A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000 V11

vHG 3575 for OpenScape 4000 SoftGate

Administratordokumentation
07/2024

P31003-H31B0-M105-01-00A9

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.

Inhalt

1 Einleitung und wichtige Hinweise

OpenScape 4000 SoftGate und Enterprise Gateway

OpenScape 4000 SoftGate ist eine IP-Telefonie-Applikation für den Anschluss von HFA- und SIP-basierten Telefonen, z. B. für die Telefonfamilien OpenStage HFA und OpenStage SIP. Sie ermöglicht IP-basierte Kommunikation im gesamten Unternehmen einschließlich kleiner Außenstellen. Der Anschluss an das öffentliche Telefonnetz wird durch SIP-Trunking (SIP-Q oder native SIP) ermöglicht.

OpenScape Enterprise Gateway liegt Hardware und Software von OpenScape 4000 zugrunde. Es handelt sich um den Nachfolger der AP 3700-9-Baugruppenrahmen mit HG3575.

vHG 3575 (Enterprise Gateway) (virtuelle HG 3575 = virtuelle NCUI) ist in OpenScape 4000 SoftGate bzw. Enterprise Gateway die zentrale Steuerung für die IPDA (IP Distributed Architecture).

Themen in diesem Kapitel

1.1 Zielgruppe dieses Buches

Dieses Handbuch ist für Mitarbeiter gedacht, die für die Administration von OpenScape 4000 SoftGate verantwortlich sind. Sie müssen bereits Erfahrung in der Administration von LANs haben und insbesondere über fundierte Kenntnisse in den folgenden Bereichen verfügen:

- Hardware für die Datenkommunikation
- OpenScape 4000 V8
- Konzepte und Begriffe für Weitbereichsnetze (WAN)
- Konzepte und Begriffe für lokale Netze (LAN)
- Konzepte und Begriffe für das Internet

Sie sollten Anweisungen für vHG 3575 (Enterprise Gateway) und OpenScape 4000 SoftGate zu folgenden Themen erhalten haben:

- Installation und Inbetriebnahme
- Konfiguration der VoIP-Funktionen
- Einrichtung und Konfiguration der Datenkommunikationsparameter

1.2 Inhalt dieses Buches

Dieses Handbuch beschreibt das WBM (Web-Based Management) für vHG 3575 (Enterpise Gateway) für OpenScape 4000 SoftGate. Dazu gehören die allgemeine Bedienung des WBMs, Beschreibungen der einzelnen Module für die Administration des SoftGate sowie die Vorgehensweise bei der Administration.

1.3 Hinweis zu Internet Explorer

Wichtig: Wenn Sie Änderungen an den Internet Explorer Sicherheitseinstellungen für eine WBM-Seite vorgenommen haben (z.B.: die Seite den Trusted Sites hinzugefügt), so wird empfohlen, den Browser neu zu starten, damit die neuen Einstellungen korrekt verwendet werden.

1.4 Verwendete Konventionen

In diesem Buch werden die folgenden typographischen Konventionen verwendet:

Konvention	Beispiel
`Courier`	Eingabe und Ausgabe Beispiel: `LOCAL` als Dateiname eingeben `Befehl nicht gefunden`
Kursiv	Variable Beispiel: *Name* kann bis zu acht Zeichen lang sein
Kursiv	Elemente der Benutzeroberfläche Beispiel: Klicken Sie auf die Schaltfläche *OK*.
Abschnitt 1.4, "Verwendete Konventionen"	Querverweis
Konfiguration	Elemente der Benutzeroberfläche als Querverweis
Fett	Besondere Hervorhebung Beispiel: Dieser Name darf **nicht** gelöscht werden
`<Courier>`	Tastenkombinationen Beispiel: <STRG>+<ALT>+<ESC>
>	Menüfolge Beispiel: *WBM* **>** *Konfiguration*
	Kennzeichnet Situationen, die Sachschäden und/oder Datenverlust zur Folge haben können.
	Kennzeichnet hilfreiche Hinweise.

2 OpenScape 4000 WBM

WBM

WBM ist die Administrationsschnittstelle von vHG 3575 (Enterpise Gateway) für OpenScape 4000 SoftGate (virtuelle HG 3575 = virtuelle NCUI). Sofern der Root-Administrator das WBM aktiviert hat, steht es über jede TCP/IP-Verbindung zur Verfügung, sowohl über LAN als auch WAN.

Jeder PC mit TCP/IP-gestützter Netzwerkverbindung, auf dem ein kompatibler Webbrowser läuft, kann nach der Anmeldung an vHG 3575 (Enterpise Gateway) für OpenScape 4000 SoftGateauf das WBM von vHG 3575 zugreifen. Das WBM verfügt über einen integrierten Webserver, sodass es über eine HTTPS-URL aufrufbar ist.

Die Bedienoberfläche des WBMs ist in den Sprachen Englisch.

Themen in diesem Kapitel

2.1 Hard- und Softwarevoraussetzungen

2.1.1 Hardware

Weitere Informationen erhalten Sie in den Anforderungen für den Webbrowser.

2.1.2 Software

Das WBM von vHG 3575 (Enterprise Gateway) besteht aus HTML/XSL-Seiten mit Frames. Sein Einsatz erfordert:

- Windows 7 und höher
- Internet Explorer Version 10 und höher, Firefox und Google Chrome

Andere Browser, die Frames, Java und JavaScript unterstützen, sind möglicherweise ebenfalls mit dem WBM kompatibel. Browser, die keine Frames unterstützen, können nicht mit dem WBM verwendet werden.

Wichtig: Wenn auf dem Administrations-PC ein DNS-Server eingerichtet wurde, der aber nicht erreichbar ist, führt dies bei der WBM-Oberfläche zu erheblichen Geschwindigkeitseinbußen. Sollte dies bei Ihnen der Fall

sein, überprüfen Sie in den Netzwerkeinstellungen des Administrations-PCs die eingestellten DNS-Server. Entfernen Sie alle nicht erreichbaren DNS-Server oder geben Sie einen erreichbaren ein. Klicken Sie dann auf *Schließen*.

2.1.3 Einstellungen in Internet Explorer

Nehmen Sie im Internet Explorer folgende Einstellungen vor:

Temporäre Internet-Dateien löschen

Extras > Internetoptionen > Erweitert > Sicherheit > Aktivieren: Leeren des Ordners "Temporary Internet Files" beim Schließen des Browsers

Proxyserver umgehen

Die Verbindung vom Administrations-PC zur vHG 3575 (Enterprise GW) darf nicht über einen Proxy-Server hergestellt werden.

Extras > Internetoptionen > Registerkarte Verbindungen > LAN-Einstellungen > Schaltfläche Einstellungen > Proxyserver > Aktivieren: Proxyserver für lokale Adressen umgehen

Download von Dateien ermöglichen

- Entweder für alle URLs:

  Extras > Internetoptionen > Registerkarte Sicherheit > Webinhaltszone Lokales Intranet > Schaltfläche Stufe anpassen > Download > Dateidownload > Aktivieren
- Oder nur für die URL des vHG 3575 (Enterprise GW) WBM:

  1) Extras > Internetoptionen > Registerkarte Sicherheit > Webinhaltszone Vertrauenswürdige Sites > Schaltfläche Sites > URL des WBMs eingeben in Diese Website zur Zone hinzufügen > Schaltfläche Hinzufügen, Aktivieren: Kontrollkästchen Für Sites dieser Zone ist eine Serverüberprüfung (https:) erforderlich

  2) Extras > Internetoptionen > Registerkarte Sicherheit > Webinhaltszone Vertrauenswürdige Sites > Schaltfläche Stufe anpassen > Download > Dateidownload > Aktivieren

Wenn Sie diese Einstellungen vorgenommen haben, schließen Sie den Internet Explorer und starten Sie ihn neu.

2.2 WBM starten und beenden

Zugangsmöglichkeiten

Es gibt zwei Optionen zum Starten von vHG 3575 (Enterpise Gateway) für OpenScape 4000 SoftGate WBM. Zum einen über OpenScape 4000 Assistant, zum anderen direkt über einen Web-Browser und die URL des WBMs. Der Zugang über OpenScape 4000 Assistant ist die am häufigsten benutzte Möglichkeit.

Themen in diesem Abschnitt

Abschnitt 2.2.1, "Über OpenScape 4000 Assistant starten"

Abschnitt 2.2.2, "Über Web-Browser starten"

Abschnitt 2.2.3, "WBM-Sitzung beenden"

2.2.1 Über OpenScape 4000 Assistant starten

Führen Sie zum Starten der WBM-Sitzung die folgenden Schritte durch:

1) Melden Sie sich mit Ihrem Benutzernamen und Ihrem Kennwort am OpenScape 4000 Assistant an.
2) Wählen Sie in der Baumstruktur *OpenScape 4000 Assistant* **>** *Experten-modus* **>** *Gateway Dashboard*. Das Fenster *Gateway Dashboard* mit den vorhandenen Baugruppen wird angezeigt.
3) Klicken Sie in der Zeile des erforderlichen Enterpise Gateway (z. B. SoftGate) in der Spalte *Remote-Zugang* auf *[WBM] [N/A]*. Die IP-Adresse der entsprechenden Baugruppe muss Ihnen bekannt sein.

   Der Webserver des WBM wird kontaktiert. Da er ausschließlich mit HTTPS (gesicherter Datenübertragung) arbeitet, sendet der Server ein Zertifikat.

   Anmerkung: Im Internet Explorer kann die Meldung erscheinen, dass ein Problem mit dem Sicherheitszertifikat der Website besteht. Klicken Sie in diesem Fall auf *Laden dieser Website fortsetzen*.

   ---

4) Bestätigen Sie den Browser-Dialog mit den Zertifikatsinformationen. Die WBM-Startseite wird angezeigt:
5) Überprüfen Sie, ob Sie sich im WBM des Enterpise Gateway befinden (z. B. SoftGate).
6) Mit den Modulen Konfiguration und Wartung können Sie jetzt das vHG 3575 (Enterprise Gateway) verwalten.

2.2.2 Über Web-Browser starten

Benutzerkennung

Für das WBM steht Ihnen die Benutzerkennung "Administrator" zur Verfügung. Diese Kennung bietet Ihnen Zugang zu den Konfigurationseinstellungen.

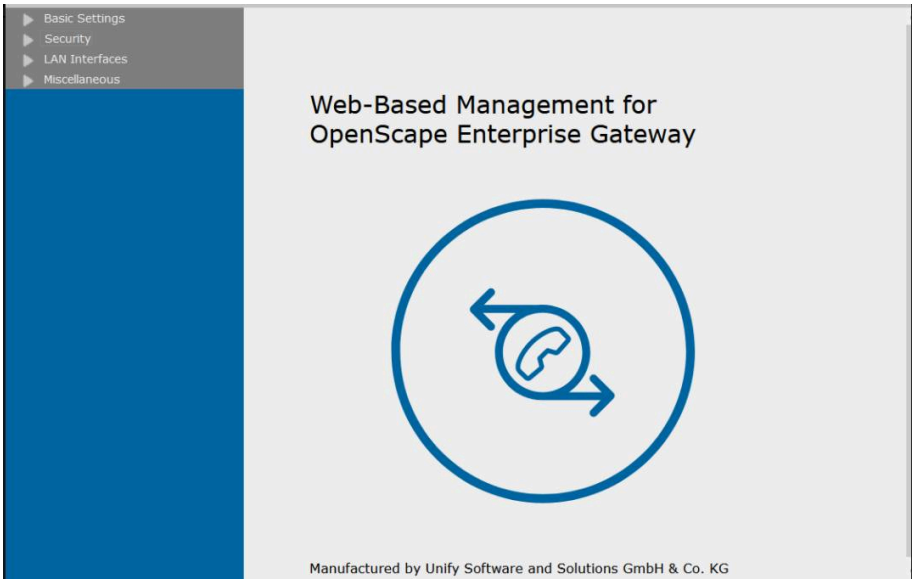
Der Standard-Benutzername lautet **TRM** und das Standard-Kennwort **HICOM** (wie im AMO STMIB konfiguriert). Diese Standard-Daten können von Ihnen im AMO STMIB geändert werden.

WBM-Sitzung starten

Führen Sie zum Starten der WBM-Sitzung die folgenden Schritte durch:

1) Öffnen Sie Ihren Web-Browser.
2) Geben Sie in die Adresszeile des Browsers die URL des gewünschtem WBM (Enterpise Gateway oder SoftGate) in folgendem Format ein: *https://999.999.999.999*. Der Webserver des WBM wird kontaktiert. Da der Server ausschließlich mit HTTPS (gesicherter Datenübertragung) arbeitet, sendet er ein Zertifikat.

3) Bestätigen Sie den Browser-Dialog mit den Zertifikatsinformationen. Der Anmeldedialog des vHG 3575 (Enterprise Gateway) WBM wird angezeigt.
4) Geben Sie den Benutzernamen und das Kennwort ein. Klicken Sie auf *Anmelden*. Die WBM-Startseite wird angezeigt.



5) Sie können jetzt die Module Konfiguration und *Wartung* verwenden.

2.2.3 WBM-Sitzung beenden

Führen Sie zum Beenden der WBM-Sitzung die folgenden Schritte durch:

1) Klicken Sie auf das Modul *Abmelden*. Die Verbindung zum WBM wird beendet und die WBM-Sitzung wird geschlossen.

Erläuterungen zum Beenden der WBM-Sitzung finden Sie im Kapitel 6, "Abmelden".

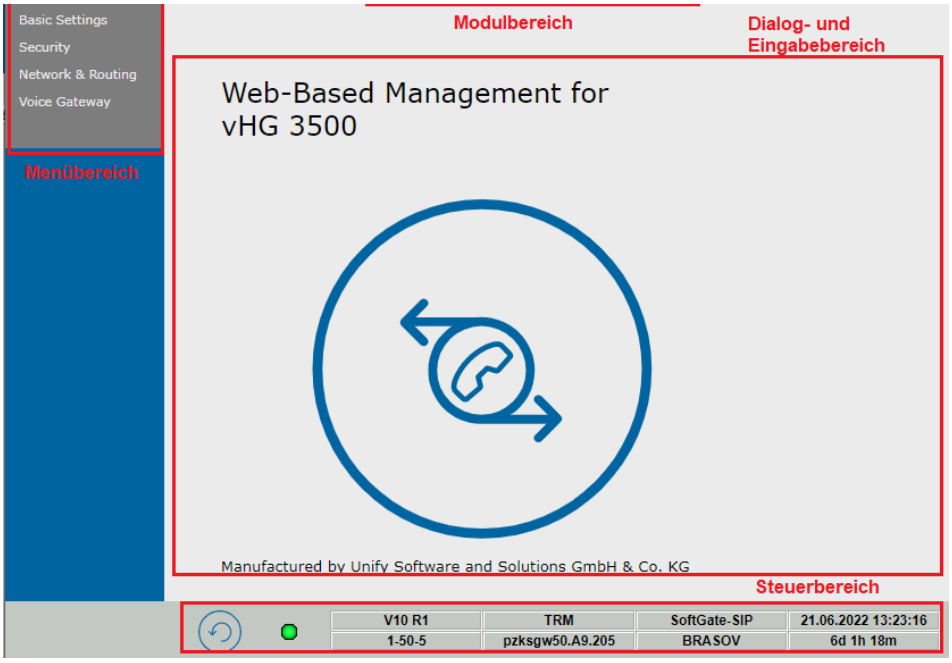
2.3 Benutzeroberfläche des WBMs

Dieser Abschnitt erklärt den grundsätzlichen Aufbau der Benutzeroberfläche, nennt die einzelnen Bedienelemente und beschreibt deren Benutzung.

Themen in diesem Abschnitt

2.3.1 Einteilung der Benutzeroberfläche

Die Benutzeroberfläche des WBMs lässt sich in die folgenden Bereiche einteilen:



Menübereich

Dieser Bereich wird für die Navigation innerhalb eines Moduls verwendet. Welche Menüeinträge dort angezeigt werden, hängt vom gewählten Modul ab.

Modulbereich

Dieser Bereich zeigt die zur Verfügung stehenden Module an. Die Module sind: *Konfiguration*, *Wartung*, *Hilfe* und *Abmelden*. Durch Klicken auf den Namen des Moduls erscheinen im Menübereich die zugehörigen Menüeinträge.

Dialog- und Eingabebereich

In diesem Bereich erscheinen nach Auswählen des Moduls und des Menüeintrages die jeweiligen Einstellungsdialoge.

Steuerbereich

Am unteren Rand finden Sie einige ständig angezeigte Statusinformationen. Zur Bedeutung der Symbole siehe Abschnitt 2.3.2, "Symbole im Steuerbereich des WBM-Fensters".

2.3.2 Symbole im Steuerbereich des WBM-Fensters

Der Steuerbereich stellt ständig Steuer- und Statusinformationen bereit. Die Abbildung unten zeigt ein Beispiel:

Es gibt folgende Steuersymbole:

Reset-Symbol (1)

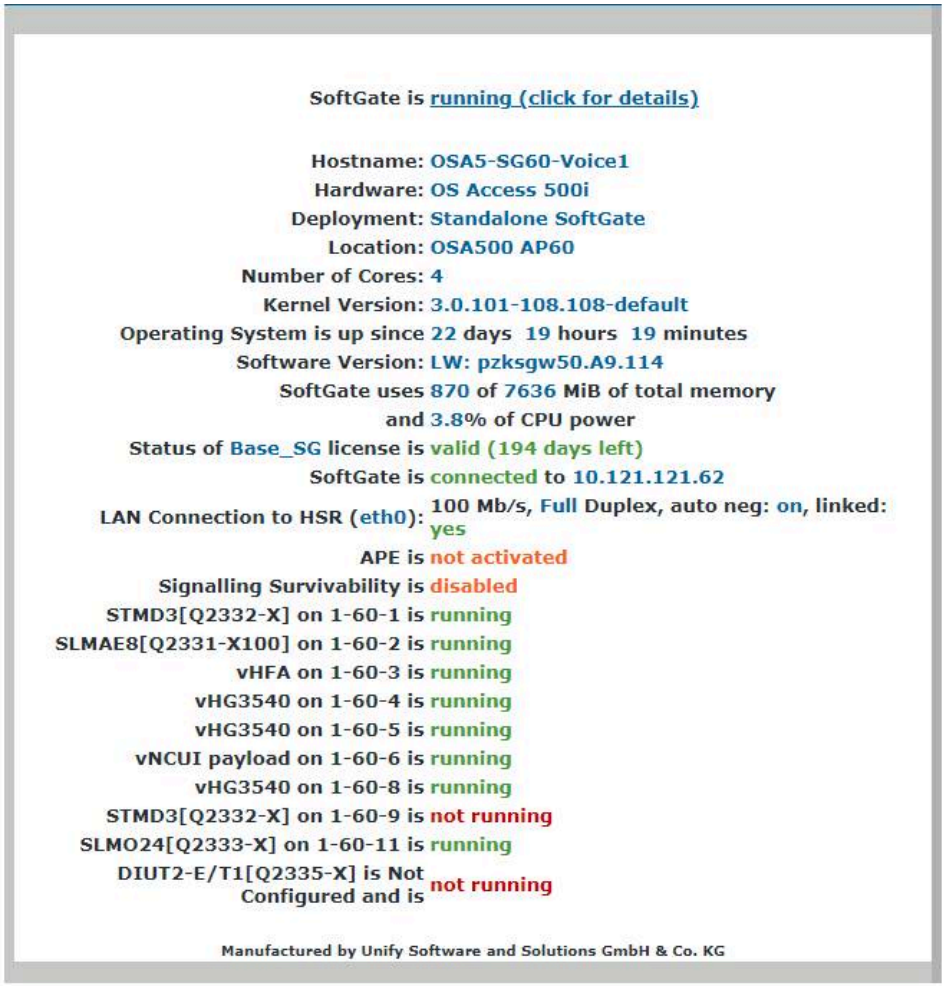
Dieses Symbol kann folgende Zustände annehmen:

Weiß/grau: Die Dateneingabe ist gesperrt. Der Benutzer kann Daten lesen aber keine Einträge ändern.

Weiß/schwarz: Die Dateneingabe ist aktiviert. Durch das Klicken auf dieses Symbol wird ein Neustart von vHG 3575 (Enterprise GW) ausgelöst.

Informations-Symbol (2)

Nach dem Klicken auf dieses Symbol werden Informationen zum Betriebsstatus von OpenScape 4000 SoftGate angezeigt, z. B. in Betrieb/nicht in Betrieb, Hostname, Ort, Softwareversion.



Aktivitäts-Symbol (3)

Das Aktivitäts-Symbol leuchtet grün, wenn eine Verbindung zum Webserver des WBMs besteht. Wenn keine Verbindung besteht, blinkt das Symbol rot.

Auß/erdem werden folgende Statusinformationen angezeigt:

- Zustandsinformation der ITIL-Version (4),
- Zugangskategorie des Benutzers und Systemversion (5),
- Name der Baugruppe und Aufstellungsort (6),
- Systemdatum und -uhrzeit sowie Zeit seit dem letzten Neustart (7).

2.3.3 Dialogelemente

Im WBM kommen die folgenden Dialogelemente vor:

Eingabefelder

Eingaben von numerischen oder alphanumerischen Werten. Vor, hinter oder über dem Feld steht die zugehörige Feldbeschriftung. Bei Passwortfeldern werden zur Sicherheit nur einheitliche Symbole wie Sternchen für jedes eingegebene Zeichen angezeigt. Nicht auf der Tastatur verfügbare Zeichen können unter Microsoft Windows z. B. über die Zeichentabelle eingefügt werden.

Auswahlfelder

(im nebenstehenden Bild link geschlosen, rechts geöffnet) Auf den Pfeil klicken, um die Liste zu öffnen oder zu schließen. Den gewünschten Eintrag mit der Maus anklicken.

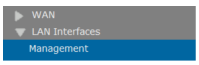
Kontrollkästchen

(im nebenstehenden Bild oben ausgeschaltet, unten eingeschaltet): Vor, hinter oder über dem Feld steht die zugehörige Feldbeschriftung. Anklicken, um die entsprechende Option ein- oder auszuschalten. Es können mehrere Kontrollkästchen aktiviert sein.

Radio-Buttons

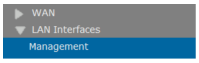
(im nebenstehenden Bild oben ausgeschaltet, unten eingeschaltet): In einer zusammengehörigen Gruppe solcher Elemente ist stets eines eingeschaltet und alle anderen ausgeschaltet. Vor, hinter oder über dem Feld steht die zugehörige Feldbeschriftung. Anklicken, um die entsprechende Funktion einzuschalten.

Dreiecke



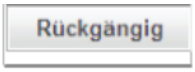
(im nebenstehenden Bild oben: Menü geschlossen, unten: Menü geöffnet): Im Menübereich kann durch Klicken auf ein Dreieck ein Menü geöffnet oder geschlossen werden. Das Öffnen von mehreren Menüs ist möglich.

Menüpunkte



(im nebenstehenden Bild oben: Menüpunkt nicht aktiv, unten: Menüpunkt aktiv): Durch Klicken auf einen Menüpunkt wird der dazugehörige Dialog angezeigt. Ein nicht aktiver Menüpunkt ist grün, ein aktiver Menüpunkt ist weiß.

Schaltflächen



Bei Anklicken wird die Aktion ausgeführt, die als Text auf der Schaltfläche steht. Die Texte sind selbsterklärend, wie z. B. *Rückgängig* oder *Übernehmen*.

Sortierreihenfolge

In einer Tabelle kann durch Anklicken des Dreiecks neben der Überschrift in einem Tabellenkopf die Sortierreihenfolge in der darunterliegenden Spalte geändert werden, z. B. alphabetisch aufsteigend oder absteigend.

3 Konfiguration

WBM-Pfad

WBM **>** Konfiguration

Das Modul Konfigurationwird angezeigt

Bevor Sie mit der Konfiguration beginnen, muss das Gateway wie im Installationshandbuch beschrieben installiert worden sein.

Das Modul Konfiguration dient zum Festlegen der Grundeinstellung und zur Konfiguration der folgenden Einstellungen des Gateways vHG 3575 bzw. der globalen Einstellungen des gesamten SoftGate:

Auswahlmöglichkeiten im Modul Konfiguration

Grundeinstellungen

SIP Load Balancer

Sicherheit

Ansagen/MoH

WAN

LAN Interfaces

Sonstiges

Picture CLIP

3.1 Grundeinstellungen

Im Menü Grundeinstellungen können grundlegende Daten zu vHG 3575 eingegeben werden.

WBM-Pfad

WBM **>** Konfiguration **>** Grundeinstellungen

Das Menü Grundeinstellungen wird angezeigt.

Menü Grundeinstellungen

Die folgenden Optionen werden in diesem Menü angezeigt:

Gateway

Lizenzinformationen

3.1.1 Gateway

WBM-Pfad

WBM > Konfiguration > Grundeinstellungen > Gateway

Der Dialog *Gateway-Eigenschaften* wird angezeigt. In diesem Dialog können Sie Grunddaten eingeben.

Eingabefelder

In diesem Dialog gibt es die folgenden Eingabefelder:

- *System-Name*: Geben Sie den Namen des vHG 3575 (Enterprise Gateway) in dieses Feld ein.
- *Gateway-Standort*: Hier wird der Standort des SoftGates angezeigt. Schreibgeschützt. Der Wert wird von AMO UCSU übernommen.

3.1.2 Lizenzinformationen

- *Advanced Locking ID (ALI):* Die ALI-Zeichenfolge wird angezeigt.

  Wenn die ALI nicht berechnet werden kann, wird der fehlende Parameter angezeigt: (z. B. *Fehlender ALI-Parameter:* Primäre DNS-IP-Adresse). ALI wird benötigt, um SoftGate- oder Enterprise Gateway-Lizenzdateien zu bestellen.
- *Lizenztyp*

  Der Lizenztyp ist entweder SoftGate- oder Enterprise Gateway-Basislizenz.
- *Lizenz-Version*

  Die Version der angeforderten SoftGate- oder Enterprise Gateway-Basislizenz wird angezeigt.
- *Lizenzstatus: (z. B.* 30-Tage-Toleranzeriode)
- *Ablauf der Lizenz:* (z. B. 15 Tage)
- SIEL-ID

  Hier wird die SIEL-ID der aktuell verwendeten SoftGate- oder Enterprise Gateway-Basislizenz angezeigt. SIEL-ID kann nur angezeigt werden, wenn eine gültige Lizenzsitzung eingerichtet werden konnte. Wenn das SoftGate oder Enterprise Gateway über keine gültige Lizenzdatei verfügt oder sich noch in der Toleranzperiode befindet, wird keine SIEL-ID angezeigt.

3.1.3 Lizenzimport

WBM-Pfad

WBM > Configuration > Basic Settings > License Import (WBM > Konfiguration > Grundeinstellungen > Lizenzimport)

Das Dialogfeld „License Import“ (Lizenzimport) wird angezeigt. Hier können Sie die SoftGate-Lizenz importieren.

Eingabefeld

In diesem Dialog wird das folgende Eingabefeld angezeigt:

- Filename (Dateiname): In dieses Feld können Sie den Namen der Lizenzdatei, die Sie importieren möchten, sowie den Pfad zu deren

Speicherort eingeben. Sie können auch auf „Durchsuchen“ klicken, um die Datei auszuwählen.

Schaltflächen:

In diesem Dialog werden folgende Schaltflächenangezeigt:

- Load (Laden): Die spezifische Lizenzdatei wird geladen.
- Undo (Rückgängig machen): Pfad und eingegebener Dateiname werden gelöscht.

Vorgehensweise

Zum Importieren der Lizenzdatei gehen Sie wie folgt vor:

1) Geben Sie den Pfad und den Namen der Lizenzdatei ein, oder wählen Sie die Datei über die Schaltfläche „Durchsuchen“ aus.
2) Klicken Sie auf die Schaltfläche „Load“ (Laden). Die Lizenzdatei ist nun geladen.

3.2 SIP Load Balancer

WBM-Pfad

WBM **>** Konfiguration **>** SIP Load Balancer

Das Menü SIP Load Balancer wird geöffnet.

Menü SIP Load Balancer

Dieses Menü bietet folgende Optionen zur Auswahl:

Einstellungen

Status

SPE (SIP Load Balancer)

Leistungsmerkmalbeschreibung

SIP-Load-Balancing wird zur Lastverteilung des SIP-bezogenen Datenverkehrs im IP-Netzwerk eingesetzt. Damit wird die Leistung der beteiligten SIP-Server skaliert, eine Überlastung der Server vermieden und eine hohe Verfügbarkeit der SIP-Dienste erreicht.

Load Balancing dient dazu, Rufe von einem Provideranschluss, einer OpenScape UC oder OpenScape Xpressions auf mehrere Gateways zu verteilen, z. B. wenn der Anschluss mehr als die maximalen Kanäle eines Gateways hat. Bei einem Provideranschluss kann nur eine Ziel-IP-Adresse konfiguriert werden, sodass ohne Load Balancing pro Gateway ein Providerderanschluss vorhanden sein muss.

Anrufe können auch selektiv über ihre Rufnummer von einer Verbindung zu mehreren sogar geografisch verteilten Gateway-Gruppen oder OpenScape 4000-Systemen mithilfe einer Routing-Nummer (z. B. Ortsvorwahl) gesendet werden, die für jedes Gateway konfiguriert werden kann. Innerhalb einer Gruppe werden die Rufe an das Gateway mit den meisten freien Kanälen gesendet.

SIP-Load-Balancing kann für jedes SIP-Gateway (HG 3500, vHG 3500 SIP oder STMIX) im Netzwerk aktiviert werden. Ist das Leistungsmerkmal korrekt

aktiviert, ist eine Registrierung der teilnehmenden Gateways am SIP Load Balancing Server nur möglich über das OpenScape 4000 SoftGate WBM.

SIP Load Balancing wird auch mit mehreren OpenScape UC Media Servern freigegeben. Diese können sich nicht automatisch beim SIP Load Balancing Server registrieren. Deshalb müssen sie manuell im OpenScape 4000 SoftGate WBM konfiguriert werden.

Serviceinformationen für OpenSIPS Load Balancer

Der OpenSIPS Load Balancer ist Teil des OpenScape 4000 SoftGate Softwarepaketes und wird mit jedem OpenScape 4000 SoftGate installiert. Er läuft auf dem OpenScape 4000 SoftGate, hat aber eine eigene (von dem OpenScape 4000 SoftGate verschiedene) IP-Adresse. Die IP-Adresse wird während der Installation eingerichtet.

Mit Hilfe seiner konfigurierten IP-Adressen holt sich der Load Balancer automatisch seinen eventuell vorhandenen DNS-Server-Namen vom DNS-Server.

Das Leistungsmerkmal Load Balancing ist standardmäßig ausgeschaltet und muss über das WBM des OpenScape 4000 SoftGate und das WBM aller teilnehmenden Gateways eingeschaltet werden.

Leistungsmerkmale

- "Load Balancing" für Inbound native SIP-Verbindungen zu virtuellen HG 3500 Gateways (OpenScape 4000 SoftGate) und den auf dem Betriebssystem vxWorks basierten HG 3500 Gateways (IPDA) (z. B. bei SIP Provider oder OpenScape UC Anbindung).
- Unterstützt native SIP Trunks ohne Registrierung.
- Virtuelle HG 3500 Gateways unterschiedlicher OpenScape 4000 SoftGates und HG 3500 Gateways in unterschiedlichen Access Points werden unterstützt.
- Error Logging/Tracing mit OpenSIPS.
- Failover-Mechanismen für Inbound-Verbindungen, die vom Gateway aufgrund von Fehlermeldungen abgewiesen wurden.
- Status Monitoring der konfigurierten Gateways über den Open SIPS Load Balancer.
- Load Balancing für verschiedene Gruppen von Gateways.

Voraussetzungen

- Im Netzverbund muss ein OpenScape 4000 SoftGate vorhanden sein.
- SIP-Load-Balancing kann nur aktiviert werden, wenn die Verwendung von SIP-Trunking-Profilen aktiviert ist.
- Damit SIP-Load-Balancing funktionieren kann, muss sichergestellt werden, dass die (Outbound)-Proxy-Einstellungen im SIP-Trunking-Profil korrekt konfiguriert sind.

Einschränkungen

- Das Leistungsmerkmal "SIP Load Balancing" kann nur bei einem "Standalone SoftGate" Deployment verwendet werden. Es steht also zum Beispiel für "Survivable SoftGate" nicht zur Verfügung.

Generierung:

Wichtig: Eine Generierung über AMOs ist nicht möglich.

3.2.1 Einstellungen

Der SIP-Load-Balance Server wird über das WBM des OpenScape 4000 SoftGates aktiviert. Dazu müssen die IP-Adresse des Load Balancers und die Netzwerkmaske eingegeben werden.

Nach jeder Aktivierung/Deaktivierung oder Änderung der IP-Adresse des Load Balancers ist ein Restart des OpenScape 4000 SoftGates notwendig.

WBM-Pfad

WBM **>** Konfiguration **>** SIP Load Balancer **>** Einstellungen

Der Dialog *SIP Load Balancer Einstellungen* wird geöffnet.

Eingabefelder/Kontrollkästchen

Im Dialog *SIP Load Balancer Einstellungen* ist einzustellen:

- *IP Adresse [IPv4]*: In dieses Eingabefeld ist die IP-Adresse des SIP-Load-Balance-Servers im IPv4-Format einzugeben.
- *Netzmaske [IPv4]*: In dieses Eingabefeld ist die Netzmaske des Subnetzes im IPv4-Format einzugeben, in dem sich SIP-Load-Balance Server befindet.
- *Default Gateway [IPv4]*: In dieses Eingabefeld ist die IP-Adresse des Default-Gateways im IPv4-Format einzugeben.
- *VLAN-Tagging verwenden*: Aktivierbar/Deaktivierbar. Mit IEEE802.1p/q wird ermöglicht, dass sich mehrere virtuelle LANs ein gemeinsames physikalisches Netz teilen. Das virtuelle LAN ist paketbasiert, im Gegensatz zu älteren portbasierten LANs. Im Datenbereich des Ethernet-Pakets befindet sich ein Tag, das definiert, zu welchem VLAN das Ethernet-Paket gehört und welche Priorität das Datenpaket hat.
- *VLAN-ID*: Jedem VLAN wird eine eindeutige Nummer zugeordnet, die VLAN-ID. Alle Geräte, welche dieselbe VLAN-ID haben, können miteinander kommunizieren.
- *Aktivieren*: Aktivierbar/Deaktivierbar. Die geänderten Einstellungen dieses Dialoges aktivieren.

Wichtig: Damit alle Konfigurationsänderungen wirksam werden, muss OpenScape 4000 SoftGate neu gestartet werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen muss das OpenScape 4000 SoftGate neu gestartet werden.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

3.2.2 Status

Es werden die konfigurierten Gateways für das SIP Load Balancing angezeigt.

WBM-Pfad

WBM > Konfiguration > SIP Load Balancer > Status

Der Dialog *SIP Load Balancer Status* wird geöffnet.

Spalten

In der Tabelle *SIP Load Balancer Status* gibt es folgende Spalten:

- *LTU* Line Trunk Unit = Leitungsanschluss. Shelf 17 - 99 sind über IPDA mit dem Prozessor verbunden. Diese Option ist im WBM konfigurierbar.
- *Slot*: Einbauteilung des OpenScape 4000 Gateways. Diese Option ist im WBM konfigurierbar.
- *Gateway IPv4-Adresse:* IP-Adresse des Gateways im IPv4-Format.
- *IPv4 Port*: Der SIP-Port wird für unverschlüsselte Signalisierungsdaten (z. B. 5060) verwendet.
- *IPv4 TLS Port:* SIP-Port 5061 wird für mit TLS (Transport Layer Security) verschlüsselte Signalisierungsdaten verwendet.
- *Gateway IPv6-Adresse:* IP-Adresse des Gateways im IPv6-Format.
- *IPv6 Port*: Der SIP-Port wird für unverschlüsselte Signalisierungsdaten (z. B. 5060) verwendet.
- *IPv6 TLS Port:* SIP-Port 5061 wird für mit TLS (Transport Layer Security) verschlüsselte Signalisierungsdaten verwendet.
- *Routing Number*: Einwahlnummern (z. B. +4982700332200 für "1" und +4982700332201 für "11")
- *Max Number of B-Channels*: Es sollte die maximal mögliche Anzahl paralleler B-Kanäle verwendet werden.
- *Laden*: Laden zum Gateway
- *Enabled*: Anzeige, ob das Gateway erreichbar ist.

Schaltflächen

In der Tabelle *SIP Load Balancer Status* gibt es folgende Schaltflächen:

- *Delete Rule*: Regel für Gateway löschen.
- Add Rule: Regel für Gateway anlegen.

3.2.3 SPE (SIP Load Balancer)

Durch SPE (Signaling & Payload Encryption) werden VoIP-Nutz- und Signalisierungsdatenströme vom und an den Load Balancer verschlüsselt. Diese Funktion basiert auf einem asymmetrischen Verschlüsselungsprozess. Öffentliche und private Schlüssel werden für diese Art von Prozess verwendet.

Die einzelnen VoIP-Gateways und Load Balancer müssen im Kommunikationssystem identifizierbar sein. Dazu werden Zertifikate mit privaten oder öffentlichen Schlüsseln verwendet.

Je nach Anforderung können Sicherheitseinstellungen zur Bewertung der Zertifikate und zur Verschlüsselung von Datenströmen aktiviert oder deaktiviert werden. So wird die Verschlüsselungssicherheit erhöht oder verringert.

WBM-Pfad

WBM > Konfiguration > SIP Load Balancer > SPE (SIP Load Balancer)

Das Menü SPE (SIP Load Balancer) wird angezeigt.

SPE (SIP Load Balancer)

Die folgenden Optionen werden in diesem Menü angezeigt:

Keycert importieren

Keycert anzeigen

Keycert löschen

SPE-Sicherheitseinstellung für HFA

3.2.4 Keycert importieren

Anmerkung: Wenn Sie bei aktiviertem SPE das erste Mal ein Zertifikat importieren, wird anschließend automatisch ein Reset durchgeführt.

WBM-Pfad

WBM **>** Konfiguration **>** SIP Load Balancer**>** SPE (SIP Load Balancer)**>** Keycert importieren

Der Dialog *Laden eines SPE Key Zertifikats über HTTP* wird angezeigt.
In diesem Dialog kann ein SPE Key Zertifikat durch Eingeben des Entschlüsselungskennworts und des Dateinamens importiert werden. Die Datei mit dem Zertifikat stammt von einer Kunden-PKI-Zertifizierungsstelle (RA/CA) oder der internen DLS-Server-Zertifizierungsstelle (CA) und muss im PEM- oder PKCS#12-Format vorliegen.

Eingabefelder

In diesem Dialog gibt es die folgenden Eingabefelder:

- *Entschlüsselungskennwort*: Geben Sie in diesem Feld das Kennwort ein, das bei der Erstellung der PEM- oder PKCS#12-Datei verwendet wurde.
- *Datei mit Zertifikat und privatem Schlüssel (PEM oder PKCS#12-Format)*: In dieses Eingabefeld sind der Pfad und der Name der Datei, die das Zertifikat enthält, einzugeben. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Fingerabdruck des Zertifikats anzeigen*: Durch Prüfen des Fingerabdrucks kann festgestellt werden, ob ein unverändertes Zertifikat vorliegt oder ob es verändert wurde.
- *Zertifikat aus Datei importieren*: Das Zertifikat wird aus der im oben genannten Eingabefeld angegebenen Datei importiert.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein SPE-Zertifikat zu laden:

1) Auswählen: *WBM* **>** Konfiguration **>** SIP Load Balancer **>** SPE (SIP Load Balancer)**>** Keycert importieren*. Laden eines SPE Key Zertifikats über HTTP* wird angezeigt. Folgende Felder können bearbeitet werden:
   - *Entschlüsselungskennwort*: Geben Sie in diesem Feld das Kennwort ein, das bei der Erstellung der PEM- oder PKCS#12-Datei verwendet wurde.
   - *Datei mit Zertifikat und privatem Schlüssel (PEM oder PKCS#12-Format)*: Geben Sie den Pfad und den Dateinamen der Datei ein, die die zu importierenden Zertifikatsdaten enthält. Klicken Sie auf *Durchsuchen*, um einen Dialog zur Suche nach der Datei zu öffnen
2) Klicken Sie auf *Fingerabdruck des Zertifikats anzeigen*. Ein Fenster mit dem Fingerabdruck des zu importierenden Zertifikats wird angezeigt:
   a) Überprüfen Sie den Fingerabdruck (Hexadezimalzahl). Wenn das Zertifikat geändert wird, ändert sich immer der Fingerabdruck. Nur ein unveränderter Fingerabdruck ist eine Gewähr für ein unverändertes Zertifikat. Sind die beiden Fingerabdrücke nicht identisch, dann liegt wahrscheinlich ein Angriffsversuch vor. In diesem Fall darf der Schlüssel nicht mehr verwendet werden; darüber hinaus sind die festgelegten Maßnahmen zu ergreifen.
   b) Klicken Sie auf *OK*, um das Fenster mit dem Fingerabdruck zu schließen.
3) Klicken Sie auf *Zertifikat aus Datei importieren*, wenn Sie mit der Prüfung des Fingerabdrucks zufrieden sind. Importieren Sie das Zertifikat nicht, falls der Fingerabdruck nicht Ihren Erwartungen entspricht.

3.2.5 Keycert anzeigen

WBM-Pfad

WBM **>** Konfiguration **>** SIP Load Balancer **>**SPE (SIP Load Balancer) **>** Keycert anzeigen

Der Dialog *Zertifikatsinformationen* wird angezeigt. In diesem Dialogfeld können Sie das SPE-Zertifikat sehen, z. B. um es zu testen.

Angezeigte Daten

Die folgenden Zertifikatsdaten werden angezeigt:

- *Allgemeine Daten:* Name des Zertifikats, Zertifikatstyp, Seriennummer des Zertifikats, Seriennummer des Zertifikats (hex), Signatur-Algorithmus-Typ, Beginn der Zertifikatsgültigkeit (GMT), Ende der Zertifikatsgültigkeit (GMT), CRL-Verteilungspunkt
- *Ausgestellt durch CA:* Land (C), Organisation (O), Organisationseinheit (OU), Allgemeiner Name (CN) (CN)
- *Antragsteller:* Land (C), Organisation (O), Organisationseinheit (OU), Allgemeiner Name (CN) (CN)
- *Alternativer Antragstellername*
- *Verschlüsselungsdaten mit öffentlichem Schlüssel:* Länge des öffentlichen Schlüssels, Öffentlicher Schlüssel, Fingerabdruck

3.2.6 Keycert löschen

WBM-Pfad

WBM **>** Konfiguration **>** SIP Load Balancer **>**SPE (SIP Load Balancer) **>** Keycert löschen

Der Dialog *Zertifikat für SPE löschen* wird angezeigt. In diesem Dialogfeld können Sie das SPE-Zertifikat entfernen, z. B. wenn ein neues Zertifikat benötigt wird.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Löschen*: Das SPE-Zertifikat kann nach einer Warnung gelöscht werden.
- *Abbrechen* Der Löschvorgang wird abgebrochen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein SPE-Zertifikat zu entfernen:

1) Auswählen: *WBM* **>** Konfiguration **>** SIP Load Balancer**>**SPE (SIP Load Balancer) **>** Keycert löschen. Eine Warnung wird angezeigt. Zu Prüfzwecken wird außerdem der Name des Zertifikats angegeben.
2) Klicken Sie auf *Löschen* und im Bestätigungsdialog auf *OK*.

3.2.7 SPE-Sicherheitseinstellung für HFA

WBM-Pfad

WBM **>** Konfiguration **>** SIP Load Balancer **>** SPE (SIP Load Balancer) **>** SPE-Sicherheitseinstellung für HFA

Der Dialog *SPE Sicherheitseinstellung für HFA* wird angezeigt. In diesem Dialog können die Sicherheitseinstellungen für Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE)) an die Sicherheitsanforderungen des Kunden angepasst werden. Dies betrifft die Verschlüsselung der Signalisierungs- und Nutzdaten bei der Kommunikation zwischen vHG 3575 und den VoIP-Clients bzw. zwischen zwei vHG 3575-Systemen.

Dropdownlisten, Eingabefelder, Kontrollkästchen

In diesem Dialog werden folgende Einstellungen angezeigt:

- *TLS für LoadBalancer aktivieren:* Diese Option wird für das Load-Balancer-Leistungsmerkmal SPE verwendet.
- *Maximales Intervall für Schlüssel-Neuverhandlung [Stunden]*: Dieser Wert gibt an, wie lange ein bestimmter Schlüssel für die Verschlüsselung der Signalisierungs- und Nutzdaten verwendet werden soll. Wenn diese Zeit verstrichen ist, wird ein neuer Schlüssel definiert.
- *Salt Key Verfahren verwenden*: Mit diesem Verfahren können Kennwörter stark verschlüsselt werden. Dies macht eine Entschlüsselung erheblich schwieriger oder sogar unmöglich. Zum Beispiel ist es nach der Verschlüsselung nicht mehr möglich zu erkennen, ob zwei Benutzer das gleiche Kennwort haben.

- *SRTP-Authentifizierung notwendig* (SRTP: Secure Real-time Transport Protocol): Durch die SRTP-Authentifizierung werden Nutzdatenfälschungen und Replay-Attacken verhindert. Es wird auch überprüft:
  - ob eine Payload-Nachricht eines VoIP-Clients gefälscht ist,
  - ob eine Payload-Nachricht bereits empfangen wurde.
- *SRTCP Verschlüsselung notwendig* (SRTCP: Secure Real-time Transport Control Protocol): Durch die SRTCP-Verschlüsselung werden Fälschungen der Signalisierungsdaten und Replay-Attacken verhindert. Es wird auch überprüft:
  - ob eine VoIP-Client-Signaldatennachricht gefälscht ist,
  - ob eine Signaldatennachricht bereits empfangen wurde.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert.
- *Rückgängig:* Die Eingaben werden verworfen und auf die Defaultwerte zurückgesetzt.

Vorgehensweise

Um die SPE-Sicherheitseinstellungen zu ändern, gehen Sie wie folgt vor:

1) Auswählen: *WBM* **>** Konfiguration **>** SIP Load Balancer**>** SPE (SIP Load Balancer) **>** SPE-Sicherheitseinstellung für HFA. Der Dialog *SPE-Sicherheitseinstellung ändern* wird angezeigt.
2) Nehmen Sie die gewünschten Einstellungen vor, siehe Abschnitt "Dropdownlisten, Eingabefelder, Kontrollkästchen".

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.
Die geänderten Daten werden in die Konfiguration übernommen.

3.3 Sicherheit

Im Menü "Sicherheit" können Sie die Master Encryption Keys (MEKs), Sicherheitsoptionen und die TLS-Konfiguration für HTTPS verwalten.

WBM-Pfad

WBM **>** Konfiguration **>** Sicherheit

Das Menü Sicherheit wird angezeigt.

Menü Sicherheit

Dieses Menü bietet folgende Optionen zur Auswahl:

Verwalten von MEKs

Sicherheitsoptionen

TLS-Konfig für HTTPS

3.3.1 Verwalten von MEKs

WBM-Pfad

WBM > Konfiguration > Sicherheit > Verwalten von MEKs

Der Dialog *Master Encryption Key (MEK) Verwaltung* wird angezeigt: In diesem Dialog können Sie MEKs für vHG 3575 hinzufügen oder entfernen. Ein MEK ist ein spezieller symmetrischer Schlüssel, der zum Aufbau einer verschlüsselten IP-Verbindung zwischen OpenScape 4000 SoftGate und dem OpenScape 4000 Host System benötigt wird. Er besteht aus genau 16 alphanumerischen Zeichen.

Eingabefeld

Dieser Dialog enthält das folgende Eingabefeld:

- *MEK [16 Zeichen]:* Hier muss derselbe MEK eingegeben werden, der zuvor im OpenScape 4000 Assistant eingegeben wurde. Sie können mehrere MEKs eingeben.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *MEK hinzufügen:* Die in das Eingabefeld *MEK* eingegebenen MEKs werden zu OpenScape 4000 SoftGate hinzugefügt.
- *Alle MEKs löschen:* Alle zuvor hinzugefügten MEKs werden entfernt.
- *Rückgängig:* Die Eingaben in diesem Fenster werden zurückgesetzt.

Vorgehensweise

Führen Sie zum Hinzufügen eines MEKs die folgenden Schritte durch:

1) Geben Sie in das Eingabefeld *MEK* die 16 alphanumerischen Zeichen des MEKs ein, den Sie hinzufügen möchten.
2) Klicken Sie auf die Schaltfläche *MEK hinzufügen*. Der MEK wird der lokalen MEK-Verwaltung hinzugefügt. Wenn einer der MEKs mit dem MEK im OpenScape 4000-System übereinstimmt, kann die Verbindung zwischen vHG 3575 (Enterprise Gateway) und dem OpenScape 4000-System aufgebaut werden.

3.3.2 Sicherheitsoptionen

WBM-Pfad

WBM > Konfiguration > Sicherheit > Sicherheitsoptionen

Der Dialog *Sicherheitsoptionen* wird angezeigt.

Kontrollkästchen

In diesem Dialog gibt es die folgenden Kontrollkästchen:

- *Sichere TLS-Neuverhandlung erzwingen (RFC 5746)*: Gilt nur für HFA. TLS ist anfällig für Situationen, in denen ein böswilliger Server eine Verbindung zu einem Zielserver herstellt, diesen mit seinen eigenen manipulierten Daten füttert und dann die neue TLS-Verbindung von einem Client zuschaltet. Der Zielserver behandelt den anfänglichen TLS-Handshake des Clients als Neuverhandlung einer bestehenden Verbindung, die der böswillige Server zuvor hergestellt hat, und geht deshalb davon aus, dass die anfänglich vom Angreifer übertragenen Daten von derselben Entity stammen wie die

nachfolgenden Client-Daten. Dieses Problem lässt sich durch eine sichere Neuverhandlung gemäß RFC 5746 vermeiden.

Anmerkung: Änderungen werden erst nach einem Neustart des SoftGates aktiv.

Anmerkung: Diese Option gilt für alle konfigurierten HFA-Baugruppen des gesamten SoftGate.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen muss das OpenScape 4000 SoftGate neu gestartet werden.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt

3.3.3 TLS-Konfig für HTTPS

WBM-Pfad

WBM **>** Konfiguration **>** Sicherheit **>** TLS-Konfig für HTTPS**>** *TLS-Konfiguration für HTTPS*

In Openscape 4000 V10 wird TLSv1.0 nicht mehr angeboten.

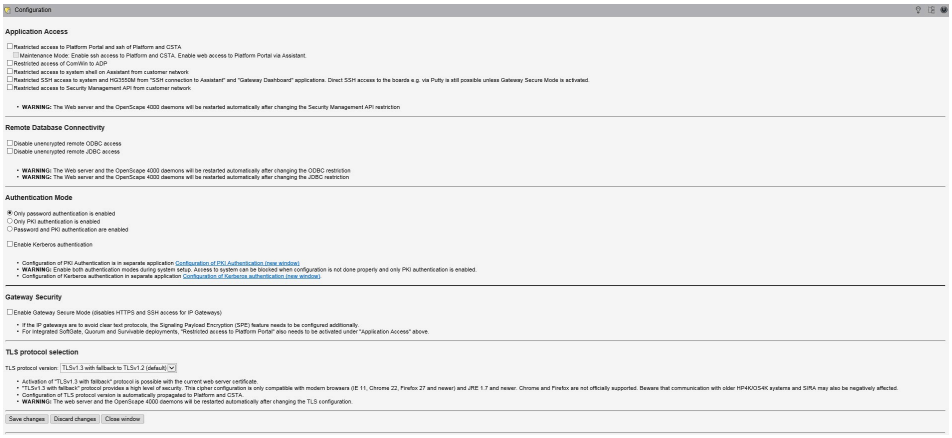
Die einzige in Assistant verfügbare Option wird TLSv1.3 mit Fallback auf TLSv1.2 sein.

SSLv2 und SSLv3 sind aus Sicherheitsgründen nicht erlaubt.

Anmerkung: Für integrierte oder survivable SoftGates erfolgt die Konfiguration der TLS-Protokollversion über Assistant SecM

Die TLS-Version kann im WBM für StandAlone SoftGates konfiguriert werden. Es wird vom Webserver des SoftGates angeboten und unterstützt. Die konfigurierten TLS-Versionen gelten für alle Boards von SoftGate.

Die Standardkonfiguration des Webservers in V10 ermöglicht die Kommunikation in TLSv1.3 mit Fallback auf TLSv1.2.



3.4 Ansagen/MoH

Im Menü Ansagen/MoH können Sie die externen und internen Ansagen und die Einstellungen für Musik im Wartezustand (Music on Hold, MoH) verwalten.

WBM-Pfad

WBM **>** Konfiguration **>** Ansagen/MoH

Der Dialog *Ansagen/MoH* wird angezeigt.

Menü Ansagen/MoH

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Externe Ansagen

Interne Ansagen

3.4.1 Externe Ansagen

WBM-Pfad

WBM **>** Konfiguration **>** Externe Ansagen

Der Dialog *Externe Ansagen verwalten* wird angezeigt.

In diesem Dialog können die Einstellungen für die Ansagebaugruppe, auf der die Ansagen gespeichert sind, vorgenommen werden.

Eingabefelder

In diesem Dialog gibt es die folgenden Eingabefelder:

- *Slot-Circuit:* Nur Slots mit konfigurierten vSLAM und vTMOM werden in der Dropdownliste angezeigt.
- *Dateiname:* In dieses Eingabefeld sind der Pfad und der Name der Datei einzugeben, welche die Ansage enthält (wav-Datei im Format "PCM16, 8 kHz, mono"). Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

Anmerkung: Während des Ladevorgangs wird die wav-Datei dahingehend überprüft, ob sie ein gültiges Format hat und ob alle Einschränkungen (PCM16, 8 kHz, mono) erfüllt werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Laden:* Die angegebene Datei wird geladen.
- *Rückgängig:* Der eingegebene Pfad und der Dateiname werden gelöscht.
- *Löschen:* Die betreffende Ansage in der Tabelle *Dateiname*/*Aktion* wird gelöscht.

Tabelle *Dateiname/Aktion*

In dieser Tabelle werden die geladenen Ansagen angezeigt.

Vorgehensweise

Führen Sie zum Laden einer Ansage die folgenden Schritte durch:

1) Geben Sie in das Eingabefeld *Circuit (0-255)* den erforderlichen Wert ein.
2) Geben Sie den Pfad und den Namen der Datei ein, welche die Ansage enthält oder wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus.
3) Klicken Sie auf *Laden*. Die Datei wird geladen und in der Tabelle *Dateiname/Aktion* angezeigt.

Mit V10 ermöglicht SoftGate den Download von konfigurierten externen Ansagedateien.

Der Download wird über einen Hyperlink auf den Dateinamen angeboten (Rechtsklick auf den Dateinamen).

3.4.2 Interne Ansagen

WBM **>** Konfiguration **>** Ansagen/MoH > Interne Ansagen

Der Dialog *Interne MoH-Einstellungen* wird angezeigt.

Schaltflächen und Kontrollkästchen

In diesem Dialog gibt es die folgenden Kontrollkästchen und Schaltflächen:

- *Klassische interne MoH aktivieren*: Mit diesem Kontrollkästchen aktivieren bzw. deaktivieren Sie das Leistungsmerkmal *Klassische interne MoH aktivieren*.
- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen muss das OpenScape 4000 SoftGate neu gestartet werden.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt

3.5 WAN

Im Menü *WAN* können Sie die Einstellungen für die WAN-Schnittstelle und für die SPE-Zertifikate konfigurieren. Die WAN-Schnittstelle wird verwendet für die Funktionen HFA@Home, SIP@Home und SIP Trunking (z. B. SIP Service Provider).

WBM-Pfad

WBM **>** Konfiguration **>** WAN

Das Menü WAN wird angezeigt.

Menü WAN

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Einstellungen

SPE (WAN)

3.5.1 Einstellungen

WBM-Pfad

WBM **>** Konfiguration **>** WAN **>** Einstellungen

Der Dialogfeld *WAN-Einstellungen* wird angezeigt:

In diesem Dialog können Sie die Einstellungen für die WAN-Schnittstelle konfigurieren und den Zugriff auf die Telefonbilder über WAN aktivieren bzw. deaktivieren.

Auswahl- und Eingabefelder, Kontrollkästchen

In diesem Dialog gibt es die folgenden Eingabefelder:

- *Reduntantes WAN – ein/aus:*Redundanz für das Management LAN aktivieren/deaktivieren. Wählen Sie die gewünschte Einstellung aus der Dropdownliste. Standardeinstellung: aus (deaktiviert).
- *WAN-Schnittstelle:*Die erforderliche Ethernet-Schnittstelle kann aus der Dropdownliste ausgewählt werden. Standard ist "Deaktiviert"

Kontrollkästchen

Dieser Dialog enthält das folgende Kontrollkästchen:

- *Telefonbilderabruf für WAN aktivieren (Bild CLIP):* Durch Aktivieren/Deaktivieren dieses Kontrollkästchens können Sie festlegen, ob das Abrufen von Telefonbildern, die auf externen Servern gespeichert sind, aktiviert oder blockiert werden soll. Wählen Sie in der Navigationsleiste die Menüoption Picture CLIP, um die Parameter für diese Funktion zu konfigurieren. Weitere Informationen erhalten Sie unter Picture CLIP.

Anmerkung: Änderungen werden erst nach einem Neustart des SoftGates aktiv.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen muss das OpenScape 4000 SoftGate neu gestartet werden.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt

3.5.2 SPE (WAN)

Durch SPE (Signaling & Payload Encryption) werden VoIP-Nutz- und Signalisierungsdatenströme von und zu vHG 3575 verschlüsselt. Diese Funktion basiert auf einem asymmetrischen Verschlüsselungsprozess. Öffentliche und private Schlüssel werden für diese Art von Prozess verwendet.

Die einzelnen VoIP-Clients und Gateways, z. B. vHG 3575, müssen im Kommunikationssystem identifizierbar sein. Dazu werden Zertifikate mit privaten oder öffentlichen Schlüsseln verwendet. Zertifikate werden entweder von einer Kunden-PKI-Zertifizierungsstelle (RA/CA) oder von der internen Zertifizierungsstelle (CA) des DLS-Servers erstellt. Der DLS-Server sendet die Dateien mit diesen Zertifikaten an den Gateway-DLS-Client.

Je nach Anforderung können Sicherheitseinstellungen zur Bewertung der Zertifikate und zur Verschlüsselung von Datenströmen aktiviert oder deaktiviert werden. So wird die Verschlüsselungssicherheit erhöht oder verringert.

WBM-Pfad

WBM **>** Konfiguration **>** WAN **>** SPE (WAN)

Das Menü SPE (WAN) wird angezeigt.

SPE (WAN)***Menü***

Die folgenden Optionen werden in diesem Menü angezeigt:

Keycert importieren

Keycert anzeigen

Keycert löschen

SPE-Sicherheitseinstellungen

3.5.3 Keycert importieren

Anmerkung: Wenn Sie bei aktiviertem SPE das erste Mal ein Zertifikat importieren, wird anschließend automatisch ein Reset durchgeführt.

WBM-Pfad

WBM **>** Konfiguration **>** WAN**>** SPE (WAN)**>** Keycert importieren

Der Dialog *Laden eines SPE Key Zertifikats über HTTP* wird angezeigt.
In diesem Dialog kann ein SPE Key Zertifikat durch Eingeben des Entschlüsselungskennworts und des Dateinamens importiert werden. Die Datei mit dem Zertifikat stammt von einer Kunden-PKI-Zertifizierungsstelle (RA/CA) oder der internen DLS-Server-Zertifizierungsstelle (CA) und muss im PEM- oder PKCS#12-Format vorliegen.

Eingabefelder

In diesem Dialog gibt es die folgenden Eingabefelder:

- *Entschlüsselungskennwort*: Geben Sie in diesem Feld das Kennwort ein, das bei der Erstellung der PEM- oder PKCS#12-Datei verwendet wurde.
- *Datei mit Zertifikat und privatem Schlüssel (PEM oder PKCS#12-Format)*: In dieses Eingabefeld sind der Pfad und der Name der Datei, die das Zertifikat enthält, einzugeben. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Fingerabdruck des Zertifikats anzeigen*: Durch Prüfen des Fingerabdrucks kann festgestellt werden, ob ein unverändertes Zertifikat vorliegt oder ob es verändert wurde.

- *Zertifikat aus Datei importieren*: Das Zertifikat wird aus der im oben genannten Eingabefeld angegebenen Datei importiert.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein SPE-Zertifikat zu laden:

1) Auswählen: *WBM* **>** Konfiguration **>** WAN **>** SPE (WAN)**>** Keycert importieren. *Laden eines SPE Key Zertifikats über HTTP* wird angezeigt. Folgende Felder können bearbeitet werden:

- *Entschlüsselungskennwort*: Geben Sie in diesem Feld das Kennwort ein, das bei der Erstellung der PEM- oder PKCS#12-Datei verwendet wurde.
- *Datei mit Zertifikat und privatem Schlüssel (PEM oder PKCS#12-Format)*: Geben Sie den Pfad und den Dateinamen der Datei ein, die die zu importierenden Zertifikatsdaten enthält. Klicken Sie auf *Durchsuchen*, um einen Dialog zur Suche nach der Datei zu öffnen

2) Klicken Sie auf *Fingerabdruck des Zertifikats anzeigen*. Ein Fenster mit dem Fingerabdruck des zu importierenden Zertifikats wird angezeigt:

a) Überprüfen Sie den Fingerabdruck (Hexadezimalzahl). Wenn das Zertifikat geändert wird, ändert sich immer der Fingerabdruck. Nur ein unveränderter Fingerabdruck ist eine Gewähr für ein unverändertes Zertifikat. Sind die beiden Fingerabdrücke nicht identisch, dann liegt wahrscheinlich ein Angriffsversuch vor. In diesem Fall darf der Schlüssel nicht mehr verwendet werden; darüber hinaus sind die festgelegten MaÃnahmen zu ergreifen.

b) Klicken Sie auf *OK*, um das Fenster mit dem Fingerabdruck zu schließen.

3) Klicken Sie auf *Zertifikat aus Datei importieren*, wenn Sie mit der Prüfung des Fingerabdrucks zufrieden sind. Importieren Sie das Zertifikat nicht, falls der Fingerabdruck nicht Ihren Erwartungen entspricht.

3.5.4 Keycert anzeigen

WBM-Pfad

WBM **>** Konfiguration **>** WAN **>**SPE (WAN) **>** Keycert anzeigen

Der Dialog *Zertifikatsinformationen* wird angezeigt. In diesem Dialogfeld können Sie das SPE-Zertifikat sehen, z. B. um es zu testen.

Angezeigte Daten

Die folgenden Zertifikatsdaten werden angezeigt:

- *Allgemeine Daten:* Name des Zertifikats, Zertifikatstyp, Seriennummer des Zertifikats, Seriennummer des Zertifikats (hex), Signatur-Algorithmus-Typ, Beginn der Zertifikatsgültigkeit (GMT), Ende der Zertifikatsgültigkeit (GMT), CRL-Verteilungspunkt
- *Ausgestellt durch CA:* Land (C), Organisation (O), Organisationseinheit (OU), Allgemeiner Name (CN) (CN)
- *Antragsteller:* Land (C), Organisation (O), Organisationseinheit (OU), Allgemeiner Name (CN) (CN)
- *Alternativer Antragstellername*

- *Verschlüsselungsdaten mit öffentlichem Schlüssel:* Länge des öffentlichen Schlüssels, Öffentlicher Schlüssel, Fingerabdruck

3.5.5 Keycert löschen

WBM-Pfad

WBM **>** Konfiguration **>** WAN **>**SPE (WAN) **>** Keycert löschen

Der Dialog *Zertifikat für SPE löschen* wird angezeigt. In diesem Dialogfeld können Sie das SPE-Zertifikat entfernen, z. B. wenn ein neues Zertifikat benötigt wird.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Löschen*: Das SPE-Zertifikat kann nach einer Warnung gelöscht werden.
- *Abbrechen* Der Löschvorgang wird abgebrochen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein SPE-Zertifikat zu entfernen:

1) Auswählen: *WBM* **>** Konfiguration **>** WAN**>** SPE (WAN) **>** Keycert löschen. Eine Warnung wird angezeigt. Zu Prüfzwecken wird außerdem der Name des Zertifikats angegeben.
2) Klicken Sie auf *Löschen* und im Bestätigungsdialog auf *OK*.

3.5.6 SPE-Sicherheitseinstellungen

WBM-Pfad

WBM **>** Konfiguration **>** WAN **>** SPE (WAN)**>** SPE-Sicherheitseinstellung

Der Dialog *SPE-Sicherheitseinstellung ändern* wird angezeigt. In diesem Dialog können die Sicherheitseinstellungen für Signalling und Payload Encryption (SPE) an die Sicherheitsanforderungen des Kunden angepasst werden.
Dies betrifft die Verschlüsselung der Signalisierungs- und Nutzdaten bei der Kommunikation zwischen vHG 3575 und den VoIP-Clients bzw. zwischen zwei vHG 3575-Systemen.

Dropdownlisten, Eingabefelder, Kontrollkästchen

In diesem Dialog werden folgende Einstellungen angezeigt:

- *Minimale Länge der RSA-Schlüssel:* Legen Sie die minimale Länge des RSA-Schlüssels in dem vom der Remote-Entity übertragenen Zertifikat fest. Je gröÃer der Wert ist, desto sicherer ist der Schlüssel. Minimum: 512 Bit; Maximum 2048 Bit.
- *Maximales Intervall für Schlüssel-Neuverhandlung [Stunden]*: Dieser Wert gibt an, wie lange ein bestimmter Schlüssel für die Verschlüsselung der Signalisierungs- und Nutzdaten verwendet werden soll. Wenn diese Zeit verstrichen ist, wird ein neuer Schlüssel definiert.

- *Sichere Neuaushandlung erzwingen (RFC 5746):* Aktivieren durch Kontrollkästchen.
- *TLS-Protokollversion:* Sie können TLS 1.2 mit Fallback auf TLS 1.0 (Standardeinstellung), Nur TLS 1.0 oder Nur TLS 1.2 auswählen.

TLS 1.2 Chiffrenauswahl

- *Schlüsselvereinbarung*: Wählen Sie mit oder ohne Perfect Forward Secrecy.
- *Verschlüsselung*: Wählen Sie AES-128 mit Fallback auf AES-256 oder Nur AES-256.
- *AES-Betriebsmodus*: Wählen Sie GCM bevorzugt, mit Fallback auf CBC, Nur GCM oder Nur CBC.

TLS-Parameter

- *Zertifikatsprüfungsstufe* Keine, vertrauenswürdig oder vollständig
- *Zertifikatsprüfung mit CRL-Prüfung erforderlich:* Aktivieren/Deaktivieren
- *Prüfung des Antragstellers:* Aktivieren / Deaktivieren

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert.
- *Rückgängig:* Die Eingaben werden verworfen und auf die Defaultwerte zurückgesetzt.

Vorgehensweise

Um die SPE-Sicherheitseinstellungen zu ändern, gehen Sie wie folgt vor:

1) Auswählen: *WBM* **>** Konfiguration **>** WAN**>** SPE (WAN) **>** SPE-Sicherheitseinstellungen. Der Dialog *SPE-Sicherheitseinstellung ändern* wird angezeigt.
2) Nehmen Sie die gewünschten Einstellungen vor, siehe Abschnitt "Dropdownlisten, Eingabefelder, Kontrollkästchen".
3) Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.
Die geänderten Daten werden in die Konfiguration übernommen.

3.6 LAN Interfaces

Mittels der Einstellungen in diesem Menü kann das Voice-LAN vollständig von den Management-, XLink-, HFA- und SIP-Interfaces getrennt werden. Zudem kann ein alternativer LAN-Weg für die Übertragung der Signalisierungsdaten eingestellt werden.

WBM-Pfad

WBM **>** Konfiguration **>** LAN Interfaces

Das Menü LAN Interfaces wird geöffnet:

Menü LAN Interfaces

Dieses Menü bietet folgende Optionen zur Auswahl:

Management Interface

Signalling Survivability Interface

XLink

HFA-Interface

SIP-Interface

3.6.1 Management Interface

Mit der Einführung des Leistungsmerkmals "Separate LAN-Konnektivität für Administration und VoIP" kann das Voice-LAN vollständig vom Management-LAN getrennt werden. Zuvor war es lediglich möglich, das IPDA-LAN vom Kunden-LAN zu trennen.

Wenn Sie das Management-LAN vom Voice-LAN trennen möchten, müssen Sie eine IP-Adresse für das Management-LAN angeben. Im WBM wird nur das LAN-Interface angegeben, auf dem die IP-Adresse für das Management-LAN eingerichtet ist bzw. eingerichtet werden soll, die IP-Adresse selbst wird im RMX-Teil mittels AMO STMIB angegeben.

Wenn eine IP-Adresse für das Management-LAN angegeben ist, verwendet OpenScape 4000 Assistant diese für die Verbindung zum Gateway-WBM über die Kunden-LAN-Schnittstelle. Wenn die IP-Adresse auf den Standardwert 0.0.0.0 eingestellt ist, verwendet OpenScape 4000 Assistant die IP-Adresse das IPDA-LAN.

Die Trennung der beiden Interfaces kann über das Gateway konfiguriert werden.

Die Menüoption *Management Interface* ermöglicht es Ihnen, die Management LAN-Schnittstelle zu aktivieren bzw. zu deaktivieren und die Einstellungen für das Management-LAN zu konfigurieren.

WBM-Pfad

WBM **>** Konfiguration **>** LAN Interfaces **>** Management Interface

Der Dialog *Management Interface Einstellungen* wird angezeigt In diesem Dialog können Sie das Management LAN Interface aktivieren bzw. deaktivieren und die Redundanz für das Management LAN ein- bzw. ausschalten.

Auswahlfelder

In diesem Dialog gibt es die folgenden Auswahlfelder:

- *Redundantes Management LAN*: Das redundante Management LAN-Interface kann ein- oder ausgeschaltet werden. Wählen Sie im Auswahlfeld die gewünschte Einstellung aus:
  - Mögliche Werte: *Ein*, *aus*
  - Standard: *Aus* (deaktiviert)
- *Management LAN Interface:* Die erforderliche Ethernet-Schnittstelle kann aus der Dropdownliste ausgewählt werden. Standard ist "Deaktiviert".

Wichtig: Für das IPDA-Interface und das Management-Interface darf nicht dieselbe LAN/Ethernet-Schnittstelle verwendet werden!

Wichtig: Damit alle Konfigurationsänderungen wirksam werden, muss OpenScape 4000 SoftGate neu gestartet werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen muss das OpenScape 4000 SoftGate neu gestartet werden.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt

3.6.2 Signalling Survivability Interface

"Signaling Survivability über alternatives LAN" schaltet im Störungsfall die Steuerungsverbindung vom IP-Netz auf einen alternativen LAN-Weg um. Die Umschaltung des Signalisierungspfades erfolgt unterbrechungsfrei.

Zusätzlich zu der Konfiguration mit den AMOs muss für die vHG 3575 im OpenScape 4000 SoftGate die LAN-Schnittstelle ausgewählt werden, die für Signaling Survivability genutzt werden soll.

Die Menüoption *Signalling Survivability Interface* ermöglicht es Ihnen, die Einstellungen für das Signalling Survivability Interface zu konfigurieren.

WBM-Pfad

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

Der Dialog *Signalling Survivability Interface Einstellungen* wird angezeigt.In diesem Dialog können Sie das LAN Interface angeben und die LAN-Redundanz ein- bzw. ausschalten. Darüber hinaus werden in diesem Dialog die internen IP-Adressen der TUN-Devices für die HSR-Verbindung angezeigt (HSR: High-availability Seamless Redundancy).

Auswahlfelder

In diesem Dialog gibt es die folgenden Auswahlfelder:

- *Redundantes LAN*: Die LAN-Redundanz für die Schnittstelle kann aktiviert bzw. deaktiviert werden. Wählen Sie im Auswahlfeld die gewünschte Einstellung aus:
  - Mögliche Werte: *Ein*, *aus*
  - Standard: *Aus* (deaktiviert)
- *LAN Interface*: Die gewünschte Ethernet-Schnittstelle kann ausgewählt werden. Die Voreinstellung ist "eth0", jedoch kann jede verfügbare Schnittstelle aus der Dropdownliste ausgewählt werden.

Eingabefelder unter *Interne IP Adressen der TUN-Devices für die HSR-Verbindung (Experten-Einstellungen)*

Für das spezifische Routing über eine HSR-Verbindung via interne TUN-Geräte sind zwei host-interne IP-Adressen erforderlich.

Die Standardeinstellungen sollten nicht geändert werden, solange es keine anderen äquivalenten externen IP-Adressen gibt, die für den Host erreichbar sein müssen.

Da die Standardeinstellungen einem reservierten Bereich angehören, sollte dieser Fall nicht allzu häufig auftreten.

In diesem Dialog gibt es die folgenden Anzeigefelder:

- *IP-Adresse für TUN-Device #1*: Interne IP-Adresse des TUN-Device # 1 für die HSR-Verbindung.
- *IP-Adresse für TUN-Device #2*: Interne IP-Adresse des TUN-Device #2 für die HSR-Verbindung.

Wichtig: Damit alle Konfigurationsänderungen wirksam werden, muss OpenScape 4000 SoftGate neu gestartet werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen muss das OpenScape 4000 SoftGate neu gestartet werden.
- *Rückgängig:* Die Eingaben werden verworfen und auf die Voreinstellung zurückgesetzt.

3.6.3 XLink

XLink (X-LINK) dient zum Anschluss der OpenScape Access (OSA) SLA, SLO, BRI, PRI, SLC und TA Module an ein OpenScape 4000 SoftGate, z. B. OpenScape 4000 Branch (OS4B) oder OpenScape Access 500i/a (OSA500). Die OSA-Module werden mit dem XLink-Schalter des SoftGate (OS4B oder OSA500) verbunden.

Der XLink-Switch des SoftGate verwendet IP, um die Backplane für die Boards innerhalb der OSA-Module zu replizieren. Aus diesem Grund besteht der XLink-Switch aus 1 Gigabit-LAN-Ports, um die notwendige hohe Bandbreite des Sprachverkehrs, d. h. der Nutzdaten/Payload, bereitzustellen.

Anmerkung: Der XLink-Switch in OS4B und OSA500 ist fest mit eth2 verbunden, daher ist diese Netzwerkschnittstelle nur für XLink reserviert.

WBM-Pfad

WBM **>** Konfiguration **>** LAN Interfaces **>** XLink

Der Dialog *XLINK Einstellungen* wird angezeigt: In diesem Dialog können Sie das XLink LAN-Interface deaktivieren oder die dafür verwendete LAN/Ethernet-Schnittstelle auswählen sowie die XLink-Netzwerk-Adresse eingeben.

Auswahl- und Eingabefelder

In diesem Dialog gibt es folgende Auswahl-/Eingabefelder:

- *XLink LAN Interface*: Das XLink LAN-Interface kann deaktiviert oder die dafür verwendete LAN/Ethernet-Schnittstelle ausgewählt werden. Wählen Sie in der Dropdown-Liste die gewünschte Einstellung aus:
  - Mögliche Werte: *Deaktiviert*, *eth2*

- *XLink Netzwerk-Adresse*: Es muss die IP-Adresse eines Netzwerks eingegeben werden, d. h. die letzten beiden Stellen müssen ".0.0" sein, z. B. "10.100.0.0".

Wichtig: Damit alle Konfigurationsänderungen wirksam werden, muss OpenScape 4000 SoftGate neu gestartet werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen muss das OpenScape 4000 SoftGate neu gestartet werden.
- *Rückgängig:* Die Eingaben werden verworfen und auf die Voreinstellung zurückgesetzt.

3.6.4 HFA-Interface

Das HFA-Interface bietet OpenScape 4000-Funktionen in einem IPDA (HFA: HiPath Feature Access, IPDA: Internet Protocol Distributed Architecture).

WBM-Pfad

WBM **>** Konfiguration**>** LAN Interfaces **>** HFA-Interface

Der Dialog *HFA Interface Einstellungen* wird angezeigt: In diesem Dialog können Sie das HFA-Interface ein- oder ausschalten und die dafür verwendete LAN/Ethernet-Schnittstelle auswählen.

Auswahl- und Eingabefelder

In diesem Dialog gibt es die folgenden Auswahlfelder:

- *Redundantes HFA LAN*: Das redundante HFA-Interface kann ein- oder ausgeschaltet werden. Wählen Sie im Auswahlfeld die gewünschte Einstellung aus:
  - Mögliche Werte: *Ein*, *aus*
  - Standard: *Aus* (deaktiviert)
- *HFA LAN Interface*: Die gewünschte Ethernet-Schnittstelle kann ausgewählt werden. Die Voreinstellung ist "Default IPDA", jedoch kann jede verfügbare Schnittstelle aus der Dropdown-Liste ausgewählt werden.

Wichtig: Für das HFA-Interface und das Management-Interface darf nicht dieselbe LAN/Ethernet-Schnittstelle verwendet werden!

Wichtig: Damit alle Konfigurationsänderungen wirksam werden, muss OpenScape 4000 SoftGate neu gestartet werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen muss das OpenScape 4000 SoftGate neu gestartet werden.
- *Rückgängig:* Die Eingaben werden verworfen und auf die Voreinstellung zurückgesetzt.

3.6.5 SIP-Interface

Das SIP-Interface dient dem Aufbau, der Steuerung und dem Abbau von Kommunikationssitzungen mithilfe des SIP in einer IPDA (SIP: Session Initiation Protocol, IPDA: Internet Protocol Distributed Architecture).

WBM-Pfad

WBM **>** Konfiguration**>** LAN Interfaces **>** SIP-Interface

Der Dialog *SIP Interface Einstellungen* wird angezeigt: In diesem Dialog können Sie das SIP-Interface ein- oder ausschalten und die dafür verwendete LAN/Ethernet-Schnittstelle auswählen.

Auswahl- und Eingabefelder

In diesem Dialog gibt es die folgenden Auswahlfelder:

- *Redundantes SIP LAN*: Das redundante SIP-Interface kann ein- oder ausgeschaltet werden. Wählen Sie im Auswahlfeld die gewünschte Einstellung aus:
  - Mögliche Werte: *Ein*, *aus*
  - Standard: *Aus* (deaktiviert)
- *SIP LAN Interface*: Die gewünschte Ethernet-Schnittstelle kann ausgewählt werden. Die Voreinstellung ist "Default IPDA", jedoch kann jede verfügbare Schnittstelle aus der Dropdown-Liste ausgewählt werden.

Wichtig: Für das SIP-Interface und das Management-Interface darf nicht dieselbe LAN/Ethernet-Schnittstelle verwendet werden!

Wichtig: Damit alle Konfigurationsänderungen wirksam werden, muss OpenScape 4000 SoftGate neu gestartet werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen muss das OpenScape 4000 SoftGate neu gestartet werden.
- *Rückgängig:* Die Eingaben werden verworfen und auf die Voreinstellung zurückgesetzt.

3.7 Sonstiges

WBM-Pfad

WBM **>** Konfiguration **>** Sonstiges

Das Menü Sonstiges wird geöffnet:

Menü Sonstiges

Dieses Menü bietet folgende Optionen zur Auswahl:

Fax-Parameter

NGS

QoS Data Collection

3.7.1 Fax-Parameter

WBM-Pfad

WBM **>** Konfiguration **>** Sonstiges **>** Fax-Parameter

Der Dialog *Fax-Parameter* wird angezeigt: In diesem Dialog können die Fax-Parameter für T.38-Fax festgelegt werden. Aufgrund der ITU-T Empfehlung T.38 ist es möglich, über ein paketvermitteltes Netz, z. B. das Internet, Faxe in Echtzeit zu übertragen. Dazu wird das IFP (Internet Facsimile Protocol), welches auf UDP bzw. TCP und IP aufsetzt, verwendet (UDP: User Datagram Protocol, TCP: Transmission Control Protocol).

Die Fax-Parameter werden für das vollständige SoftGate verwendet.

Dropdownlisten, Eingabefelder, Kontrollkästchen

In diesem Dialog werden folgende Einstellungen angezeigt:

- T.38 Fax:
  - *Max. UDP-Datagramm-Größe (Byte):* Zeigt die Maximale Größe eines T.38-UDP-Datagramms in Byte.
  - *Verwendete Fehlerkorrektur (UDP):* Legt fest, welche Methode zur Fehlerkorrektur eingesetzt werden soll (*t38UDPRedundancy* oder *t38UDPFEC*).
  - *Fehler-Korrektur-Modus*: Wenn dieses Kontrollkästchen aktiviert ist, wird einer von 2 möglichen Fehlerkorrekturmechanismen ausgewählt, die das T.38 Fax-Protokoll über UDP zur Verfügung stellt. Beide Mechanismen dienen dazu, dass eine Faxübertragung auch bei begrenzten Paketverlusten im Netzwerk fehlerfrei abläuft.
  - *Fax-Kanal mit ermitteltem Ton öffnen:* Wählton, der von vHG 3575 (Enterprise Gateway) an das Faxgerät gesendet wird. Danach wählt das Faxgerät die Rufnummer.
  - *Anzahl redundanter Pakete*Es kann ausgewählt werden, wie viele redundante Pakete bei den Fehlerkorrekturmechanismen ausgewählt werden. Je größer dieser Wert ist, desto robuster ist die Faxübertragung

gegenüber Paketverlusten auf dem Netzwerk. Dafür steigt bei größeren Werten die benötigte Bandbreite an. Auswählbare Werte: 0, 1, 2

  - *Maximaler Netzwerk-Jitter (ms)*: Wenn der maximale Jitter im Netzwerk bekannt ist, dann geben Sie ihn in diesem Feld ein. Dadurch verkürzt sich die Übertragungszeit bei einigen Faxgeräten. Der Wert muss als Dezimalzahl eingegeben werden. Wertebereich: 140 ms – 500 ms. Standard: 200 ms
- Sonstiges:
  - *ClearMode (ClearChannelData)*: Es kann festgelegt werden, ob der Clear Channel Codec nach RFC 4040 in den RTP-Datenpaketen zu verwenden ist.
  - *Rahmengröße*: Die Größe des Rahmens für den Clear Channel Codec kann festgelegt werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

Vorgehensweise

Führen Sie zum Festlegen der Fax-Parameter die folgenden Schritte durch:

1) Nehmen Sie die gewünschten Einstellungen vor, siehe Absatz *"*Dropdownlisten, Eingabefelder, Kontrollkästchen*"*.
2) Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.
   Die geänderten Daten werden in die Konfiguration übernommen.

3.7.2 NGS

Die Webservice-Lösung NextGen-Service (NGS) überträgt verschiedene Konfigurationsdaten vom zentralen NGS-Server zu den SoftGates (z. B. IPv6-Adressen, SNMP-Konfigurationsdaten oder die IP-Adresse des CICA).

WBM-Pfad

WBM **>** Konfiguration **>** Sonstiges **>** NGS

Der Dialog *NGS-Einstellungen* wird angezeigt.

Wichtig: Damit alle Konfigurationsänderungen wirksam werden, muss OpenScape 4000 SoftGate neu gestartet werden.

Sie können die Nutzung des NGS-Dienstes für Szenarien deaktivieren, bei denen keine HTTPS-Verbindung zum NGS-Server möglich ist (z. B. in einer DMZ).

Eingabefelder

In diesem Dialog gibt es die folgenden Eingabefelder:

- *IP-Adresse des NGS-Servers [IPv4 oder IPv6]*: Die IP-Adresse kann im Format IPv4 oder IPv6 eingegeben werden. Das Standardformat ist IPv4: 0.0.0.0.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen muss das OpenScape 4000 SoftGate neu gestartet werden.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

3.7.3 QoS Data Collection

Quality of Service Data Collection (QDC) - Aufgaben und Funktionen:

Mit dem OpenScape-IP-Service "QoS-Data-Collection" steht ein Tool zur Verfügung, das Daten von OpenScape-Produkten sammelt. Diese Daten werden zur Analyse der Sprach- und Netzwerk-Qualität der Produkte verwendet.

Ziele des "QoS-Data-Collection"-Service mit seinen Leistungsmerkmalen sind:

- Reduzierung der allgemeinen Aufwendungen bei der Analyse von QoS-Problemen.
- Erhöhung der "remote clearance rate".
- Frühzeitiges Erkennen von Netzwerkproblemen zur Vorbeugung gegen Störungen der Sprachqualität.

Das führt zu:

- Reduzierung der Service-Aufwendungen und Kosten.
- Konkurrenzfähigen Wartungsverträgen.
- Schnellen und qualifizierten Antworten zu einem Kundenproblem.
- Erhöhung der allgemeinen Kundenzufriedenheit mit dem Produkt und der Technologie.
- Möglichkeit, Änderungen in der Netzwerkumgebung des Kunden zu erkennen und die Marketing-Aktivitäten von OpenScape-Services entsprechend auszurichten.

Durch den Einsatz von QDC können wichtige Verbesserungen im gesamten Service-Prozess (break/fix process) erzielt werden.

Hintergrundinformationen zu QDC

Siehe *OpenScape 4000 V8 Gateways HG 3500 und HG 3575, Administratordokumentation.*

WBM-Pfad

WBM **>** Konfiguration **>** Sonstiges **>** QoS Data Collection

Der Dialog *Quality of Service Data Collection* wird angezeigt.

Auswahl- und Eingabefelder

Folgende Felder können Sie bearbeiten:

QDC-Konfiguration

- *Senden an QCU*: Aktivieren Sie dieses Kontrollkästchen, wenn Daten an die QCU gesendet werden sollen.

  Standardwert: Kontrollkästchen ist nicht aktiviert.
- *QCU-IP-Adresse*: Geben Sie hier die IP-Adresse oder den Name des QCU-Host ein.

  Standardwert: 0.0.0.0.
- *QCU-Empfangsport*: Empfangsport für QCU. Geben Sie hier die Portnummer des QCU-Host ein.

  Standardwert: 12010.
- *Senden an Network Management aktiv*: Aktivieren Sie dieses Kontrollkästchen, wenn Daten an das Network Management gesendet werden sollen.

  Standardwert: Kontrollkästchen ist nicht aktiviert.
- *IP-Adresse des Network Managements*: Geben Sie die IP-Adresse des Ziels ein.

  Standardwert: 0.0.0.0.
- *Community-String*: n/a

Wichtig: Wenn eines der Kontrollkästchen **Senden an QCU** oder **Senden an Network Management** aktiviert ist (Haken gesetzt), werden QoS-Reports erzeugt.

QDC-Reportmodus

- *Sende Bericht, wenn*: Wählen Sie aus dem Listenfeld den gewünschten Zeitpunkt zur Berichtübertragung aus. Es stehen die folgenden Optionen zur Verfügung:
  - *Session-Ende und Schwellwert überschritten*: Ein Report wird nur am Ende einer Session gesendet und nur wenn der Schwellwert erreicht wurde.
  - *Ende des Berichtsintervalls und Schwellwert überschritten*: Ein Report wird in jedem Berichtsintervall gesendet, wenn der Schwellwert erreicht wurde.
  - *Session-Ende, unbedingt*: Am Session-Ende wird immer ein Report gesendet.
  - *Ende des Berichtsintervalls, unbedingt*: Am Ende des Berichtsintervalls wird immer ein Report gesendet.
- *Berichtsintervall (s)*: Geben Sie das Intervall (in Sekunden) ein, in dem die Berichte gesendet werden sollen. Für jeden Berichtsintervall wird ein QoS-Report gesendet wenn der Reportmodus entsprechend gesetzt wurde.

  Standardwert: 60 Sek.

  Gültige Werte: 0 ... 65535
- *Beobachtungszeitraum (s)*: Dieser Parameter kann nicht eingestellt werden.

  Standardwert: 10 Sek.

- *Minimale Session-Dauer (*100 ms)*: Geben Sie die minimale Session-Dauer

  (*100 ms) hier ein. Besteht eine Session (z. B. eine Gesprächsverbindung) kürzer als dieses Minimum, dann wird kein QoS-Report gesendet.

  Standardwert: 20 (2 s)

  Gültige Werte: 0 ... 255

  Wichtig: Die Zeitskala ist im Beobachtungszeitraum und im Berichtsintervall segmentiert. Jeder Beobachtungszeitraum wird auf eine Schwellwertüberschreitung geprüft. Für jeden Berichtsintervall wird ein QoS-Report gesendet, wenn der Reportmodus entsprechend gesetzt wurde.

QDC-Schwellwerte

- *Oberer Jitter-Schwellwert (ms)*: Geben Sie hier den oberen Jitter-Schwellwert für die Reportauslösung ein. Der Jitter wird gegen diesen Schwellwert geprüft und zwischen zwei aufeinanderfolgenden RTP Paketen gemessen.

  Standardwert: 20 ms

  Gültige Werte: 0 ... 255
- *Schwellwert für durchschn. Paketlaufzeitverzögerung (ms)*: Die Paketlaufzeitverzögerung spiegelt die Gesamtlaufzeiten in beiden Richtungen wider. , ; geben Sie in dieses Feld den Schwellwert für die durchschnittliche Paketlaufzeitverzögerung ein, der die Reportauslösung bewirkt.

  Standardwert: 100msec,

  Gültige Werte: 0 ... 65535
- *Schwellwerte für Komprimierungs-Codec*: Geben Sie hier die gewünschte Anzahl in Paketen der Schwellwerte für die Komprimierungs-Codec ein. Es stehen die folgenden Optionen zur Verfügung:
  - *Verlorene Pakete (pro 1000 Pakete)*: Geben Sie hier den Schwellwert für die Pakete ein, welche bei der Sprachdecodierung verlorengegangen sind. Der Wert ist das Verhältnis von verlorenen Paketen zur Gesamtzahl der Pakete.

    Standardwert: 10

    Gültige Werte: 0 ... 255
  - *Aufeinanderfolgend verlorene Pakete*: Geben Sie hier den Schwellwert für die aufeinanderfolgend verlorenen Pakete ein. Es wird gezählt, wie viele Pakete aufeinanderfolgend (ohne Unterbrechung durch fehlerfreie Pakete) verloren gegangen sind. Wenn der gezählte Wert gröÃer als der angegebene Wert ist, liegt eine Schwellwertüberschreitung vor. Standardwert: 2 Gültige Werte: 0 ... 255
  - *Aufeinanderfolgend verarbeitete Pakete*: Geben Sie hier den Schwellwert der aufeinanderfolgend verarbeiteten Pakete ein. Es wird gezählt, wie viele Pakete hintereinander fehlerfrei waren, ohne durch verlorene Pakete unterbrochen zu sein. Wenn der gezählte Wert kleiner als der angegebene Wert ist, liegt eine Schwellwertüberschreitung vor. Standardwert: 8 Gültige Werte: 0 ... 255
- *Schwellwerte für Nicht-Komprimierungs-Codec*: Geben Sie hier die gewünschte Anzahl von Paketen für die Schwellwerte der Nicht-Komprimierungs-Codec ein. Es stehen die folgenden Optionen zur Verfügung:

- – *Verlorene Pakete (pro 1000 Pakete)*: Erklärung siehe *Schwellwerte für Komprimierungs-Codec*.
  – *Aufeinanderfolgend verlorene Pakete*: Erklärung siehe *Schwellwerte für Komprimierungs-Codec*.
  – *Aufeinanderfolgend verarbeitete Pakete*: Erklärung siehe *Schwellwerte für Komprimierungs-Codec*.

  Erklärung und Verwendung von Komprimierungs- und Nicht-Komprimierungs-Codec:

  Tabelle 1: Codec - Betriebsarten

Codec	Audio-Mode	Anwendung
Hohe Qualität bevorzugt	Unkomprimierte Sprachübertragung.	Unkomprimierte Sprachübertragung verwenden. Geeignet für breitbandige Intranetverbindungen.
Niedrige Bandbreite bevorzugt	Bevorzugt komprimierte Sprachübertragung verwenden.	Geeignet für Verbindungen mit unterschiedlicher Bandbreite.
Nur geringe Bandbreite	AusschlieÃlich komprimierte Sprachübertragung verwenden.	Geeignet für Verbindungen mit geringer Bandbreite.

  Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK* (neuen Konfigurationszustand dauerhaft speichern mit Speichern-Symbol im Steuerbereich). Der Dialog *Quality of Service Data Collection* wird angezeigt.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen sind OpenScape Access 500i/a bzw. OpenScape 4000 SoftGate neu zu starten.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt

3.7.4 WSI-Status

Auf dieser Seite werden die zentrale Konfiguration des auf dem Plattformportal des zentralen Hosts erstellten WSI sowie weitere Informationen zum Status der WSI-Benutzer wie folgt angezeigt:

- Letzte Aktualisierung von Konfiguration und Datenbank: das Datum und die Uhrzeit, zu der das SoftGate die Konfiguration und die Datenbank mit dem zentralen Portal synchronisiert hat
- Anzahl der zur Zeit angemeldeten WSI-Benutzer
- Logbuch der WSI-Benutzeraktivität: zeigt authentifizierte/unauthentifizierte WSI-Benutzer und den Zeitpunkt der Anmeldung/Abmeldung an.

Zum Ändern der WSI-Konfiguration siehe Administratordokumentation für OpenScape 4000 V10, Platform Administration (Portal).

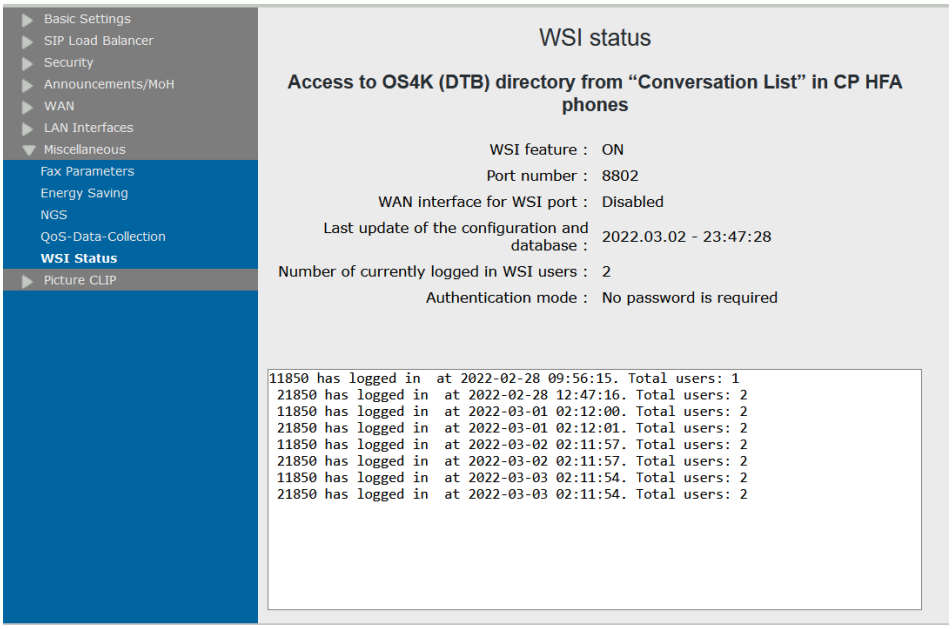


Abbildung 1: WSI-Status

Um die WSI-Konfiguration zu ändern, siehe OpenScape 4000 V10, Platform Administration (Portal), Administratordokumentation.

Anmerkung:

Bei einem CP HFA-Telefon müssen die folgenden Felder leer gelassen werden, wenn das Telefon mit OS4K verbunden ist, damit WSI ordnungsgemäß funktioniert:

- UC-Benutzername aus dem Menü UC-Anmeldeinformationen;
- UC-Passwort aus dem Menü UC-Anmeldedaten;
- UC-Server-Adresse aus dem Menü UC-Server.

---

4 Wartung

Das Modul Wartung stellt Funktionen für die Wartung und Administration von OpenScape 4000 SoftGate zur Verfügung. Dazu gehören das Durchführen von Software-Updates, das Sichern der Konfiguration, das Arbeiten mit Protokolldateien, das Aktivieren von Trace-Profilen, das Erstellen eines Secure Trace, das Erstellen von Diagnosedateien und das Ermitteln von Status-Informationen über OpenScape 4000 SoftGate.

WBM-Pfad

WBM **>** Wartung

Das Modul Wartung wird geöffnet.

Auswahlmöglichkeiten im Modul Wartung

SW-Update

Backup/Restore

Logs

Trace

Secure Trace

Diagnose

Status-Information

Reboot/Shutdown OS

4.1 SW-Update

Im Menü SW-Update (SW: Software) werden Funktionen zum Anzeigen der Software-Version, für das Software-Update und für die Software-Aktivierung von vHG 3575 (Enterprise Gateway) zur Verfügung gestellt.

WBM-Pfad

WBM **>** Wartung **>** SW-Update

Das Menü SW-Update wird angezeigt.

Menü SW-Update

Die folgenden Optionen werden in diesem Menü angezeigt:

SW-Version anzeigen

LW-Update

LW-Aktivierung

OS-Update

4.1.1 SW-Version anzeigen

WBM-Pfad

WBM **>** Wartung **>** SW-Update **>** SW-Version anzeigen

Der Dialog *Softwareversion* wird angezeigt. Dieser Dialog enthält Details über die momentan installierten Software- und Hardwareversionen.

Information

Im Einzelnen werden folgende Angaben gemacht:

- Systemversion (PBX): Dieser Bereich zeigt die OpenScape 4000 Version unter:

  System-Version
- Plattform-Version: Dieser Bereich zeigt an, auf welcher Hardware der vHG 3575 (Enterprise Gateway) läuft, z. B. OpenScape Access 500. Die Angaben dazu sind:

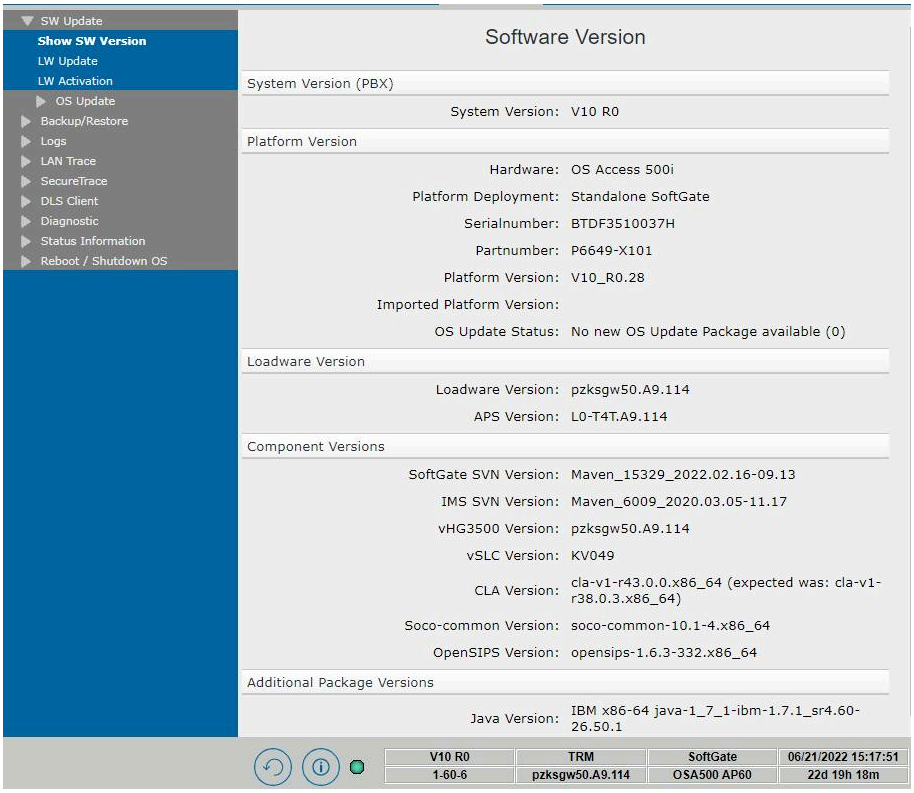
  Hardware, *Plattformbereitstellung*, *Plattformversion*, *Importierte Plattformversion*, *OS-Update-Status*
- Loadwareversion: Dieser Bereich zeigt die installierte Software- und Loadwareversion an. Beispiel:

  Loadwareversion, *APS-Version, RTMX-Loadwareversion.*
- Komponentenversionen: Dieser Bereich zeigt die installierten SoftGate-Komponenten und ihre Versionen. Beispiel:

  IMS SVN Version, *SoftGate SVN Version*, VSLC Version, *CLA Version*, *Soco-common Version*, *OpenSIPS Version*

- Zusätzliche Packageversionen: Dieser Bereich zeigt zusätzlich benötigte Software und ihre Versionen. Beispiel:

  Java Version



4.1.2 LW-Update

WBM-Pfad

WBM > Wartung > SW-Update > LW-Update

Der Dialog *Loadwareaktualisierung* wird angezeigt. In diesem Dialog kann die SoftGate-Loadware geladen werden.

Eingabefeld

Dieser Dialog enthält das folgende Eingabefeld:

- *Dateiname:* In dieses Eingabefeld sind der Pfad und der Name der Datei einzugeben, welche die aktuelle Software enthält. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Laden:* Die angegebene Datei wird geladen.
- *Rückgängig:* Der eingegebene Pfad und der Dateiname werden gelöscht.

Vorgehensweise

Führen Sie zum Laden der SoftGate-Loadware die folgenden Schritte durch:

1) Geben Sie den Pfad und den Namen der Datei ein, welche die aktuelle Software enthält, oder wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus.
2) Klicken Sie auf *Laden*. Die Software wird geladen. Nach dem Laden wird die nächste WBM-Seite automatisch eingeblendet.

4.1.3 LW-Aktivierung

WBM-Pfad

WBM **>** Wartung **>** SW-Update **>** LW-Aktivierung

Der Dialog *Loadwareaktivierung* wird angezeigt. In diesem Dialog kann die geladene SoftGate-Loadware entweder sofort oder zeitgesteuert - zu einem bestimmten Zeitpunkt oder nach einer bestimmten Dauer - aktiviert werden.

Information

In diesem Dialog gibt es die folgenden Angaben:

- *Softwareversion*: Zeigt die Softwareversion der im Dialog *Softwareaktualisierung* geladenen SoftGate-Loadware an.
- *Start der Aktion am*: Die Aktivierung der geladenen SoftGate Loadware soll zu einem bestimmten Zeitpunkt stattfinden. Der Tag dieses Zeitpunktes ist entweder über die Auswahlfelder oder über die Schaltfläche *Kalender* festlegbar.
- *Start der Aktion in*: Die Aktivierung der geladenen SoftGate-Loadware soll nach Ablauf einer bestimmten Zeitdauer stattfinden.
- *Aktion stoppen*: Eine bereits vorher gestartete Aktion für die zeitgesteuerte Aktivierung wird gestoppt.
- *Systemzeit*: Diese Zeit ist die lokale Zeit des OpenScape und die Bezugszeit für die zeitgesteuerte Aktivierung. Diese Daten können nicht bearbeitet werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die geänderten Einstellungen werden gespeichert.
- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf die Defaultwerte zurückgesetzt.
- *Sofort starten:* Die Aktivierung der vHG 3575 (Enterprise Gateway)-Applikation wird sofort gestartet.

Vorgehen für sofortige Aktivierung

Führen Sie zum sofortigen Aktivieren der geladenen Software die folgenden Schritte durch:

1) Klicken Sie auf die Schaltfläche *Sofort starten*. Die Software wird aktiviert.

Vorgehen für zeitgesteuerte Aktivierung

Führen Sie zum zeitgesteuerten Aktivieren der geladenen Software die folgenden Schritte durch:

1) Zeitpunkt oder Dauer festlegen:

- Zeitpunkt, zu dem die Aktivierung erfolgen soll:Aktivieren Sie den Radio-Button *Start der Aktion am* und geben Sie in den Auswahl- und Eingabefeldern *Tag*, *Monat*, *Jahr*, *STD:MM* den Zeitpunkt an. Die Schaltfläche *Kalender* kann dazu ebenfalls benutzt werden.
- Dauer, nach der die Aktivierung erfolgen soll: Aktivieren Sie den Radio-Button *Start der Aktion in* und geben Sie in den Eingabefeldern *Tagen* und *STD:MM* die Dauer an.

2) Klicken Sie auf *Übernehmen*. Die Änderungen werden gespeichert. Die Aktion für die zeitgesteuerte Aktivierung wird gestartet.

Vorgehen für Stoppen der zeitgesteuerten Aktivierung

Führen Sie zum Stoppen einer Aktion für die zeitgesteuerte Aktivierung die folgenden Schritte durch:

1) Aktivieren Sie den Radio-Button *Aktion stoppen*.
2) Klicken Sie auf die Schaltfläche *Übernehmen*. Die Aktion wird gestoppt.

4.1.4 OS-Update

WBM-Pfad

WBM **>** Wartung **>** SW-Update **>** OS-Update

Menü OS-Update

Dieses Menü bietet folgende Optionen zur Auswahl:

OS-Update Einstellungen

OS-Update Aktionen

4.1.4.1 OS-Update Einstellungen

WBM-Pfad

WBM **>** Wartung **>** SW-Update **>** OS-Update **>** OS-Update Einstellungen

Der Dialog OS-Update Einstellungenwird angezeigt. In diesem Dialog können die Transferparameter vom zentralen Host für das Update des OS (Operating System) eingestellt werden. Diese Einstellungen können nur für Standalone-SoftGates und STMIX vorgenommen werden.

Wichtig: Diese Einstellungen sind mit OpenScape 4000 V7R1 bei Standalone-SoftGates noch nicht möglich. Benutzen Sie stattdessen die Funktion "Remote Appliance Reinstall (RAR)".

P2P-Transferparameter vom zentralen Host (nur Standalone SoftGates und STMIX)

- *Max. Downloadgeschwindigkeit beschränken:* Aktivieren/Deaktivieren Sie das Kontrollkästchen. Die maximale Download-Geschwindigkeit für das Update des OS kann auf den Wert, der im darunter stehenden Eingabefeld festgelegt wird, beschränkt werden.
- *Max. Download-Geschwindigkeit (KB/s)*: Eingabefeld für die maximale Downloadgeschwindigkeit in KByte je Sekunde.
- *Max. Upload-Geschwindigkeit beschränken*: Aktivieren/Deaktivieren Sie das Kontrollkästchen. Die maximale Upload-Geschwindigkeit für das Update des OS kann auf den Wert, der im darunter stehenden Eingabefeld festgelegt wird, beschränkt werden.
- *Max. Upload-Geschwindigkeit (KB/s)*: Eingabefeld für die maximale Upload-Geschwindigkeit in KByte je Sekunde.

Schaltflächen

- *Übernehmen*: Die Eingaben werden gespeichert.
- *Rückgängig*: Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

4.1.4.2 OS-Update Aktionen

WBM-Pfad

WBM > Wartung > SW-Update > OS-Update > OS-Update Aktionen

Der Dialog OS-Update Aktionenwird angezeigt. In diesem Dialog kann der Transfer vom zentralen Host für das Update des OS (Operating System) abgebrochen werden (nur für einzelnstehende SoftGates). Für survivable SoftGates kann das OS-Update aktiviert werden.

Wichtig: Diese Einstellungen sind mit OpenScape 4000 V7R1 bei Standalone-SoftGates noch nicht möglich. Benutzen Sie stattdessen die Funktion "Remote Appliance Reinstall (RAR)".

OS-Update Transfer vom zentralen Host (nur Standalone SoftGates und STMIX)

Schaltfläche:

- *Transfer abbrechen*: Der Transfer der OS-Software wird abgebrochen.

OS-Update Aktivierung (nur Surv. SoftGates)

- *Plattform-Version*: Anzeige der OpenScape 4000-Version.
- *Importierte Plattform-Version*: Zeigt die importierte OpenScape 4000-Version an.
- *SoftGate-LW aus dem Updatepaket verwenden (empfohlen)*: Aktivierbar/Deaktivierbar.
- *OS-Update-Status*: Anzeige, ob ein neues Updatepaket für das OS verfügbar ist.

Schaltfläche:

- *OS-Update aktivieren*: Das OS-Update für das Survivable SoftGate aktivieren.

4.2 Backup/Restore

Im Menü Backup/Restore kann die Konfiguration und die Sicherheitskonfiguration der SoftGate-Konfiguration lokal gesichert (exportiert) werden. Diese lokale Sicherung kann geladen (importiert) und anschließend aktiviert werden. Die Sicherung umfasst die lokale Konfiguration aller aktiven Baugruppen des SoftGate.

WBM-Pfad

WBM **>** Wartung**>** Backup/Restore

Das Menü Backup/Restore wird angezeigt.

Menü Backup/Restore

Die folgenden Optionen werden in diesem Menü angezeigt:

Export Konfiguration

Export Sicherheitskonfiguration

Import Konfiguration

Import Sicherheitskonfiguration

4.2.1 Export Konfiguration

WBM-Pfad

WBM **>** Wartung **>** Backup/Restore **>** Export Konfiguration

Der Dialog *Konfiguration exportieren* wird angezeigt. In diesem Dialog kann die SoftGate-Konfiguration lokal gesichert (exportiert) werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Das Exportieren der Konfiguration wird gestartet.
- *Rückgängig:* Das Exportieren der Konfiguration wird abgebrochen.

Vorgehensweise

Führen Sie zum Exportieren der Konfiguration die folgenden Schritte durch:

1) Klicken Sie auf *Übernehmen*. Die Konfiguration wird in eine ZIP-Datei exportiert. Es erscheint das Fenster *Dateidownload* mit der Frage, ob die zip-Datei geöffnet oder gespeichert werden soll.

2) Klicken Sie auf die Schaltfläche *Speichern* und wählen Sie den gewünschten Ordner für die Datei aus. Klicken Sie dann auf die Schaltfläche *OK*. Die ZIP-Datei wird gespeichert.

4.2.2 Export Sicherheitskonfiguration

WBM-Pfad

WBM > Wartung > Backup/Restore > Export Sicherheitskonfiguration

Der Dialog *Sicherheitskonfiguration exportieren* wird angezeigt. In diesem Dialog kann die Sicherheitskonfiguration des SoftGate lokal gesichert (exportiert) werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Das Exportieren der Sicherheitskonfiguration wird gestartet.
- *Rückgängig:* Das Exportieren der Sicherheitskonfiguration wird abgebrochen.

Vorgehensweise

Führen Sie zum Exportieren der Sicherheitskonfiguration die folgenden Schritte durch:

1) Klicken Sie auf *Übernehmen*. Die Sicherheitskonfiguration wird in eine ZIP-Datei exportiert. Es erscheint das Fenster *Dateidownload* mit der Frage, ob die zip-Datei geöffnet oder gespeichert werden soll.
2) Klicken Sie auf die Schaltfläche *Speichern* und wählen Sie den gewünschten Ordner für die Datei aus. Klicken Sie dann auf die Schaltfläche *OK*. Die ZIP-Datei wird gespeichert.

4.2.3 Import Konfiguration

WBM-Pfad

WBM > Wartung> Backup/Restore > Import Konfiguration

Der Dialog *Konfiguration importieren* wird angezeigt. In diesem Dialog kann die zuvor lokal gesicherte SoftGate-Konfiguration wieder importiert werden.

Eingabefeld

Dieser Dialog enthält das folgende Eingabefeld:

- *Dateiname:* In dieses Eingabefeld sind der Pfad und der Name der Datei einzugeben, welche die zu importierende Konfiguration enthält. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Laden:* Die angegebene Konfigurationsdatei wird geladen.
- *Rückgängig:* Der eingegebene Pfad und der Dateiname werden gelöscht.

Vorgehensweise

Führen Sie zum Importieren einer Konfigurationsdatei die folgenden Schritte durch:

1) Geben Sie den Pfad und den Namen der Konfigurationsdatei ein oder wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus.
2) Klicken Sie auf die Schaltfläche *Laden*. Die Konfigurationsdatei wird geladen.

Wichtig: Damit alle Konfigurationsänderungen wirksam werden, muss SoftGate neu gestartet werden.

4.2.4 Import Sicherheitskonfiguration

WBM-Pfad

WBM **>** Wartung**>** Backup/Restore **>** Import Sicherheitskonfiguration

Der Dialog *Sicherheitskonfiguration importieren* wird angezeigt. In diesem Dialog kann die zuvor lokal gesicherte vHG 3575 Sicherheit-Konfiguration wieder importiert werden.

Eingabefeld

Dieser Dialog enthält das folgende Eingabefeld:

- *Dateiname:* In dieses Eingabefeld sind der Pfad und der Name der Datei einzugeben, welche die zu importierende Sicherheitskonfiguration enthält. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Laden:* Die angegebene Datei wird geladen.
- *Rückgängig:* Der eingegebene Pfad und der Dateiname werden gelöscht.

Vorgehensweise

Führen Sie zum Importieren einer Sicherheitskonfiguration die folgenden Schritte durch:

1) Geben Sie den Pfad und den Namen der Datei ein, welche die zu importierende Sicherheitskonfiguration enthält, oder wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus.
2) Klicken Sie auf *Laden*. Die Datei wird geladen.

Wichtig: Damit alle Konfigurationsänderungen wirksam werden, muss vHG 3575 neu gestartet werden.

4.3 Logs

Im Menü Logs können für Diagnosezwecke die Protokolldateien in eine ZIP-Datei exportiert werden. Zum Anlegen neuer Protokolldateien ist das Löschen der alten, d. h. exportierten, Protokolldateien möglich.

WBM-Pfad

WBM **>** Wartung **>** Logs

Das Menü Logs wird angezeigt.

Menü Logs

Die folgenden Optionen werden in diesem Menü angezeigt:

Logs exportieren

Protokolle löschen

Trace-Profile

RTMx-Trace-Profile

4.3.1 Logs exportieren

WBM-Pfad

WBM **>** Wartung **>** Logs**>** Logs exportieren

Der Dialog *Protokolldateien exportieren* wird angezeigt. Sie können die Protokolldateien aller aktiven SoftGate-Baugruppen sichern (exportieren).

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Exportieren:* Die über die Kontrollkästchen ausgewählten Protokolldateien werden lokal gesichert (exportiert).

Vorgehensweise

Führen Sie zum Exportieren von Protokolldateien die folgenden Schritte durch:

1) Klicken Sie auf *Exportieren*. Die Protokolldateien werden in eine ZIP-Datei exportiert. Es erscheint das Fenster *Dateidownload* mit einer Abfrage, ob die ZIP-Datei geöffnet oder gespeichert werden soll.
2) Klicken Sie auf die Schaltfläche *Speichern* und wählen Sie den gewünschten Ordner für die Datei aus. Klicken Sie dann auf die Schaltfläche *OK*. Die ZIP-Datei wird gespeichert.

4.3.2 Protokolle löschen

WBM-Pfad

WBM **>** Wartung **>** Logs**>** Protokolle löschen

Der Dialog *Protokolldateien löschen* wird angezeigt. In diesem Dialog können Sie eine oder mehrere der aufgelisteten Protokolldateien löschen.

Kontrollkästchen

In diesem Dialog gibt es die folgenden Kontrollkästchen:

- *Soco*, *JLM*, *IMS*, ETS, *SPA, Status Collector*, *Update*, *Backtrace*, *Heap Dump*, *Corelogs*, *Garbage Collection*, *Gateway (vHG) Logs, LS-DCL, Load Balancer*, *DHCP, System Diagnostics*
- *Alles:* Es werden alle (Diagnose-)Protokolldateien markiert.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Löschen:* Alle markierten Protokolldateien werden gelöscht.
- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf die Defaultwerte zurückgesetzt.

Vorgehensweise

Führen Sie zum Löschen von Protokolldateien die folgenden Schritte durch:

1) Aktivieren Sie die Kontrollkästchen derjenigen Protokolldateien, die Sie löschen möchten.
2) Klicken Sie auf *Löschen*. Die markierten Protokolldateien werden gelöscht.

4.4 Trace

Unter Trace können Trace-Profile aktiviert werden.

WBM-Pfad

WBM **>** Wartung

Menü Trace

WBM **>** Wartung**> Logs > Trace-Profile**

4.4.1 Profile

Anmerkung: Diese Funktion darf nur von Entwicklern benutzt werden. Für die Standard-Analyse werden die Funktionen im Dialog *Diagnose-Dateien* empfohlen (siehe Section 4.7.2, "Diagnose-Dateien").

WBM-Pfad

WBM > Wartung > Trace > Profile

Der Dialog *Trace-Profile-Konfiguration bearbeiten* wird angezeigt. In diesem Dialog können Trace-Profile für eine detaillierte Analyse des SoftGate aktiviert werden. Durch jedes Trace-Profil werden spezielle Informationen aufgezeichnet.

Trace-Profile

Aktivieren Sie die hier aufgeführten Trace-Profile, um folgende Probleme zu ermitteln:

- *acw-cc*: Entwickler-spezifisch
- *announcement: Entwickler-spezifisch*
- *cg*: Entwickler-spezifisch
- *dataloading*: Entwickler-spezifisch
- *dcl2*: Entwickler-spezifisch
- *debug-all*: Entwickler-spezifisch
- *dmc-detail*: Entwickler-spezifisch
- *dls-client:* Entwickler-spezifisch
- ecoap: Entwickler-spezifisch (Enterprise GW)
- ecoap-light: Entwickler-spezifisch (Enterprise GW)
- evtlog: Entwickler-spezifisch
- h323-performance: Entwickler-spezifisch
- *heap-diag*: Entwickler-spezifisch
- *hfa-call*: Wird verwendet bei Problemen mit der Signalisierung von HFA-Verbindungen und dem An- und Abmelden der HFA-Endgeräte.
- *hfa-reg*: Wird verwendet bei Problemen mit der Registrierung der HFA-Endgeräte, z. B. bei fehlerhaften Anzeigen in den Endgeräte-Displays.
- *hsr*: Wird verwendet bei Problemen mit der Verbindung zwischen SoftGate und Host.
- *hsr-message-dump*: Entwickler-spezifisch Beeinträchtigt die Leistung des Systems!
- hsr-message-light: Entwickler-spezifisch
- *ipconfig*: Entwickler-spezifisch
- *ipv6*: Wird verwendet, wenn Probleme bei der Vernetzung über IP V6 bestehen.
- icphone: Entwickler-spezifisch
- *maintenance*: Entwickler-spezifisch
- *mmx*: Entwickler-spezifisch
- *osa*: Trace-Profil für OpenScape Access
- *osa-clock*: Trace-Profil für OpenScape Access
- *osa-light*: Trace-Profil für OpenScape Access
- *osa-trace*: Trace-Profil für OpenScape Access
- *payload*: Wird verwendet bei Problemen mit der Sprachdurchschaltung (wie *payload-light*). Beeinträchtigt die Leistung des Systems! Aufgrund der Erzeugung umfangreicher Trace-Ausgaben darf dieses Profil nicht bei hoher Systemlast aktiviert werden.
- *payload-light*: Wird verwendet bei Problemen mit der Sprachdurchschaltung. Kann bei erhöhter Systemlast aktiviert werden. Siehe auch Absatz "payload".
- *payload-native*: Entwickler-spezifisch

- *qdc*: Entwickler-spezifisch
- *reconnect*: Entwickler-spezifisch
- *scc*: Wird verwendet bei allgemeinen Payload-Problemen, bei Konferenz-Verbindungen und bei IPDA-Verbindungen.
- *sigsurv*: Entwickler-spezifisch
- *sip*: Nach Aktivierung dieses Trace-Profils werden die Trace-Meldungen der vHG 3575 (Enterprise Gateway), die im lokalen WBM der vHG 3575 (Enterprise Gateway) konfiguriert wurden, in die SoftGate-Protokolldatei übernommen. AuÃerdem werden die SIP-relevanten scc-Traces aufgezeichnet.
- *siux*: Entwickler-spezifisch
- *slc*: Entwickler-spezifisch
- snmp: Entwickler-spezifisch
- *startup*: Wird verwendet bei Hochfahrproblemen des SoftGates und der virtuellen Baugruppen.
- *sysinfo*: Entwickler-spezifisch
- *system*: Dieses Traceprofil ist immer aktiviert und kann nicht ausgeschaltet werden.
- *telnumlookup*: Entwickler-spezifisch
- *thread-profiling*: Entwickler-spezifisch
- *vSlma*: Entwickler-spezifisch
- *vTmom*: Entwickler-spezifisch
- *wbm*: Entwickler-spezifisch

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Einstellungen der aktivierten/deaktivierten Kontrollkästchen werden gespeichert.
- *Rückgängig:* Die Einstellungen der aktivierten/deaktivierten Kontrollkästchen werden zurückgesetzt.
- *Standard wiederherstellen:* Die Einstellungen der aktivierten/deaktivierten Kontrollkästchen werden auf die Default-Einstellungen zurückgesetzt.

Vorgehensweise

Führen Sie zum Aktivieren von Trace-Profilen die folgenden Schritte durch:

1) Aktivieren Sie die Kontrollkästchen derjenigen Trace-Profile, die Sie für eine Analyse benötigen.
2) Klicken Sie auf *Übernehmen*. Die Einstellungen der aktivierten/deaktivierten Kontrollkästchen werden gespeichert.

RTMx-Trace-Profile

Aktivieren Sie die hier aufgeführten Trace-Profile, um Folgendes zu ermitteln:

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

- switching_detailed:

4.5 LAN-Verfolgung

Unter „LAN Trace“ (LAN-Verfolgung) können Einstellungen zur Überwachung von IP-Verbindungen vorgenommen und Diagnose-Dateien erstellt werden.

WBM-Pfad

WBM > Maintenance > LAN Trace (WBM > Wartung > LAN-Verfolgung)

Das Menü „LAN Trace“ (LAN-Verfolgung) wird angezeigt.

Menü „LAN Trace“ (LAN-Verfolgung)

Die folgenden Optionen werden in diesem Menü angezeigt:

- Interne LAN-Verfolgung

4.5.1 Interne LAN-Verfolgung

WBM-Pfad

WBM > Maintenance > LAN Trace > Internal LAN Trace (WBM > Wartung > LAN-Verfolgung > Interne LAN-Verfolgung)

Der Dialog „Internal LAN Trace“ (Interne LAN-Verfolgung) wird angezeigt. In diesem Dialog können Einstellungen zur Überwachung von IP-Verbindungen, die interne LAN Capture-Kontrolle und Sip-LAN-Verfolgung vorgenommen werden.

Bereiche

In diesem Dialog gibt es die folgenden Bereiche:

- Interne LAN Capture-Kontrolle
- SIP-LAN-Verfolgung

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- Apply (Übernehmen): Änderungen an den Einstellungen werden gespeichert.
- Undo (Rückgängig machen): Geänderte Einstellungen werden gelöscht und durch Standardwerte ersetzt.

4.5.1.1 Interne LAN Capture-Kontrolle

WBM-Pfad

WBM **>** Wartung **>** Diagnose **>** Diagnose-Funktionen **>** Bereich Interne LAN Capture-Kontrolle

Im Bereich Interne LAN Capture-Kontrolle können Einstellungen für die interne Überwachung von IP-Paketen im LAN vorgenommen werden. Diese Überwachung erfolgt z. B. mit tshark oder tcpdump. Im Falle eines kritischen Neustarts

wird der aktuelle Inhalt in die Backtrace-Datei geschrieben. Beim Starten der Überwachung werden ältere Capture-Dateien gelöscht. Falls diese noch benötigt werden, müssen Sie über Logs **>** Logs exportieren einen Export durchführen.

Bedienelemente und Anzeigen

Dieser Bereich enthält die folgenden Bedienelemente und Anzeigen:

- Kontrollkästchen:
  - *Nur Headers:* Es sollen nur die Header der IP-Pakete überwacht werden.
  - *Start:* Die interne LAN Capture-Kontrolle soll gestartet werden.
  - *LoopBack-Schnittstelle (nur):* Es soll nur die LoopBack-Schnittstelle benutzt werden.
- Auswahlfeld:
  - *Filter:* Ein Filter zum Überwachen von IP-Paketen kann ausgewählt werden. Auswählbar sind:
    - *keiner* (kein Filter)
    - *tcp* (nur IP-Pakete des Transmission Control Protocol)
    - *udp* (nur IP-Pakete des User Datagram Protocol)
- Anzeige:
  - *Status*: Es wird angezeigt, ob die interne LAN Capture-Kontrolle aktiv ist.

4.5.1.2 SIP-LAN-Verfolgung

WBM-Pfad

WBM > Wartung > LAN-Verfolgung > Interne LAN-Verfolgung

Die Kontrolle für die interne Überwachung von IP-Paketen im SIP LAN kann im Bereich „SIP LAN Trace“ (SIP-LAN-Verfolgung) vorgenommen werden. Die Überwachung erfolgt z. B. mit tshark oder tcpdump. Im Falle eines kritischen Neustarts wird der aktuelle Inhalt in die Backtrace-Datei geschrieben. SIP LAN Trace wird standardmäßig gestartet. Wenn Sie eine neue Erfassung starten, werden die neuesten 10 Dateien beibehalten und die anderen gelöscht. Wenn Sie diese benötigen, können Sie sie mit Protokolle > Protokolle exportieren exportieren.

Die SIP-LAN-Verfolgung erfasst nur Pakete auf den SIP-Standardports: 5060 und 5061.

Bedienelemente und Anzeigen

Dieser Bereich enthält die folgenden Bedienelemente und Anzeigen:

- Kontrollkästchen:
  - Stopp: Der SIP LAN Trace sollte gestoppt werden.
- Anzeige:
  - Status: Die Statusanzeige gibt an, ob die interne LAN-Erfassungssteuerung aktiv ist.

4.6 Secure Trace

Ein Secure Trace dient zum Ermitteln von Störungen im Kommunikationssystem. Durch den Secure Trace werden Aufzeichnungen über verschlüsselte VoIP-Nutz- und Signalisierungsdatenströme vom und zum vHG 3575 angefertigt.

Der Secure Trace enthält verschlüsselte Aufzeichnungen. Diese Aufzeichnungen können vom Entwickler durch einen Schlüssel entschlüsselt werden.

WBM-Pfad

WBM **>** Wartung **>** Secure Trace

Das Menü Secure Trace wird angezeigt.

Menü Secure Trace

Die folgenden Optionen werden in diesem Menü angezeigt:

Zertifikat importieren

Zertifikat anzeigen

Status

Trace starten

Trace stoppen

Prinzipieller Ablauf der Secure Trace-Erstellung

Zum Erstellen eines Secure Trace ist der folgende Ablauf einzuhalten:

1) Der Servicetechniker stellt ein Problem im Netzwerk des Kunden fest. In einer Besprechung mit dem Entwickler wird die Notwendigkeit erkannt, einen Secure Trace zu erzeugen.

2) Der Kunde wird von der Notwendigkeit informiert und muss bestätigen, dass er informiert wurde. Danach gibt der Kunde eine Bestellung zum Erzeugen eines Secure Trace auf, in der Beginn und Ende (mit Datum und Uhrzeit) der Überwachung genannt sind.

3) Die Entwicklung erstellt ein Schlüsselpaar, das aus dem öffentlichen Schlüssel und dem privaten Schlüssel besteht. Mit dem Schlüsselpaar kann nur ein einziger Secure Trace erstellt werden. Die Zertifikate werden folgendermaßen verwendet:

- Das Zertifikat mit dem privaten Schlüssel ist streng geheim und kann nur von autorisierten Entwicklern benutzt werden.
- Das Zertifikat mit dem öffentlichen Schlüssel wird an den Servicetechniker übergeben bzw. kann von der HiSat Homepage (https://hisat.global-intra.net/wiki/index.php/SecureTrace) heruntergeladen werden.

4) Der Servicetechniker informiert den Kunden über den Beginn der Trace-Aktivitäten. Der Kunde muss die betroffenen Teilnehmer informieren.

Anmerkung: Das Aufzeichnen von Gesprächen und Verbindungsdaten ist ein Straftatbestand, wenn die betroffenen Teilnehmer nicht informiert wurden.

---

5) Der Servicetechniker stellt das Zertifikat für das vHG 3575 (Enterprise Gateway)-Gateway bereit, für das ein Secure Trace erstellt wird, siehe Section 4.5.1, "Zertifikat importieren".
6) Der Servicetechniker aktiviert die Secure Trace-Funktion, siehe Section 4.5.4, "Trace starten". Ein Secure Trace wird erstellt. Die Aktivierung und die spätere Deaktivierung (Section 4.5.5, "Trace stoppen") werden von den beteiligten Kommunikationssystemen protokolliert.
7) Nachdem der Secure Trace erstellt wurde, wird der Kunde über das Ende der Trace-Aktivitäten informiert. Der Servicetechniker entfernt das Zertifikat vom System.
8) Der Secure Trace wird dem Entwickler zur Verfügung gestellt.
9) Der Entwickler entschlüsselt den Secure Trace, indem er den privaten Schlüssel anwendet. Danach analysiert er die entschlüsselten Aufzeichnungen.
10) Nach dem Ende der Analyse müssen alle relevanten Materialien und Daten auf eine sichere Art und Weise zerstört werden. Dies beinhaltet auch das Zerstören des privaten Schlüssels, damit eine eventuell angefertigte unerlaubte Kopie des Secure Trace nicht mehr entschlüsselt werden kann.

4.6.1 Zertifikat importieren

WBM-Pfad

WBM **>** Wartung **>** Secure Trace **>** Zertifikat importieren

Der Dialog *Laden des Secure Trace Zertifikats über HTTP* wird angezeigt.
In diesem Dialog kann ein Secure Trace-Zertifikat importiert werden. Dieses Zertifikat ist die Voraussetzung dafür, dass ein Secure Trace erstellt werden kann. Der Servicetechniker bekommt es vom Entwickler. Es enthält den öffentlichen Schlüssel und muss im PEM- oder im binären Format vorliegen. Das Zertifikat ist maximal einen Monat gültig.

Eingabefeld

Dieser Dialog enthält das folgende Eingabefeld:

- *Datei mit dem Zertifikat (PEM- oder Binär-Format)*: In dieses Eingabefeld sind der Pfad und der Name der Datei, die das Zertifikat enthält, einzugeben. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Fingerabdruck des Zertifikats anzeigen*: Durch Prüfen des Fingerabdrucks kann festgestellt werden, ob ein unverändertes Zertifikat vorliegt oder ob es verändert wurde.

- *Zertifikat aus Datei importieren*: Das Zertifikat wird aus der im oben genannten Eingabefeld angegebenen Datei importiert.

Vorgehensweise

Führen Sie zum Importieren des Zertifikats die folgenden Schritte durch:

1) Auswählen: *WBM* > Wartung > Secure Trace > Zertifikat importieren. Der Dialog *Laden des Secure Trace Zertifikats über HTTP* wird angezeigt.
2) Wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus, die das Zertifikat enthält, und bestätigen Sie mit *Öffnen*. Die Datei wird geladen.
3) Klicken Sie auf *Fingerabdruck des Zertifikats anzeigen*. Ein Fenster mit dem Fingerabdruck des zu importierenden Zertifikats wird angezeigt:
   a) Überprüfen Sie den Fingerabdruck (Hexadezimalzahl). Wenn das Zertifikat geändert wird, ändert sich immer der Fingerabdruck. Nur ein unveränderter Fingerabdruck ist eine Gewähr für ein unverändertes Zertifikat. Sind die beiden Fingerabdrücke nicht identisch, dann liegt wahrscheinlich ein Angriffsversuch vor. In diesem Fall darf der Schlüssel nicht mehr verwendet werden; darüber hinaus sind die festgelegten Maßnahmen zu ergreifen.
   b) Klicken Sie auf *OK*, um das Fenster mit dem Fingerabdruck zu schließen.
4) Klicken Sie auf *Zertifikat aus Datei importieren*, wenn Sie mit der Prüfung des Fingerabdrucks zufrieden sind. Importieren Sie das Zertifikat nicht, falls der Fingerabdruck nicht Ihren Erwartungen entspricht.

Das Erstellen des Secure Trace ist nun möglich.

4.6.2 Zertifikat anzeigen

WBM-Pfad

WBM > Wartung > Secure Trace > Zertifikat anzeigen

Der Dialog *Zertifikatsinformationen* wird angezeigt. In diesem Dialog kann das Secure Trace-Zertifikat angezeigt werden, z. B. um es zu überprüfen.

Angezeigte Daten

Die folgenden Zertifikatsdaten werden angezeigt:

- Allgemeine Daten: *Name des Zertifikats*, *Zertifikatstyp*, *Seriennummer des Zertifikats*, *Seriennummer des Zertifikats (hex)*, *Signatur-Algorithmus-Typ*, *Beginn der Zertifikatsgültigkeit (GMT)*, *Ende der Zertifikatsgültigkeit (GMT)*, *CRL-Verteilungspunkt*
- *Ausgestellt durch CA*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Antragsteller*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Alternativer Antragstellername*
- *Daten des öffentl. Schlüssels*: *Länge des öffentlichen Schlüssels*, *Öffentlicher Schlüssel*, *Fingerabdruck*

4.6.3 Status

WBM-Pfad

WBM > Wartung > Secure Trace > Status

Der Dialog *Secure Trace Status* wird angezeigt. In diesem Dialog können Sie feststellen, ob gerade ein Secure Trace erstellt wird.

Angezeigte Daten

Es werden die folgenden Daten angezeigt:

- *Secure Trace aktiviert*: Diese Zeile zeigt an, ob gerade ein Secure Trace erstellt wird.
- *Automatischer Deaktivierungszeitpunkt*: Diese Zeile zeigt an, wann der Secure Trace voraussichtlich erstellt wird und die Secure Trace-Funktion automatisch deaktiviert wird.
- *Secure Trace für folgende Protokolle*: Diese Zeile zeigt an, für welche Protokolle der Secure Trace erstellt wird. Das könnten sein: Media Server (SRTP).

4.6.4 Trace starten

WBM-Pfad

WBM > Wartung > Secure Trace > Trace starten

Der Dialog *Secure Trace starten* wird angezeigt. In diesem Dialog kann der Secure Trace gestartet werden. Dazu müssen die folgenden Voraussetzungen vorliegen:

- Der Secure Trace ist noch nicht aktiviert.
- Der Kunde hat die Erstellung des Secure Trace veranlasst und möchte seine *Secure Trace Aktivierungs-Passphrase* in das WBM eingeben.
- Sie haben einen öffentlichen Schlüssel vom Entwickler bekommen und in das WBM geladen.

Eingabefelder und Kontrollkästchen

- *Start Parameter*:
  - *Secure Trace Aktivierungs-Passphrase*: Um die Nutzung der Secure Trace-Funktion zu begrenzen, wird die Aktivierung durch eine besondere Passphrase, die nur der Kunde kennt, geschützt. Somit ist diese Passphrase der Schlüssel des Kunden und das Zertifikat der Schlüssel des Servicetechnikers. Beide Schlüssel sind notwendig, um die Secure Trace-Funktion zu aktivieren.

    Eine Passphrase ist ein aus mehreren Wörtern bestehendes Passwort mit einer maximalen Länge von 20 Zeichen.
  - *Dauer des Secure Trace (Min.)*: Das Eingeben der Dauer des Secure Trace (in Minuten) ist unbedingt erforderlich.

- *Secure Trace für folgende Protokolle*:
  - *MMX (PEP) -verwendet für* : Der Secure Trace für MMX wird erstellt. Das Protokoll PEP (Protocol Extension Protocol) erweitert HTTP für Applikationen wie z. B. HTTP-Clients, Server und Proxy-Server.
  - *MediaServer (SRTP)*: Der Secure Trace für MediaServer wird erstellt. Das Protokoll SRTP (Secure Real-Time Transport Protocol) dient der verschlüsselten Übertragung über IP-basierte Netze und verwendet AES (Advanced Encryption Standard) für die Verschlüsselung.

Schaltflächen

In diesem Dialog gibt es die folgende Schaltfläche:

- *Secure Trace einschalten*: Damit wird die Secure Trace gestartet. Die oben genannten Voraussetzungen für das Starten des Secure Trace müssen vorliegen.

Vorgehensweise

Führen Sie zum Starten des Secure Trace die folgenden Schritte durch:

1) Prüfen Sie, ob die oben genannten Voraussetzungen vorliegen.
2) Auswählen: *WBM* **>** Wartung **>** Secure Trace **>** Trace starten. Der Dialog *Secure Trace starten* wird angezeigt.
3) Geben Sie im Bereich *Start Parameter* die *Secure Trace Aktivierungs-Passphrase* und die *Dauer des Secure Trace (Min.)* ein.
4) Aktivieren Sie das Protokoll *MediaServer (SRTP)*.
5) Klicken Sie auf die Schaltfläche *Secure Trace einschalten*. Der Secure Trace wird für die angegebene Zeitdauer erstellt.

4.6.5 Trace stoppen

WBM-Pfad

WBM **>** Wartung **>** Secure Trace **>** Trace stoppen

Der Dialog *Secure Trace beenden* wird angezeigt. In diesem Dialog kann ein laufender Secure Trace gestoppt werden, wenn die unter Trace startenfestgelegte Zeitdauer noch nicht abgelaufen ist.

Schaltfläche

In diesem Dialog gibt es die folgende Schaltfläche:

- *Secure Trace beenden*: Der Secure Trace wird beendet.

4.7 DLS-Client

Der DLS-Client dient zur Verwaltung von PKI-Daten und der QDC-Konfiguration (DLS: **D**ep**l**oyment **S**ervice oder **D**eployment and **L**icensing **S**erver, PKI: **P**ublic **K**ey **I**nfrastructure, QDC: **Q**uality of Service **D**ata **C**ollection).

WBM-Pfad

WBM **>** Wartung **>** DLS-Client

Das Menü DLS-Client wird geöffnet:

Menü DLS-Client

Dieses Menü bietet folgende Optionen zur Auswahl:

DLS-ClientPIN EingabeBootstrapping zurücksetzenDLS kontaktieren

Bootstrapping

Durch das Bootstrapping soll eine auf Zertifikaten basierende zuverlässige SSL-Verbindung zwischen DLS-Server und DLS-Client aufgebaut werden.

Ausgehend von einer Verbindungsanfrage des DLS-Clients an einen DLS-Server sowie der darauffolgenden Antwort â“also einer noch unzuverlässigen Verbindungâ“, wird über die wechselseitige Authentifizierung und den Austausch von Zertifikaten eine zuverlässige Verbindung aufgebaut (d. h. Bootstrapping = ein einfaches System entwickelt sich zu einem komplexen System aus sich selbst heraus).

Da sich auf die Verbindungsanfrage des DLS-Clients anstatt des gewollten DLS-Servers auch ein anderer DLS-Server melden könnte, um die gewünschte Verbindung an sich zu ziehen, sind SicherungsmaÃnahmen notwendig. Mittels AMO kann der DLS-Server (d. h. dessen IP-Adresse und Port) administriert werden, den der DLS-Client kontaktieren soll.

Es wird empfohlen, den DLS-Client gegenüber dem DLS-Server durch Eingeben einer Bootstrap-PIN am vHG 3575 WBM, die zuvor vom DLS-Server per Zufall generiert wurde, zu autorisieren. Die Autorisierung des DLS-Clients kann auch mit einer nicht einzugebenden systeminternen Standard-PIN erfolgen, oder auf die Autorisierung mittels PIN kann auch ganz verzichtet werden. Diese beiden Möglichkeiten werden jedoch nicht empfohlen.

Nach dem Herstellen der zuverlässigen Verbindung werden die Zertifikate ausgetauscht, s. u.

Zertifikatsgenerierung und -verteilung für die Kommunikation zwischen DLS-Client und DLS-Server:

Alle Zertifikate und privaten Schlüssel für die verschlüsselte Kommunikation zwischen DLS-Client und DLS-Server werden durch eine selbst-signierende Zertifizierungsstelle (CA) des DLS-Servers erzeugt und durch den DLS-Server während des Bootstrappings zum DLS-Client gesendet.

Die vom DLS-Server zum DLS-Client gesendete PKCS#12-Datei enthält das DLSC Client-Zertifikat, den darin enthaltenen privaten Schlüssel und das Zertifikat der Zertifizierungsstelle des DLS-Servers (DLSC CA-Zertifikat). Der DLS-Server kann alle von ihm gelieferten Zertifikate zurücklesen, jedoch nicht den privaten Schlüssel.

Zertifikatsgenerierung und -verteilung für die sichere Verbindung des WBM zum DLS-Server:

Der Administrator sendet manuell das von der Kunden PKI-Zertifizierungsstelle erstellte WBM-Zertifikat, das den privaten Schlüssel enthält, zum OpenScape 4000 Assistant. AnschlieÃend sendet OpenScape 4000 Assistant das WBM-Zertifikat automatisch an alle Gateways. Mit diesem Zertifikat weist sich dann der DLS-Client gegenüber dem DLS-Server aus.

4.7.1 DLS Einstellungen

Außer dem automatischen Registrieren des DLS-Client am DLS-Server mittels der ContactMe-Antwort kann der DLS-Client auch manuell registriert werden. Dafür müssen Ihnen vom DLS-Server die IP-Adresse und der Port für den Bootstrapping-Modus bekannt sein. Die IP-Adresse und der Port des DLS-Servers können mittels AMO konfiguriert werden. Diese Änderung wird erst wirksam, wenn das SoftGate neu gestartet wurde.

Nach Setzen von IP-Adresse und Port des DLS-Servers erfolgt beim Neustart (und jedem weiteren Neustart) ein einmaliger Versuch, durch Senden einer Verbindungsanfrage das Bootstrapping einzuleiten.

Unter dem Menüpunkt *DLS kontaktieren* können manuell weitere Verbindungsversuche eingeleitet werden. Falls noch kein Bootstrapping durchgeführt wurde, wird dies dabei automatisch eingeleitet, andernfalls wird lediglich geprüft, ob der DLS erreichbar ist.

WBM-Pfad

WBM **>** Wartung **>** DLS-Client **>** DLS Einstellungen

Der Dialog *DLS Client Grundeinstellung ändern* wird geöffnet.

Eingabefeld

Im Bereich *Aktuelle DLS Client Grundeinstellung* gibt es folgendes Eingabefeld:

- *Zeitintervall für ContactMeAntwort*: Zeit, die der DLS-Client nach Absenden seiner Verbindungsanfrage wartet, um die ContactMe-Antwort vom DLS-Server zu erhalten. Die Wartezeit muss begrenzt sein, damit ContactMe-Antworten von ungewollten DLS-Servern nicht empfangen werden können.

Anzeigen

In diesem Dialog gibt es die folgenden Anzeigen:

- *Aktuelle DLS Client Grundeinstellung*:
  - *PIN für DLS-Bootstrapping erforderlich*: Die PIN kann unter der Menüoption PIN Eingabe eingegeben werden. *Ja*: Es wurde eine PIN eingegeben. *Nein*: Es wurde keine PIN eingegeben.
  - *Sichere Kommunikation mit DLS-Server*: *Aktiviert* oder *Deaktiviert*
- *Aktuelle DLS Client Server Einstellung*:
  - *IP-Adresse des DLS-Servers*: IP-Adresse des DLS-Servers für den Bootstrapping-Modus kann mittels AMO konfiguriert werden. Das SoftGate muss neu gestartet werden.
  - *Port des DLS-Servers*: Der Port des DLS-Servers für den Bootstrapping-Modus kann mittels AMO konfiguriert werden. Ein Neustart von SoftGate und Enterprise Gateway ist erforderlich.
  - *Port für sichere Verbindung zum DLS-Server*: Port des vHG 3575 (Enterprise Gateway) für die sichere Verbindung zum DLS-Server.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die geänderten Einstellungen werden gespeichert.
- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf den Defaultwert zurückgesetzt.

4.7.2 PIN Eingabe

WBM-Pfad

WBM > Wartung > DLS-Client > PIN Eingabe

Der Dialog *Eingabe der Bootstrap-PIN* wird geöffnet. In diesem Dialog kann die vom DLS-Server per Zufall generierte Bootstrap PIN eingegeben werden.

Eingabefeld

In diesem Dialog gibt es folgendes Eingabefeld:

- *Bootstrap PIN*: Wenn in dieses Eingabefeld eine PIN eingegeben und durch Klicken auf *Übernehmen* gespeichert wurde, wird im Dialog *DLS Client Grundeinstellung ändern* (Menüpunkt DLS Einstellungen) angezeigt, dass für das DLS-Bootstrapping eine PIN erforderlich ist.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die geänderten Einstellungen werden gespeichert.
- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf den Defaultwert zurückgesetzt.

4.7.3 Bootstrapping zurücksetzen

WBM-Pfad

WBM > Wartung > DLS-Client > Bootstrapping zurücksetzen

Der Dialog *DLS Client Bootstrapping zurücksetzen* wird geöffnet.

Schaltfläche

In diesem Dialog gibt es die folgende Schaltfläche:

- *Bootstrapping zurücksetzen*: Das Bootstrapping des DLS-Clients wird zurückgesetzt.

4.7.4 DLS kontaktieren

Unter dem Menüpunkt *DLS kontaktieren* können manuell weitere Verbindungsversuche zum DLS-Server eingeleitet werden. Falls noch kein Bootstrapping durchgeführt wurde, wird dies dabei automatisch eingeleitet, andernfalls wird lediglich geprüft, ob der DLS erreichbar ist.

WBM-Pfad

WBM > Wartung > DLS-Client > DLS kontaktieren

Der Dialog *DLS kontaktieren* wird geöffnet.

Menü *DLS kontaktieren*

Dieses Menü bietet folgende Optionen zur Auswahl:

DLSC-Client-Zertifikate

DLSC CA-Zertifikate

Dialog *DLS kontaktieren*

In diesem Dialog gibt es die folgende Schaltfläche:

- *Kontaktieren*: Der DLS-Server wird kontaktiert, um zu überprüfen, ob er noch verfügbar ist.

4.7.4.1 DLSC-Client-Zertifikate

Unter diesem Menüpunkt befinden sich die DLSC Client-Zertifikate mit dem privaten Schlüssel. Mit diesen Zertifikaten weist sich der DLS-Client gegenüber dem DLS-Server aus. Während des Bootstrapping-Modus bekommt der DLS-Client das Zertifikat vom DLS-Server.

WBM-Pfad

WBM **>** Wartung **>** DLS-Client **>** DLSC-Client-Zertifikate

Das Menü DLSC-Client-Zertifikate wird geöffnet.

Menü DLSC-Client-Zertifikate

Unter diesem Menüpunkt sind die einzelnen DLSC Client-Zertifikate auswählbar:

1. DLSC Client-Zertifikate

4.7.4.2 1. DLSC Client-Zertifikate

WBM-Pfad

WBM **>** Wartung **>** DLS-Client **>** DLSC-Client-Zertifikate **>** 1. DLSC Client-Zertifikate

Der Dialog *Zertifikatsinformationen* wird angezeigt.

Angezeigte Daten

Es werden die folgenden Daten aus dem Zertifikat angezeigt:

- Allgemeine Daten: *Zertifikatstyp*, *Seriennummer des Zertifikats*, *Seriennummer des Zertifikats (hex)*, *Signatur-Algorithmus-Typ*, *Beginn der Zertifikatsgültigkeit (GMT)*, *Ende der Zertifikatsgültigkeit (GMT)*, *CRL-Verteilungspunkt*
- *Ausgestellt durch CA*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Antragsteller*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Alternativer Antragstellername*
- *Verschlüsselungsdaten mit öffentlichem Schlüssel*: *Länge des öffentlichen Schlüssels (Parameter)*, *Öffentlicher Schlüssel*, *Fingerabdruck*

4.7.4.3 DLSC CA-Zertifikate

Dieser Ordner enthält die vom DLS-Server während des Bootstrapping-Modus gelieferten DLSC CA-Zertifikate.

WBM-Pfad

WBM > Wartung > DLS-Client > DLSC CA-Zertifikate

Das Menü DLSC CA-Zertifikate wird geöffnet:

Menü DLSC CA-Zertifikate

Unter diesem Menüpunkt sind die einzelnen DLSC Client-Zertifikate auswählbar:

"1. DLSC CA-Zertifikat", "2. DLSC CA-Zertifikat"

4.7.4.4 "1. DLSC CA-Zertifikat", "2. DLSC CA-Zertifikat"

WBM-Pfad

WBM > Wartung > DLS-Client > DLSC-Client-Zertifikate > "1. DLSC CA-Zertifikat", "2. DLSC CA-Zertifikat"

Der Dialog *Zertifikatsinformationen* wird angezeigt.

Angezeigte Daten

Es werden die folgenden Daten aus dem Zertifikat angezeigt:

- Allgemeine Daten: *Zertifikatstyp*, *Seriennummer des Zertifikats (hex)*, *Signatur-Algorithmus-Typ*, *Beginn der Zertifikatsgültigkeit (GMT)*, *Ende der Zertifikatsgültigkeit (GMT)*, *CRL-Verteilungspunkt*
- *Ausgestellt durch CA*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Antragsteller*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Alternativer Antragstellername*
- *Daten des öffentl. Schlüssels*: *Länge des öffentlichen Schlüssels (Parameter)*, *Öffentlicher Schlüssel*, *Fingerabdruck*

4.8 Diagnose

Unter Diagnose können Einstellungen zur Überwachung von IP-Verbindungen vorgenommen und Diagnose-Dateien erstellt werden.

WBM-Pfad

WBM > Wartung > Diagnose

Das Menü Diagnose wird angezeigt.

Menü Diagnose

Die folgenden Optionen werden in diesem Menü angezeigt:

Diagnose-Funktionen

Diagnose-Dateien

4.8.1 Diagnose-Funktionen

WBM-Pfad

WBM > Wartung > Diagnose> Diagnose-Funktionen

Der Dialog *Diagnose-Funktionen* wird angezeigt. In diesem Dialog können Einstellungen zur Überwachung von IP-Verbindungen vorgenommen werden, für das Thread Profiling und für die Heap-Überwachung.

Bereiche

In diesem Dialog gibt es die folgenden Bereiche:

Thread-Profiling

Heap-Überwachung

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die geänderten Einstellungen werden gespeichert.
- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf die Defaultwerte zurückgesetzt.

4.8.1.1 Interne LAN Capture-Kontrolle

WBM-Pfad

WBM > Wartung > Diagnose > Diagnose-Funktionen > Bereich Interne LAN Capture-Kontrolle

Im Bereich Interne LAN Capture-Kontrolle können Einstellungen für die interne Überwachung von IP-Paketen im LAN vorgenommen werden. Diese Überwachung erfolgt z. B. mit tshark oder tcpdump. Im Falle eines kritischen Neustarts wird der aktuelle Inhalt in die Backtrace-Datei geschrieben. Beim Starten der Überwachung werden ältere Capture-Dateien gelöscht. Falls diese noch benötigt werden, müssen Sie über Logs > Logs exportieren einen Export durchführen.

Bedienelemente und Anzeigen

Dieser Bereich enthält die folgenden Bedienelemente und Anzeigen:

- Kontrollkästchen:
  - *Nur Headers:* Es sollen nur die Header der IP-Pakete überwacht werden.
  - *Start:* Die interne LAN Capture-Kontrolle soll gestartet werden.
  - *LoopBack-Schnittstelle (nur):* Es soll nur die LoopBack-Schnittstelle benutzt werden.

- Auswahlfeld:
  - *Filter:* Ein Filter zum Überwachen von IP-Paketen kann ausgewählt werden. Auswählbar sind:
    - *keiner* (kein Filter)
    - *tcp* (nur IP-Pakete des Transmission Control Protocol)
    - *udp* (nur IP-Pakete des User Datagram Protocol)
- Anzeige:
  - *Status*: Es wird angezeigt, ob die interne LAN Capture-Kontrolle aktiv ist.

4.8.1.2 Thread-Profiling

WBM-Pfad

WBM **>** Wartung **>** Diagnose**>** Diagnose-Funktionen **>** Bereich Thread-Profiling

Mit dem Thread Profiling kann überprüft werden, ob Threads die CPU, wie geplant, ausnutzen. D. h. ob ein Thread, von dem man eine niedrige CPU-Belastung erwartet, dies auch wirklich tut.

Bedienelemente und Anzeigen

Dieser Bereich enthält die folgenden Bedienelemente und Anzeigen:

- Kontrollkästchen:
  - *Start:* Das Thread Profiling soll gestartet werden.
- Eingabefelder:
  - *Sample Rate, ms (100-500):* Die Abtastrate kann eingestellt werden, Default ist 250.
  - *Thread-CPU-Nutzung-Grenzwert für Stacktrace, % (10-90):* Sie können die maximale CPU-Nutzung einstellen, Default ist 50.
- Anzeige:
  - *Status*: Es wird angezeigt, ob das Thread Profiling aktiv ist.

4.8.1.3 Heap-Überwachung

WBM-Pfad

WBM **>** Wartung **>** Diagnose**>** Diagnose-Funktionen **>** Bereich Heap-Überwachung

Durch das Erzeugen eines Heap-Dumps können alle Objekte, die sich auf dem Heap befinden, in eine Datei geschrieben werden.

Bedienelemente und Anzeigen

Dieser Bereich enthält die folgenden Bedienelemente und Anzeigen:

- Kontrollkästchen:
  - *Start:* Die Heap-Überwachung soll gestartet werden.

- Eingabefelder:
  - *Sample Rate, ms (500-5000):* Die Abtastrate kann eingestellt werden, Default ist 1000.
  - *Speichergebrauch-Grenzwert für Heapdump, % (50-90):* Es kann eingestellt werden, wie viel Speicher für den Heapdump genutzt werden kann, Default ist 80.
- Anzeige:
  - *Status*: Es wird angezeigt, ob die Heap-Überwachung aktiv ist.

4.8.2 Diagnose-Dateien

WBM-Pfad

WBM **>** Wartung **>** Diagnose**>** Diagnose-Dateien

Der Dialog Diagnose-Dateien wird angezeigt.

Auf der RAM-Disk, d. h. einem virtuellen temporären Datenträger im Arbeitsspeicher, werden Protokolldateien abgelegt. Diese Protokolldateien können ausgelesen und in eine Archivdatei gepackt werden. Eine Backtrace-Datei enthält den Inhalt des Stacks im Moment des Erzeugens.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Heap-Dump Erzeugen* Erzeugt eine Datei, die alle im Moment des Erzeugens erreichbaren Java-Objekte enthält. Anhand dieser Datei lässt sich der Arbeitsspeicherverbrauch analysieren.

Anmerkung: Die Backtrace-Archivdatei (Inhalt der RAMDISK/ramdisk.zip) enthält alle Protokolldateien der RAM-Disk und ist nun beim gewöhnlichen Log-Export enthalten.

4.9 Status-Information

WBM-Pfad

WBM **>** Wartung **>** Status-Information

Das Menü Status-Information wird angezeigt.

Menü Status-Information

Die folgenden Optionen werden in diesem Menü angezeigt:

System-Informationen

Verbindungskontrolle

H323-Status

HFA WAN Clients

4.9.1 System-Informationen

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** System-Informationen

Das Menü System-Informationen wird geöffnet:

Menü System-Informationen

Die folgenden Optionen werden in diesem Menü angezeigt:

Thread Zustände anzeigen

Details Periphere Baugruppen

Info Periphere Baugruppen

OpenScapeAccess Clocking

AP Emergency

4.9.1.1 Thread Zustände anzeigen

Anmerkung: Diese Funktion darf nur von Entwicklern benutzt werden.

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** System-Informationen**>** Thread Zustände anzeigen

Die Tabelle *Thread Zustände* wird angezeigt. In dieser Tabelle werden die gerade aktiven Threads angezeigt. Die folgenden Informationen werden angezeigt: *Thread Name*, *Thread ID*, *Hashcode Kontextklasse*, *blockierte Zeit [ms]*, *max. blockierte Zeit [ms]*.

4.9.1.2 Details Periphere Baugruppen

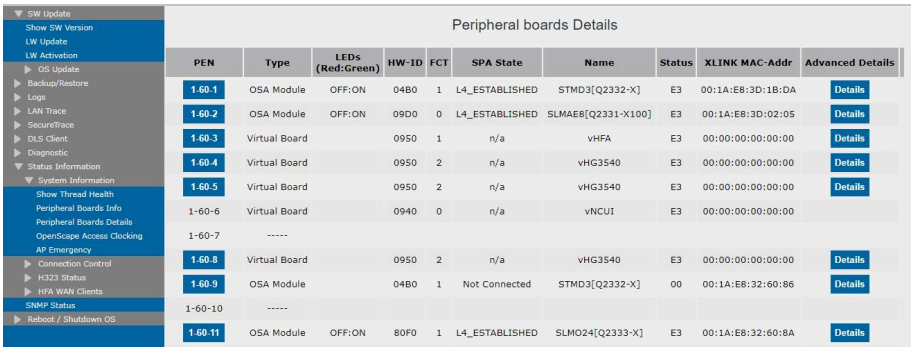
WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** System-Informationen**>** Details Periphere Baugruppen

Die Tabelle *Periphere Baugruppen* wird angezeigt. In dieser Tabelle werden die mit OpenScape 4000 SoftGate verbundenen virtuellen peripheren Baugruppen angezeigt. Dazu werden folgende Angaben gemacht:

- *PEN*: Peripheral Equipment Number
- *Typ*: Art der Baugruppe
- *HW-ID*
- *FCT*
- *SPA State*

- *Name:* Name der physischen Peripheriebaugruppe
- Status



PEN	Type	LEDs (Red:Green)	HW-ID	FCT	SPA State	Name	Status	XLINK MAC-Addr	Advanced Details
1-60-1	OSA Module	OFF:ON	04B0	1	L4_ESTABLISHED	STMD3[Q2332-X]	E3	00:1A:E8:3D:1B:DA	Details
1-60-2	OSA Module	OFF:ON	09D0	0	L4_ESTABLISHED	SLMAE8[Q2331-X100]	E3	00:1A:E8:3D:02:05	Details
1-60-3	Virtual Board		0950	1	n/a	vHFA	E3	00:00:00:00:00:00	Details
1-60-4	Virtual Board		0950	2	n/a	vHG3540	E3	00:00:00:00:00:00	Details
1-60-5	Virtual Board		0950	2	n/a	vHG3540	E3	00:00:00:00:00:00	Details
1-60-6	Virtual Board		0940	0	n/a	vNCUI	E3	00:00:00:00:00:00	
1-60-7	-----								
1-60-8	Virtual Board		0950	2	n/a	vHG3540	E3	00:00:00:00:00:00	Details
1-60-9	OSA Module		04B0	1	Not Connected	STMD3[Q2332-X]	00	00:1A:E8:32:60:86	Details
1-60-10	-----								
1-60-11	OSA Module	OFF:ON	80F0	1	L4_ESTABLISHED	SLMO24[Q2333-X]	E3	00:1A:E8:32:60:8A	Details

- XLINK-MAC-Adresse

Schaltflächen

In dieser Tabelle gibt es die folgenden Schaltflächen:

- Details

Schaltflächen in der Spalte *PEN*

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** System-Informationen**>** Details Periphere Baugruppen**>** Schaltflächen in der Spalte *PEN*

Die *Tabelle für Software PEN...* wird angezeigt. In dieser Tabelle werden für die ausgewählte virtuelle periphere Baugruppe folgende Informationen angezeigt: *PEN* (Peripheral Equipment Number), *SubNr.*, *L*, *Status*, *IP-Adresse*, *H225-Port*, *TSA-Status*, *Gesprächs-Ref. ID*, *TSL*, *HWY*, *B-Kanal*.

Schaltflächen

Unter dieser Tabelle gibt es die folgende Schaltfläche:

- *Zurück zu peripheren Baugruppen*: Die Tabelle *Periphere Baugruppen* wird erneut angezeigt.

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** System-Informationen**>** Details Periphere Baugruppen**>** Schaltflächen *Detail*

Dort werden gemeinsame Eigenschaften für BMSPA und CGSPA angezeigt. Die Tabelle *Baugruppen-Details für [PEN]* wird angezeigt (wenn von der Baugruppe unterstützt). In dieser Tabelle werden für die ausgewählte virtuelle periphere Baugruppe folgende Detail-Informationen angezeigt:

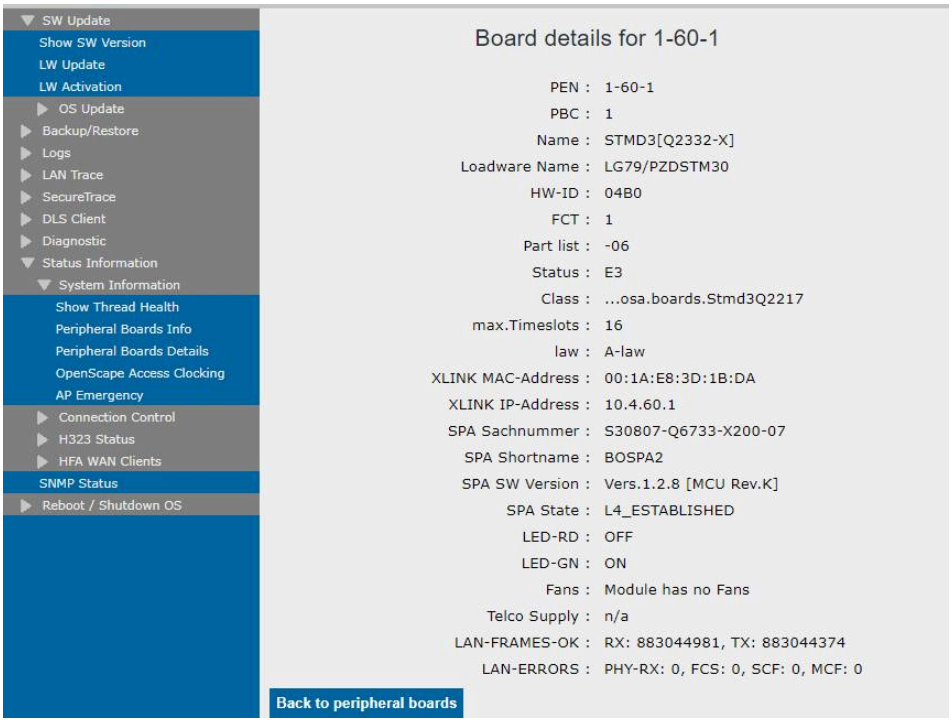
- *PEN*: Peripheral Equipment Number
- *PBC*
- *Name*: Name und Sachnummer der physischen peripheren Baugruppe, die virtualisiert wurde
- *Status*
- *Max. Timeslots*: Maximale Anzahl der Timeslots
- *Law*: Digitalisierungsverfahren für analoge Audiosignale (A-law oder Âµ-law)
- *XLINK MAC-Adresse*: MAC-Adresse des XLink LAN-Interfaces
- *XLINK IP-Adresse*: IP-Adresse des XLink LAN-Interfaces
- *SPA Sachnummer*

- *SPA-Kurzname:*
  - BMSPA
  - BOSPA - wie BMSPA, aber ohne PHY
  - BOSPAV - wie BOSPA, jedoch mit verschiedenen integrierten Schaltern auf xlink
  - CGSPA - CGSPA ist ein leistungsfähiges BMSPA mit eigenem Taktgenerator für präzisen Dect Clock.
- *SPA SW Version*
- *SPA State*
- LED_RD: LED_OFF
- LED_GN: LED_ON â“ Status der Peripheriebaugruppen-LEDs, dieser Status ist OK. Wenn rot und gleichzeitig grün leuchtet, zeigt dies ein Problem an.
- *Lüfter*: Zustand des Lüfters, in Betrieb oder nicht in Betrieb
- *Telco Spannung*
- *LAN-FRAMES-OK*: Anzahl der korrekten LAN-Frames für TX (Senden) und RX (Empfangen)
- *LAN-ERRORS*: Anzahl der Fehler für PHY-RX, FCS, SCF und MCF

Speziell für CGSPA-Boards:

- *GPS_IN-LEFT-LED: GPSIN_OFF*
- GPS_IN-RIGHT-LED: *GPSIN_ON*-Schnittstelle aktiv und Verarbeitung läuft. Die GPS-Task ist für die Signalverarbeitung eingerichtet, wartet aber auf den 1-Sekunden-Impuls und den GPS-Zeitstempel (weitere Details zu diesen LEDs finden Sie in Kapitel 9.2.2.3 des OpenScape Cordless Enterprise V7-Dokuments)
- SLC-Rolle: MASTER - Diese Baugruppe ist für die Messung der Phasenverschiebung des CDLSYN-Signals zuständig, standBy folgt auf Master und muss im ISS-Szenario auch mit Meinberg GPS-Empfänger verkabelt werden. UNBEKANNT - Wenn die QDCL-Funktionalität nicht aktiv ist, kennt SG sie nicht, da Informationen über SLC-Rollen nicht weitergeleitet werden.
- Kettenrolle: MASTER - Diese Baugruppe versorgt andere Baugruppen in der Taktkette mit dem Takt, der SLAVE empfängt den Takt vom MASTER und passt den eigene Takt daran an.
- CLK-Kettenposition: 1 - Zeigt die Reihenfolge der Baugruppe in der Taktkette an, SLC-Master muss 1 sein und SLC-StandBy muss 2 sein. Bei N/A ist kein Kabel mit der Kette verbunden.
- GPS-Kettenposition: 1 - Zeigt die Reihenfolge der Baugruppe in der GPS-Kette, im Falle des ISS-Szenarios muss der SLC-Master nicht 1 sein. Bei N/A ist kein Kabel mit der Kette verbunden.
- CDLSYN State: OK_REFERENCE - Muss auf jeder Baugruppe OK, sonst stimmt etwas nicht bei der Verkabelung.
- FRONTREF State: NO_REFERENCE - Wenn Meinberg angeschlossen ist, kann jede Baugruppe den Status des FRONTREF-Signals über die Taktverkettung lesen.
- CKA State: OK_REFERENCE - Muss auf jeder Baugruppe OK, sonst stimmt etwas nicht bei der Verkabelung.
- VCXO State: OK_REFERENCE - Muss immer OK sein, es spielt keine Rolle bei der Verkabelung.

- Referenztakt: TCXO:
  - TCXO ist ein integrierter Referenztakt, der für dect. ausreicht. Die Option wird für die Kettenmasterplatine gewählt
  - NO REFERENCE, in diesem Fall wird VCXO verwendet, wenn OSA-DIUT mit verfügbarem Referenztakt vorhanden ist. Die Option wird für die Kettenmasterplatine gewählt. VCXO wird über xlink an OSA-DIUT-Referenz angepasst
  - FRONTREF wird von Meinberg verwendet, wenn mehr Referenzen haben, hängt es von der Priorität in refta ab. Die Option wird für die Kettenmasterplatine gewählt
  - CKA wird von der Taktkette für alle Kettenslaves verwendet
- Sync to Ref Clock: true - Muss immer true sein, außer wenn Kettenmaster Referenztakt hat: NO_REFERENCE



Schaltflächen

Unter dieser Tabelle gibt es die folgende Schaltfläche:

- *Zurück zu peripheren Baugruppen:* Die Tabelle *Periphere Baugruppen* wird erneut angezeigt.

4.9.1.3 Info Periphere Baugruppen

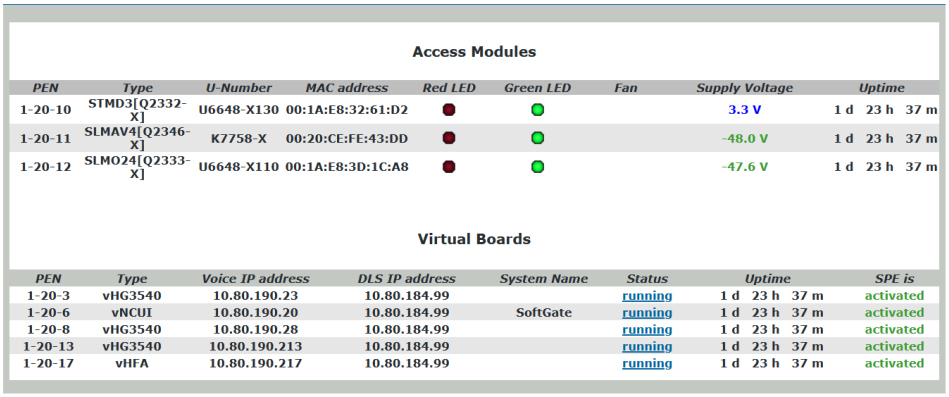
WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** System-Informationen**>** Info Periphere Baugruppen

In dieser Tabelle werden die OpenScape Access Module angezeigt. Dazu werden folgende Angaben gemacht:

- *PEN: Peripheral Equipment Number*
- *Typ*

- *LEDs*
- *System-Name*: Name der physischen peripheren Baugruppe, die virtualisiert wurde
- *Status:* in Betrieb oder nicht in Betrieb



Access Modules

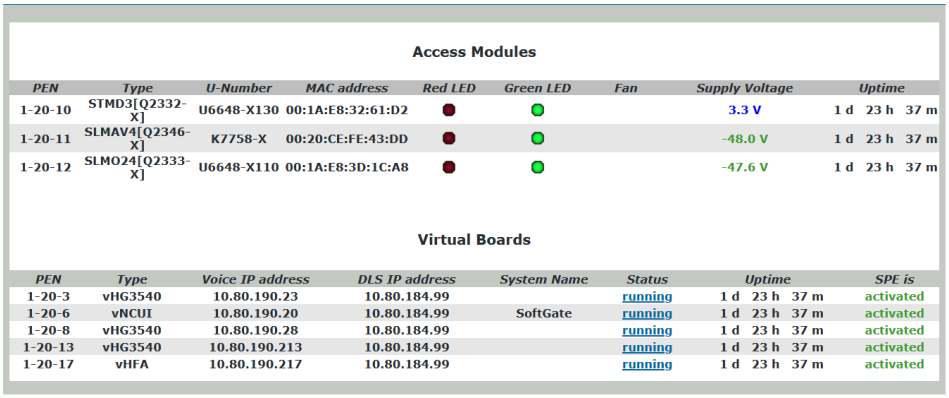
PEN	Type	U-Number	MAC address	Red LED	Green LED	Fan	Supply Voltage	Uptime
1-20-10	STMD3[Q2332-X]	U6648-X130	00:1A:E8:32:61:D2				3.3 V	1 d 23 h 37 m
1-20-11	SLMAV4[Q2346-X]	K7758-X	00:20:CE:FE:43:DD				-48.0 V	1 d 23 h 37 m
1-20-12	SLMO24[Q2333-X]	U6648-X110	00:1A:E8:3D:1C:A8				-47.6 V	1 d 23 h 37 m

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 OpenScapeAccess Clocking

Softgate-Status (Schaltfläche im unteren Bereich mit Markierung "i") ->läuft (für Details anklicken):



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

Auf dieser Seite kann der Status der Peripherieplatine (rote, grüne LED), SLC-Rollen überprüft werden, wobei der Master die niedrigste SLC-Nummer und standBy die zweitniedrigste haben muss. Wenn die SLC-Rolle unbekannt ist, ist die QDCL-Funktionalität nicht aktiv, SG kennt sie nicht, da die Informationen über die SLC-Rollen nicht weitergeleitet werden. SLC Master muss 1 und SLC StandBy 2 sein. GPS_IN-LEDs sind im ISS-Szenario nützlich. Weitere Details - Abschnitt 9.2.2.3 des OpenScape Cordless Enterprise V7 Dokuments

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** System-Informationen**>** Info Periphere Baugruppen

Die Tabelle *OpenScape Access Clocking* wird angezeigt: Die Werte für die Taktung des OpenScape Access Moduls werden in dieser Tabelle angezeigt. Dazu werden folgende Angaben gemacht:

- *PEN*: Peripheral Equipment Number
- *PBC*

- *Name*: Name und Sachnummer der physischen peripheren Baugruppe, die virtualisiert wurde
- *Trunk*
- *SM*
- *CLK-SRC*
- *Status*
- *CNT*
- *dF*
- *dP*
- *Sync.Verluste*
- *dP-Avg*
- *VCXO Center*: Voltage-Controlled Crystal Oscillator
- *VCXO-Avg*: Voltage-Controlled Crystal Oscillator

Schaltflächen

In dieser Tabelle gibt es die folgenden Schaltflächen:

Schaltflächen in der Spalte PEN

Details-Schaltflächen

Schaltflächen in der Spalte PEN

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** System-Informationen**>** OpenScapeAccess Clocking**>** Schaltflächen in der Spalte PEN

In diesem Dialog werden für das ausgewählte Access Module Informationen angezeigt.

Details-Schaltflächen

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** System-Informationen**>** OpenScapeAccess Clocking**>** Details-Schaltflächen

Der Dialog *HPA Clocking Details* wird angezeigt. In diesem Dialog werden folgende Grafiken angezeigt:

- *Phase Jitter Distribution*: Verteilung der Phasenschwankungen um einen Mittelwert
- *Phase Jitter*: Phasenschwankungen um einen Mittelwert

Schaltfläche

In diesem Dialog gibt es die folgende Schaltfläche:

- *Zurück zu OpenScape Access Clocking:* DieTabelle *OpenScape Access Clocking* wird erneut angezeigt.

4.9.1.5 AP Emergency

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** System-Informationen**>** AP Emergency

Die Tabelle *AP Emergency* wird angezeigt. In dieser Tabelle werden die Daten des AP Emergency dargestellt. Diese Daten umfassen: *AP*, *Kontrolleinheit*, *Host-CC verbunden*, *CC-AP verbunden*.

AP Emergency übernimmt den Betrieb der Access Points, wenn die zentrale Steuerung ausfällt.

4.9.2 Verbindungskontrolle

WBM-Pfad

WBM **>** Wartung **>** Status-Information**>** Verbindungskontrolle

Das Menü *SoftGate-Verbindungskontrolle* wird geöffnet.

Menü Verbindungskontrolle

Dieses Menü bietet folgende Optionen zur Auswahl:

IPDA Verbindungen anzeigen

IPDA DMC Verbindungen anzeigen

Alle Verbindungen anzeigen

4.9.2.1 IPDA Verbindungen anzeigen

Anmerkung: Diese Funktion darf nur von Entwicklern benutzt werden.

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** Verbindungskontrolle **>** IPDA Verbindungen anzeigen

Die Tabelle *SCC-N IPDA-Verbindungsliste* wird angezeigt. In dieser Tabelle werden die gerade aktiven IPDA-Verbindungen angezeigt (IPDA: IP Distributed Architecture). Dazu werden folgende Angaben gemacht: *NPCI*, *Teilnehmer A*, *Teilnehmer B*, *SW-Attr. Codes*, *Ziel-Port*, *Quell-Port*, *IP-Adresse*, *Index*.

Schaltfläche

Aktualisieren: Durch Klicken auf diese Schaltfläche wird die Verbindungsliste manuell aktualisiert.

Kontrollkästchen

Aktualisieren: Aktivierbar/Deaktivierbar. Wenn dieses Kontrollkästchen aktiviert ist, wird die Verbindungsliste alle 60 Sekunden automatisch aktualisiert.

Anzeige

Sekunden bis zur nächsten Aktualisierung: Anzeige, nach wie vielen Sekunden die Verbindungsliste automatisch aktualisiert wird.

4.9.2.2 IPDA DMC Verbindungen anzeigen

Anmerkung: Diese Funktion darf nur von Entwicklern benutzt werden.

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** Verbindungskontrolle **>** IPDA DMC Verbindungen anzeigen

Die Tabelle *SCC-DMC IPDA-Verbindungsliste* wird angezeigt. In dieser Tabelle werden die gerade aktiven IPDA-Verbindungen angezeigt (IPDA: IP Distributed Architecture). Dazu werden folgende Angaben gemacht: *NPCI*, *CorrelationID*, *ForwardCodec*, *ReverseCodec*, *Quell-Port*, *Ziel-Port*, *IP-Adresse*.

Schaltfläche

Aktualisieren: Durch Klicken auf diese Schaltfläche wird die Verbindungsliste manuell aktualisiert.

Kontrollkästchen

Aktualisieren: Aktivierbar/Deaktivierbar. Wenn dieses Kontrollkästchen aktiviert ist, wird die Verbindungsliste alle 60 Sekunden automatisch aktualisiert.

Anzeige

Sekunden bis zur nächsten Aktualisierung: Anzeige, nach wie vielen Sekunden die Verbindungsliste automatisch aktualisiert wird.

4.9.2.3 Alle Verbindungen anzeigen

Anmerkung: Diese Funktion darf nur von Entwicklern benutzt werden.

WBM-Pfad

WBM **>** Wartung **>** Status-Information**>** Verbindungskontrolle**>** Alle Verbindungen anzeigen

Die Tabelle *SCC-Verbindungsliste* wird angezeigt. In dieser Tabelle werden alle gerade aktiven SCC-Verbindungen angezeigt. Die folgenden Informationen werden angezeigt: *Gerät*, *Typ*.

Schaltfläche

Aktualisieren: Durch Klicken auf diese Schaltfläche wird die Verbindungsliste manuell aktualisiert.

Kontrollkästchen

Aktualisieren: Aktivierbar/Deaktivierbar. Wenn dieses Kontrollkästchen aktiviert ist, wird die Verbindungsliste alle 60 Sekunden automatisch aktualisiert.

Anzeige

Sekunden bis zur nächsten Aktualisierung: Anzeige, nach wie vielen Sekunden die Verbindungsliste automatisch aktualisiert wird.

4.9.3 H323-Status

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** H323-Status

Das Menü H323-Status wird geöffnet.

Menü H323-Status

Die folgenden Optionen werden in diesem Menü angezeigt:

H323 Endpunkte

4.9.3.1 H323 Endpunkte

WBM-Pfad

WBM **>**

Wartung **>**

Status-Information **>**

H323-Status **>**

H323 Endpunkte

Die Tabelle *H.323 Endpunkte* wird angezeigt. In dieser Tabelle werden die an OpenScape 4000 SoftGate angemeldeten und gerade in Verbindung stehenden H.323-Telefone angezeigt. Dazu werden folgende Angaben gemacht:

- *EP-ID*: Endpunkt-ID
- *Gespräche*: Alle Gespräche am jeweiligen H.323-Endpunkt
- *Ausgehend*: Ausgehende Gespräche am jeweiligen H.323-Endpunkt
- *Ankommend*: Ankommende Gespräche am jeweiligen H.323-Endpunkt
- *Klasse*

Schaltflächen

In dieser Tabelle gibt es die folgenden Schaltflächen:

Schaltflächen in der Spalte *EP-ID*

Details-Schaltflächen

Schaltflächen in der Spalte *EP-ID*

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** H323-Status **>** H323 Endpunkte **>** Schaltflächen in der Spalte *EP-ID*

Die Tabelle *H.323 Endpunkt ...* wird angezeigt.

Diese Tabelle zeigt die folgenden Informationen für das ausgewählte H.323-Telefon an: *Int. Schlüssel*, *Gesprächs-Ref. Richtung*, *rufender Teilnehmer*, *angerufener Teilnehmer*.

Schaltflächen

Unter dieser Tabelle gibt es die folgende Schaltfläche:

- *Zurück zu H.323 Endpunkteliste*: Die Tabelle *H.323 Endpunkt ...* wird erneut angezeigt.

Details-Schaltflächen

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** H323-Status**>** H323 Endpunkte**>** *<Leitung für ein H.323-Telefon>* **>** *Details*

Die Tabelle *H.323 Endpunkt Details ...* wird angezeigt.

Diese Tabelle enthält detaillierte Angaben über das ausgewählte H.323-Telefon. Diese Angaben sind:

- *EP-ID*, *H.323 Produkt ID*, *Nutzer*, *Gesprächsgröße*, *RFC 2198 PT* (Payload for Redundant Audio Data), *RFC 2833 PT* (RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals), *RFC 2833 Ereignisse*
- *Ressourcen*, *ptime*, *maxPtime*, *VAD* (Voice Activity Detection)

Schaltflächen

Unter dieser Tabelle gibt es die folgende Schaltfläche:

- *Zurück zu H.323 Endpunkteliste*: Die Tabelle *H.323 Endpunkt ...* wird erneut angezeigt.

4.9.4 HFA WAN Clients

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** HFA WAN Clients

Das Menü HFA WAN Clientswird geöffnet.

Menü HFA WAN Clients

Dieses Menü bietet folgende Optionen zur Auswahl:

Status

Logon Versuche

4.9.4.1 Status

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** HFA WAN Clients **>** Status

Die Tabelle HFA WAN Clients wird angezeigt. Die folgenden Informationen werden in dieser Tabelle für jeden Teilnehmeranschluss (HFA WAN-Client)

angezeigt: *Anschluss*, *PEN*, *Status*, *Adresse*, *Logon um*, *Logoff um*, *Gespräch seit*.

4.9.4.2 Logon Versuche

WBM-Pfad

WBM **>** Wartung **>** Status-Information **>** HFA WAN Clients **>** Logon Versuche

Die Tabelle HFA WAN Clients wird angezeigt. In dieser Tabelle werden die Teilnehmer (HFA WAN Clients) angezeigt, die vergebliche Logon-Versuche unternommen haben.

4.10 Reboot/Shutdown OS

WBM-Pfad

WBM **>** Wartung **>** Reboot/Shutdown OS

Das Menü Reboot/Shutdown OS wird geöffnet.

Menü Reboot/Shutdown OS

In diesem Menü gibt es die folgende Auswahlmöglichkeit:

Reboot OS

Shutdown OS

Wichtig: Bei integrierten SoftGates kann der OpenScape 4000-Dienst neu gestartet oder angehalten werden.

Wichtig: Bei Survivable SoftGates kann die OpenScape 4000 Survivability Unit neu gestartet oder angehalten werden.

4.10.1 Reboot OS

WBM-Pfad

WBM **>** Wartung **>** Reboot/Shutdown OS **>** Reboot OS

Das Fenster Reboot OS wird geöffnet. In diesem Fenster kann das Betriebssystem des SoftGates entweder neu gestartet oder heruntergefahren werden.

Schaltfläche

- *Reboot OS*: Durch Klicken auf diese Schaltfläche wird das Betriebssystem des SoftGates heruntergefahren und dann automatisch neu gestartet.

4.10.2 Shutdown OS

WBM-Pfad

WBM **>** Wartung **>** Reboot/Shutdown OS **>** Shutdown OS

Das Fenster Shutdown OS wird geöffnet. In diesem Fenster kann das Betriebssystem des SoftGates entweder neu gestartet oder heruntergefahren werden.

Schaltfläche

- *Shutdown OS*: Durch Klicken auf diese Schaltfläche wird das Betriebssystem des SoftGates heruntergefahren.

5 Hilfe

Im Modul *Hilfe* werden Informationen über das WBM angezeigt.

WBM-Pfad

WBM **>** *Hilfe*

Ein neues Browserfenster mit der Online-Hilfe für *OpenScape 4000 vHG 3575 (Enterprise GW) für OpenScape 4000 SoftGate* wird geöffnet.

Voraussetzung

Die IP-Adresse des OpenScape 4000 Assistant muss in der AMO STMIB konfiguriert werden.

6 Abmelden

Nach Klicken auf *Abmelden* wird die Verbindung zum OpenScape 4000 SoftGate beendet und die WBM-Sitzung geschlossen.

WBM-Pfad

WBM **>** *Abmelden*

Index

N

O

P

Q

R

S

T

V

W

X

Z