A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000

OpenScape 4000 V11 vHG 3500 HFA for OpenScape 4000 SoftGate

Administrator Documentation
07/2024

P31003-H34B0-M104-01-76A9

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Contents

1 Introduction and Important Notes

OpenScape 4000 SoftGate and vHG 3500 HFA

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).

The vHG 3500 HFA (virtual HG 3500 HFA = virtual STMI) is the central controller for IPDA (IP Distributed Architecture) in the OpenScape 4000 SoftGate.

Topics in this Chapter

1.1 Target Audience for this Manual

This manual is aimed at employees who are responsible for managing vHG 3500 HFA and 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 3500 HFA 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 3500 HFA for OpenScape 4000 SoftGate WBM (Web-Based Management). This includes general operation of the WBM, descriptions of individual modules for administering vHG 3500 HFA 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
	Designates situations that may result in property damage or loss of data.
	Designates useful information.

2 WBM

WBM

WBM is the administration interface for the vHG 3500 HFA for OpenScape 4000 SoftGate (virtual HG 3500 HFA = virtual STMI). 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 3500 HFA WBM if logged in to OpenScape 4000 Assistant. WBM has an integrated Web server, and can thus be accessed via a HTTPS URL.

The WBM user interface is available in English only.

Topics in this Chapter

2.1 Hardware and Software Requirements

2.1.1 Hardware

You need an administration PC with the following minimum configuration for WBM:

- 128 MB memory (RAM)
- 400 MHz processor

2.1.2 Software

The vHG 3500 HFA WBM consists of HTML/XSL pages with frames. The requirements for using it are:

- Windows NT 4.0, 2000, XP, Vista or Windows 7
- Microsoft Internet Explorer 10, 11

Other browsers which support frames, Java 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 servers.

2.2 Starting and Finishing WBM

Access options

There are two options for starting the vHG 3500 HFA for OpenScape 4000 SoftGate 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.

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

Topics in this chapter

1) 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'

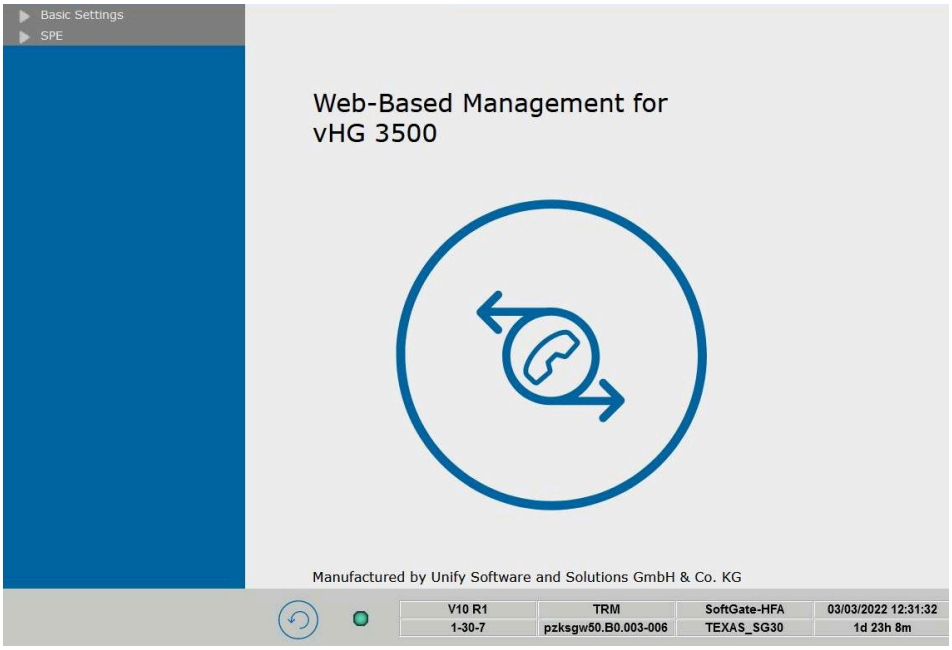
2.2.1 Starting via OpenScape 4000 Assistant

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 vHG 3500 HFA (e.g. vHG 3500 - HG 3530) in the *Remote access* column. You need to know the IP address of the relevant board.
4) The vHG 3500 HFA 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 the browser to the effect that there is a problem with the security certificate for the website. In this case, click *Continue to this website*.

5) Confirm the browser dialog with the certificate information. The vHG 3500 HFA WBM homepage is displayed:



1) Check whether you are in the vHG 3500 HFA WBM (e.g. SoftGate-HFA).
2) You can now use the Configuration and Maintenance modules to administer vHG 3500 HFA.

2.2.2 Starting via Web Browser

User Account

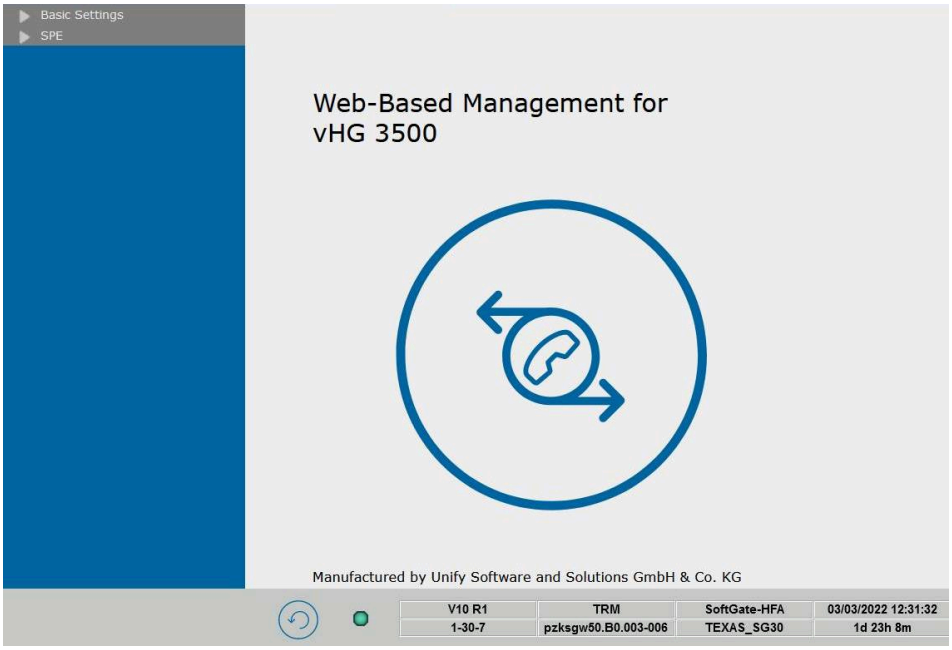
The user account "Administrator" is available for WBM. This account provides access to configuration settings.

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

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 vHG 3500 HFA 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 3500 HFA WBM login dialog is displayed:
4) Enter the user name and password. Click *Login*. The vHG 3500 HFA WBM homepage is displayed:



1) You can now use the Configuration and Maintenance modules to administer vHG 3500 HFA.

2.2.3 Finishing a WBM Session

To finish the WBM session, follow these steps:

1) Click the *Logoff* module. The connection to vHG 3500 HFA 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

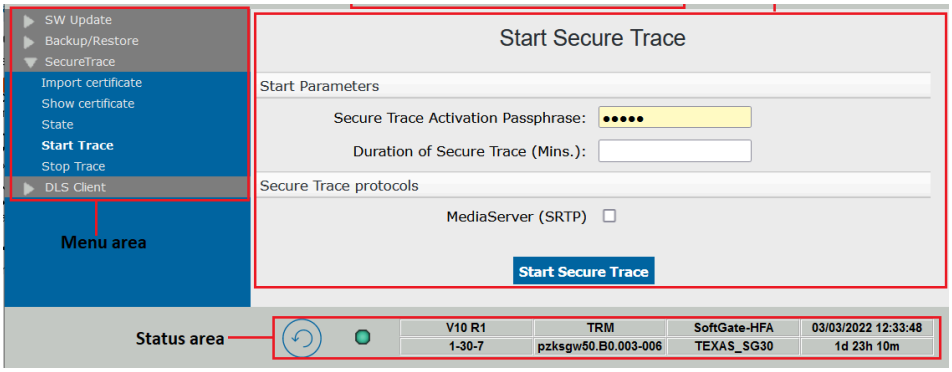
This chapter outlines the basic structure of the user interface, names the individual control elements, and describes their use.

Topics in this chapter

1) 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:



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

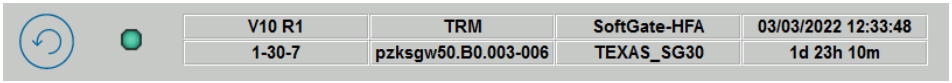
Once you have selected a module and a menu entry, this area shows the settings dialogs.

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:



The following control icons are used:

Reset icon (1)

This icon may be in one of the following states:

White/gray: Data entry is blocked. Users can read data, but they cannot edit entries.

White/black: Data input is enabled. Click this icon to restart vHG 3500 HFA.

Action icon (2)

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 (3),
- Access category of the user and system version (4),
- Name of the board and installation location (5),
- System date and time and how long since the last restart (6).

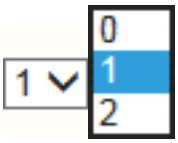
2.3.3 Dialog Elements

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.

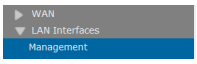
Radio buttons

(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

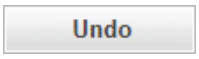
(in the figures to the left: top figure = menu closed; bottom figure = menu open): In the menu area, you can click these arrows to open or close a menu. Multiple menus can be opened.

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

You can use the Configuration module for defining the vHG 3500 HFA gateway properties (Basic Settings) and administering the Signaling & Payload Encryption (SPE) feature.

Options in the Configuration module

1) Basic Settings SPE

3.1 Basic Settings

In the Basic Settings menu, you can enter fundamental data about vHG 3500 HFA.

WBM path

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

The Basic Settings menu is displayed.

Basic Settings **menu**

The following options are shown in this menu:

1) Gateway

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 3500 HFA name in this field, e. g. if multiple vHG 3500 HFA systems are operated on a single OpenScape 4000 SoftGate.
- *Gateway Location*: Read-only. The vHG 3500 HFA location is displayed in this field.

Buttons

The following buttons are shown in this dialog:

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

3.2 SPE

SPE (Signaling & Payload Encryption) encrypts VoIP payload and signaling data streams to and from vHG 3500 HFA. 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 3500 HFA, 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 server's 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 **>** SPE

The SPE menu is displayed.

SPE ***menu***

The following options are shown in this menu:

1) Import Keycert Show Keycert Delete Keycert SPE Security Setup for HFA

3.2.1 Import Keycert

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

Supported Public Key Algorithms for SPE certificates are

- **RSA** with a minimum key length of 2048 bit.
- **ECDSA**

WBM path

WBM **>** Configuration**>** SPE **>** 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 SPE **>** 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.

3.2.2 Show Keycert

WBM path

WBM **>** Configuration **>** SPE **>** 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*

3.2.3 Delete Keycert

WBM path

WBM **>** Configuration SPE **>** 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 cancelled.

Procedure

To remove an SPE certificate, perform the following steps:

1) Select: *WBM* **>** Configuration SPE **>** 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.

3.2.4 SPE Security Setup for HFA

WBM path

WBM **>** Configuration **>** SPE **>** SPE Security Setup for HFA

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 customer's security requirements. This affects the encryption of signaling and payload data in communication between the vHG 3500 HFA and the VoIP clients, or between two vHG 3500 HFA systems.

Dropdown lists, input fields, check boxes

The following settings are shown in this dialog:

- *Minimal length of RSA keys*: You can select *512*, *1024* and *2048*. The larger the value, the more secure the key.
- *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 SPE **>** 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".
3) Click *Apply* and then click *OK* in the confirmation dialog. The modified data is accepted into the configuration.

4 Maintenance

The Maintenance module provides features for maintaining and administering vHG 3500 HFA. These features includes saving configurations and creating a secure trace.

WBM path

WBM **>** Maintenance

The Maintenance module is displayed.

Options in the Maintenance **module**

1) SW-Update Backup/Restore Secure Trace DLS Client

4.1 SW-Update

The SW-Update menu (SW: software) provides functions for displaying the software.

WBM path

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

The SW-Update menu is displayed.

SW-Update **menu**

The following options are shown in this menu:

1) Show SW-Version

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
- Platform Version: This pane indicates the hardware on which the SoftGate 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 Name*, *APS 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*

4.2 Backup/Restore

In the Backup/Restore menu, you can backup (export) the vHG 3500 HFA configuration locally. This local backup can be loaded (imported) and activated.

WBM path

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

The Backup/Restore menu is displayed.

Backup/Restore **menu**

The following options are shown in this menu:

1) 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 vHG 3500 HFA 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 vHG 3500 HFA 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 vHG 3500 HFA 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: vHG 3500 HFA 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 3500 HFA 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 3500 HFA has to be restarted for the configuration changes to take effect.

4.3 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 3500 HFA.

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 Trace **menu**

The following options are shown in this menu:

1) 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:
4) • 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).
5) 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.

---

1) The service technician supplies the certificate to the vHG 3500 HFA gateway for which the secure trace is being created; see Section 4.3.1, 'Import certificate'.
2) The service technician activates the secure trace function; see Section 4.3.4, 'Start Trace'. A secure trace is created. The activation and later deactivation (Section 4.3.5, 'Stop Trace') are logged by the communication systems involved.
3) 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.
4) The secure trace is provided to the developer.
5) The developer decrypts the secure trace using the private key. The developer then analyzes the decrypted records.
6) 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.

4.3.1 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:
4) **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.

Click *OK* to close the fingerprint window.
5) 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.

4.3.2 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*

4.3.3 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).

4.3.4 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*:
- – *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.

4.3.5 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.

4.4 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:

1) 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 3500 HFA 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 CGWs. The DLS client uses this certificate to identify itself at the DLS server.

4.4.1 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 vHG 3500 HFA.

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 reboot vHG 3500 HFA.
  – *Port of DLS Server*: The port of the DLS server for bootstrapping mode can be configured using the AMO. You must reboot vHG 3500 HFA.
  – *Secure Port of DLS Server*: vHG 3500 HFA 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.

4.4.2 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.

4.4.3 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.

4.4.4 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:

1) 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.

4.4.4.1 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

4.4.4.2 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*

4.4.4.3 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"

4.4.4.4 "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*

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 3500 HFA* for OpenScape 4000 SoftGate.

NOTICE: The IP address of the OpenScape 4000 Assistant has to be configured in the AMO CGWB.

---

6 Logoff

The vHG 3500 HFA connection is cleared down when you click Logoff and the WBM session is ended.

WBM path

WBM **>** Logoff

Index

W