRL verification required:* Activate/Deactivate
- *Subjectname check:* Activate / Deactivate

Buttons

The following buttons are shown in this dialog:

- *Apply:* Save your entries.
- *Undo:* The entries made are deleted and replaced by default values.

Procedure

To modify SPE security settings, perform the following steps:

1) Select: *WBM* **>** Configuration **>** WAN **>** SPE (WAN) **>** SPE Security Setup.
The *Edit SPE Security Setup* dialog is displayed.

2) Make the required settings, see section "Dropdown lists, input fields, check boxes".

3) Click *Apply* and then click *OK* in the confirmation dialog. The modified data is accepted into the configuration.

3.6 LAN Interfaces

The settings in this menu can be used to separate Voice LAN fully from the management, XLink, HFA and SIP interfaces. In addition, an alternative LAN path can be defined for transmitting signaling data.

WBM path

WBM **>** Configuration **>** LAN Interfaces

The LAN Interfaces menu opens:

Menu LAN Interfaces

The following selection options are offered in this menu:

Management Interface

Signalling Survivability Interface

XLink

HFA Interface

SIP Interface

3.6.1 Management Interface

With the introduction of the feature "Separate LAN Connectivity for Administration and VoIP", the Voice LAN can be completely split from the Management LAN. Before it was only possible to split the IPDA LAN from the Customer LAN.

If you want to separate the Management LAN from the Voice LAN, you have to enter an IP address for the Management LAN. In the WBM you only specify the LAN Interface on which the IP address for the Management LAN is or shall be configured, the IP address itself is specified in the RMX part via the AMO STMIB.

If an IP address is entered for the Management LAN, OpenScape 4000 Assistant will use it to connect to the gateway WBM and reaches it via the Customer LAN interface. If the IP address has the default value 0.0.0.0, OpenScape 4000 Assistant will use the IP address of the IPDA LAN.

Separation of the two interfaces can be configured via the gateway.

The *Management Interface* menu option allows you to enable/disable the Management LAN Interface and to configure the settings for the Management LAN.

WBM path

WBM **>** Configuration **>** LAN Interfaces **>**Management Interface

The *Management Interface Settings*dialog is displayed: In this dialog you can enable/disable the Management LAN Interface and turn on/off the Redundancy for the Management LAN.

Dropdown lists

The following dropdown lists are shown in this dialog:

- *Management LAN Redundancy*: The Redundant Management LAN interface can be activated or deactivated. Choose the required setting in the dropdown list:
  - Possible values: *On*, *off*
  - Default: *Off* (deactivated)
- *Management LAN Interface:* The required Ethernet interface can be selected from the drop down list. The default is *"*Deactivated*".*

> **IMPORTANT:** The same LAN/Ethernet interface must not be used for the IPDA interface and the Management interface!

> **IMPORTANT:** OpenScape 4000 SoftGate must be restarted in order to activate all configuration changes.

Buttons

The following buttons are shown in this dialog:

- *Apply:* The input is saved. OpenScape 4000 SoftGate must be restarted to activate the changes.
- *Undo:* The input is rejected and reset to the default value.

3.6.2 Signalling Survivability Interface

With "Signaling Survivability via Alternate LAN", an alternative route for signaling via a second LAN path is set up as soon as a fault in the IP path is detected. The switching of the signaling path is done without power interruption.

In addition to configuring the AMOs, the LAN Interface to be used for signalling survivability must be selected for the vHG 3575 in the OpenScape 4000 SoftGate.

The *Signalling Survivability Interface* menu option allows you to configure the settings for the Signalling Survivability Interface.

WBM path

WBM **>** Configuration **>** LAN Interfaces **>**Signalling Survivability Interface

The *Signalling Survivability Interface Settings*dialog is displayed. You can specify the LAN interface and activate and deactivate LAN redundancy in this dialog. The internal IP addresses of the TUN devices for the HSR connection are also displayed in this dialog (HSR: High-availability Seamless Redundancy).

Dropdown lists

The following dropdown lists are shown in this dialog:

- *LAN Redundancy*: LAN redundancy for the interface can be activated or deactivated. Choose the required setting in the dropdown list:
  - Possible values: *On*, *off*
  - Default: *Off* (deactivated)
- *LAN Interface*: The required Ethernet interface can be selected. The default is "eth0" however any available interface from the drop down list can be chosen.

Input fields under *Internal IP Addresses of TUN Devices for the HSR Connection (Expert Settings))*

Two internal host IP addresses are required for specific routing over a HSR connection via internal TUN devices.

The default settings should not be changed as long as there are no other equivalent external IP addresses that have to be reachable by the host.

Since the default settings are from a reserved range, this should not happen too often.

The following display fields are shown in this dialog:

- *IP Address for TUN Device #1*: Internal IP address of TUN Device #1 for HSR connection.
- *IP Address of TUN Device #2*: Internal IP Address of TUN Device #2 for the HSR Connection.

> **IMPORTANT:** OpenScape 4000 SoftGate must be restarted in order to activate all configuration changes.

Buttons

The following buttons are shown in this dialog:

- *Apply:* The input is saved. OpenScape 4000 SoftGate must be restarted to activate the changes.
- *Undo:* The input is rejected and the default restored.

3.6.3 XLink

XLink (X-LINK) is used to connect the OpenScape Access (OSA) SLA, SLO, BRI, PRI, SLC and TA modules to an OpenScape 4000 SoftGate e. g. OpenScape 4000 Branch (OS4B) or OpenScape Access 500i/a (OSA500). The OSA modules need to be connected with the XLink switch of the SoftGate (OS4B or OSA500).

The XLink switch of the SoftGate uses IP to replicate the Backplane for the Boards inside the OSA modules. Due to this the XLink switch consists of 1 Gigabit-LAN Ports to provide the necessary high bandwith of the voice traffic, i. e. the user data/payload.

> **NOTICE:** The XLink switch inside OS4B and OSA500 is hardwired to eth2, therefore this network interface is reserved for XLink only.

WBM path

WBM **>** Configuration **>** LAN Interfaces **>**XLink

The *XLINK Properties* dialog is displayed: The XLink LAN interface can be deactivated or the LAN/Ethernet interface used for it selected in this dialog as well as the XLink network address entered.

Dropdown lists and input fields

The following dropdown lists/input fields are shown in this dialog:

- *XLink LAN Interface*: The XLink LAN interface can be deactivated or the LAN/Ethernet interface used for it selected. Select the required setting in the dropdown list:
  - Possible values: *Deactivated*, *eth2*
- *XLink Network Address*: The IP address of a network must be entered, i.e. the last two positions must be ".0.0", e.g. "10.100.0.0".

> **IMPORTANT:** OpenScape 4000 SoftGate must be restarted in order to activate all configuration changes.

Buttons

The following buttons are shown in this dialog:

- *Apply:* The input is saved. OpenScape 4000 SoftGate must be restarted to activate the changes.
- *Undo:* The input is rejected and the default restored.

3.6.4 HFA Interface

The HFA interface provides OpenScape 4000 features in an IPDA (HFA: HiPath Feature Access, IPDA: Internet Protocol Distributed Architecture).

WBM path

WBM **>** Configuration **>** LAN Interfaces **>** HFA Interface

The *HFA Interface Settings* dialog is displayed: You can activate or deactivate the HFA interface and select the LAN/Ethernet interface used for it in this dialog.

Dropdown lists and input fields

The following dropdown lists are shown in this dialog:

- *HFA LAN Redundancy*: The redundant HFA interface can be activated or deactivated. Choose the required setting in the dropdown list:
  - Possible values: *On*, *off*
  - Default: *Off* (deactivated)
- *HFA LAN Interface*: The required Ethernet interface can be selected. The default is "Default IPDA" however any available interface from the drop down list can be chosen.

> **IMPORTANT:** The same LAN/Ethernet interface must not be used for the HFA interface and the Management interface!

> **IMPORTANT:** OpenScape 4000 SoftGate must be restarted in order to activate all configuration changes.

Buttons

The following buttons are shown in this dialog:

- *Apply:* The input is saved. OpenScape 4000 SoftGate must be restarted to activate the changes.

- *Undo:* The input is rejected and the default restored.

3.6.5 SIP Interface

The SIP interface is used for setting up, controlling and clearing down communication settings with the aid of the SIP in an IPDA (SIP: Session Initiation Protocol, IPDA: Internet Protocol Distributed Architecture).

WBM path

WBM **>** Configuration **>** LAN Interfaces **>** SIP Interface

The *SIP Interface Settings* dialog is displayed: You can activate or deactivate the SIP interface and select the LAN/Ethernet interface used for it in this dialog.

Dropdown lists and input fields

The following dropdown lists are shown in this dialog:

- *SIP LAN Redundancy*: The Redundant SIP interface can be activated or deactivated. Choose the required setting in the dropdown list:
  - Possible values: *On*, *off*
  - Default: *Off* (deactivated)
- *SIP LAN Interface*: The required Ethernet interface can be selected. The default is "Default IPDA" however any available interface from the drop down list can be chosen.

IMPORTANT: The same LAN/Ethernet interface must not be used for the SIP interface and the Management interface!

IMPORTANT: OpenScape 4000 SoftGate must be restarted in order to activate all configuration changes.

Buttons

The following buttons are shown in this dialog:

- *Apply:* The input is saved. OpenScape 4000 SoftGate must be restarted to activate the changes.
- *Undo:* The input is rejected and the default restored.

3.7 Miscellaneous

WBM path

WBM **>** Configuration **>** Miscellaneous

The Miscellaneous menu opens:

Menu Miscellaneous

The following selection options are offered in this menu:

Fax Parameters

NGS

QoS Data Collection

3.7.1 Fax Parameters

WBM path

WBM **>** Configuration **>** Miscellaneous **>** Fax Parameters

The *Fax Parameters* dialog is displayed: You can define fax parameters for T.38 fax machines in this dialog. The ITU-T T.38 recommendation makes it possible to transmit faxes in real time via a packet-switched network, e.g. the Internet. To do this, the IFP (Internet Facsimile Protocol) is used, which is based on UDP or TCP and IP (UDP: User Datagram Protocol, TCP: Transmission Control Protocol).

The parameters for Fax are used for the complete SoftGate.

Dropdown lists, input fields, check boxes

The following settings are shown in this dialog:

- T.38 Fax:
  - *Max. UDP Datagram Size (bytes):* Shows the maximum size of a T.38 UDP datagram in bytes.
  - *Error Correction Used (UDP):* Defines the methods for error correction that should be used (*t38UDPRedundancy* or *t38UDPFEC*).
  - *Error Correction Mode*: If this check box is enabled, one of the two error correction mechanisms available to the T.38 fax protocol via UDP is selected. Both mechanisms are intended to enable successful fax transmissions without errors even in cases where restricted packet losses occur in the network.
  - *Open the Fax Channel with detected Tone:* Dial tone sent by vHG 3575 (Enterprise Gateway) to the fax machine. When it receives this tone, the fax machine dials the number.
  - *Number of Redundancy Packets:*The number of redundancy packets selected for the error correction mechanism can be selected. The larger the value, the greater the protection for fax transmissions against packet losses in the network. Please note, however, that larger values also increase the bandwidth requirements. Values available for selection: 0, 1, 2
  - *Maximum Network Jitter (ms)*: If the maximum network jitter is known, enter it in this field. This helps reduce the transmission time for some fax devices. The value must be entered as a decimal figure. Value range: 140 msec - 500 msec. Default: 200 msecs.
- Other:
  - *ClearMode (ClearChannelData)*: It can be defined whether the Clear Channel Codec as per RFC4040 is to be used in the RTP data packets.
  - *Frame Size*: The size of the frame for the Clear Channel Codec can be defined.

Buttons

The following buttons are shown in this dialog:

- *Apply:* The input is saved.
- *Undo:* The input is rejected and the default value restored.

Procedure

To define the fax parameters, perform the following steps:

1) Make the required settings, see Section *"*Dropdown lists, input fields, check boxes*"*.
2) Click *Apply* and then click *OK* in the confirmation dialog. The changed data is incorporated into the configuration.

3.7.2 NGS

The NextGen Service (NGS) Webservice solution transmits several configuration data from the central NGS server to the SoftGates such as IPv6 addresses, SNMP config data or the IP address of the CiCa.

WBM path

WBM **>** Configuration **>** Miscellaneous **>** NGS

The *NGS Settings* dialog is displayed.

> **IMPORTANT:** OpenScape 4000 SoftGate must be restarted in order to activate all configuration changes.

You can deactivate the usage of the NGS service for scenarios where a HTTPS connection to the NGS server is not possible, e.g. in DMZ.

Input fields

The following input fields are shown in this dialog:

- *IP Address of NGS Server [IPv4 or IPv6]*: The IP address can be entered in the format IPv4 or IPv6. The default format is IPv4: 0.0.0.0.

Buttons

The following buttons are shown in this dialog:

- *Apply:* The input is saved. OpenScape 4000 SoftGate must be restarted to activate the changes.
- *Undo:* The input is rejected and the default value restored.

3.7.3 QoS Data Collection

Quality of Service Data Collection (QDC) - tasks and functions:

The OpenScape IP service "QoS Data Collection" is a tool which collects data on OpenScape products. This data is used to analyze the voice and network quality of the products.

With its range of features, the QoS Data Collection service aims to:

- reduce general expenses for QoS problem analysis
- increase the remote clearance rate

- detect network malfunctions in good time in order to prevent voice quality problems

This results in:

- reduced service outlay
- competitive maintenance contracts
- quick and qualified responses to customer problems
- increased general customer satisfaction with products and technologies
- the possibility to identify changes in the customer network environment and to align the marketing activities of OpenScape services accordingly

By using QDC, key improvements can be achieved in the entire service (break/ fix) process.

Background Information on QDC

Please refer to *OpenScape 4000 V8, Gateways HG 3500 and HG 3575, Administrator Documentation.*

WBM path

WBM **>** Configuration **>** Miscellaneous **>** QoS Data Collection

The *Quality of Service Data Collection* dialog is displayed.

Selection and Input Fields

The following fields can be edited:

QDC Configuration

- *Send to QCU*: Enable this check box if you want to send data to the QCU. Default value: Check box not activated.
- *QCU IP Address*: Enter the IP address or the name of the QCU host here. Default value: 0.0.0.0.
- *QCU Receiving Port*: Receive port for QCU. Enter the port number for the QCU host here. Default value: 12010.
- *Send to Network Management enabled*: Enable this check box if you want to send data to the Network Management system. Default value: Check box not activated.
- *IP Address of Network Management*: Enter the IP address or name here. Default value: 0.0.0.0.
- *Community String*: n/a

> **IMPORTANT:** If one of the check boxes **Send to QCU** or **Send to Network Management enabled** is activated (checked), QoS reports will be generated.

QDC Report Mode

- *Send Report if*: Select the send time for the report from the list box. The following options are available:
  - *End of session and threshold exceeded*: A report will only be sent at the end of a session and only if the threshold is exceeded.
  - *End of report interval and threshold exceeded*: A report will be sent for each report interval once the threshold has been exceeded.
  - *End of session, unconditional*: A report is always sent when the session ends.
  - *End of report interval, unconditional*: A report is always sent at the end of a reporting interval.
- *Report Interval (sec)*: Enter the interval (in sec.) at which the reports should be sent. A QoS report will be sent for each report interval if the report mode is set correspondingly. Default value: 60 sec. Valid values: 0 ... 65535
- *Observation Period (sec)*: This parameter cannot be adjusted. Default value: 10 sec.
- *Minimum Session Length (* 100 msec)*: Enter the minimum session length (* 100 msec) here. A QoS report will not be sent if a session (for example, a call) is shorter than the set minimum value. Default value: 20 (2 sec) Valid values: 0 ... 255

IMPORTANT: The time scale is segmented during the observation period and the report interval. Each observation period is checked to monitor if the threshold has been exceeded. A QoS report will be sent for each report interval if the corresponding report mode setting is enabled.

QDC Threshold Values

- *Upper Jitter Threshold (msec)*: In this field, enter the upper threshold value for report generation. The jitter is checked to monitor if this threshold has been exceeded and is measured in the time between two consecutive RTP packets.

  Default value: 20 msec

  Valid values: 0 ... 255
- *Average Round Trip Delay Threshold (msec)*: Round trip delay reflects the total runtimes in both directions. , ; In this field, enter a threshold value for the average round trip delay that results in report generation.

  Default value: 100msec

  Valid values: 0 ... 65535
- *Thresholds Values (for) Compression Codec*: In this field, enter the required number of packets for the compression codec thresholds. The following options are available:
  - *lost packets (per 1000 packets)*: In this field, enter a threshold value for the packets lost during voice decoding. This value represents the packet loss in relation to the total number of packets.

    Default value: 10

    Valid values: 0 ... 255
  - *consecutive lost packets*: In this field, enter a threshold value for consecutive lost packets. The number of consecutive packets lost (uninterrupted

by "good" packets) is counted. If the value counted is greater than the value specified, the threshold has been exceeded.

Default value: 2

Valid values: 0 ... 255

  - *consecutive good packets*: In this field, enter a threshold value for consecutive good packets. The number of consecutive "good" packets (uninterrupted by lost packets) is counted. If the value counted is less than the value specified, the threshold has been exceeded.

    Default value: 8

    Valid values: 0 ... 255

- *Thresholds Values (for) Non-Compression Codec*: In this field, enter the required number of packets for the non-compression codec thresholds. The following options are available:
  - *lost packets (per 1000 packets)*: For a description see *Thresholds Values (for) Compression Codec*.
  - *consecutive lost packets*: For a description see *Thresholds Values (for) Compression Codec*.
  - *consecutive good packets*: For a description see *Thresholds Values (for) Compression Codec*.

  Description and application of compression and non-compression codecs:

Table 1: Codec - Types

Codec	Audio Mode	Application
High quality preferred	Uncompressed voice transmission.	Use uncompressed voice transmission. Suitable for broadband intranet connections.
Low bandwidth preferred	Use compressed voice transmission (preferred).	Suitable for connections with different bandwidths.
Low bandwidth only	Use compressed voice transmission only.	Suitable for connections with low bandwidth.

Click *Apply* followed by *OK* in the confirmation dialog (save the new configuration status permanently with the Save icon in the control area). The *Quality of Service Data Collection* dialog is displayed.

Buttons

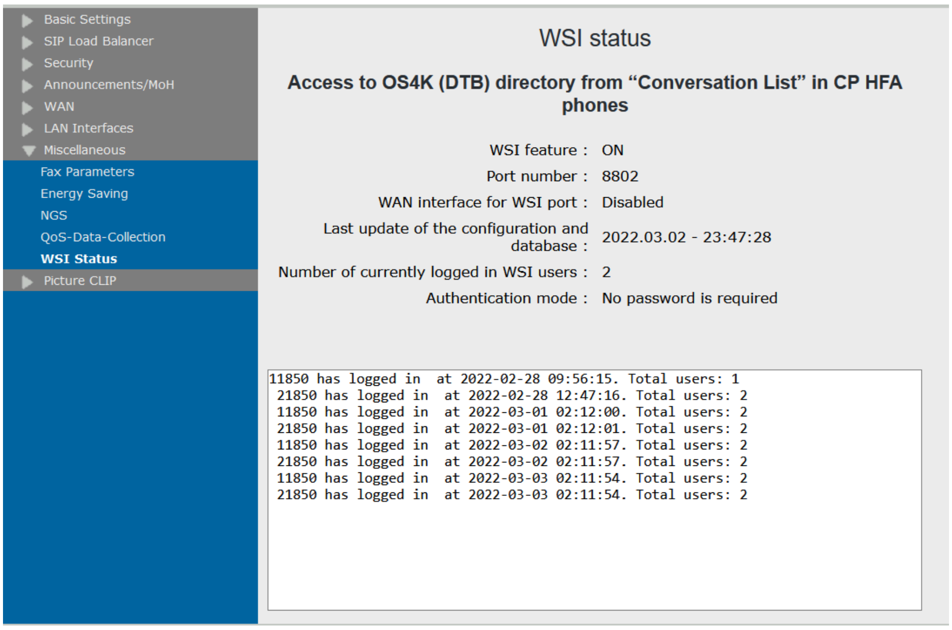
The following buttons are shown in this dialog:

- *Apply:* The input is saved. OpenScape Access 500i/a and/or OpenScape 4000 SoftGate must be restarted to activate the changes.
- *Undo:* The input is rejected and reset to the default value.

3.7.4 WSI Status

This page displays the central configuration of the WSI created on the platform Portal of the central host as well as further information about the status of the WSI users, as follows:

- Last update of the configuration and database: the date and time when the SoftGate synchronized the configuration and the database with the central Portal
- Number of currently logged in WSI users
- Log-book of WSI user activity: displays the authenticated/unauthenticated WSI users and the time of the login/logout.



WSI status

Access to OS4K (DTB) directory from "Conversation List" in CP HFA phones

WSI feature : ON
Port number : 8802
WAN interface for WSI port : Disabled
Last update of the configuration and database : 2022.03.02 - 23:47:28
Number of currently logged in WSI users : 2
Authentication mode : No password is required

```
11850 has logged in  at 2022-02-28 09:56:15. Total users: 1
 21850 has logged in  at 2022-02-28 12:47:16. Total users: 2
 11850 has logged in  at 2022-03-01 02:12:00. Total users: 2
 21850 has logged in  at 2022-03-01 02:12:01. Total users: 2
 11850 has logged in  at 2022-03-02 02:11:57. Total users: 2
 21850 has logged in  at 2022-03-02 02:11:57. Total users: 2
 11850 has logged in  at 2022-03-03 02:11:54. Total users: 2
 21850 has logged in  at 2022-03-03 02:11:54. Total users: 2
```

Figure 1: WSI Status

To change the WSI configuration, see the OpenScape 4000 V10, Platform Administration (Portal), Administrator Documentation.

NOTICE:

On a CP HFA phone, the following fields must be left blank when the phone is connected to OS4K, for WSI to work properly:

- UC user name from UC credentials menu;
- UC password from UC credentials menu;
- UC server address form UC Server menu.

3.8 Picture CLIP

WBM path

WBM > Configuration > Picture CLIP

The Picture CLIP menu opens:

Menu Miscellaneous

The following selection options are offered in this menu:

Settings

Test

Description of features

The "Picture CLIP" feature allows you to configure the parameters for direct or indirect retrieval of telephone pictures stored either in the LDAP directory (direct retrieval) or on an external directory server (indirect retrieval).

The "PIcture CLIP" feature provides the option of showing centrally stored contact data (name and picture) of the remote telephone party on an IP phone's display during the call.

In order to display centrally stored contact data, the OpenStage phones request the data from a OpenScape 4000 SoftGate which then forwards the request to a central directory server, retrieves the data and makes it available to the OpenStage phones.

The display format (positioning, style, size etc.) of the contact data remains the same as for local phonebook lookup, since the same mechanisms are used.

The directory server is queried for all numbers. If an entry for the number is found on the LDAP directory server, the name and picture from the directory server are displayed. If there is no entry for the number in the directory server, the name from the local phonebook is displayed.

> **NOTICE:** In the case of an outgoing call from the phone, the picture for the called contact is not shown, because the call icon (e.g. free, busy, forwarding symbol, etc.) must be displayed in this case.

Two different modes for picture retrieval are currently supported:

Direct Picture Retrieval

Preconditions:

- Direct picture retrieval configured.
- Contact data with picture stored on LDAP server.

=> The user sees the name and picture of the remote party as stored in the LDAP directory.

The OpenStage phone performs a lookup on the OpenScape 4000 SoftGate. The OpenScape 4000 SoftGate forwards the request to the LDAP server and receives the name and picture of the requested phone number in return. The name and picture are then forwarded together by the OpenScape 4000 SoftGate to the OpenStage phone and shown on the display.

Indirect Picture Retrieval

Preconditions:

- Indirect picture retrieval configured.

- Contact data stored on LDAP server with valid reference to a picture stored on another web server.

=> The user sees the name of the remote party as stored in the LDAP directory and the picture as stored on the web server.

The OpenStage phone performs a lookup on the OpenScape 4000 SoftGate. The OpenScape 4000 SoftGate forwards the request to the LDAP server and receives the name and an URL of the web server with the relevant photo ID where the picture is stored. In the next step, the OpenScape 4000 SoftGate receives the picture on the basis of the previously received URL and photo ID. The name and picture are then forwarded together by the OpenScape 4000 SoftGate to the OpenStage phone and shown on the display.

Picture CLIP - Service Information

- This feature is supported for OpenScape 4000 SoftGate and OpenScape Access 500.
- If no picture is available, only the name and number from the LDAP directory entry are displayed.
- If the LDAP directory server is not available, the PBX name is displayed after a timeout.
- Only OpenStage 60/80 HFA support this feature.
- The OpenStage phones have to be able to access the OpenScape 4000 SoftGate, which is configured for Picture CLIP. The OpenStage phones therefore do not necessarily have to be configured on the respective OpenScape 4000 SoftGate or OpenScape Access 500.
- The OpenStage phones only accept pictures encoded in jpg and of max. 50k in size.
- An LDAP directory server is required for central storage of the contact data and pictures. A Webserver is required additionally for indirect retrieval of pictures.
- The contact data is stored on the LDAP directory server using the keys that were configured on the OpenScape 4000 SoftGate via WBM.
- It is recommended that the telephone numbers are stored in a fully qualified format including country code and area code (e.g. 4989700754321). If the numbers are stored using separators such as brackets, dashes or plus signs (e.g. +49 (89) 7007-54321), then the LDAP directory server has to apply conversion rules when checking for a match. The OpenStage phone issues an LDAP query using plain digits without separators.
- The contact data from the LDAP directory server is only shown in some cases after a short delay, because a secure connection has to be established to the OpenScape 4000 SoftGate via https. During this time, the display entry provided by the OpenScape 4000 system may become visible briefly. In indirect retrieval mode, a further request/response cycle is needed to retrieve the picture.

3.8.1 Settings

WBM path

WBM **>** Configuration **>** Picture CLIP > *Properties*

The *Picture CLIP Settings*dialog is displayed.

Dropdown lists and input fields

The following dropdown lists/input fields are shown in this dialog:

Field	Description
LDAP-Server-Einstellungen (LDAP Server Properties)	
LDAP Server URL	The URL (including protocol and port) for accessing the Directory Server
User DN	LDAP account
Password	Password
LDAP-Basisknoten (LDAP Basic Node)	Node where the contact data is saved
Search from	Path where the contact data is saved
LDAP key	
Büronummer (Office Phone)	Number of the office telephone
Handynummer (Mobile Phone)	Mobile phone number
Weitere Büronummer (Other Office Phone)	Alternative phone number for office phone
Vornamen (First Name)	Employee's first name(s)
Nachname (Last Name)	Employee's last name
Direkter Bild-Zugriff (Direct Picture Access)	
Picture	Name (key) under which the picture is saved
Indirekter Bild-Zugriff (Indirect Picture Access)	
Bilddateiname (Picture File Name)	File name of picture (for indirect picture access, can remain blank for direct picture access)
URL des -Bilderverzeichnisses (URL of Picture Folder)	URL of folder where the pictures are saved (for indirect picture access, can remain blank for direct picture access)

Buttons

The following buttons are shown in this dialog:

- *Apply:* The input is saved. OpenScape Access 500i/a and OpenScape 4000 SoftGate must be restarted to activate the changes.
- *Undo:* The input is rejected and the default value restored.

3.8.2 Test

You can test if LDAP server access is properly configured.

WBM path

WBM **>** Configuration **>** Picture CLIP > *Test*

The *Test Picture CLIP* dialog is displayed.

Procedure

1) Click the **Open in separate window** button. The *Telephone Number Look Up* window opens.

2) Enter a phone number in the *Telephone Number* input field and click **OK**.

If LDAP server access has been correctly configured and if an entry exists for the phone number in the LDAP directory, a "result" is displayed at the lower margin.

The last and first name can be identified. The subsequent characters indicate that a picture is also available.

If LDAP server access is not configured correctly, a unique error message is issued, for example *Problem connecting to LDAP Server*.

4 Maintenance

The Maintenance module provides features for maintaining and administering OpenScape 4000 SoftGate. These features include software updating, saving configurations, working with log files, activating trace profiles, creating a secure trace, creating diagnostic files and determining status information on OpenScape 4000 SoftGate.

WBM path

WBM **>** Maintenance

The Maintenance module is displayed.

Options in the Maintenance**module**

SW-Update

Backup/Restore

Logs

Trace

LAN Trace

Secure Trace

Diagnostic

Status Information

Reboot / Shutdown OS

4.1 SW-Update

The SW-Update menu (SW: software) provides functions for displaying the software version, for updating software and for activating software in vHG 3575.

WBM path

WBM **>** Maintenance **>** SW-Update

The SW-Update menu is displayed.

SW-Update **menu**

The following options are shown in this menu:

Show SW-Version

LW Update

LW Activation

OS Update

4.1.1 Show SW-Version

WBM path

WBM **>** Maintenance **>** SW-Update **>** Show SW-Version

The *Software Version* dialog is displayed. This dialog contains details of the currently installed software and hardware versions.

Information

The following entries are made here:

- System Version (PBX): This area shows the OpenScape 4000 Version under:

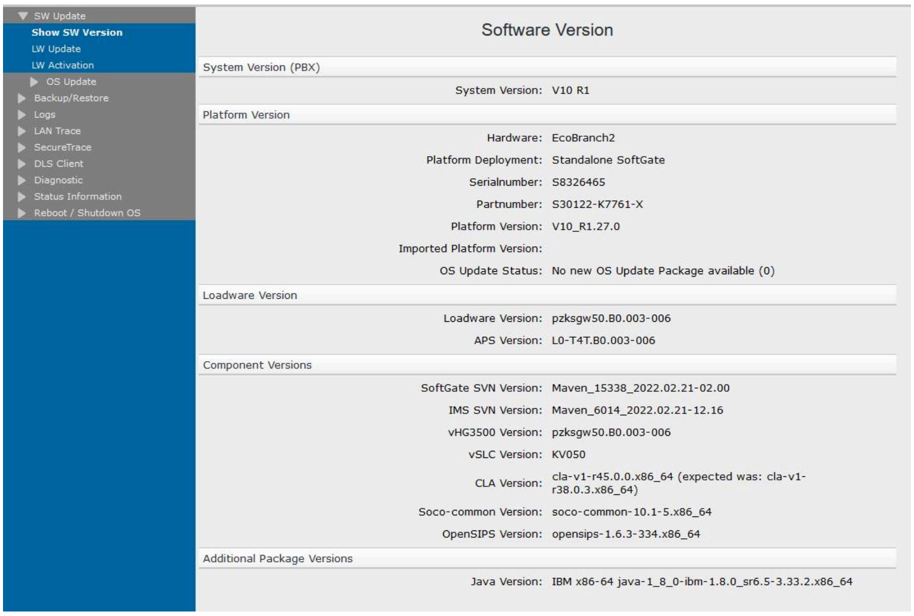
  System Version
- Platform Version: This pane indicates the hardware on which the vHG 3575 (Enterprise Gateway) is running, e.g. OpenScape Access 500. The details include:

  Hardware, *Platform Deployment*, *Platform Version*, *Imported Platform Version*, *OS Update Status*
- Loadware Version: This pane shows the installed software and loadware versions. For example:

  Loadware Version, *APS Version, RTMX Loadware Version.*
- Component Versions: This pane shows the versions of the installed SoftGate components. For example:

  IMS SVN Version, *SoftGate SVN Version*, VSLC Version, *CLA Version*, *Soco-common Version*, *OpenSIPS Version*
- Additional Package Versions: This pane shows any additional software and associated versions required. For example:

  Java Version



Software Version

System Version (PBX)

System Version: V10 R1

Platform Version

Hardware: EcoBranch2

Platform Deployment: Standalone SoftGate

Serialnumber: S8326465

Partnumber: S30122-K7761-X

Platform Version: V10_R1.27.0

Imported Platform Version:

OS Update Status: No new OS Update Package available (0)

Loadware Version

Loadware Version: pzksgw50.B0.003-006

APS Version: L0-T4T.B0.003-006

Component Versions

SoftGate SVN Version: Maven_15338_2022.02.21-02.00

IMS SVN Version: Maven_6014_2022.02.21-12.16

vHG3500 Version: pzksgw50.B0.003-006

vSLC Version: KV050

CLA Version: cla-v1-r45.0.0.x86_64 (expected was: cla-v1-r38.0.3.x86_64)

Soco-common Version: soco-common-10.1-5.x86_64

OpenSIPS Version: opensips-1.6.3-334.x86_64

Additional Package Versions

Java Version: IBM x86-64 java-1_8_0-ibm-1.8.0_sr6.5-3.33.2.x86_64

4.1.2 LW Update

WBM path

WBM **>** Maintenance **>** SW-Update **>** LW Update

The *Loadware Update* dialog is displayed. You can load the SoftGate loadware in this dialog.

Input field

This dialog contains the following input field:

- *Filename:* Enter the path and file name containing the current software in this field. You can also click *Browse* to select the file.

Buttons

The following buttons are shown in this dialog:

- *Load:* The specified file is loaded.
- *Undo:* The path and file name entered are deleted.

Procedure

To load the SoftGate loadware, take the following steps:

1) Enter the path and file name where the current software is stored or click *Browse* to select the file.
2) Click *Load*. The software is loaded. Once the software is loaded, the next WBM page is displayed.

4.1.3 LW Activation

WBM path

WBM **>** Maintenance **>** SW-Update **>** LW Activation

The *Loadware Activation* dialog is displayed. In this dialog, you can activate the loaded SoftGate loadware either immediately, at a specific time in the future, or after a certain amount of time has passed.

Information

The following information is provided in this dialog:

- *Software Version*: Shows the software version for the SoftGate loadware loaded in the *Software Update* dialog.
- *Start Action on*: The SoftGate loadware should be activated at a specific time. The day should be entered using the dropdown lists or via the *Calendar* button.
- *Start Action in*: The SoftGate loadware should be activated after a certain time period.
- *Stop Action*: A previously started action for scheduled activation is stopped.
- *System Time*: This is the local time on OpenScape and the reference time for scheduled activation. This information cannot be edited.

Buttons

The following buttons are shown in this dialog:

- *Apply:* Modifications made to settings are saved.
- *Undo:* Modifications made to settings are deleted and replaced by default values.
- *Start immediately:* Activation of the vHG 3575 (Enterprise Gateway) application is started immediately.

Procedure for immediate activation

To immediately activate the loaded software, follow these steps:

1) Click *Start immediately*. The software is activated.

Procedure for scheduled activation

To schedule activation for the loaded software, follow these steps:

1) Specify time or duration:

- Time when the activation should occur: Select the *Start Action on* radio button and enter the *Day*, *Month*, *Year*, *HH:MM* in the dropdown lists and input fields. You can also use the *Calendar* button.
- Duration after which the activation should occur: Select the *Start Action in* radio button and enter the *Days* and *HH:MM* in the input fields.

2) Click *Apply*. The modifications are saved. The action for scheduled activation is started.

Procedure for stopping the scheduled activation

To stop an action for scheduled activation, follow these steps:

1) Activate the *Stop Action* radio button.

2) Click the *Apply* button. The action is stopped.

4.1.4 OS Update

WBM path

WBM **>** Maintenance **>** SW-Update **>** OS Update

Menu OS Update

The following selection options are offered in this menu:

OS Update Settings

OS Update Actions

4.1.4.1 OS Update Settings

WBM path

WBM **>** Maintenance **>** SW-Update **>** OS Update **>** OS Update Settings

The OS Update Settings dialog is displayed. The transfer parameters from the central host for updating the OS (Operating System) can be defined in this dialog. These settings can only be made for standalone SoftGates and STMIX/ STMIY.

> **IMPORTANT:** These settings are not yet possible for standalone SoftGates in OpenScape 4000 V7R1. The "Remote Appliance Reinstall (RAR)" function should be used instead.

P2P Transfer Parameter from Central Host (only standalone SoftGates and STMIX/STMIY)

- *Limit Max. Download Speed*: Activate/Deactivate check box. The maximum download speed for updating the OS can be limited to a value that is defined in the input field below.
- *Max. Download Speed (KB/s)*: Input field for defining the maximum download speed in KBytes per second.
- *Limit Max. Upload Speed*: Activate/Deactivate check box. The maximum upload speed for updating the OS can be limited to a value that is defined in the input field below.
- *Max. Upload Speed (KB/s)*: Input field for defining the maximum upload speed in KBytes per second.

Buttons

- *Apply*: The input is saved.
- *Undo*: The input is rejected and the default value restored.

4.1.4.2 OS Update Actions

WBM path

WBM **>** Maintenance **>** SW-Update **>** OS Update **>** OS Update Actions

The OS Update Actions dialog is displayed. The transfer from the central host for updating the OS (Operating System) can be canceled in this dialog (only for standalone SoftGates). The OS update can be activated for survivable SoftGates.

> **IMPORTANT:** These settings are not yet possible for standalone SoftGates in OpenScape 4000 V7R1. The "Remote Appliance Reinstall (RAR)" function should be used instead.

OS Update Transfer from Central Host (standalone SoftGates and STMIX/STMIY only)

Button:

- *Cancel Transfer*: Transfer of the OS software is canceled.

OS Update Activation (Surv. SoftGates only)

- *Platform Version*: Indicates the OpenScape 4000 Version.
- *Imported Platform Version*: Indicates the imported OpenScape 4000 Version.
- *Use SoftGate LW from the Update Package (recommended)*: Can be activated/deactivated.
- *OS Update Status*: Indicates whether a new update package is available for the OS.

Button:

- *Activate OS Update*: Activate the OS update for the survivable SoftGate.

4.2 Backup/Restore

In the Backup/Restore menu, you can backup (export) the SoftGate configuration locally. This local backup can be loaded (imported) and activated. The backup contains the local configuration of all active boards within the SoftGate.

WBM path

WBM **>** Maintenance**>** Backup/Restore

The Backup/Restore menu is displayed.

Backup/Restore**menu**

The following options are shown in this menu:

Export Config

Export Sec Config

Import Config

Import Sec Config

4.2.1 Export Config

WBM path

WBM **>** Maintenance **>** Backup/Restore **>** Export Config

The *Export Configuration* dialog is displayed. You can back up (export) the SoftGate configuration locally using this dialog.

Buttons

The following buttons are shown in this dialog:

- *Apply:* Start the configuration export.
- *Undo:* Cancel the configuration export.

Procedure

To export the configuration, follow these steps:

1) Click *Apply*. The configuration is exported to a ZIP file. A *File Download* window appears, asking you to open or save the ZIP file.

2) Click *Save* and select the folder where you wish to store the file. Then click *OK*. The ZIP file is saved.

4.2.2 Export Sec Config

WBM path

WBM **>** Maintenance **>** Backup/Restore **>** Export Sec Config

The *Export Security Configuration* dialog is displayed. You can back up (export) the SoftGate security configuration locally using this dialog.

Buttons

The following buttons are shown in this dialog:

- *Apply:* Start the security configuration export.
- *Undo:* Cancel the security configuration export.

Procedure

To export the security configuration, follow these steps:

1) Click *Apply*. The security configuration is exported to a ZIP file. A *File Download* window appears, asking you to open or save the ZIP file.
2) Click *Save* and select the folder where you wish to store the file. Then click *OK*. The ZIP file is saved.

4.2.3 Import Config

WBM path

WBM **>** Maintenance **>** Backup/Restore **>** Import Config

The *Import Configuration* dialog is displayed. In this dialog, you can import the SoftGate configuration saved locally.

Input field

This dialog contains the following input field:

- *Filename:* Enter the path and file name where the configuration you wish to import is stored in this field. You can also click *Browse* to select the file.

Buttons

The following buttons are shown in this dialog:

- *Load:* The specified configuration file is loaded.
- *Undo:* The path and file name entered are deleted.

Procedure

Proceed as follows to import a configuration file:

1) Enter the path and name of the configuration file or select the file with the *Browse* button.
2) Click the *Load* button. The configuration file is loaded.

> **IMPORTANT:** SoftGate has to be restarted for the configuration changes to take effect.

4.2.4 Import Sec Config

WBM path

WBM **>** Maintenance **>** Backup/Restore **>** Import Sec Config

The *Import Security Configuration* dialog is displayed. In this dialog, you can import the vHG 3575 security configuration saved locally.

Input field

This dialog contains the following input field:

- *Filename:* Enter the path and file name where the security configuration you wish to import is stored in this field. You can also click *Browse* to select the file.

Buttons

The following buttons are shown in this dialog:

- *Load:* The specified file is loaded.
- *Undo:* The path and file name entered are deleted.

Procedure

Proceed as follows to import the security configuration:

1) Enter the path and file name where the security configuration you wish to import is stored or click *Browse* to select the file.
2) Click *Load*. The file is loaded.

IMPORTANT: vHG 3575 has to be restarted for the configuration changes to take effect.

4.3 Logs

In the Logs menu, you can export log files for diagnostic purposes to a ZIP file. To create new log files, you can delete the old (i. e. exported) log files.

WBM path

WBM **>** Maintenance **>** Logs

The Logs menu is displayed.

Logs**menu**

The following options are shown in this menu:

Export Logs

Delete Logs

Trace Profiles

RTMX Trace Profiles

4.3.1 Export Logs

WBM path

WBM **>** Maintenance **>** Logs **>** Export Logs

The *Export Logfiles* dialog is displayed. You can store (export) logs of all active boards of the SoftGate.

Buttons

The following buttons are shown in this dialog:

- *Export:* The log files selected via check box are stored locally (exported).

Procedure

To export log files, follow these steps:

1) Click *Export*. The log files are exported to a ZIP file. A *File Download* window appears, prompting you to open or save the ZIP file.
2) Click *Save* and select the folder where you wish to store the file. Then click *OK*. The ZIP file is saved.

4.3.2 Delete Logs

WBM path

WBM **>** Maintenance **>** Logs **>** Delete Logs

The *Delete Logfiles* dialog is displayed. In this dialog, you can select and delete one or several of the log files listed.

Check boxes

The following check boxes are shown in this dialog:

- *Soco*, *JLM*, *IMS*, ETS, *SPA, Status Collector*, *Update*, *Backtrace*, *Heap Dump*, *Corelogs*, *Garbage Collection*, *Gateway (vHG) Logs, LS-DCL, Load Balancer*, *DHCP, System Diagnostics*
- *All:* All log (diagnostic) files are selected.

Buttons

The following buttons are shown in this dialog:

- *Delete:* All selected log files are deleted.
- *Undo:* Modifications made to settings are deleted and replaced by default values.

Procedure

To delete log files, follow these steps:

1) Enable the check boxes next to the log files you wish to delete.
2) Click *Delete*. The selected log files are deleted.

4.4 Trace

Under Trace, you can activate trace profiles.

WBM path

WBM **>** Maintenance

Trace **menu**

WBM **>** Maintenance **> Logs > Trace profiles**

4.4.1 Profiles

> **NOTICE:** This function may only be used by developers. For standard analysis, we recommend using the functions in the *Diagnostic Files* dialog (see Section 4.8.2, "Diagnostic Files").

WBM path

WBM > Maintenance > Trace > Profiles

The *Edit Trace Profile Configuration* dialog is displayed. In this dialog, you can enable trace profiles for detailed analysis of the SoftGate. Each trace profile records special information.

Trace Profiles

Enable the trace profiles listed here to explore following problems:

- *acw-cc*: Developer-specific
- *announcement: Developer-specific*
- *cg*: Developer-specific
- *dataloading*: Developer-specific
- *dcl2*: Developer-specific
- *debug-all*: Developer-specific
- *dmc-detail*: Developer-specific
- *dls-client:* Developer specific
- ecoap: Developer-specific (Enterprise GW)
- ecoap-light: Developer-specific (Enterprise GW)
- evtlog: Developer-specific
- h323-performance: Developer-specific
- *heap-diag*: Developer-specific
- *hfa-call*: Used for problems with HFA connection signaling and HFA device login/logoff.
- *hfa-reg*: Used for problems with HFA device registration, e. g. faulty displays on the devices.
- *hsr*: Used for problems with the connection between SoftGate and host.
- *hsr-message-dump*: Developer-specific. Affects system performance!
- hsr-message-light: Developer specific
- *ipconfig*: Developer-specific
- *ipv6*: Used if problems occur when networking via IP V6.
- icphone: Developer-specific
- *maintenance*: Developer-specific
- *mmx*: Developer-specific
- *osa*: Trace profile for OpenScape Access
- *osa-clock*: Trace profile for OpenScape Access
- *osa-light*: Trace profile for OpenScape Access
- *osa-trace*: Trace profile for OpenScape Access
- *payload*: Used for problems with voice connections (like *payload-light*). Affects system performance! Due to the creation of comprehensive trace output, this profile may not be enabled in cases of heavy system load.
- *payload-light*: Used for problems with voice connections. Can also be enabled in cases of increased system load. See also paragraph "payload".
- *payload-native*: Developer-specific

- *qdc*: Developer-specific
- *reconnect*: Developer-specific
- *scc*: Used for general payload problems, conference connections and IPDA connections.
- *sigsurv*: Developer-specific
- *sip*: When this trace profile is enabled, the vHG 3575 (Enterprise Gateway) trace messages configured in the local vHG 3575 (Enterprise Gateway) WBM are transferred to the SoftGate log file. At the same time, SIP-relevant scc traces are recorded.
- *siux*: Developer-specific
- *slc*: Developer-specific
- snmp: Developer-specific
- *startup*: Used for boot problems on the SoftGate and virtual boards.
- *sysinfo*: Developer-specific
- *system*: This trace profile is always enabled and cannot be disabled.
- *telnumlookup*: Developer-specific
- *thread-profiling*: Developer-specific
- *vSlma*: Developer-specific
- *vTmom*: Developer-specific
- *wbm*: Developer-specific

Buttons

The following buttons are shown in this dialog:

- *Apply:* The settings for the enabled/disabled check boxes are saved.
- *Undo:* The settings for the enabled/disabled check boxes are reset.
- *Restore Default:* The settings for the enabled/disabled check box is set to default.

Procedure

To enable trace profiles, follow these steps:

1) Select the check box for the trace profile you need for an analysis.

2) Click *Apply*. The settings for the enabled/disabled check boxes are saved.

RTMX Trace Profiles

Enable the trace profiles listed here to explore following:

- conference:
- conference_detailed:
- default:
- siu_all:
- siu_init:
- siu_tds:
- startup_shutdown:
- switching:
- switching_detailed:

4.5 LAN Trace

Under LAN Trace, you can configure settings for monitoring IP connections and create capture files.

WBM path

WBM > Maintenance > LAN Trace

LAN Trace menu is displayed.

LAN Trace menu

The following options are shown in this menu:

- Internal LAN Trace

4.5.1 Internal LAN Trace

WBM path

WBM > Maintenance > LAN Trace > Internal LAN Trace

The Internal LAN Trace dialog is displayed. In this dialog, you can modify settings for IP connection monitoring, internal LAN capture control and SIP LAN Trace.

Areas

The following areas are shown in this dialog:

- Internal LAN Capture Control
- SIP LAN Trace

Buttons

The following buttons are shown in this dialog:

- Apply: Modifications made to settings are saved.
- Undo: Modifications made to settings are deleted and replaced by default values.

4.5.1.1 Internal LAN Capture Control

WBM path

WBM **>** Maintenance **>** *LAN Trace* **>** Pane Internal LAN Capture Control

Settings for internal monitoring of IP package in the LAN can be made in the pane. This monitoring is carried out with tshark or tcpdump for example. The current content is written to the backtrace file in case of a critical restart. Older capture files are deleted when monitoring is started. If these are still needed, you have to export them using Logs**>** Export Logs.

Controls and indicators

This area contains the following controls and indicators:

- Check boxes:
  - *Headers Only:* Only the IP packet headers should be monitored.
  - *Start:* The internal LAN capture control should be started.
  - *LoopBack Interface (only):* Only the LoopBack interface should be used.
- Selection field:
  - *Filter:* You can select a filter for monitoring IP packets. Choose from:
    - *none* (no filter)
    - *tcp* (only Transmission Control Protocol IP packets)
    - *udp* (only User Datagram Protocol IP packets)
- Display:
  - *Status*: The status display indicates whether internal LAN capture control is active.

4.5.1.2 SIP LAN Trace

Control for internal monitoring of IP packages in the SIP LAN is available in the SIP LAN Trace panel.

The SIP LAN Trace will be automatically activated once the LW is updated to the version which supports the feature. This trace can be manually stopped, but after a LW update or board restart, the trace is reactivated. The SIP LAN trace can be downloaded via WBM of SoftGate or STMIX/STMIY (HFA part) from Maintenance\Logs\Export\Logs. The content of the trace is available in the "GW_logs.zip\soco\lantrace.zip" path.

In case of a critical restart, the current content will be saved and moved to the "backtrace" archive and can be downloaded from the same location as the "lantrace" file.

The feature is implemented for:

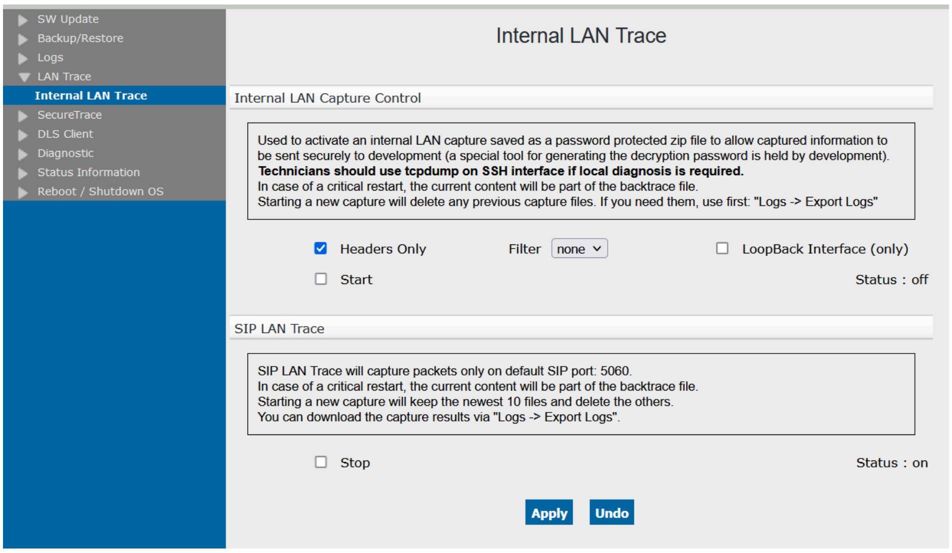
- All SoftGate deployments
- STMIX/STMIY

Location: Maintenance > LAN Trace > Internal LAN Trace.

A new menu was created for this feature under **LAN Trace**.

Internal LAN Capture Control has been moved from **Diagnostic Functions** to **LAN Trace**.

Additional control for switching on/off the permanent SIP LAN trace has been added. By default, the SIP LAN trace is set to ON.



Internal LAN Trace

Internal LAN Capture Control

Used to activate an internal LAN capture saved as a password protected zip file to allow captured information to be sent securely to development (a special tool for generating the decryption password is held by development).
Technicians should use tcpdump on SSH interface if local diagnosis is required.
In case of a critical restart, the current content will be part of the backtrace file.
Starting a new capture will delete any previous capture files. If you need them, use first: "Logs -> Export Logs"

☑ Headers Only   Filter none   □ LoopBack Interface (only)

□ Start   Status : off

SIP LAN Trace

SIP LAN Trace will capture packets only on default SIP port: 5060.
In case of a critical restart, the current content will be part of the backtrace file.
Starting a new capture will keep the newest 10 files and delete the others.
You can download the capture results via "Logs -> Export Logs".

□ Stop   Status : on

Figure 2: Internal LAN Trace

NOTICE: The SIP LAN Trace will capture packets only on the default SIP port 5060.

4.6 Secure Trace

A secure trace is used to detect faults in the communication system. The secure trace produces records via encrypted VoIP payload and signaling streams to and from vHG 3575.

The secure trace contains encrypted records. These records can be decrypted by developers using a key.

WBM path

WBM **>** Maintenance **>** Secure Trace

The Secure Trace menu is displayed.

Secure Tracemenu

The following options are shown in this menu:

Import certificate

Show certificate

State

Start Trace

Stop Trace

Basic procedure for creating a secure trace

To create a secure trace, proceed as follows:

1) The service technician detects a problem in the customer network. Upon consultation with the developer, the necessity of creating a secure trace is determined.

2) The customer is informed of this need and must confirm that they have been informed. The customer orders the creation of a secure trace, including the date and time when the monitoring should start and end.

3) Development creates a pair of keys consisting of a public and a private key. Only one secure trace can be created with this pair of keys. Certificates are applied as follows:

   - The certificate with the private key is strictly confidential and can only be used by authorized developers.
   - The certificate with the public key is provided to the service technician or can be downloaded from the Hi Sat home page (https://hisat.global-intra.net/wiki/index.php/SecureTrace).

4) The service technician informs the customer about the beginning of trace activities. The customer must inform the affected users.

> **IMPORTANT:** Recording calls and connection data is a criminal offence if the affected users have not been informed.

5) The service technician supplies the certificate to the vHG 3575 (Enterprise Gateway) gateway for which the secure trace is being created; see Section 4.6.1, "Import certificate".

6) The service technician activates the secure trace function; see Section 4.6.4, "Start Trace". A secure trace is created. The activation and later deactivation (Section 4.6.5, "Stop Trace") are logged by the communication systems involved.

7) After a secure trace has been created, the customer is informed about the end of trace activities. The service technician removes the certificate from the system.

8) The secure trace is provided to the developer.

9) The developer decrypts the secure trace using the private key. The developer then analyzes the decrypted records.

10) After the analysis is complete, all relevant materials and data must be securely destroyed. This includes the destruction of the private key, preventing unauthorized copies of the secure trace from being decrypted.

4.6.1 Import certificate

WBM path

WBM **>** Maintenance **>** Secure Trace **>** Import certificate

The *Load the Secure Trace Certificate via HTTP* dialog is displayed. You can import a secure trace certificate using this dialog. This certificate is a requirement for creating a secure trace. The service technician receives it from the developer. It contains the public key and must be available in PEM or binary format. The certificate is always valid for a maximum of one month.

Input field

This dialog contains the following input field:

- *Certificate file (PEM or binary)*: Enter the path and name of the file containing the certificate in this input field. You can also click *Browse* to select the file.

Buttons

The following buttons are shown in this dialog:

- *View Fingerprint of Certificate*: You can check the fingerprint to determine whether an unchanged certificate is available or whether it has been modified.
- *Import Certificate from File*: The certificate is imported from the file specified in the above input field.

Procedure

Proceed as follows to import the certificate:

1) Select: *WBM* **>** Maintenance **>** Secure Trace **>** Import certificate. The *Load the Secure Trace Certificate via HTTP* dialog is displayed.

2) Click *Browse* to select the file containing the certificate and confirm by clicking *Open*. The file is loaded.

3) Click *View Fingerprint of Certificate*. A window appears showing the fingerprint of the certificate you wish to import:

   a) Check the fingerprint (hexadecimal figure). When the certificate is changed, the fingerprint always changes. Only an unchanged fingerprint guarantees an unchanged certificate. If the two fingerprints are not identical, an attack was probably attempted. In this case, the key should no longer be used and the specified measures should be taken.

   b) Click *OK* to close the fingerprint window.

4) Click *Import Certificate from File* if you are satisfied with your examination of the fingerprint. Do not import the certificate if the fingerprint does not satisfy your expectations.

A secure trace can now be created.

4.6.2 Show certificate

WBM path

WBM **>** Maintenance **>** Secure Trace **>** Show certificate

The *Certificate Information* dialog is displayed. In this dialog, you can see the secure trace certificate, e. g. to test it.

Displayed data

The following certificate data is displayed:

- General data: *Certificate Name*, *Certificate Type*, *Serial Number of Certificate*, *Serial Number of Certificate (hex)*, *Type of Signature Algorithm*, *Start Time of Validity Period (GMT)*, *End Time of Validity Period (GMT)*, *CRL Distribution Point*
- *Issued by CA*: *Country (C)*, *Organization (O)*, *Organization Unit (OU)*, *Common Name (CN)*
- *Subject Name*: *Country (C)*, *Organization (O)*, *Organization Unit (OU)*, *Common Name (CN)*
- *Subject Alternative Name*
- *Public Encryption Key Data*: *Public Key Length*, *Public Key*, *Fingerprint*

4.6.3 State

WBM path

WBM **>** Maintenance **>** Secure Trace **>** State

The *Secure Trace State* dialog is displayed. In this dialog, you can find out whether a secure trace is being created.

Displayed data

The following data is displayed:

- *Secure Trace is active*: This line shows if a secure trace is currently being created.
- *Automatic Deactivation Time*: This line shows when the secure trace is to be created and when the secure trace function will be automatically deactivated.
- *Secure Trace for these protocols*: This line shows the protocols for which the secure trace was created. These may be: Media Server (SRTP).

4.6.4 Start Trace

WBM path

WBM **>** Maintenance **>** Secure Trace **>** Start Trace

The *Start Secure Trace* dialog is displayed. You can start the secure trace in this dialog. The following requirements must be met:

- The secure trace is not yet active.
- The customer has authorized the creation of a secure trace and wishes to enter their *Secure Trace Activation Passphrase* in the WBM.
- You have received a public key from the developer and loaded it to the WBM.

Input fields and check boxes

- *Start Parameters*:
  - *Secure Trace Activation Passphrase*: To limit the usage of the secure trace function, activation is secured by a special passphrase known only to the customer. This passphrase is the customer's key and the certificate is the service technician's key. Both keys are required to activate the secure trace function.

    Passphrases are passwords that consist of multiple words up to a maximum length of 20 characters.
  - *Duration of Secure Trace (Mins.)*: You must enter the duration of the secure trace in minutes.
- *Secure Trace protocols*:
  - *MMX (PEP) - used for*: The secure trace is created for MMX. The PEP (Protocol Extension Protocol) enhances HTTP for applications such as HTTP clients, servers and proxy servers.
  - *MediaServer (SRTP)*: The secure trace is created for MediaServer. The SRTP (Secure Real-Time Transport Protocol) is used for encrypted transmission via IP-based networks and uses AES (Advanced Encryption Standard) for encryption.

Buttons

The following button is shown in this dialog:

- *Start Secure Trace*: This starts the secure trace. The requirements named in this document must be fulfilled to start the secure trace.

Procedure

Proceed as follows to start the secure trace:

1) Check if the requirements named earlier have been fulfilled.
2) Select: *WBM* **>** Maintenance **>** Secure Trace **>** Start Trace. The *Start Secure Trace* dialog is displayed.
3) In the *Start Parameters* area, enter the *Secure Trace Activation Passphrase* and the *Duration of Secure Trace (Mins.)*.
4) Select the *MediaServer (SRTP)* protocol.
5) Click the *Start Secure Trace* button. The secure trace is created for the duration specified.

4.6.5 Stop Trace

WBM path

WBM **>** Maintenance **>** Secure Trace **>** Stop Trace

The *Stop Secure Trace* dialog is displayed. In this dialog, you can stop an active secure trace, even if the duration specified under Start Trace has not yet elapsed.

Button

The following button is shown in this dialog:

- *Stop Secure Trace*: The secure trace is stopped.

4.7 DLS Client

The DLS client is used for administration of PKI data and the QDC configuration (DLS: **D**ep**l**oyment **S**ervice or **D**eployment and **L**icencing **S**erver, PKI: **P**ublic **K**ey **I**nfrastructure, QDC: **Q**uality of Service **D**ata **C**ollection).

WBM path

WBM **>** Maintenance **>** DLS Client

The DLS Client menu opens:

Menu DLS Client

The following selection options are offered in this menu:

DLS Client

Enter PIN

Reset Bootstrapping

Contact DLS

Bootstrapping

Bootstrapping allows a secure, certificate-based SSL connection to be established between the DLS server and DLS client.

Based on a connection request from the DLS client to a DLS server as well as the subsequent response - i.e. still an unreliable connection - a reliable connection is established through the alternating authentication and exchange of certificates (i.e. bootstrapping = a simple system develops inherently into a complex system).

Because a different DLS server can respond to the connection request from the DLS client instead of the desired DLS server in order to take the desired connection for itself, security measures must be put in place. The DLS server (i.e. its IP address and port) that is to contact the DLS client can be administered using the AMO.

It is recommended to authorize the DLS client at the DLS server by entering a bootstrap pin on the vHG 3575 WBM, which was previously generated randomly by the DLS server. Authorization of the DLS client can also be performed with an internal standard system PIN that does not have to be entered, or PIN authorization can also be relinquished completely. These two options are not recommended however.

The certificates are exchanged once the reliable connection has been established, see below.

Certificate generation and distribution for communication between the DLS client and DLS server:

All certificates and private keys for encrypted communication between the DLS client and DLS server are generated by the DLS server's self-signing certification authority (CA) and sent by the DLS server during bootstrapping to the DLS client.

The PKCS#12 file sent from the DLS server to the DLS client contains the DLSC client certificate, the private key contained in it and the certificates of the DLS server's certification authority (DLSC CA certificate). The DLS server can read all certificates it delivers apart from the private key.

Certificate generation and distribution for the secure connection between WBM and the DLS server:

The administrator manually sends the WBM certificate containing the private key generated by the customer's PKI certification authority to OpenScape 4000 Assistant. OpenScape 4000 Assistant then automatically sends its WBM certificate to all gateways. The DLS client uses this certificate to identify itself at the DLS server.

4.7.1 DLS Settings

Apart from automatic registration of the DLS client at the DLS server with the ContactMe response, the DLS client can also be registered manually. To do this, you need the IP address and port of the DLS server for bootstrapping mode. The IP address and the port of the DLS server can be configured using the AMO. This change only becomes effective after restarting the SoftGate.

Once the IP address and port of the DLS server have been set, another attempt is made when the system reboots (and each subsequent reboot) to initiate bootstrapping by sending a connection request.

Other connection setup attempts can be initiated manually with the menu option *Contact DLS*. If bootstrapping has still not been performed, it is initiated automatically, otherwise it is simply checked whether the DLS is accessible.

WBM path

WBM **>** Maintenance **>** DLS Client **>** DLS Settings

The *Edit DLS Client Basic Setup* dialog opens.

Input field

The following input field is shown in the *Current DLS Client Basic Configuration* area:

- *Time interval for ContactMe Response*: Amount of time the DLS client waits after sending its connection request to receive the ContactMe response from the DLS server. The wait time must be restricted so that ContactMe responses cannot be intercepted by unwanted DLS servers.

Displays

The following displays are shown in this dialog:

- *Current DLS Client Basic Configuration*:
- – *PIN required for DLS Bootstrapping*: The PIN can be entered under the menu option Enter PIN. *Yes*: A PIN was entered. *No*: No PIN was entered.
  – *Secure Communication with DLS Server*: *Enabled* or *Disabled*
- *Current DLS Client Server Configuration*:
- – *IP Address of DLS Server*: The IP address of the DLS server for bootstrapping mode can be configured using the AMO. You must restart the SoftGate.
  – *Port of DLS Server*: The port of the DLS server for bootstrapping mode can be configured using the AMO. You must restart the SoftGate and Enterprise Gateway.
  – *Secure Port of DLS Server*: vHG 3575 (Enterprise Gateway) port for secure connection to the DLS server.

Buttons

The following buttons are shown in this dialog:

- *Apply:* The modified settings are saved.
- *Undo:* The modified settings are rejected and the default value is restored.

4.7.2 Enter PIN

WBM path

WBM **>** Maintenance **>** DLS Client **>** Enter PIN

The *Enter the Bootstrap PIN* dialog opens. The bootstrap PIN generated randomly by the DLS server can be entered in this dialog.

Input field

The following input field is shown in this dialog:

- *Bootstrap PIN*: If a PIN was entered in this input field and saved by clicking *Apply*, the *Edit DLS Client Basic Setup* dialog (menu option DLS Settings) shows that a PIN is required for DLS bootstrapping.

Buttons

The following buttons are shown in this dialog:

- *Apply:* The modified settings are saved.
- *Undo:* The modified settings are rejected and the default value is restored.

4.7.3 Reset Bootstrapping

WBM path

WBM **>** Maintenance **>** DLS Client **>** Reset Bootstrapping

The *Reset DLS Client Bootstrapping* dialog opens.

Button

The following button is shown in this dialog:

- *Reset Bootstrapping*: Bootstrapping for the DLS client is reset.

4.7.4 Contact DLS

Additional attempts to set up a connection to the DLS server can be initiated manually with the menu option *Contact DLS*. If bootstrapping has still not been performed, it is initiated automatically, otherwise it is simply checked whether the DLS is accessible.

WBM path

WBM **>** Maintenance **>** DLS Client **>** Contact DLS

The *Contact DLS* dialog opens.

Contact DLS menu

The following selection options are offered in this menu:

DLSC Keycert

DLSC CA Certs

Contact DLS dialog

The following button is shown in this dialog:

- *Contact*: The DLS server is contacted in order to check whether it is still available.

4.7.4.1 DLSC Keycert

The DLSC client certificate with the private key can be found under this menu option. The DLS client uses these certificates to identify itself at the DLS server. The DLS client receives the certificate from the DLS server in bootstrapping mode.

WBM path

WBM **>** Maintenance **>** DLS Client **>** DLSC Keycert

The DLSC Keycert menu opens:

Menu DLSC Keycert

The individual DLSC client certificates can be selected under this menu option:

1. DLSC Keycert

4.7.4.2 1. DLSC Keycert

WBM path

WBM **>** Maintenance **>** DLS Client **>** DLSC Keycert **>** 1. DLSC Keycert

The *Certificate Information* dialog opens.

Data displayed

The following data from the certificate is shown:

- General data: *Certificate Type*, *Serial Number of Certificate*, *Serial Number of Certificate (hex)*, *Type of Certificate Algorithm*, *Start Time of Validity Period (GMT)*, *End Time of Validity Period (GMT)*, *CRL Distribution Point*
- *Issued by CA*: *Country (C)*, *Organization (O)*, *Organizational Unit (OU)*, *Common Name (CN)*
- *Subject Name*: *Country (C)*, *Organization (O)*, *Organizational Unit (OU)*, *Common Name (CN)*
- *Subject Alternative Name*
- *Public Key Encryption Data*: *Public Key Length (parameter)*, *Public Key*, *Fingerprint*

4.7.4.3 DLSC CA Certs

This folder contains the DLSC CA certificates delivered by the DLS server in bootstrapping mode.

WBM path

WBM **>** Maintenance **>** DLS Client **>** DLSC CA Certs

The DLSC CA Certs menu opens:

Menu DLSC CA Certs

The individual DLSC client certificates can be selected under this menu option:

"1. DLSC CA Cert", "2. DLSC CA Cert"

4.7.4.4 "1. DLSC CA Cert", "2. DLSC CA Cert"

WBM path

WBM **>** Maintenance **>** DLS Client **>** DLSC Keycert **>** "1. DLSC CA Cert", "2. DLSC CA Cert"

The *Certificate Information* dialog opens.

Data displayed

The following data from the certificate is shown:

- General data: *Certificate Type*, *Serial Number of Certificate*, *Type of Certificate Algorithm*, *Start Time of Validity Period (GMT)*, *End Time of Validity Period (GMT)*, *CRL Distribution Point*
- *Issued by CA*: *Country (C)*, *Organization (O)*, *Organizational Unit (OU)*, *Common Name (CN)*
- *Subject Name*: *Country (C)*, *Organization (O)*, *Organizational Unit (OU)*, *Common Name (CN)*
- *Subject Alternative Name*
- *Public Key Encryption Data*: *Public Key Length (parameter)*, *Public Key*, *Fingerprint*

4.8 Diagnostic

Under Diagnostic, you can configure settings for monitoring IP connections and create diagnostic files.

WBM path

WBM **>** Maintenance **>** Diagnostic

The Diagnostic menu is displayed.

Diagnostic **menu**

The following options are shown in this menu:

Diagnostic Functions

Diagnostic Files

4.8.1 Diagnostic Functions

WBM path

WBM **>** Maintenance **>** Diagnostic**>** Diagnostic Functions

The *Diagnostic Functions* dialog is displayed. In this dialog, you can modify settings for IP connection monitoring, for thread profiling and for heap monitoring.

Areas

The following areas are shown in this dialog:

Thread Profiling

Heap Monitoring

Buttons

The following buttons are shown in this dialog:

- *Apply:* Modifications made to settings are saved.
- *Undo:* Modifications made to settings are deleted and replaced by default values.

4.8.1.1 Thread Profiling

WBM path

WBM **>** Maintenance **>** Diagnostic**>** Diagnostic Functions **>** Thread Profiling area

Thread profiling can be used to check whether threads fully utilize the CPU as planned. This means that threads where low CPU utilization is expected should meet this expectation.

Controls and indicators

This area contains the following controls and indicators:

- Check boxes:
  - *Start:* Thread profiling should be started.
- Input fields:
  - *Sample Rate, ms (100-500):* You can set the sample rate, with the default setting at 250.
  - *Thread CPU Load Threshold for Stacktrace, % (10-90):* You can set the maximum CPU usage; default: 50.
- Display:
  - *Status*: This shows whether thread profiling is active.

4.8.1.2 Heap Monitoring

WBM path

WBM **>** Maintenance **>** Diagnostic**>** Diagnostic Functions **>** Heap Monitoringarea

Create a heap dump to write all objects in the heap to a file.

Controls and indicators

This area contains the following controls and indicators:

- Check boxes:
  - *Start:* Start heap monitoring.
- Input fields:
  - *Sample Rate, ms (500-5000):* You can set the sample rate, with the default setting at 1000.
  - *Memory Usage Threshold for Heapdump, % (50-90):* You can set the amount of memory to be used for the head dump; default: 80.

- Display:
  - *Status*: This shows whether heap dump monitoring is active.

4.8.2 Diagnostic Files

WBM path

WBM **>** Maintenance **>** Diagnostic **>** Diagnostic Files

The Diagnostic Files dialog is displayed.

Log files are stored on the RAM disk, i. e. on a virtual temporary data medium in the main memory. These log files can be exported and unpacked in an archive file. A backup trace file contains the content of the stack at the time of generation.

Buttons

The following buttons are shown in this dialog:

- *Create Heap Dump:* Creates a file containing all Java objects reachable at the moment of creation. You can use this file to analyze main memory usage.

NOTICE: The Backtrace archive file (content of RAMDISK/ramdisk.zip) contains all log files stored on the RAM disk and is now included in the ordinary log export.

4.9 Status Information

WBM path

WBM **>** Maintenance **>** Status Information

The Status Information menu is displayed.

Status Information**menu**

The following options are shown in this menu:

System Information

Connection Control

H323 Status

HFA WAN Clients

4.9.1 System Information

WBM path

WBM **>** Maintenance **>** Status Information **>** System Information

The System Information menu is displayed:

System Information**menu**

The following options are shown in this menu:

Show Thread Health

Peripheral Boards details

Peripheral Boards Info

OpenScape Access Clocking

AP Emergency

4.9.1.1 Show Thread Health

NOTICE: This function may only be used by developers.

WBM path

WBM **>** Maintenance **>** Status Information **>** System Information **>** Show Thread Health

The *Thread Health* table is displayed. This table displays currently active threads. The following information is displayed: *Thread Name*, *Thread ID*, *Context Class Hashcode*, *time blocked [ms]*, *max. time blocked [ms]*.

4.9.1.2 Peripheral Boards details

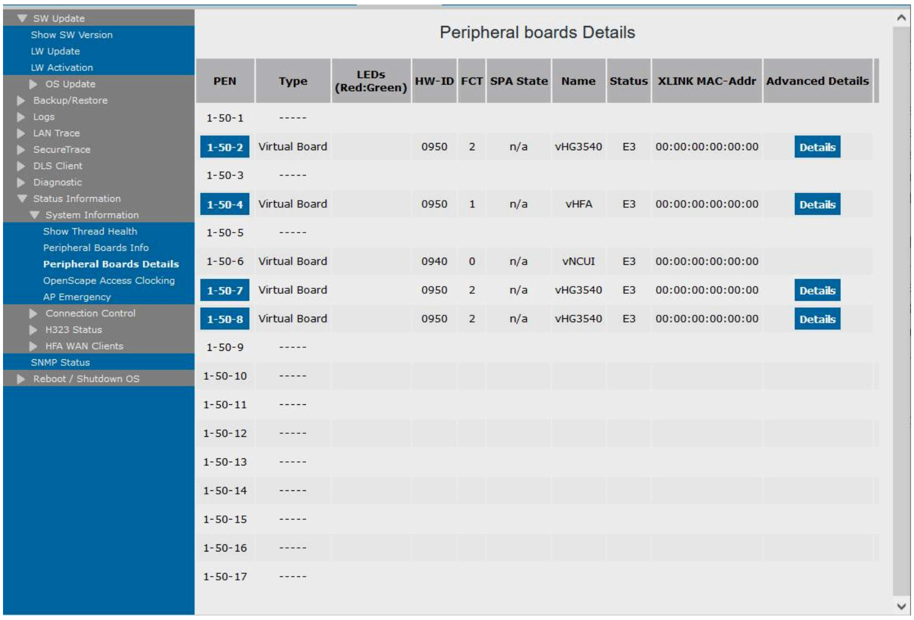
WBM path

WBM **>** Maintenance **>** Status Information **>** System Information**>** Peripheral Boards details

The *Peripheral Boards* table is displayed. This table shows the virtual peripheral boards connected to OpenScape 4000 SoftGate. The following details are provided:

- *PEN*: Peripheral Equipment Number
- *Type*: Type of board
- *HW-ID*
- *FCT*
- *SPA State*
- *Name:* Name of the physical peripheral board

- Status



Peripheral boards Details

PEN	Type	LEDs (Red:Green)	HW-ID	FCT	SPA State	Name	Status	XLINK MAC-Addr	Advanced Details
1-50-1	-----								
1-50-2	Virtual Board		0950	2	n/a	vHG3540	E3	00:00:00:00:00:00	Details
1-50-3	-----								
1-50-4	Virtual Board		0950	1	n/a	vHFA	E3	00:00:00:00:00:00	Details
1-50-5	-----								
1-50-6	Virtual Board		0940	0	n/a	vNCUI	E3	00:00:00:00:00:00	
1-50-7	Virtual Board		0950	2	n/a	vHG3540	E3	00:00:00:00:00:00	Details
1-50-8	Virtual Board		0950	2	n/a	vHG3540	E3	00:00:00:00:00:00	Details
1-50-9	-----								
1-50-10	-----								
1-50-11	-----								
1-50-12	-----								
1-50-13	-----								
1-50-14	-----								
1-50-15	-----								
1-50-16	-----								
1-50-17	-----								

- XLINK -MAC Address

Buttons

The following buttons are shown in this table:

- Details

Buttons in the *PEN* column

WBM path

WBM **>** Maintenance **>** Status Information **>** System Information**>** Peripheral Boards details**>** buttons in the *PEN* column

The *Table for Software PEN...* is displayed. The following information is displayed in this table for the selected virtual peripheral board: *PEN* (Peripheral Equipment Number), *SubNo.*, *L*, *Status*, *IP Address*, *H225 port*, *TSA status*, *Call ref. ID*, *TSL*, *HWY*, *B-Channel*.

Buttons

Under this table, the following button is displayed:

- *Back to peripheral boards*: The *Peripheral boards* table is displayed once more.

WBM path

WBM **>** Maintenance **>** Status Information **>** System Information**>** Peripheral Boards details**>** *detail* buttons

Common properties for BMSPA and CGSPA are shown there. The *Board details for [PEN]* table is displayed (if supported by the board). The following details are displayed in this table for the selected virtual peripheral board:

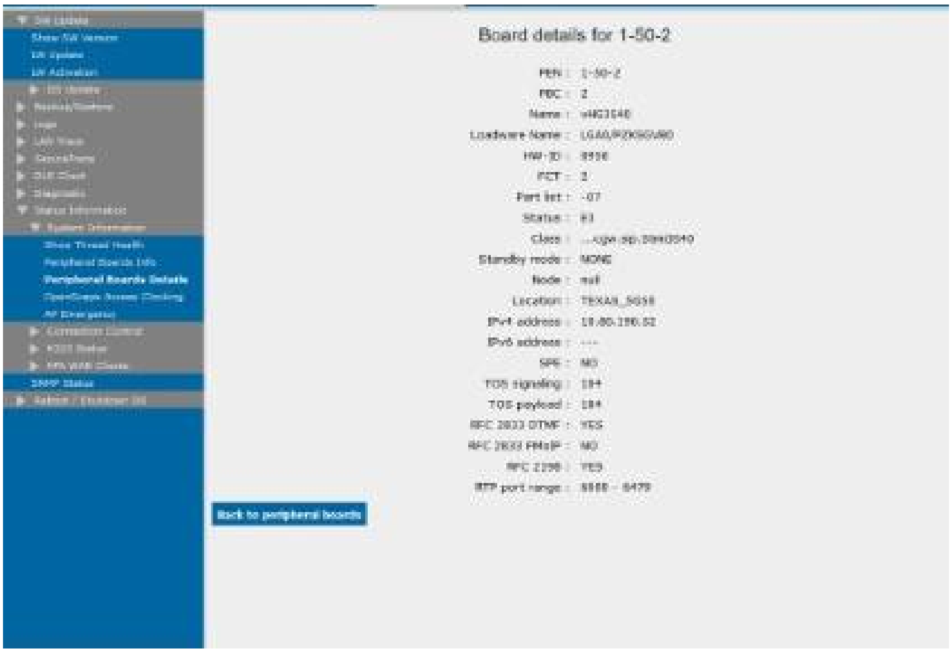
- *PEN*: Peripheral Equipment Number
- *PBC*
- *Name*: Name and part number of the physical peripheral board that was virtualized
- *Status*

- *Max. timeslots*: Maximum number of timeslots
- *law*: Digitization procedure for analog audio signals (A-law or Âµ-law)
- *XLINK MAC address*: MAC address of XLink LAN interface
- *XLINK IP address*: IP address of XLink LAN interface
- *SPA Sachnummer*
- *SPA Shortname:*
  - BMSPA
  - BOSPA - the same as BMSPA, but with no PHY
  - BOSPAV - the same as BOSPA, but with different integrated switch on xlink
  - CGSPA - CGSPA is powerful BMSPA with own clock generator for precise dect clock.
- *SPA SW version*
- *SPA state*
- LED_RD: LED_OFF
- LED_GN: LED_ON - status of peripheral board leds, this status is OK. Red and simultaneously green led on show problem.
- *Fans*: Status of fan, in operation or not in operation
- *Telco voltage*
- *LAN-FRAMES-OK*: Number of correct LAN frames for TX (send) and RX (receive)
- *LAN-ERRORS*: Number of errors for PHY-RX, FCS, SCF and MCF

Specific for CGSPA board:

- *GPS_IN-LEFT-LED: GPSIN_OFF*
- GPS_IN-RIGHT-LED: *GPSIN_*ON -Interface active and processing. The GPS task is up and running for processing signals, but waiting for the 1 second pulse and GPS Time stamp (more details about these leds can be found in chapter 9.2.2.3 of OpenScape Cordless Enterprise V7 document)
- SLC Role: MASTER - this board is responsible for measuring of phase shift of CDLSYN signal, standBy is successor of Master and in ISS scenario must be wired with Meinberg GPS receiver too. UNKNOWN - If QDCL functionality isn't active, SG doesn't know it, because information about SLC roles isn't forwarded.
- Chain Role: MASTER - this board provides clocks to another boards on clock chain, SLAVE receives clocks from MASTER and adapts own clocks to it
- CLK Chain Position: 1 - shows order of board in clock chain, SLC master must be 1 and SLC standBy must be 2. If is N/A, no cabel on chain is plugged.
- GPS Chain Position: 1 - shows order of board on gps chain, in case of ISS scenario, SLC master doesnât need to be 1. If is N/A, no cabel on chain is plugged.
- CDLSYN State: OK_REFERENCE - must be OK on each board, otherwise something wrong in wiring.
- FRONTREF State: NO_REFERENCE - if Meinberg is connected, each board can read status of FRONTREF signal through clock daisy chain
- CKA State: OK_REFERENCE - must be OK on each board, otherwise something wrong in wiring.
- VCXO State: OK_REFERENCE - must be always OK, it doesnât matter on wiring.

- Reference Clock: TCXO:
  - TCXO is onboard reference clock, which is sufficient for dect. It is chosen for chain master board
  - NO REFERENCE, in this case, VCXO is used, if we have OSA-DIUT with available reference clock. It is chosen for chain master board. VCXO is adapt through xlink to OSA-DIUT reference
  - FRONTREF is used from Meinberg, if we have more references, it depends on priority in refta. It is chosen for chain master board
  - CKA is used from clock chain for all chain slaves
- Sync to Ref Clock: true - it must be always true with exception, when chain master has Reference Clock: NO_REFERENCE



Board details for 1-50-2

PEN : 1-50-2
PBC : 2
Name : vHG3540
Loadware Name : LGA0/PZKSGV80
HW-ID : 8598
FCT : 2
Port list : -07
Status : R3
Class : ...cgw.sp.39H3540
Standby mode : NONE
Node : null
Location : TEXAS_5058
IPv4 address : 10.80.190.52
IPv6 address : ---
SPE : NO
TOS signaling : 184
TOS payload : 184
RFC 2833 DTMF : YES
RFC 2833 FMoIP : NO
RFC 2198 : YES
RTP port range : 8888 - 8479

Buttons

Under this table, the following button is displayed:

- *Back to peripheral boards:* The *Peripheral boards* table is displayed once more.

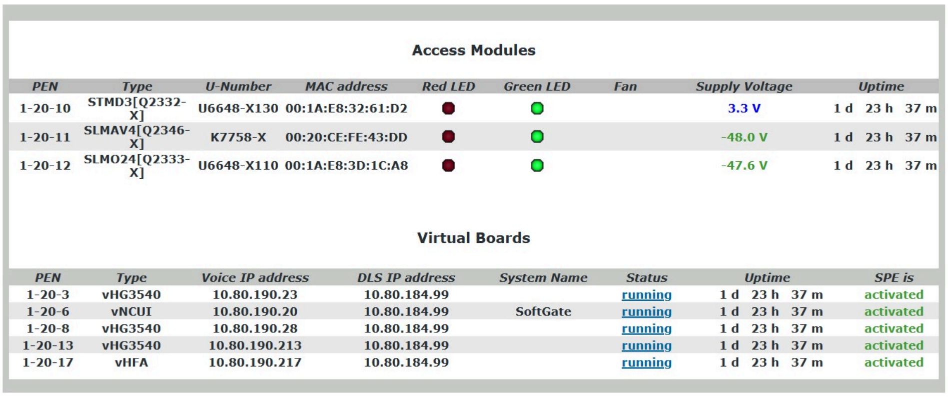
4.9.1.3 Peripheral Boards Info

WBM path

WBM **>** Maintenance **>** Status Information **>** System Information**>** Peripheral Boards Info

The OpenScape Access Modules are displayed in this table. The following details are provided:

- *PEN: Peripheral Equipment Number*
- *Type*
- *LEDs*
- *System Name*: Name of the physical peripheral board that was virtualized
- *Status:* in operation or not in operation



Access Modules

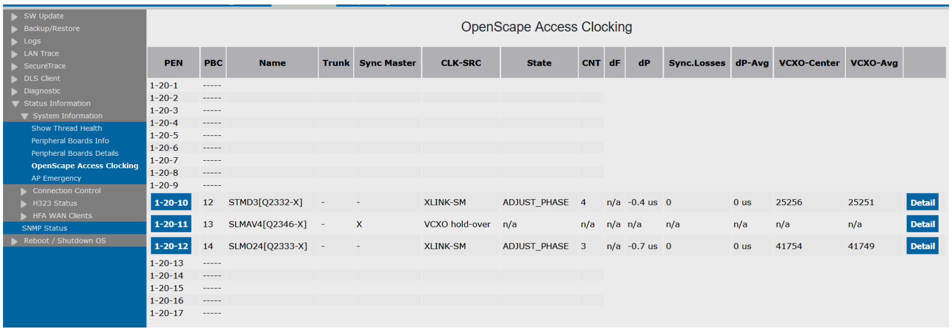
PEN	Type	U-Number	MAC address	Red LED	Green LED	Fan	Supply Voltage	Uptime
1-20-10	STMD3[Q2332-X]	U6648-X130	00:1A:E8:32:61:D2	●	●		3.3 V	1 d 23 h 37 m
1-20-11	SLMAV4[Q2346-X]	K7758-X	00:20:CE:FE:43:DD	●	●		-48.0 V	1 d 23 h 37 m
1-20-12	SLMO24[Q2333-X]	U6648-X110	00:1A:E8:3D:1C:A8	●	●		-47.6 V	1 d 23 h 37 m

Virtual Boards

PEN	Type	Voice IP address	DLS IP address	System Name	Status	Uptime	SPE is
1-20-3	vHG3540	10.80.190.23	10.80.184.99		running	1 d 23 h 37 m	activated
1-20-6	vNCUI	10.80.190.20	10.80.184.99	SoftGate	running	1 d 23 h 37 m	activated
1-20-8	vHG3540	10.80.190.28	10.80.184.99		running	1 d 23 h 37 m	activated
1-20-13	vHG3540	10.80.190.213	10.80.184.99		running	1 d 23 h 37 m	activated
1-20-17	vHFA	10.80.190.217	10.80.184.99		running	1 d 23 h 37 m	activated

4.9.1.4 OpenScape Access Clocking

Softgate Status (button on bottom panel with mark "i")->running (click for details):



OpenScape Access Clocking

PEN	PBC	Name	Trunk	Sync Master	CLK-SRC	State	CNT	dF	dP	Sync.Losses	dP-Avg	VCXO-Center	VCXO-Avg	
1-20-1	-----													
1-20-2	-----													
1-20-3	-----													
1-20-4	-----													
1-20-5	-----													
1-20-6	-----													
1-20-7	-----													
1-20-8	-----													
1-20-9	-----													
1-20-10	12	STMD3[Q2332-X]	-	-	XLINK-SM	ADJUST_PHASE	4	n/a	-0.4 us	0	0 us	25256	25251	Detail
1-20-11	13	SLMAV4[Q2346-X]	-	X	VCXO hold-over	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Detail
1-20-12	14	SLMO24[Q2333-X]	-	-	XLINK-SM	ADJUST_PHASE	3	n/a	-0.7 us	0	0 us	41754	41749	Detail
1-20-13	-----													
1-20-14	-----													
1-20-15	-----													
1-20-16	-----													
1-20-17	-----													

On this page can be verified status of peripheral board (red, green LED), SLC roles, where master must has the lowest SLC number and standby the second lowest. If SLC role is unknown, QDCL functionality isn't active, SG doesn't know it, because information about SLC roles isn't forwarded.CLK chain position shows right daisy chain wiring. SLC master must be 1 and SLC standBy 2. GPS_IN leds are useful in ISS scenario. More details - Section 9.2.2.3 of OpenScape Cordless Enterprise V7 document

WBM path

WBM **>** Maintenance **>** Status Information **>** System Information**>** Peripheral Boards Info**>**OpenScape Access Clocking

The *OpenScape Access Clocking* table is displayed: The values for OpenScape Access Module clocking are displayed in this table. The following details are provided:

- *PEN*: Peripheral Equipment Number
- *PBC*
- *Name*: Name and part number of the physical peripheral board that was virtualized
- *Trunk*
- *SM*
- *CLK-SRC*
- *State*
- *CNT*

- *dF*
- *dP*
- *Sync. losses*
- *dP-Avg*
- *VCXO Center*: Voltage-Controlled Crystal Oscillator
- *VCXO-Avg*: Voltage-Controlled Crystal Oscillator

Buttons

The following buttons are shown in this table:

Buttons in the PEN column

detail buttons

Buttons in the PEN column

WBM path

WBM **>** Maintenance **>** Status Information **>** System Information**>** OpenScape Access Clocking**>** Buttons in the PEN column

Information is displayed in this dialog for the selected Access Module.

detail buttons

WBM path

WBM **>** Maintenance **>** Status Information **>** System Information**>** OpenScape Access Clocking**>** detail buttons

The *HPA Clocking Details* dialog is displayed. The following graphics are displayed in this dialog:

- *Phase Jitter Distribution*: Distribution of phase fluctuations by a mean value
- *Phase Jitter*: Phase fluctuations by a mean value

Button

The following button is shown in this dialog:

- *Back to OpenScape Access Clocking:* The *OpenScape Access Clocking* table is displayed again.

4.9.1.5 AP Emergency

WBM path

WBM **>** Maintenance **>** Status Information **>** System Information **>** AP Emergency

The *AP Emergency Status* table is displayed. This table displays AP Emergency data. This data includes: *AP*, *Control Unit*, *Host-CC connected*, *CC-AP connected*.

AP Emergency takes over access point operation if the central control unit fails.

4.9.2 Connection Control

WBM path

WBM **>** Maintenance **>** Status Information**>** Connection Control

The *SoftGate Connection Control* menu opens.

Menu Connection Control

The following selection options are offered in this menu:

Show IPDA Connections

Show IPDA DMC Connections

Show all connections

4.9.2.1 Show IPDA Connections

NOTICE: This function may only be used by developers.

WBM path

WBM **>** Maintenance **>** Status Information **>** Connection Control **>** Show IPDA Connections

The *SCC-N IPDA connection list* table is displayed. This table displays currently active IPDA connections (IPDA: IP Distributed Architecture). The following details are provided: *NPCI*, *Station A*, *Station B*, *SW Attr.*, *Codes*, *Target Port*, *Source Port*, *IP Address*, *Index*.

Button

Refresh: The connection list is refreshed manually by clicking this button.

Check boxes

Refresh: Can be activated/deactivated. The connection list is refreshed automatically every 60 seconds if this check box is enabled.

Display

Seconds to next refresh: Indicates in how many seconds the connection list will be refreshed automatically.

4.9.2.2 Show IPDA DMC Connections

NOTICE: This function may only be used by developers.

WBM path

WBM **>** Maintenance **>** Status Information **>** Connection Control **>** Show IPDA DMC Connections

The *SCC-DMC IPDA connection list* table is displayed. This table displays currently active IPDA connections (IPDA: IP Distributed Architecture). The following details are provided: *NPCI*, *CorrelationID*, *ForwardCodec*, *ReverseCodec*, *Source Port*, *Target Port*, *IP Address*.

Button

Refresh: The connection list is refreshed manually by clicking this button.

Check boxes

Refresh: Can be activated/deactivated. The connection list is refreshed automatically every 60 seconds if this check box is enabled.

Display

Seconds to next refresh: Indicates in how many seconds the connection list will be refreshed automatically.

4.9.2.3 Show all connections

NOTICE: This function may only be used by developers.

WBM path

WBM **>** Maintenance **>** Status Information **>** Connection Control **>** Show all connections

The *SCC connection table* is displayed. This table displays all currently active SCC connections. The following information is displayed: *Device*, *Type*.

Button

Refresh: The connection list is refreshed manually by clicking this button.

Check boxes

Refresh: Can be activated/deactivated. The connection list is refreshed automatically every 60 seconds if this check box is enabled.

Display

Seconds to next refresh: Indicates in how many seconds the connection list will be refreshed automatically.

4.9.3 H323 Status

WBM path

WBM **>** Maintenance **>** Status Information **>** H323 Status

The H323 Statusmenu is displayed.

H323 Status**menu**

The following options are shown in this menu:
H323 Endpoints

4.9.3.1 H323 Endpoints

WBM path

WBM **>** Maintenance **>** Status Information **>** H323 Status **>** H323 Endpoints

The *H.323 Endpoints* table is displayed. This table displays H.323 phones that are logged in to OpenScape 4000 SoftGate and currently connected. The following details are provided:

- *EP-ID*: Endpoint ID
- *Calls*: All calls on the respective H.323 endpoint
- *Outbound*: Outgoing calls on the respective H.323 endpoint
- *Inbound*: Incoming calls on the respective H.323 endpoint
- *Class*

Buttons

The following buttons are shown in this table:

Buttons in *EP ID* column

Details buttons

Buttons in *EP ID* column

WBM path

WBM **>** Maintenance **>** Status Information **>** H323 Status **>** H323 Endpoints**>** buttons in the *EP ID* column

The *H.323 Endpoint ...* table is displayed.

This table displays the following information for the H.323 phone selected: *Int.Key*, *Call Ref.*, *Direction*, *calling party*, *called party*.

Buttons

Under this table, the following button is displayed:

- *Back to H.323 Endpoints list*: The *H323 Endpoint...* table is displayed again.

Details buttons

WBM path

WBM **>** Maintenance **>** Status Information **>** H323 Status**>** H323 Endpoints**>** *<line for a H.323 phone>* **>** *Details*

The *H.323 Endpoint details ...* table is displayed.

This table contains detailed information on the selected H.323 phone. This information includes:

- *EP ID*, *H.323 Product ID*, *User*, *Calls size*, *RFC 2198 PT* (payload for redundant audio data), *RFC 2833 PT* (RTP payload for DTMF digits, telephony tones and telephony signals), *RFC 2833 events*
- *Capabilities*, *ptime*, *maxPtime*, *VAD* (Voice Activity Detection)

Buttons

Under this table, the following button is displayed:

- *Back to H.323 Endpoints list*: The *H323 Endpoint...* table is displayed again.

4.9.4 HFA WAN Clients

WBM path

WBM **>** Maintenance **>** Status Information **>** HFA WAN Clients

The HFA WAN Clientsmenu opens.

Menu HFA WAN Clients

The following selection options are offered in this menu:

Status

Logon Attempts

4.9.4.1 Status

WBM path

WBM **>** Maintenance **>** Status Information **>** HFA WAN Clients **>** Status

The HFA WAN Clients table is displayed. The following information is displayed in this table for every station (HFA WAN Client): *Station*, *PEN*, *Status*, *Address*, *Logon at*, *Logoff at*, *Call since*.

4.9.4.2 Logon Attempts

WBM path

WBM **>** Maintenance **>** Status Information **>** HFA WAN Clients **>** Logon Attempts

The HFA WAN Clients table is displayed. The stations (HFA WAN Clients) that have made unsuccessful logon attempts are displayed in this table.

4.10 Reboot / Shutdown OS

WBM path

WBM **>** Maintenance **>** Reboot / Shutdown OS

The Reboot / Shutdown OS menu opens.

Menu Reboot / Shutdown OS

The following selection option is offered in this menu:

Reboot OS

Shutdown OS

IMPORTANT: On Integrated SoftGates the OpenScape 4000 service will be restarted or shutdown also.

IMPORTANT: On Survivable SoftGates the OpenScape 4000 survivability unit will be restarted or shutdown also.

4.10.1 Reboot OS

WBM path

WBM **>** Maintenance **>** Reboot / Shutdown OS **>** Reboot OS

The Reboot OS window opens. The SoftGate operating system can either be restarted or shut down in this window.

Button

- *Reboot OS*: The SoftGate operating system is shut down and then automatically restarted by clicking this button.

4.10.2 Shutdown OS

WBM path

WBM **>** Maintenance **>** Reboot / Shutdown OS **>** Shutdown OS

The Shutdown OS window opens. The SoftGate operating system can either be restarted or shut down in this window.

Button

- *Shutdown OS*: The SoftGate operating system is shut down by clicking this button.

5 Help

Information on the WBM is displayed in the *Help* module.

WBM path

WBM **>** Help **>** *Product Docu*

A new browser window will open with the Online Help of the OpenScape 4000 vHG 3575 for SoftGate and Enterprise Gateway.

Prerequisite

The IP address of the OpenScape 4000 Assistant has to be configured in the AMO STMIB.

6 Logoff

The connection is cleared down when you click Logoff and the WBM session is ended.

WBM path

WBM **>** Logoff

Index

mitel.com

Mitel®