Unify OpenScape Session Border Controller

OpenScape SBC V10

Security Checklist

July 2024

A31003-S53A0-P100-10-76A9

Mitel

Notices

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

Trademarks

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

Contents

1 Introduction

1.1 History of Change

Date	Version	What
2011-03-14	1.0	Initial version based on OSB V1R4
2011-06-16	1.1	Updates based on OpenScape Session Border Controller V1 field trial findings
2011-06-20	2.0	Updates for OpenScape Session Border Controller V2
2011-06-29	2.1	Updates for OpenScape Session Border Controller V7
2012-04-02	2.2	Updates for OpenScape Session Border Controller V7 with new template, review comments:
2012-06-26	2.3	**Updates for OpenScape Session Border Controller V7 review comments:** • Changing Default Certificates for https access • Firewall considerations for remote endpoints / subscribers
2012-06-27	2.4	Updates for OpenScape Session Border Controller V7R1
2012-06-27	2.5	Updates for OpenScape Session Border Controller V8
2013-04-12	2.6	• Updated for V8 including comments received during review • V8 IF picture updated • SNORT IP message rate configuration guidelines updated • Port list report generation procedures updated • SIP Registration Denial of Service (DoS) Mitigation
2014-06-02	2.7	**V8 updates as a result of System Testing**: • Changing the SNMP Community Name
2014-06-20	2.8	**V8 updates as a result of System Testing**: • OSB Apache resources subject to resource exhaustion
2015-06-26	2.9	**V8R1 updates**: • Conform to UNIFY documentation template • FRN8981 - TLS v1.2 • FRN6983 - SNMPv3 • Toll fraud prevention notes added
2015-06-18	3.0	Initial version V9

Date	Version	What
2016-10-18	3.1	Initial version V9R1
2017-03-15	3.2	Initial version V9R2
2017-08-17	3.3	Initial version V9R3
2018-08-21	4.0	Initial version V9R4
2019-02-26	5.0	Initial version V10
2020-08-10	6.0	Initial version V10R1
2022-09-06	7.0	Documentation enhancements and updates
2023-04-07	8.0	Documentation enhancements and updates
2023-10-04	9.0	Documentation improvements
2024-07-23	10.0	Rebranded to Mitel layout

1.2 General Remarks

Information and communication and their seamless integration in “Unified Communications and Collaboration“ (UCC) are important, valuable assets forming the core parts of an enterprise business. These assets require every enterprise provide specific levels of protection, depending on individual requirements to availability, confidentiality, integrity and compliance for the communication system and IT infrastructure it utilizes.

Unify attempts to provide a common standard of features and settings of security parameters within delivered products. Beyond this, we generally recommend

- to adapt these default settings to the needs of the individual customer and the specific characteristic of the solution to be deployed
- to weigh the costs of implementing security measures against the risks of omitting a security measure and to “harden” the systems appropriately.

Security Checklists are published as a basis to support the customer and service department in both direct and indirect channels, as well as self-maintainers, to document security setting agreements and discussions.

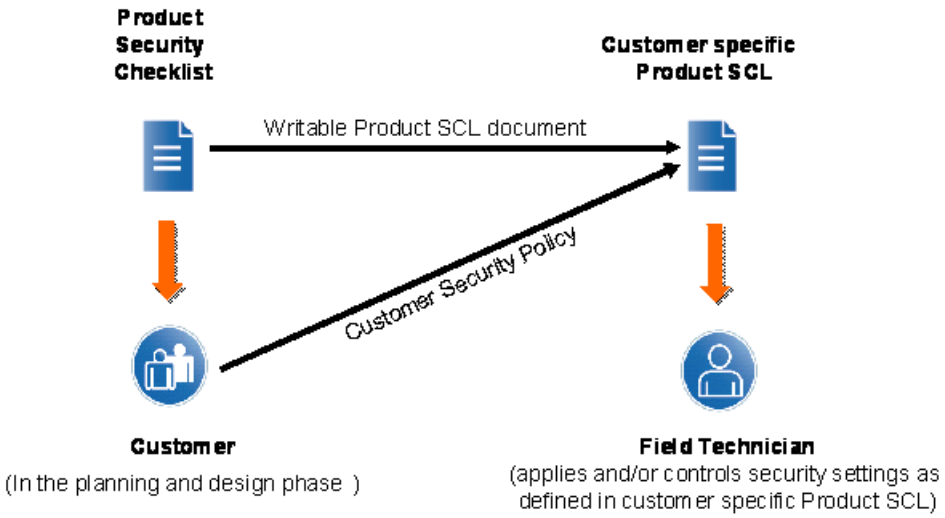
The Security Checklists can be used for two purposes:

1. In the planning and design phase of a particular customer project: Use the Product Security Checklists of every relevant product to evaluate, if all products that make part of the solution can be aligned with the customer’s security requirements – and document in the Checklist, how they can be aligned. The Product Security

Checklist containing customer alignments can be identified as Customer specific Product Security Checklist.
This ensures that security measures are appropriately considered and included in the Statement of Work to build the basis for the agreement between Unify and the customer: who will be responsible for the individual security measures:

- During installation/setup of the solution
- During operation

2. During installation and during major enhancements or software upgrade activities:
   The Customer specific Product Security Checklists are used to apply and/or control the security settings of every individual product.



Update and Feedback

- By their nature, security-relevant topics are prone to continuous changes and updates. New findings, corrections and enhancements of this checklist are being included as soon as possible.
  Therefore, we recommend using always the latest version of the Security Checklists of the products that are part of your solution.
  They can be retrieved from the partner portal (SEBA) http://www.unify.com/us/partners/partner-portal.aspx by locating the OpenScape Session Border Controller V10R1 product.
- We encourage you to provide feedback in any cases of unclarity, or problems with the application of this checklist.

Please contact the Mitel Security Advisories.

1.3 Security Strategy for Unify Products

Reliability and security is a key requirement for all products, services and solutions delivered by Unify. This requirement is supported by a comprehensive security software development lifecycle that applies to

all new products or product versions being developed from design phase until end of life of the product.

Products of Unify are developed according to the Baseline Security Policy, which contains the technical guidelines for the secure development, release and sustaining of the company's products. It defines the fundamental measures for software security that are taken throughout the whole lifecycle of a product, from design phase until end of life:

Product Planning & Design

Threat and Risk analysis (Theoretical Security Assessment) to determine the essential security requirements for the product.

Product Development & Test

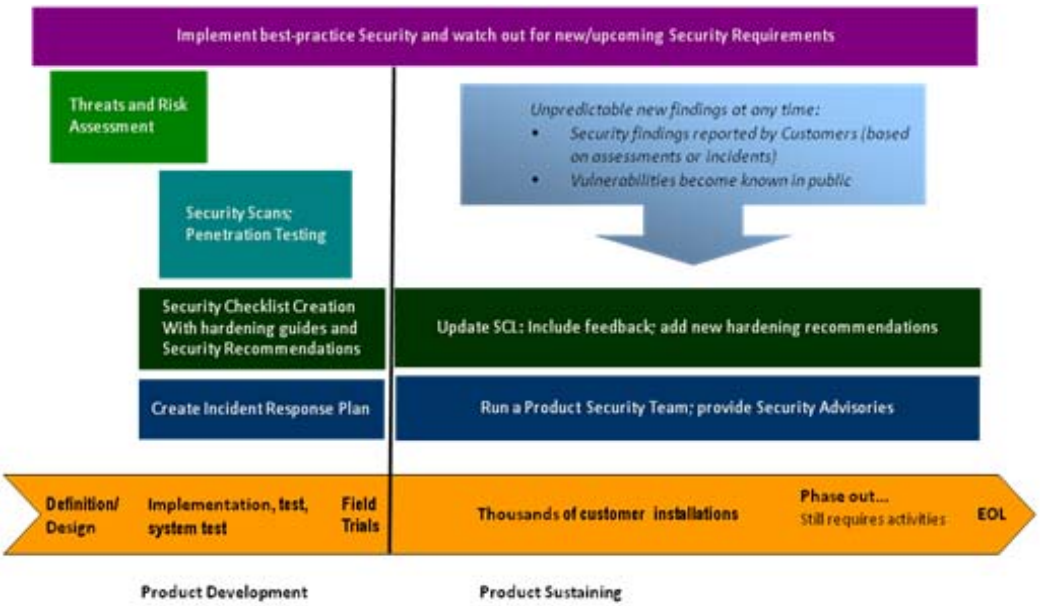
Penetration Tests (Practical Security Assessment) to discover implementation vulnerabilities and to verify the hardening of the default system configuration.

Installation & start of operation

Hardening Guides (Security Checklist) to support the secure configuration of the product according to the individual customer's security policy.

Operation & Maintenance

Proactive Vulnerability Management to identify, analyze and resolve security vulnerabilities that emerge after products have been released, and to deliver guidance to customers how to mitigate or close these vulnerabilities.



For more information about the Unify product security strategy we refer to the relevant Security Policies available at https://www.unify.com/security/advisories.

As we at Unify define a secure product, our products are not secure, but - they can be installed, operated and maintained in a secure way. The level of the products security should be scheduled by the customer.

The necessary information for that is drawn up in the Product Security Checklist. For OpenScape Session Border Controller V10 the Product Security Checklist is this document.

1.4 Security Policies for OSB / SBC

OpenScape Branch and OpenScape Session Border Controller are defined as Software appliances.

As such, the following security policies are applied:

1. **The ability to update 3rd party components with security updates or patches in the field**
   The update of any 3rd party component embedded in the product (including the Operating System) is provided by Unify in the context of regular product maintenance releases (or hotfixes in case of critical updates). The Operating System is based but not identical to a community developed distribution. Even when the community declares a version deprecated this does not necessary means that the OSB/SBC OS is deprecated as the packages and kernel are individually updated by the regular OSB/SBC releases or hotfixes. Applying such security updates in the field is not possible. Instead, customers should stay up-to-date with regard to the product fix and hotfix releases as a whole: this ensures the continuous inclusion of 3rd party component security fixes (if relevant to the product). Also refer to the Mitel Security Advisories.
2. **The ability to install and operate additional security software on the same system (such as Antivirus SW, host-based IDS, logging / monitoring agents etc.)**
   The installation of additional software is not possible. Instead, the product's built-in capabilities and interfaces have to be used to integrate them into overall customer's IT/managed services security concepts (e.g. run Antivirus SW in the virtual host, configure network-based IDS solutions appropriately, etc.)

1.5 Unify Services Security Foundation(SF)

Unify Services objective is to provide a set of essential security elements for all Unify products. This basic set of security measures is marked in the Product Security Checklist with “SF” for Security Foundation. One can find the “SF” tag in the Headlines of chapters in this document that contain SF measures. Within the affected chapters itemized measures are marked with SF if not all measures in the chapter are SF measures.

Currently the essential security requirements that at least should be configurable are the following:

- **Latest SW updates from SW Server are used for initial installation of system** (chapter 2)
- **Server Hardening (chapter 3)**
  - OS Hardening (chapter 3.3)
- **Unify Product hardening** (chapter 5)
  - Secure Billing (chapter 5.10)
  - SNMP community Strings (chapter 5.9)
- **3rd Party component hardening (chapter 6)**
  - Web server (chapter 6.1)
  - Data Base (chapter 6.3)
- **Secure Administration (chapter 7)**
  - Remote Administration (chapter 7.8)
  - SNMP community Strings (chapter 7.9)
- **Product requirements to infrastructure (chapter 9)**
  - Firewall (chapter 9.3)
  - Network Design (chapter 9.1)
  - Separate Paper for network design of UC deployments under construction
- **Super ordinate product specific Security Measures**
  - PW Policy (chapter 10.1)
  - Configuration of accounts with Least privileges and change of default PW (chapter 10.2)
  - Change of default certificates (chapter 10.3)
  - Port Table (chapter 10.4)

For detailed information refer to the corresponding chapters.

1.5.1 Security Implementation Checklist

The purpose of the Security Checklist is to assure that solutions that are being implemented in a secure way. The objective is to implement at least fundamental security measures as part of the implementation of the whole solution.

Complementary to the Product Security Checklists issued for individual products providing a complete collection of security measures applicable to each individual product. It's up to the individual customer to decide which of the Product SCL measures are appropriate within the respective project.

1.6 Customer Deployment - Overview

This Security Checklist covers the product OpenScape Session Border Controller V10R1 listing security relevant topics and settings in a comprehensive form.

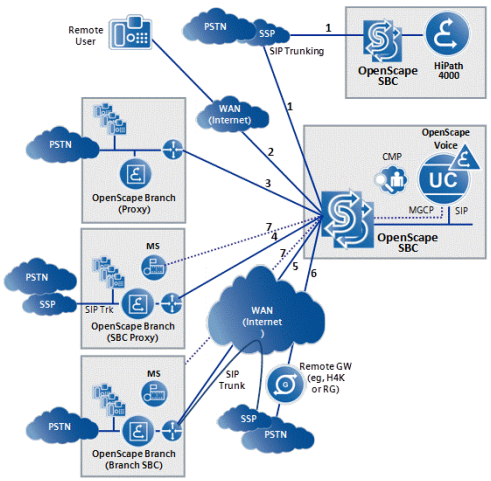
	Customer	Supplier
Company		
Name		
Address		
Telephone		
E-mail		
Covered Systems (e.g. System, SW version, devices, MAC/IP-addresses)		
Referenced Master Security Checklist	Version:	
	Date:	
General Remarks		
Open issues to be resolved until		
Date		

2 SF - OpenScape Session Border Controller V10R1 Hardening Procedures in General

OpenScape Session Border Controller (SBC) was developed by Unify as a solution component of the award-winning OpenScape solution portfolio to enable VoIP networks to extend SIP-based communication and applications beyond the Enterprise network boundaries.

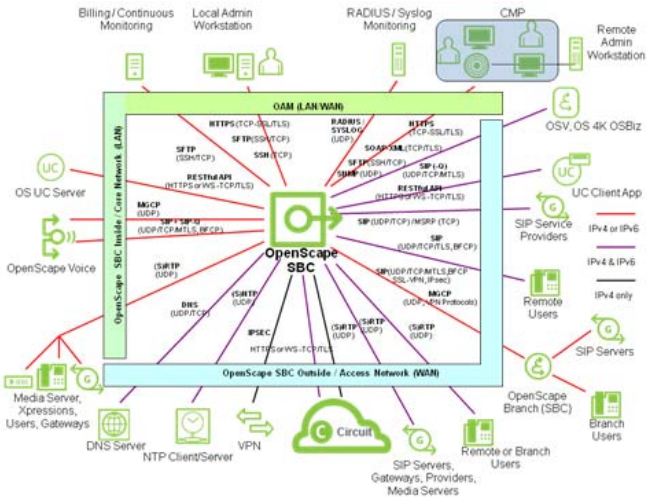
The OpenScape Session Border Controller provides three key functions in support of network deployment scenarios as shown below:

- secure termination of SIP-based trunking from a service provider
- secure voice communications for remote workers
- connection to branch offices as part of a distributed OpenScape Voice deployment



Considering hardening of the OpenScape Session Border Controller V10R1, all interfaces and ports have to be analyzed.

Relevant interfaces for OpenScape Session Border Controller V10R1 are shown in the landscape below. Both the OpenScape Session Border Controller inside or core network (LAN) and outside or access network (WAN) interface /IP and ports are included in the release notes as well as from the partner portal (SEBA Service Support - Interface Management).



The recommended security hardening measures are listed in the following chapters.

To tighten security on OpenScape Session Border Controller V10R1, the following measures are recommended:

For SNMP

- **SNMPv2** -Changing the SNMP Community Name from the defaults since these are essentially passwords used for SNMP discovery and data exchange of SNMP trap information.
- **SNMPv3 - configuring the passphrases for the encryption and integrity check -** Changing predefined user account passwords from their defaults as these are well known.
- Changing the system default password policies.
- If applicable, configure RADIUS User Authentication.
- When performing a system upgrade ensure all security measures put in place are maintained.
- If the internal firewall is used, ensure it is properly configured.
- Ensure appropriate IP message rate limits are set for normal operation.
- Closing Unused IP Ports – Configure the ports required for operation of the system. If an external firewall is used, ensure that it is properly configured to pass the required traffic towards the system.
- Use secure transport connections for SIP signaling whenever possible. Using unsecured transport for SIP signaling provided opportunities for possible eavesdropping and disclosure.
- Adopt appropriate media policies for using secure RTP media according to the network peer capability and profile wherever possible. Using unsecured media may lead to eavesdropping.
- Disable Local GUI access.

- Minimize exposure to Denial of Service SIP message flooding attacks by limiting the SIP message rate that SIP endpoints can send SIP messages.
- Minimize exposure to Denial of Service SIP registration attacks by quarantining SIP endpoints which are unable to provide valid registration identities or digest authentication credentials.
- Deviations of the recommended security settings based on customer request shall be documented.

The recommended measures are listed in the following chapters.

First point is to install only up-to-date software. The newest Software versions of software that is delivered by Unify always are available on Unify Software Server. While no additional OpenScape Session Border Controller 3rd party software is required for operation, we recommend installation of up-to-date software versions and patches of additional 3rd party software which may be used on products used to manage the OpenScape Session Border Controller. Please also take into account manufacturer advisories as well as Unify security advisories (see chapter 11 [5]).

CL-SF:SW Status All components	**Up-to-date SW, SW that is delivered by Unify as well as additionally necessary Software.**					
Measures	Up-to-date SW installed for the below listed components. SW that is delivered by Unify can be downloaded from the SW Server.					
References	Release Notes					
Sample Product Vxy	Yes:		No:			
Central Components						
1	Yes:		No:		Version:	
2	Yes:		No:		Version:	
…						
Clients						
Web Client	Yes:		No:		Version:	
Mobile Client	Yes:		No:		Version:	
OpenStage Client	Yes:		No:		Version:	
…						
Further 3rd party components NOTE:Please only list 3rd Party components that can be updated independently of the Product.						

CL-SF:SW Status All components	**Up-to-date SW, SW that is delivered by Unify as well as additionally necessary Software.**					
Browser	Yes:		No:		Version:	
OS	Yes:		No:		Version:	
DB	Yes:		No:		Version:	
...						
PCs / Servers / Devices						
Servers	Yes:		No:		Version:	
Client PCs	Yes:		No:		Version:	
Devices (e.g. OpenStage phones for every device category one entry please).	Yes:		No:		Version:	
...						
Circuit / Telephony Connector						
Circuit Cloud	Yes:		No:		Sprint/HF:	
Client PC Browser/ Chrome	Yes:		No:		Sprint/HF/ Browser:	
Client PC Browser / FireFox	Yes:		No:		Sprint/HF/ Browser:	
Telephony Connector Client	Yes:		No:		Sprint/HF:	
Customer Comments and Reasons						

INFO: Based on the SW installed, the necessary Patch management for the customer shall be defined. Patch management is out of scope of the Product Security Checklist.

INFO: It is recommended to integrate a centralized SBC into the customer's DMZ (Demilitarized Zone).

3 Server Hardening

3.1 OS Hardening

OS has been hardened based on the best practices and recommendations of OS and its components communities.

3.2 Clean Customer Deployment

SNMPv2 uses the notion of communities to establish trust between managers and agents. Community names are essentially passwords. A community name allows a level of access to MIB data. Data retrieval access levels are read-only (RO). An access level of read-write (RW) is not used.

CL-CleanDeploy-mentSample Product VxyServer PC	**All SW coming from Unify that is not necessary for the customer deployment has to be removed from the Sample Product Vxy Server.**
Measures	After Installation all SW that were necessary as installation help (Diagnostic tools like Wireshark, putty, old SW Versions ...) shall be removed from Server
References	SNMP v2
Needed Access Rights	
Executed Server 1:	Yes: No:
Customer Comments and Reasons	

3.3 Changing the SNMP Community Name

SNMPv2 uses the notion of communities to establish trust between managers and agents. Community names are essentially passwords. A community name allows a level of access to MIB data. Data retrieval access levels are read-only (RO). An access level of read-write (RW) is not used.

CL-OS_SBC-SNMP	Change SNMP Community Name
Measures	Change default values for Read-Only (RO) community name for SNMP Discovery since SNMP v2 community name is sent in clear text unless other security measures (e.g. VPN) are used for this traffic. By default, the OpenScape Session Border Controller sets the RO community name to "public". It is very important to change this default at installation as it is well known to the general public. See additional setting information below.
References	SNMP v2
Needed Access Rights	root
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

NOTICE: Changing the SNMP RO Community Name does not have any effect on the community name sent on the trap messages. SNMP RO Community Name is only used for the SNMP Discovery process.

NOTICE: In a redundant system, the Community Name is automatically synchronized to the Backup node.

NOTICE: It is possible to backup and restore the configured Community Name.

Additional Information for Settings:

From OpenScape Session Border Controller V10 it is possible to change the SNMP RO community name locally via the local GUI and OpenScape Session Border Controller Assistant.

Changing via CMP Profile

A profile for the configuration of security parameters allows entering the new Community Name and the IP address of the SNMP agent which is allowed to perform SNMP discovery.

Changing via the Local GUI and OpenScape Session Border Controller Assistant

From OpenScape Session Border Controller V8R1 it is possible to change the Community Name from the Local GUI and also from the OpenScape Session Border Controller Assistant.

The Community Name can be changed on the SNMP Configuration screen under SNMP v2c Trap Destinations.

3.4 Configuring SNMPv3

SNMPv3 supports the encryption and integrity check of the discovery and trap messages. It is recommended to activate the encryption (Privacy) and integrity check (Authentication) of the SNMPv3 interface.

CL-OS_SBC-SNMPv3	Activate SNMPv3 encryption & integrity check
Measures	Activate the encryption and integrity check of the SNMPv3 interface. The encryption shall be configured to be performed with AES and the security check with SHA1. A pass-phrase shall be configured for encryption and another one for integrity check.
References	
Needed Access Rights	Administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

Up to 5 destinations can be configured for the SNMPv3 traps. For each of the destinations it is possible to configure:

- Security Level – three options are offered: None, Auth Only and Auth+Priv. it is recommended to choose Auth+Priv in order to activate encryption (Privacy) and Integrity check (Authentication).
- Auth Protocol – two options are offered: SHA-1 and MD5.which selects either HMAC-SHA-1 or HMAC-MD5 as the Message Authentication Code algorithm being used to authenticate SNMPv3 messages.. It is recommended to choose SHA-1 as this can currently be seen as the most secure authentication protocol in USM for SNMPv3.
- Auth Password – a passphrase of at least 8 and a maximum of 32 characters shall be configured.
- Priv Protocol – two options are offered: AES and DES. It is highly recommended to choose AES. Notice that DES is not considered a secure encryption algorithm anymore.

- Priv Password – a passphrase of at least 8 and a maximum of 32 characters shall be configured.

> ***NOTICE:*** The Engine ID is used to identify the SNMP Agent. The user is able to select the algorithm to generate the Engine ID from the following options: **Generate Automatically, Generate from IP address**, **Generate from MAC address**, **Text entry** and **Hex string entry**. If the user does not set the algorithm the system will generate automatically.

The SNMP gets is disabled by default, once enable it allows the read access of several internal MIB. To prevent the unauthorized access the SNMP get settings have to change the username and passwords.

The following settings are used in SNMPV3 get:

- Readonly user - A username with at least 6 and a maximum 32 characters shall be configured.
- Authentication pass - passphrase of at least 10 and a maximum of 32 characters shall be. Per configuration the minimum is 8, however 10 is recommended.
- Encryption pass - passphrase of at least 10 and a maximum of 32 characters shall be configured. Per configuration the minimum is 8, however 10 is recommended.

Regarding the mibs, current the walkthrough in following several mibs are allowed.

To disable the mibs that should not be accessed a change in the /etc/init.d/snmpdx have to be done.

Fill the “” on the /etc/init.d/snmpdx with mibs that should be disable as below:

```
case "$1" in
start)
echo -n "Starting SNMPD "
if grep -Fq "SNMPV3GET=1" $SNMPD_CONFIG ; then
SNMPD_DISABLED_MODULES="<Mib to be disable here>"
```

3.5 Configuring MSRP

MSRP supports the integrity check (Authentication) of the MSRP interface at core and access side.

CL-OS_SBC-MSRP	Activate MSRP integrity check
Measures	Activate integrity check of the MSRP interface. A passphrase shall be configured for integrity realm check.
References	
Needed Access Rights	Administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

The administration should decide if the core side authentication should be used as well, in most of cases the core side is consider secured enough to not require authentication.

3.6 Changing Default Passwords for Accounts

After the installation, a default password is available for each account.Since the default passwords are publicly available, it is required that all default passwords be changed for “administrator”, “service”, “guest”, “assistant”, “redundancy” (see after the installation completes.

CL-OS_SBC-Pass-words	Use non-default OpenScape SBC passwords
Measures	During the installation, all accounts are created with default passwords, which are generally known. Thus, all passwords must be changed upon deployment. IMPORTANT: Even if RADIUS is used to authenticate predefined users, local passwords must be changed from their default values.
References	
Needed Access Rights	administrator IMPORTANT: Access Rights to change "root" password is "root".

CL-OS_SBC-Passwords	Use non-default OpenScape SBC passwords
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

The passwords can be administered via SSH, Local GUI or the OSB Assistant as indicated in Pre-defined Accounts)

In case of password administration via console or ssh, the following command shall be used:

`passwd user`

Where “user” is: “administrator”, “service”, “guest”, “assistant”,“redundancy”.

Passwords should be 8-36 characters long in accordance with the customer’s password policy.

> ***NOTICE:*** The password of “assistant” shall be synchronized between CMP and the OpenScape Session Border Controller, otherwise CMP will not be able to administer the OpenScape Session Border Controller. Notice that if the password for user “assistant” is modified in the CMP – OpenScape Session Border Controller Assistant, is automatically synchronized with the OpenScape Session Border Controller.

In redundant OpenScape Branch deployments, the passwords are automatically synchronized between the master and the backup nodes. It is not possible to change the password in the backup node. Except for the "redundancy" user which must be synchronized manually.

> ***NOTICE:*** It is also possible to change the password of the users of a set of selected OpenScape Session Border Controllers by means of CMP Profiles which are applied with Job Management.

> ***NOTICE:*** User passwords can be backed up and restored to a file. Passwords are stored in an encrypted format.

3.7 Change Default Password Policies

Verify if the Password Policies required by the Customer matches to the default policies provided by the OpenScape Session Border Controller. If they do not match; the Password Polices must be changed.

CL-OS_SBC-New_Account_Passwords	**Change customer's password policy within the OpenScape Session Border Controller**
Measures	Ensure the customer's password policy has been applied to the system, preferably by using the **/etc/pam.d** mechanism.
References	
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

The procedures to manage the password policy are described in Password Policies

The password policy must be changed on each OpenScape Session Border redundant node since they are not synchronized.

3.8 Disable not used users

It is possible to disable via Management Portal the user accounts that are not used. This is not valid for native users, that are present on the system after full install: root, administrator, service, guest, assistant and redundancy.

CL-OSB-Disable Not Used accounts	**Disable accounts for not used users**
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

3.9 Perform User Authentication via RADIUS

It is possible to authenticate the users via a RADIUS server. Up to two RADIUS servers may be con-figured to perform user authentication on the OpenScape Session Border Controller. Each time a user performs a logon to the OpenScape Session Border Controller through the management interface using HTTPS, SSH, via SFTP or console, an exchange will be performed with the RADIUS server to authenticate the user. The RADIUS server will accept or reject the user authentication by comparing the provided credentials with the configured credentials.

CL-OS_SBC-RADIUS	**User Authentication via RADIUS**
Measures	The user authentication is performed by a RADIUS server. Up to two RADIUS server IP addresses may be configured. Both the OpenScape Session Border Controller and each RADIUS server must be configured with a shared secret to enable communication for the RADIUS client / server.
References	OpenScape Session Border Controller Administrator Documentation [2]
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information about the Functionality:

If the RADIUS server is accessible, user authentication will be performed by the RADIUS server. If however, the RADIUS server is inaccessible, user authentication will be performed locally; therefore, it

is still required that all local user authentication passwords must be changed from their default.

Note that users configured only in RADIUS will have the same privileges as the pre-defined service user. The length of user names is limited to 44 characters by the OpenScape Session Border Controller console, This limit also applies to users configured in RADIUS.

Communication between the OpenScape Session Border Controller and the RADIUS server is performed by means of the EAP protocol using MD5 encryption.

Additional Information for Settings:

RADIUS server user authentication may be enabled in the OpenScape Session Border Controller. At least one RADIUS server must be configured. RADIUS server access redundancy is possible by configuring two RADIUS servers.

The RADIUS service port (2115) is recommended, however any value in the port range (0-65535) can be used.

Each OpenScape Session Border Controller redundant node physical IP address shall be configured in the RADIUS server (not the virtual IP address).

Regarding the timeout, configuring a value of 1 or 2 is not recommended since network issues would lead to a timeout of the RADIUS authentication. If a RADIUS authentication timeout occurs, the user is locally authenticated.

RADIUS server user authentication may be separately enabled for https (web) access, CLI (Console access), SSH (and SFTP).

INFO: Authentication of users via the su command is performed internally (via Console CLI and SSH only). OpenScape Session Border Controller pre-defined users shall also be configured in the RADIUS server so that RADIUS user authentication can be used while the RADIUS server is accessible. Users which are not pre-defined within the OpenScape Session Border Controller may login for all services except SSH and SFTP.

INFO: Internal users “assistant” and “redundancy” must not be created on the RADIUS server. RADIUS Accounting may be enabled, in which case the RADIUS server is made aware of the duration of user sessions and vendor identification. The Accounting service may also be separately enabled for CLI (Console access), SSH (and SFTP) and https (web) access.

INFO: The Accounting service uses one port higher than the RADIUS authentication port. If the default RADIUS Authentication port is used, RADIUS Accounting service will use port 2116.A shared secret of 16 characters (fixed size) must be configured for each RADIUS server and the OpenScape Session Border Controller. In order to increase security the secret length has been fixed at 16 characters.

INFO: For SSH access it is not possible to login with user identities which are only defined in the RADIUS server. The SSH application requires that user identities be configured locally. In order to get around this issue either the administrator, and/or service user identities must be configured in the RADIUS server or user authentication is performed locally.

3.10 Perform User Authentication in SSH with PKI

It is possible to authenticate the users in SSH with PKI. In order to be authenticated, the client sends a signed message to the OpenScape SBC. This message is signed with the private key of the client. The OpenScape SBC verifies this message with the public key of the client which is associated to the user in the OpenScape SBC. The verification is only successful if the client has used the right private key. It is very important that the client computer is properly hardened to protect against undesired access to the client private key.

CL-SBC-SSH-PKI	**User Authentication in SSH with PKI**
Measures	The user authentication in SSH is performed with PKI. The client computer shall be properly hardened in order to avoid undesired access to the client private key.
References	OpenScape SBC V10 Administrator Documentation [2]
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information about the Functionality:

The External User will begin by logging into their own machine. They will then generate a public/private key pair. The private key will remain on their computer, but the public key will be sent to a person who has authority to append their public key on the OpenScape SBC. For example, if the External User wants to be able to log in to the OpenScape SBC as the administrator user without having to enter the administrator password; they would send their public key to the administrator user (e.g., in an email). The administrator user will associate the public key to its user. Now, when the External User logs in on the OpenScape SBC as the administrator user, a password is not required.The management of the public keys and their association to the user is done in the PKI Configuration section in the Security tab.

In order to configure a PKI for SSH the following steps shall be executed:

- Enable PKI Configuration;
- Open the PKI Configuration screen;
- Click on the Add button;
- Select the internal user (administrator or service) to which the key will be associated;
- Select the public key file and click to import it;
- Apply the configuration.

Regarding to the public key, the OpenScape SBC supports .ppk files which are generated with:

- RCF4716 format (a multi-line text file beginning with the line '---- BEGIN SSH2 PUBLIC KEY ----') – the external user name is located either in the Subject or in the Comment field.
  Example:---- BEGIN SSH2 PUBLIC KEY ----
  Comment: "rsa-key"Subject: "rsa-key-20120529"
  AAAAB3NzaC1yc2EAAAABJQAAAIB4aDWB7v6rYmfvlADlKuUPFL3dX
  eUHMOhUEx5q9/
  GpsyEnhNa85IYq0fiDP1NSHK9CmT04JjdWqev4habcdipHPXV2YY8H
  w5LI3MygLHWWPgzxcdbu+gR5/
  bSyIkE8cxjb20XUwuYoTv8yd5TUF8ViyEJIxUWlGpoaTU9y2t/DQ==
- Linux format – the external user name is located in the 3rd field in the file.
  Example:ssh-rsa
  AAAAB3NzaC1yc2EBCDABJQAAAIB4aDWB7v6rYmfvlADlKuUPFL3dX
  eUHMOhUEx5q9/
  GpsyEnhNa85IYq0fiDP1NSHK9CmT04JjdWqev4hl9gJipHPXV2YY8H
  w5LI3MygLHWWPgzxcdbu+gR5/
  bSyIkE8cxjb20XUwuYoTv8yd5TUF8ViyEJIxUWlGpoaTU9y2t/DQ==
  rsa-key-20120529

Perform VoiceMail Password changes

Passwords are needed to retrieve the recorded messages by the user. The format of the passwords is digits with the length of min 3 up to 8 digits. Other entries like characters should not be allowed.

OSB-VoiceMail-Passwords	**Use non-default OpenScape Branch passwords**
Measures	Password for Accessing/Retrieving the VoiceMail Messages by User.Verify only digits can be entered for such passwords
References	
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

3.11 Circuit Telephony Connector Hardening

This session describes the configuration changes that should apply to the SBC to secure connection with Circuit.

3.11.1 Circuit Certificate

For the SBC to successfully security connect to Circuit, we need the RootCA certificate of Circuit obtained from the system administrator. Go to SBC administration page and navigate to **Security/General** and click on **Certificate Management**. Go to **CA Certificates** and upload the certificate from Circuit. Finally under **Certificates Profiles** click on **Add** and configure it like the following picture. Take note of profile name, as later on we need to reference it.

CL-OS_SBC-TC_CERTIFICATE	**Circuit Certificate**
Measures	Use circuit RootCA certificate to connect to circuit via https/websocket
References	OpenScape Session Border Controller Administrator Documentation [2]
Needed Access Rights	Administrator

CL-OS_SBC-TC_CERTIFICATE	Circuit Certificate
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

3.11.2 ATC Digest Authentication

It is recommended that Digest Authentication is turned on for the OSV remote endpoint representing the ATC trunk, opposed to trusted endpoint. Decision is based on security requirements. Also subscribers associated to Circuit users should use DA.

If DA authentication is turned on, the SIP requests from the ATC users are challenged based on their subscriber credentials (subscriber DA) while Conference Dial-In/Dial-Out SIP requests are challenged based on the endpoint's credentials (trunk DA).

CL-OS_SBC-CIRCUIT_DA	Digest Authentication
Measures	Enable Digest Authentication and Change realm and password s for ATC trunks and subscribers associated to Circuit Users
References	OpenScape Session Border Controller Administrator Documentation [2]
Needed Access Rights	Administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

3.11.3 DTLS Certificate

It is recommended that a new DTLS certificate profile be created to secure the media path when using the DTLS. If the certificate is not created a default certificate is created automatically.

This is done by adding a new Media DTLS certificate under **Security**>**General**> **Certificate Management** using a previously imported certificate.

CL-OS_SBC-CIR-CUIT-DTLS	**Digest Authentication**
Measures	Change the DTLS Certificate profile
References	OpenScape Session Border Controller Administrator Documentation [2]
Needed Access Rights	Administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

3.12 Push Notification

The Push notification is used in mobile users to wake up the OSMO application when a call is received. This measures should be executed only if this feature is enabled.

CL-OS_SBC-PUSH-NOT	**Configure Push Notification**
Measures	The push notification certificate passphrase shall be configured for integrity check. This passphrase, account ID, application bundle ID and certificate are needed to create the connection to Push Notification Server.
References	
Needed Access Rights	Administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

The settings are done in two different menu options, in Security > General > Certificate management and on Features > Push Notification Service.

Since the connections to Push Notification server is established from the SBC no additional configuration is needed.

3.13 SIPREC

As the OpenScape SBC act as a client no special measures are needed. When possible however is recommended to use TLS connections with properly assigned certificates.

3.14 SIP Load Balancer

If the SIP Load Balancer feature is enabled most of SBC functionalities are disabled. The firewall however is still fully operational and ports not used are lock. To avoid DDoS attacks the message rate limit should be configured (see Changing the Maximum IP Message Rate Threshold).

CL-OS_SLB-M-RATE	**Configure Message Rate Limit**
Measures	The Message rate limit should be configured with a value compatible with the expected traffic.
References	
Needed Access Rights	Administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

3.15 Single Arm Configuration

If the SBC is configured to have the access and core realms combined in a single interface an external firewall is needed that restricts access to administrative interfaces:

- Always use an external firewall to restrict access to the Session Border Controller.
- Disable access to administrative interfaces (https, ssh, snmp) of the Session Border Controller from the external firewall.
- Restrict access on administrative interfaces for https, snmp, ssh in the firewall configuration of the Session Border Controller.

CL-OS_SLB-AS-CONF	**Configure Administrative Access in SA**
Measures	In the external firewall the SSH/HTTPS/SNMP services should be disabled and at same time machines that need access to those services from the local network should be added in administrative access control.
References	
Needed Access Rights	Administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

3.16 Unify Phone hardening

This section includes information about implementing security measures for your Unify Phone.

CL-OS_SLB-AS-CONF	**Configure Administrative Access in SA**
Measures	Certificate Installation and firewall setting configuration for Unify Phone.
References	Unify Phone Administration chapters: **2.4 Configuring the OpenScape SBC (for OpenScape Voice or OpenScape 4000)** **3.5 Configuring the OpenScape SBC (for OpenScape Voice or OpenScape 4000)** **6.4 Certificates** **11 Firewall and proxy considerations**
Needed Access Rights	Administrator

CL-OS_SLB-AS-CONF	Configure Administrative Access in SA
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

It is recommended that a new DTLS certificate profile be created to secure the media path when using the DTLS. For more information, see DTLS Certificate.

3.16.1 Digest Authentication

It is recommended that Digest Authentication is turned on for the OSV/ OS4K remote users that are configured as Unify Phone users. Decision is based on security requirements.

If DA authentication is turned on, the SIP requests from the Unify Phone users are challenged based on their subscriber credentials (subscriber DA).

CL-OS_SBC-UNIFY_PHONE_DA	Digest Authentication
Measures	Enable Digest Authentication and Change realm and passwords for Unify Phone Users
References	OpenScape Session Border Controller Administrator Documentation [2]
Needed Access Rights	Administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

4 Securing the OpenScape Session Border Controller

4.1 Configuring the Internal Firewall (WAN)

The OpenScape Session Border Controller must be protected against attacks by using either an external firewall or own internal firewall.

CL-OS_SBC-Firewall-WAN	**Firewall Protection for the OpenScape Session Border Controller outside or access network (WAN).**
Measures	For the OpenScape Session Border Controller outside network (WAN), the OpenScape Session Border Controller internal firewall must be used if no other external firewall is used. If an external firewall is used it must be configured either to operate in transparent mode or in a no-NAT mode.If operating in a no-NAT mode the OpenScape Session Border Controller near-end NAT must be configured. Regardless of the external firewall operation mode, the external firewall must provide equivalent protection as the internal firewall to allow/disallow communication between the OpenScape Session Border Controller and external networks.
References	OpenScape Session Border Controller Administrator Documentation [2]
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

The OpenScape Session Border Controller Firewall settings and criteria for the “Allow” setting shall be applied as detailed below for all networks considering both IPv4 and IPv6 address types as supported in the network.

If the internal firewall is configured to block incoming traffic for a certain service, it will block new in-coming connections. However, if the connection is initiated by the OpenScape Session Border Controller, the incoming flow will be allowed for that service and for the peer to which the connection had been established. This exception is valid for both UDP and TCP.

Under no circumstances shall “all protocols” be allowed for the OpenScape Session Border Controller outside or access network (WAN). Each protocol listed in the configuration shall be set to “blocked“ unless explicit requirements are identified for setting to “allow”.

- SIP
- TLS
- RTP/sRTP
- MGCP, only if OpenScape Branch remote Media Servers are used
- NTP if sRTP is used and media security key negotiation protocol is MIKEY#0

Additionally it is recommended, the internal firewall White/Black list be configured using CIDR notation according to customer requirements to allow / block communications from specific network IP addresses on the OpenScape Session Border Controller outside network Access network or WAN.

Specific firewall settings may be overridden for remote endpoints or remote subscriber subnets. Apply any overrides only where necessary. The internal firewall rules are valid for TCP and UDP.

IANA defines the following IP addresses for special use:

- 10.0.0.0/8 – Private Use
- 172.16.0.0/12 –Private Use
- 192.168.0.0/16 – Private Use
- 169.254.0.0/16 – Autoconfiguration
- 127.0.0.0/8 – Loopback

Since these IP addresses are often used for spoofing they are automatically added to the internal firewall blacklist.

NOTICE: If the outside or access network supports Virtual LAN (VLAN), each LAN is distinct and requires its own firewall configuration.

In case ALL available eth interfaces are bonded the respective **Realm Network IDs** cannot be added under Firewall Settings.

Firewall override settings should be done in a consistent manner so as to not defeat the OpenScape SBC firewall policy.

For the OpenScape Session Border Controller inside or core network, sometimes referred to as the LAN, an external firewall may be used, in which case the firewall must be configured to protect the inside network and operate in a transparent, non-NAT mode.

4.2 Changing the Maximum IP Message Rate Threshold

The OpenScape Session Border Controller utilizes the internal firewall to limit IP message traffic through the system to thwart denial of service (DoS) attacks. A large amount of data is transferred, to and from software servers, and between nodes of the cluster during installation. In order to prevent impeding this process, the detection threshold for a DoS attack has been intentionally set at 20,000 Kbytes per second. After installation, this value should be adjusted based on the OpenScape Session Border Controller outside or access network (WAN) configuration, traffic patterns (calls per second), simultaneous calls and background message traffic in support of subscriber registrations requiring far-end NAT traversal.

CL-OS_SBC-DoS_Thresholds	**Configure DoS thresholds according to traffic models**
Measures	Change the default packet rate that will trigger a denial of service lock-out.
References	OpenScape Session Border Controller Installation Guide [1]
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

IP message rate limit thresholds are provisioned in the GUI as parameters and applied to the internal Message Rate Control logic. The following default ranges are used:

- Block Period: 1 to 2048 seconds, with default of 60 seconds.
- Rate Threshold: 1 to 120,000 Kbytes per second, with a default of 20,000 packets per second.

Typically, no single network IP-Address (for example, single phone or server) will deliver heavy amounts of packet traffic; however, message concentrators such as another Session Border Controller or SIP proxy can create heavier amounts of packet traffic and need to be taken into account when setting the rate threshold value. Additionally, note that the “white list” of trusted hosts, identified by their IP addresses, is exempt from the rate threshold limit. For VoIP, a threshold value of 600 kbps is recommended. This value is enough to support up to 6 simultaneous VoIP RTP G.711 codec based sessions for users behind a single IP address, e.g., NAT router. If all connections came over a near end NAT then higher values have to be considered.

A lower threshold may be used to improve the OpenScape Session Border Controller VoIP DoS attack protection, provided it can be determined that individual IP addresses are only able to support a finite number of simultaneous RTP sessions. Likewise, a larger threshold may be used if larger networks exist behind a single NAT which requires support for a higher number of simultaneous RTP sessions. Note however that any increase reduces the OpenScape Session Border Controller ability to detect VoIP DoS attacks by network interfaces which send IP packets at a rate below the threshold value.

The user must follow the procedures below for managing the threshold value:

1. A threshold value of 20000 must be used during system upgrades if the IP address of the file server used for file uploads cannot be identified.
2. Once the file upload completes, each OpenScape Session Border Controller network interface having a rate potential higher than the VoIP threshold which is not statically configured must be included in the white list. As an example, the OpenScape Media Server is a candidate since it may support multiple simultaneous conference media sessions. Alternatively, the VoIP threshold value stated earlier may be used in all cases provided all network interfaces having the potential of exceeding the VoIP threshold, including the CMP file server are included in the white list.

The administrator should carefully monitor the system after reducing the threshold values and modify the threshold and “white list” to values for the specific customer configuration.

5 Securing the OpenScape Session Border Controller Interfaces

5.1 Secure SIP Signaling with Remote Endpoints

OpenScape Voice Remote Endpoints are configured in the OpenScape Session Border Controller to represent and identify remote network servers, e.g., SIP Service Providers, SIP media gateways, SIP proxy servers, etc. UDP, TCP may be used for the signalling transport however information is sent in clear-text which can be easily sniffed in a network. Furthermore, TCP is vulnerable to commonly known threats against integrity and availability of SIP Messages such as fuzzing, flooding, or attacks against SIP registrations..

It is highly recommended that SIP signaling is secured using TLS over TCP between the OpenScape Session Border Controller and OpenScape Session Border Controller Remote Endpoints representing OpenScape Branches, Media Gateways in a Branch, SIP Service Providers or Remote Media Gateways.

CL-OS_SBC-TLS-Remote_Endpoint	**Secure Remote Endpoint Signaling using TLS**
Measures	The OpenScape Session Border Controller provides a set of default TLS CA Certificates that can be used to establish TLS connections however, it is highly recommended that these default factory certificates be exchanged for real customer CA certificates from the Public Key Infrastructure (PKI). See Handling of Key Material, references and additional information below for installing CA certificates.
References	Refer to the following documents: • OpenScape Session Border Controller Installation Guide [1] for installing CA Certificates • The SIP Remote Endpoint server or gateway administration documentation should be referenced for installing CA certificates and configuring TLS connections for SIP servers or gateways..
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

Within the OpenScape Session Border Controller Certificate Authority (CA) Certificates may be associated with remote endpoints or remote subscribers using OpenScape Session Border Controller certificate profiles:

- Install CA Certificates
- Create / Modify CA certificate profiles, configuring them according to their planned usage, including:
  - Type of authentication to be performed
  - CA certificate file reference identifying as a local or remote CA file.
  - Select a key file (optional)
  - CA Certificate validation and revocation parameters
  - CA Certificate renegotiation parameters
  - TLS version to be supported
- Configure the remote endpoint transport security (TLS) for the type of TLS authentication sup-ported and associate with the appropriate CA Certificate profile.

If an unsecured SIP signalling connection is used, the OpenScape Session Border Controller and other OpenScape Voice solution elements may be vulnerable to network endpoints “masquerading” or performing "man-in-the-middle" attacks. Even though the OpenScape Session Border Controller is supporting the signalling with the remote endpoint, failure to follow these procedures may provide a false sense of security.

INFO: It is possible to download up to 10 certificate profiles in the OpenScape Session Border Controller.

NOTICE: TLS is established on a hop-by-hop basis. To apply end-to-end signaling security, equivalent measures must be applied to the OpenScape Session Border Controller inside or core network (LAN) interface according to Secure SIP Server VoIP Communications. Additionally remote interfaces supported by OpenScape Branch or SIP Proxy server requires the local hop between the remote endpoint and OpenScape Branch or SIP Proxy server be secured in a similar manner.

INFO: Only the basic constraint certificate critical extension is validated by the OpenScape Session Border Controller. Other critical extensions used in certificates are not validated.

5.2 Secure SIP Signaling with Remote Subscribers

OpenScape Voice Remote Subscribers registering through the Session Border Controller are recommended to use TCP transport for SIP signalling. TCP however transports signalling information in clear-text which can be easily sniffed in a network. Furthermore, TCP is vulnerable to commonly known threats against integrity and availability of SIP Messages such as fuzzing, flooding, or attacks against SIP registrations.

It is highly recommended that SIP signaling be secured using TLS between the OpenScape Session Border Controller and Remote Subscribers.

> ***INFO:*** The use of TLS avoids to open an incoming ("listener") port on remote subscriber devices (such as an OpenStage/OpenScape Desk Phone IP device), as it is the case for TCP connect ions (since a SIP-TLS connection is always established by the device and kept alive for incoming calls or notifications). This further reduces the overall attack surface (in this case on the subscribers'/ devices' side)

CL-OS_SBC-TLS-Subscribers	**Secure Remote Subscriber Signaling using TLS**
Measures	The OpenScape Session Border Controller provides a set of default TLS CA certificates that can be used to establish TLS connections. It is highly recommended that these default factory certificates be exchanged for real customer CA certificates from the Public Key Infrastructure (PKI). The certificate profiles shall be created with the parameter Minimum TLS version shall be set to TLSv1.2. IMPORTANT: By default the certificate profiles are created with a cipher suite priority which gives preference to ephemeral cipher suites in order to provide Perfect Forward Secrecy.. See Handling of Key Material, references and additional information below for installing CA certificates.
References	Refer to the following documents: • OpenScape Session Border Controller Installation Guide [1] for installing CA Certificates • SIP Remote Subscriber user device reference material should be referenced for installing CA Certificates and subscriber configuration for using TLS connections.
Needed Access Rights	administrator

CL-OS_SBC-TLS-Subscribers	Secure Remote Subscriber Signaling using TLS
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

Within the OpenScape Session Border Controller Certificate Authority (CA) Certificates may be associated with remote endpoints or remote subscribers using OpenScape Session Border Controller certificate profiles:

- Install CA Certificates
- Create / Modify CA certificate profiles, configuring them according to their planned usage, including:
  - Type of authentication to be performed
  - CA certificate file reference identifying as a local or remote CA file.
  - Select a key file (optional)
  - CA Certificate validation and revocation parameters
  - CA Certificate renegotiation parameters
  - Minimum TLS version to be supported (set to TLS v1.2)
  - Cipher suites selection by means of the parameters: Perfect Forward Secrecy, Encryption and Mode of operation.
- Associate remote subscriber location domain(s) with the appropriate CA Certificate profile.

If an unsecured SIP signalling connection is used, the OpenScape Session Border Controller and other OpenScape Voice solution elements may be vulnerable to network endpoints “masquerading” or per-forming "man-in-the-middle" attacks. Even though the OpenScape Session Border Controller is supporting the signalling with the remote endpoint, failure to follow these procedures may provide a false sense of security.

NOTICE: TLS is established on a hop-by-hop basis. To apply end-to-end signaling security, equivalent measures must be applied to the OpenScape Session Border Controller inside or core network (LAN) interface according to Secure SIP Server VoIP Communications.

5.3 Secure SIP Server VoIP Communications

By default, the OpenScape Session Border Controller interface with the SIP server (OpenScape Voice) uses TCP transport for SIP signaling, which sends information in clear-text which can be easily sniffed in the customer's network. Furthermore, TCP is vulnerable to commonly known threats against integrity and availability of SIP Messages such as fuzzing, flooding, or attacks against SIP registrations. The SIP signaling connection should be secured using TLS.

If the signalling channel is unsecured the SIP server and OpenScape Session Border Controller is vulnerable to "man in the middle" attacks from within the customer's own network.

The OpenScape Session Border Controller supports mutual authentication TLS with OpenScape Voice.

CL-OS_SBC-TLS-Core	**Secure OpenScape SIP Server VoIP communications using TLS**
Measures	The OpenScape Session Border Controller platform and OpenScape SIP server come with a set of default CA certificates that can be used to establish TLS connections. It is highly recommended that these default factory certificates be exchanged for real customer CA certificates from the Public Key Infrastructure (PKI). The certificate profile which is configured in System TLS Certificate shall be set with the parameter Minimum TLS version as TLSv1.2. IMPORTANT: By default the certificate profiles are created with a cipher suite priority which gives preference to ephemeral cipher suites in order to provide Perfect Forward Secrecy. IMPORTANT: See Handling of Key Material, references and additional information below for installing CA certificates.
References	Refer to the following documents: • *OpenScape Session Border Controller Installation Guide[1] for installing CA Certificates* • *OpenScape Voice V10 Installation Guide*
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

NOTICE: TLS is established on a hop-by-hop basis. To apply end-to-end signaling security, equivalent measures must be applied to all connections on the OpenScape Session Border Controller outside or access network (WAN) interface involved in the call. Securing the OpenScape Session Border Controller outside or access network (WAN) connections for remote subscribers and remote endpoints is covered in other sections of this document.

NOTICE: TLS V1.2 enforced with optional fallback to TLS V1.0 is supported.

5.4 Configure OpenScape Session Border Controller Outside or Access Network (WAN) SIP Signaling IP Ports

The SIP signalling IP ports used in OpenScape Session Border Controller and its associated servers are listed in the Interface Management Data Base.

Refer to Port Table for more information.

The OpenScape Session Border Controller SIP listening ports default to the well known SIP ports:

- 5060 - UDP
- 5060 - TCP
- 5061 - TLS

Since these ports are well known in the network external attackers may instigate attacks to these ports more likely.

It is therefore recommended that the OpenScape Session Border Controller SIP listening ports be changed to other values which do not conflict with other provisioned ports (Although this measure can be considered only as “security by obscurity”, it adds some limited protection and therefore contributes to the overall security posture of the installation)

CL-SBC-SIP_Ports	**Configure OpenScape Session Border Controller Outside or Access Network (WAN) ports required for VoIP communication**
Measures	It is recommended that the OpenScape Session Border Controller SIP listening ports be changed to other non-conflicting ports to lessen the susceptibility to external attacks
References	OpenScape Session Border Controller Installation Guide[1]
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

For example, within the port range 65000 to 65535, the SIP listening ports could be configured to:

- 65060 - UDP
- 65060 - TCP
- 65061 – TLS

When the SIP listening ports are changed to other values; the OpenScape Session Border Controller will only accept SIP requests received on the new SIP listening ports on both the outside or access network and the inside or core network. All SIP servers, OpenScape Branch Proxy Servers, Remote Subscribers (phones) and OpenScape Voice interfacing with the OpenScape Session Border Controller must be reconfigured to use the assigned ports otherwise no SIP communication will be possible.

Additionally, it can generally be noted; that according to the SIP protocol, phones send a REGISTER message with 'Contact' information about their own IP address and port number. Network endpoints are typically provisioned as static with the same ‘Contact’ information.

On the OpenScape Session Border Controller outside access or WAN network, OpenScape Session Border Controller sends SIP messages to the IP address / port number provided by the phones during registration or as statically provisioned for remote endpoints. Usually, these ports are 5060 (for UDP or TCP) or 5061 (for TLS over TCP), but can sometimes be configurable like the OpenScape Session Border controller above.

On the OpenScape Session Border Controller inside or core (LAN) network, the OpenScape Session Border Controller sends SIP messages to the OpenScape Voice provisioned IP address / port

number, which is usually 5060 (for TCP) or 5061 (for Mutual Authentication TLS).

5.5 Configure OpenScape Session Border Controller Outside for Video Incoming and Outgoing Calls from Internet

To allow OpenScape customers to attend to a video conference which is organized by another company, call external video users or receive video calls from Internet the Domain based Routing functionality was enhanced.

As this functionality exposes the SIP interfaces from not configurable endpoints an extra precaution should be taken.

First the internal video domains should be added to the whitelist. This will prevent callers to start calling unknown users from UC and flooding the OSV with video calls.

Second to increase even more the system against TTDoS a separated network access realm should be used, and untrusted networks should be connected to this realm just for outgoing and incoming video calls.

The access realm settings for this network should set the trusted level to minimal so not many calls can be placed simultaneously.

The rate limits should be adjusted to prevent many packets but still accept the video traffic accord to the customer needs.

CL-SBC-Video White List	**Configure OpenScape Session Border Controller remote endpoint used for video**
Measures	It is recommended that the OpenScape Session Border Con¬troller using the Domain based Routing (alphanumeric video) be configured with the whitelist in support Foreign peer domains with the OSV video domains. Wildcards should be avoided as much as possible.
References	OpenScape Session Border Controller Installation Guide[1]
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

CL-SBC-Video Separated Realm	Configure OpenScape Session Border Controller remote endpoint used for video
Measures	It is recommended that the OpenScape Session Border Con-troller using the Domain based Routing (alphanumeric video) have a separated network realm for the video calls. In addition, the trust level should be set to minimum for this domain.
References	OpenScape Session Border Controller Installation Guide[1]
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

For example, within the port range 65000 to 65535, the SIP listening ports could be configured to:

- 65060 - UDP
- 65060 - TCP
- 65061 – TLS

When the SIP listening ports are changed to other values; the OpenScape Session Border Controller will only accept SIP requests received on the new SIP listening ports on both the outside or access network and the inside or core network. All SIP servers, OpenScape Branch Proxy Servers, Remote Subscribers (phones) and OpenScape Voice interfacing with the OpenScape Session Border Controller must be reconfigured to use the assigned ports otherwise no SIP communication will be possible.

Additionally, it can generally be noted; that according to the SIP protocol, phones send a REGISTER message with 'Contact' information about their own IP address and port number. Network endpoints are typically provisioned as static with the same ‘Contact’ information.

On the OpenScape Session Border Controller outside access or WAN network, OpenScape Session Border Controller sends SIP messages to the IP address / port number provided by the phones during registration or as statically provisioned for remote endpoints. Usually, these ports are 5060 (for UDP or TCP) or 5061 (for TLS over TCP), but can sometimes be configurable like the OpenScape Session Border controller above.

On the OpenScape Session Border Controller inside or core (LAN) network, the OpenScape Session Border Controller sends SIP messages to the OpenScape Voice provisioned IP address / port number, which is usually 5060 (for TCP) or 5061 (for Mutual Authentication TLS).

5.6 Configure OpenScape Session Border Controller Outside or Access Network (WAN) MSRP Port

The MSRP port used in OpenScape Session Border Controller and its associated servers are listed in the Interface Management Data Base.

Refer to Port Table for more information.

The default port used by MSRP protocol is 2855, is also recommended to change this port, however this has to be done in accordance with the administrators of other ESINET components.

Since this port are well known in the network external attackers may instigate attacks to these ports more likely.

It is therefore recommended that the OpenScape Session Border Controller MSRP listening port be changed to other values which do not conflict with other provisioned ports. (Although this measure can be considered only as “security by obscurity”, it adds some limited protection and therefore contributes to the overall security posture of the installation.)

CL-SBC-MSRP_Port	**Configure OpenScape Session Border Controller Outside or Access Network (WAN) ports required for MSRP communication**
Measures	It is recommended that the OpenScape Session Border Controller MSRP listening port be changed to other non-conflicting ports to lessen the susceptibility to external attacks.
References	OpenScape Session Border Controller Installation Guide[1]
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

5.7 Configure OpenScape Session Border Controller Media Stream Security (SRTP)

SIP media sessions (RTP) established through the OpenScape Session Border Controller may be encrypted (SRTP). These media sessions establish media streams which traverse the OpenScape Session Border Controller which may be passed through virtually untouched (e.g., media proxy) or terminated depending on the network configuration and media security requirements of the media endpoints.

To establish a secure media session the SIP client, i.e., SIP phone, SIP soft client or SIP server must negotiate the secure media session using a SRTP key negotiation protocol according to:

- MIKEY [RFC 3830]
- SDP Security Descriptions (SDES)[RFC 4568]

If both media endpoints are within the same subnet and use the same media security key negotiation protocols it is possible to optimize the media session to allow direct media flow.

OpenScape Session Border Controller supports the following media configurations. These are based upon configuration and SRTP key negotiation protocol requirements.

Both the SDES and MIKEY#0 key negotiation profiles identified below are best effort allowing the media security using SRTP to be downgraded to insecure RTP if required or SRTP only. A remote endpoint can be configured with Best effort SDES to support profiles utilizing either a single or dual media line specification. The following media policies including security key management protocol combinations are possible:

- SRTP (SDES) – SRTP (SDES)
- SRTP (MIKEY#0) – SRTP (MIKEY#0)
- SRTP (MIKEY#0) – SRTP (SDES) (termination necessary)
- SRTP (MIKEY#0) – RTP (termination necessary)
- SRTP (SDES) – RTP (termination necessary)

For each SRTP - RTP termination scenario above, the intention of media security key negotiation may have been to establish an end-to-end secure media session. Since the media security key negotiation is best effort, the call destination may instead decide to downgrade to an insecure media session (RTP). While the OpenScape Session Border Controller is able to support such a media session end-to-end, customer security policies may instead require maintaining the secure media session for the calling interface. In other network configurations some media endpoints may be unable to support secure media or the best effort media security key negotiation procedures. Likewise, in these situations the customer security policy may require that the media session remain secure except in extenuating circumstances requiring media termination for these network interfaces.

CL-OS_SBC-Media_Security	**Configure OpenScape Session Border Controller Media Security for outside or access network (WAN) and inside or core network (LAN)**
Measures	Identify media security as the preferred profile for media endpoints whenever possible. See additional information below for more information.
References	OpenScape Session Border Controller Installation Guide[1]
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

OpenScape Session Border Controller media policies are configured for each remote endpoint peer or remote subscriber subnet to support the media policy combinations identified above. The media security applied for a call is determined in real time, based upon the OpenScape Session Border Controller provisioned media profile for peer endpoints or subnets, how the call was routed between the peers and signalling information supplied by the remote peer identifying its support for the desired media profile.

- Each network peer identified in the OpenScape Session Border Controller remote endpoint configuration which is capable of supporting media security (SRTP) should be configured to establish secure media calls.
- The OpenScape Session Border Controller remote endpoint shall be configured to support media security, identifying the supported media security key negotiation protocol.
- The OpenScape Session Border Controller remote subscribers using a common media security key management protocol within the same subnet should be configured to support media security.
- The OpenScape Session Border Controller inside or core network (LAN) should be configured to use SRTP with the media security key management protocol used by media peers in the Open-Scape Voice network.

If secure media sessions using MIKEY#0 as the media security key negotiation protocol profile must be terminated, the OpenScape Session Border Controller must be configured with a synchronized time base using Network Time Protocol (NTP).

CL-OS_SBC-NTP	**Configure OpenScape Session Border Controller Secure Network Time Protocol**
Measures	Secure media termination using the MIKEY#0 secure media key profile for negotiation requires a synchronized time base using the customer's Network Time Protocol (NTP) server. Configure the address of the NTP server in the OpenScape Session Border Controller configuration.
References	OpenScape Session Border Controller Installation Guide [1]
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

5.8 Change Default Certificates for Web Server (HTTPS)

Provisioning of the OpenScape Session Border Controller is performed by means of a web interface using secure HTTPS using the default certificates for the OpenScape Session Border Controller web server. Some customers may request that the default certificates be changed to those issued by the company PKI.

CL-OSBC-HTTPS-PKI	**Replace HTTPS default certificates by those issued by the company PKI**
Measures	If the customer requires PKI issued certificates for HTTPS be used, the default certificate for HTTPS shall be replaced. The certificate profile which is configured in System TLS Certificate shall be set with the parameter Minimum TLS version as TLSv1.2.TLSv1.0 is also supported as fallback. IMPORTANT: By default the certificate profiles are created with a cipher suite priority which gives preference to ephemeral cipher suites in order to provide Perfect Forward Secrecy
References	OpenScape Session Border Controller Administrator Documentation [2]
Needed Access Rights	Administrator, root

CL-OSBC-HTTPS-PKI	Replace HTTPS default certificates by those issued by the company PKI
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

If by mistake an invalid https certificate is installed, it will not be possible to communicate with the Web server. If this should occur, the following steps shall be followed to recover the previous HTTPS Profile:

- Login to OpenScape Session Border Controller via SSH session with service user.
- Increase the user privileges to root: su + <password>.
- Type the CLI command "pmc recover" - This command recovers the previous database with a last valid https certificate.

> ***INFO:*** The management of the HTTPS certificates and their association to the HTTPS system profile is done in the Certificate management and PKI Configuration sections in the Security tab, as described in the OpenScape Session Border V10 Controller Administrator Documentation [2].

5.9 Protect LAN Interface for Administrative Access

OpenScape Session Border administration is performed using the LAN interface:

- Secure web server (HTTPS) is used for central management CMP or Local GUI provisioning.
- Network services for SSH and SFTP are used for service personnel access.

Only CMP HTTPS access should be supported, while access for network services should be restricted to as few computers and users as possible.

CL-SBC-ADMIN-PROTECT	**Protect LAN for Administrative Access, disabling the Local GUI, to only allow provisioning from the central CMP and limit network service computer access**
Measures	The CMP provisioning interface and service access computer IP addresses must be identified and placed in the administrative access control list.
References	OpenScape Session Border Controller V10 Administrator Documentation [2]. Refer to Security Configuration, section *Configuration of Administrative Access Control*.
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

The central CMP IP address is provisioned identifying https access as allowed within the security tab, firewall section, administrative access control list for the main network interface. While it is possible to provision an IP address / mask, the CMP IP address is required.

Service computer IP address(s) used for ssh and sftp access are provisioned in the same manner.

It is recommended that a service computer address or secured secondary ssh IP address be identified for access in the administrative access control list to prevent lockout situations. For example, if by mistake an incorrect IP address is inserted in the administrative access control list or CMP IP address and a network reconfiguration takes place, the OpenScape Session Border Controller Web server will be inaccessible. If this should occur, the following steps must be followed to regain access:

- Login to OpenScape Session Border Controller via an SSH session from the secured server as the service user•Increase the user privileges to root: su + <password>.
- Increase the user privileges to root: su + <password>.
- Type the CLI command "iptables -F" - This command removes all firewall rules until the corrective action can be completed.
- Use the central CMP access to correct the mistake which also reapplies the firewall rules.

INFO: These steps cause bypassing the OpenScape Session Border Controller firewall rules until the

corrective action is completed requiring this maintenance activity to be planned accordingly.

In case of single arm configuration follow the recommendations below:

- Always use an external firewall to restrict access to the Session Border Controller.
- Disable access to administrative interfaces (https, ssh, snmp) of the Session Border Controller from the external firewall.
- Restrict access on administrative interfaces for https, snmp, ssh in the firewall configuration of the Session Border Controller.

5.10 Limiting SIP Message Rates

The OpenScape Session Border Controller may be configured to ensure SIP messages received from external SIP network interfaces do not exceed expected thresholds as a DoS prevention mechanism. SIP message rate limiting may be applied to each OpenScape Session Border Controller WAN destination address within each logical network interface.

CL-OS_SBC-MRL	**SIP Message Rate Limiting**
Measures	If message rate limiting is used, the OpenScape Session Border Con-troller WAN or access network interface must be reorganized or partitioned according to expected message rate profiles. Servers with traffic patterns matching these message rate profiles may need to be reconfigured to use a different OpenScape Session Border Controller destination address which is associated with the corresponding mes-sage rate profile.
References	OpenScape Session Border Controller V10 Administrator Documentation [2]
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

Message Rate limiting is available only on the OpenScape Session Border Controller's WAN or access network interface. Message rate limits may be configured for an OpenScape Session Border Controller

destination addresses, applying to all remote network interfaces which use the OpenScape Session Border Controller destination address for SIP signalling. Whenever a SIP messages arrives on the OpenScape Session Border Controller destination address, the message source IP address and port is logged against the destination address. If the received message exceeds the message rate threshold logged for the source address then the message discarded. The message source IP address is quarantined for a time interval in which no further messages are accepted from the source address.

NOTICE: Utilizing this feature may require some network reconfiguration with special consideration given to the limited number of available OpenScape destination addresses and ability to assign only one message rate limit per address.

NOTICE: An incorrect configuration may lead to remote network interfaces exhibiting legitimate SIP message rate patterns being inadvertently quarantined which may lead to a loss of service.

5.11 Protect Against SIP Registration DoS Attacks

The OpenScape Session Border Controller may be configured to protect itself and OpenScape Voice against a class of SIP registration attacks by detecting abnormal registration sequences. When a SIP interface attempting to gain unauthorized access provides invalid credentials or uses an invalid identity, the sender's IP address is blacklisted or quarantined for a finite period.

Two SIP registration DoS attack detection mechanisms are used:

1. SIP users with valid OpenScape Voice identities which are unable to provide valid digest authentication credentials after several successive registration attempts.
2. SIP interfaces attempting to register to OpenScape Voice using identities which are unknown.

Each type of violation uses its own quarantine time interval.

CL-OS_SBC-Registration-DoS	**Protect Against SIP Registration DoS Attacks**
Measures	Enable Remote User DoS Mitigation options for: - Unauthorized Users - Block Unknown Users Establish minimum quarantine intervals for each type of violation
References	OpenScape Session Border Controller V10 Administrator Documentation [2]
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

OpenScape Voice SIP Digest Authentication must be enabled and users configured with proper credentials.

Once a violator for the respective detection mechanism is determined, the message source IP address (sender) is quarantined for the specified time interval. The quarantine time interval may be adjusted. Note that too small of a value may prevent a potential attacker from moving on and provide insufficient DoS protection while too large a value may prevent legitimate SIP users which may have been incorrectly configured from being reinstated into service in a timely manner. The administrator may manually reinstate an IP address allowing the remote interface to resume operation if necessary.

5.12 Protect Against Unauthorized SIP Calling (Possible Toll Fraud)

While the OpenScape Session Border Controller can be configured to establish secure connections with remote subscriber endpoints, other actions may be necessary to ensure unauthorized SIP calls from remote user endpoints are not allowed, SIP server authentication for remote user access for making calls and access to features must rely on SIP application level authentication using SIP digest authentication. The OpenScape Voice SIP server configuration must ensure that the OpenScape Session Border Controller or any intermediate signaling network element in the signaling path for remote user access is not trusted so that SIP digest authentication is not bypassed.

INFO: If you can manage to setup MTLS-only at the remote subscriber interface, all subscribers have to have valid credentials (a valid TLS client certificate's private key); without that, no SIP message ever will pass the SBC.

While there are some OpenScape Session Border Controller configuration options mentioned earlier which may be used to limit exposure for possible toll fraud calls, it is paramount that OpenScape Voice be properly configured to eliminate the possibility. For more information, refer to the OpenScape Voice Security Checklist, Planning Guide, topic in the section *Never Trust Proxies and SBCs*.

Toll fraud is one the most significant VoIP security issue for enterprises. There is direct financial incentive for attackers and it is potentially easy to perform anonymously from remote (wherever a Session Border Controller or another SIP server is directly connected to the Internet, allowing incoming registration and call requests from anywhere). In most cases, toll fraud is initiated by external attackers who find a way to take an inbound call and "hair-pin" this call out to an international (or otherwise revenue-generating) number. Automatic generation of many such fraudulent calls may lead to high financial loss for the enterprise. It is paramount that OpenScape Voice (or any other SIP server served by OpenScape Session Border Controller) be properly configured to protect against toll fraud attacks. This includes to configure SIP digest authentication for all subscribers using individual and strong passwords.

For more information, refer to the OpenScape Voice Security Checklist, Planning Guide, topic in the section *Never Trust Proxies and SBCs*.

The following configuration options of OpenScape Session Border Controller may additionally be used to limit exposure to potential toll fraud:

- If possible (that is, if supported by all remote endpoints that legitimately connect to OpenScape Session Border Controller), allow only MTLS (mutual TLS) connections at the WAN/Internet interface. This effectively blocks any unauthorized remote SIP endpoint from placing any SIP message
- If MTLS cannot be used, use TLS (instead of TCP) as the SIP communication protocol on the WAN/Internet interface for remote subscribers and configure a different port than the default port 5061
- If TCP is used and cannot be changed to TLS: configure a different port than the default port 5060

5.13 Removal of debug information in SIP headers

This session is used to remove headers and additional information that could be used to exploit any security breach, i.e software versions and error messages.

CL-OS_SBC-Information Filtering	Protect Against SIP Registration DoS Attacks
Measures	Enable the flags: • Warning Info on Error responses removal • Internal Names and additional headers removal
References	OpenScape Session Border Controller V10 Administrator Documentation [2]
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

OpenScape Voice SIP Digest Authentication must be enabled and users configured with proper credentials.

Once a violator for the respective detection mechanism is determined, the message source IP address (sender) is quarantined for the specified time interval. The quarantine time interval may be adjusted. Note that too small of a value may prevent a potential attacker from moving on and provide insufficient DoS protection while too large a value may prevent legitimate SIP users which may have been incorrectly configured from being reinstated into service in a timely manner. The administrator may manually reinstate an IP address allowing the remote interface to resume operation if necessary.

6 Administration / Management Security

The OpenScape Session Border Controller is managed using:

- The central Common Management Portal OpenScape Session Border Controller Assistant interfaces with the OpenScape Session Border Controller application using HTTPS. The OpenScape Session Border Controller Assistant user or “assistant” is authenticated against the OpenScape Session Border Controller application. The “assistant” password must be synchronized between the OpenScape Session Border Controller Assistant and the OpenScape Session Border Controller.
- A local instance of OpenScape Session Border Controller Assistant runs on the same server as the OpenScape Session Border Controller application by default. The client for the local instance of OpenScape Session Border Controller Assistant is a standard web browser. The interface from the client to this OpenScape Session Border Controller Assistant is HTTPS.

NOTICE: The local instance of OpenScape Session Border Controller GUI shall be disabled in normal operation.

The OpenScape Session Border Controller user authentication can also be configured to via a RADIUS server (Refer to Perform User Authentication via RADIUS).

Recommended configuration steps

- Separate WAN and LAN interface of the Session Border Controller and integrate them into different IP networks.
- Do not expose the administration interface to the WAN interface.
- Restrict access on administrative interfaces for https, snmp, ssh in the firewall configuration of the Session Border Controller.

Alternate "Single Arm Configuration" without external access to administrative interfaces (not recommended)

In case LAN and WAN interface of the Session Border Controller are connected to the same interface:

- Always use an external firewall to restrict access to the Session Border Controller.
- Disable access to administrative interfaces (https, ssh, snmp) of the Session Border Controller from the external firewall.
- Restrict access on administrative interfaces for https, snmp, ssh in the firewall configuration of the Session Border Controller.

Alternate configuration with external access to administrative interfaces (not recommended)

- Use an overlay vpn solution to provide administrative access (e.g. Unify Remote Service Platform or similar solution).

or

- Always use an external firewall to restrict access to the Session Border Controller.
- Disable access to administrative interfaces (https, ssh, snmp) of the Session Border Controller from the external firewall.
- Enable administrative access on the external firewall on demand for the time that access is needed and for ip addresses that require access.
- Implement additional security measures as two-factor authentication, encrypted connections etc.

6.1 Local Authentication

6.1.1 PAM Framework

The enforcement of the user account and password settings is done using PAM framework configuration files located in the **/etc/pam.d** directory which are password-related—login, passwd, sshd, and su. The configuration of these files specifies the default behavior for all applications that manipulate the password.

Module Type	Module Flag	Module Name	Arguments
password	requisite	pam_passwdqc.so	pw_iteration_nr=3 retry=3 match=4 similar=deny passphrase=0 enforce=everyone pw_iteration_length=180 min=disable, disable, disabled,8,8 max=40 random=42
password	requisite	pam_unix2.so	**use_authtok nullok**

IMPORTANT: The arguments that appear in **bold text** must not be changed.

6.1.2 Editing PAM Configuration Files

Editing of the PAM configuration files is performed from the command line. Standard OS-level commands and custom commands assist in this activity.

For example, to change the number of cycles before a password can be reused (password iterations number) from the default value of 3 to the new value of 4, the system administrator must do the following:

1. Log on to OpenScape Session Border Controller
2. Get super-user rights
3. Edit password-related file `/etc/pam.d/common-password-pc`.
4. Change "pw_iteration_nr=3" to "pw_iteration_nr=4" as follows:
   password requisite pam_passwdqc.so
   min=disabled,disabled,disabled,8,8 max=40 passphrase=0
   match=4 similar=deny random=42 enforce=everyone retry=3
   pw_iteration_nr=4 pw_iteration_length=180
5. Save the file
6. Log off

NOTICE: For the meaning of the parameters in ***/etc/pam.d/common-password-pc*** please refer to Password Rules and Aging Management for Local Authentication.

IMPORTANT: Manual changes are overwritten when a release upgrade takes place.

To retain manual changes, the `/etc/pam.d/common-password-pc` file must be saved before an upgrade and restored after an upgrade.

In a redundant OpenScape Session Border Controller, the PAM configuration file `/etc/pam.d/common-password-pc` is automatically synchronized to the backup OpenScape Session Border Controller.

7 Virtualization

The OpenScape Session Border Controller may be virtualized using VMWare vSphere supported versions (refer to the Virtualization guide)

7.1 Virtualization Hardening According to VMWare

The primary hardening is for the Hypervisor. The most up-to-date version of the VMWare Hardening Guide shall be used. Refer to the VMWare homepage:

http://www.vmware.com/support/support-resources/hardening-guides.html

8 Addendum

8.1 GDPR

The OpenScape SBC is compliant with GDPR. The OpenScape SBC does not store any personal data, and any personal data transported (names) can be encrypted via TLS. The closest thing we have for personal data is administration passwords, and these are stored encrypted by the Operating System.

8.2 Password Policies

8.2.1 Password Rules and Aging Management for Local Authentication

Password rules are globally enforced using custom PAM module **pam_passwdqc.so** in **/lib/security**.

This module checks password strength for PAM-aware password changing programs, such as passwd. In addition to checking regular passwords, it offers support for password history and pass phrases, and can provide randomly generated passwords. All features are optional and can be reconfigured without rebuilding.

It is possible to modify the password rules and aging management either via Command Line Interface.

Via Command Line Interface

There are a number of supported parameters which can be used to modify the behavior of **pam_passwdqc**. The table below lists and describes each; defaults are in brackets.

NOTICE: Some parameters are not allowed to be modified (such that security would be lessened) and some parameters have strict modification limitations compared to standard PAM. Validation is not performed while using a standard editor, so it is possible to change some settings to invalid values. Care should be taken to ensure changes are valid.

NOTICE: Changing any parameter does not affect a new user or current password. Password syntax rule changes take effect the next time a user's password is changed.

Parameter	Description
min=N0,N1,N2,N3,N4	This parameter sets the minimum allowed password lengths for different kinds of passwords and pass phrases. The keyword disabled can be used to disallow passwords of a given kind regardless of their length. Each subsequent number is required to be no larger than the preceding one. • N0 is used for passwords consisting of characters from one character class only. The character classes are digits, lowercase letters, uppercase letters, and other characters. There is also a special class for non-ASCII characters, which cannot be classified, but are assumed non-digits. – N0 is not supported • N1 is used for passwords consisting of characters from two character classes, which do not meet the requirements for a pass phrase. – N1 is not supported • N2 is used for pass phrases. A pass phrase must consist of sufficient words (see the pass phrase parameter description below). • N3 is used for passwords consisting of characters from three character classes. The minimum supported value is 8. • N4 is used for passwords consisting of characters from four character classes. Default: [min=disabled,disabled,disabled,8,8] When calculating the number of character classes, uppercase letters used as the first character and digits used as the last character of a password are not counted. In addition to being long enough, passwords are required to contain: • Enough different characters for the character classes • The minimum length they have been checked against
max=N	This parameter sets the maximum allowed password length. This can be used to prevent users from setting passwords which may be too long for some system services. The value 8 is treated specially : if max is set to 8,passwords longer than 8 characters will not be rejected, but will be truncated to 8 characters for the strength checks and the user will be warned. Default: [max=40]

Parameter	Description
passphrase=N	This parameter sets the number of words required for a pass phrase, or 0 to disable the support for pass phrases. Default: [passphrase=0]
match=N	This parameter sets the length of common substring required to conclude that a password is at least partially based on information found in a character string, or 0 to disable the substring search. Note that the password is not rejected if a weak substring is found; it is instead subjected to the usual strength requirements with the weak substring removed. The substring search is case-insensitive, and is able to detect and remove a common substring spelled backwards. Default: [match=4]
similar=permit|deny	This parameter specifies whether a new password can be similar to the old one. The passwords are considered to be similar when there is a sufficiently long common substring and the new password with the substring removed would be weak. Default: [similar=deny]
random=N[,only]	This parameter sets the size of randomly generated passwords in bits, (24 to 72 bits), or 0 to disable this feature. Passwords that contain the offered randomly-generated string are allowed regardless of other possible restrictions. Default: [random=42] The only modifier can be used to disallow user-chosen passwords.
enforce=none|users| everyone	This parameter permits the module to be configured to warn of weak passwords only, but not actually enforce strong passwords. The users setting enforces strong passwords for invocations by non-root users only. Default: [enforce=everyone]
retry=N	This parameter sets the number of times the module requests a new password if the user fails to provide a sufficiently strong password and enter it twice the first time. Default: [retry=3]

Parameter	Description
pw_iteration_nr=N	This parameter remembers the last N number of passwords and does not allow the user to use it again for the next N password changes. It is recommended to set N higher than 100. However, if the password is not used for pw_iterations_length days, it can be used again. Default: [pw_iteration_nr=3]
pw_iteration_length=N	This parameter is the length in N days during which the password cannot be reused. N is number between 180 and 3650. However,if the password is changed more than pw_iterations_nr after a certain password has been used, this password can be used again. Default: [pw_iteration_length=180]
use_authok [ ]	Use the new password obtained by modules stacked before pam_passwd_mgmt. This disables user interaction within pam_passwd_mgmt. With this module, the only difference between "use_first_pass" and "use_authtok" is that the former is incompatible with "ask_oldauthtok". Default: use_authtok []

Password Rules as agreed for customer deployment:

The above are the recommended OpenScape Session Border Controller password rules. Please implement according to these rules unless other company specific rules are required at customer site.

Parameter	Values & Description
min=N0,N1,N2,N3,N4	
max=N	
passphrase=N	
match=N	
similar=permit|deny	
random=N[,only]	
enforce=none |users|everyone	
retry=N	
pw_iteration_nr=N	
pw_iteration_length=N	
use_authok[]	

8.2.2 Password Aging

Password aging rules are globally enforced by one of the following methods:

- By accepting the defaults for accounts creation in /**etc/login.defs**, which indicate the password aging controls (used by useradd) listed in the table below.
  Additionally, the following command must be executed to require the user to change the password upon initial logon:
  chage -d 0 <username>
- By using the passwd command, as follows:
  passwd -x 90 -n 1 -w 14 -i 30 <username>

In this command:

- -x sets the maximum number of days before the expiration.
- -n sets the minimum number of days before the next change.
- -w sets the number of days of warning days before the expiration.
- -i sets the login grace period after password expired before the account is locked.

Parameter	Description
PASS_MAX_DAYS	This parameter specifies the maximum number of days a password may be used. Default: PASS_MAX_DAYS=99999
PASS_MIN_DAYS	This parameter specifies the minimum number of days allowed between password changes. Default: PASS_MIN_DAYS=1
PASS_WARN_AGE	This parameter specifies the number of days' warning given before a password expires. Default: PASS_WARN_AGE=7
LOGIN_RETRIES	Max number of login retries if password is bad. Default: LOGIN_RETRIES=3
LOGIN_TIMEOUT	Max time in seconds for login. Default:LOGIN_TIMEOUT=60

NOTICE: The root password does not age.

Password Aging as agreed for customer deployment:

The above are the recommended OpenScape Session Border Controller password aging settings. Please implement according to these specifications unless there are other customer specific requirements.

Parameter	Value
PASS_MAX_DAYS	
PASS_MIN_DAYS	
PASS_WARN_AGE	
LOGIN_RETRIES	
LOGIN_TIMEOUT	

The file /etc/profile.local defines the rules to be applied to SSH sessions:

Parameter	Description
TMOUT=60	Longest duration of an inactive SSH session
MAXSESSIONS=5	Maximum number of parallel SSH sessions

The longest duration of a Local GUI https session can be configured in the screen **Maintenance & Diagnostics > Administration** (Default value = 1 hour).The longest duration of a CMP session can be configured in **Configuration > CMP > System Settings** (Default value = 30 minutes).

The number of times a user may try to login with the wrong password before the ssh session is blocked, is configured in the file `/etc/ssh/sshd_config`:

- MaxAuthTries=3 (by default)

NOTICE: This parameter is only honored with the PuTTy tool version 0.60 or higher. Previous versions of PuTTy do not honor this configuration and closes the session if the wrong password is entered on the first attempt.

NOTICE: By changing the parameter MaxAuthTries, the ssh application shall be restarted by means of the following command: `systemctl restart sshd`

8.2.3 Temporarily Blocking Accounts

The user accounts can be temporarily blocked in case of a certain number of wrong attempts to enter the password. In order to define the conditions of temporarily blocking the following files shall be changed by adding the configuration lines in bold:

```
/etc/pam.d/login
#%PAM-1.0
auth [success=done new_authtok_reqd=done default=ignore
auth_err=die] pam_radius_auth.so
```

```
auth requisite pam_nologin.so auth requisite pam_tally2.so
onerr=fail deny=3 unlock_time=60auth include common-auth
account include common-account
password include common-password
session required pam_loginuid.so
session optional pam_radius_auth.so
session include common-session
account required pam_access.so account required pam_tally2.so
```

/etc/pam.d/sshd

```
#%PAM-1.0
#
#
auth [success=done new_authtok_reqd=done default=ignore
auth_err=die] pam_radius_auth.so
auth required pam_nologin.so auth required pam_tally2.so onerr=fail
deny=3 unlock_time=60auth include common-auth
account include common-account account required
pam_tally2.sopassword include common-password
#session required pam_loginuid.so
session optional pam_radius_auth.so
session include common-session
account required pam_lastlog.so nowtmp
```

/etc/pam.d/password

```
auth [success=done new_authtok_reqd=done default=ignore
auth_err=die] pam_radius_auth.so
auth include common-auth auth requisite pam_tally2.so onerr=fail
deny=3 unlock_time=60account include common-account account
required pam_tally2.sopassword include common-password
session optional pam_radius_auth.so
```

The parameter “deny” indicates the number of times the wrong password can be entered before the user account is blocked. The parameter “unlock_time” (in seconds) indicates for how long the user account will be blocked.

INFO: The account blocking shall be carefully used because it can be used by an attacker for a Denial of Service attack by blocking the users indefinitely. It is recommended to protect the access via SSH and Web by creating a white list of the IP addresses which are allowed to manage the system (see Change Default Certificates for Web Server (HTTPS)).

8.3 Pre-defined Accounts

The following OpenScape Session Border Controller accounts (users) are supported by default:

#	User Name	PW Policy config-ured	Unify Default PW (to be changed immedi-ately)	Description
1	guest			- Read-only Local GUI access only, i.e., no central CMP interface sup-port - user group membership - no ssh / no sftp capabilities - May only change own password (see Changing Default Passwords for Accounts)
2	assistant			- Read-Write central CMP inter-face only, i.e., no local GUI access-assistant, sshlogin group member-ship - No ssh / sftp only - Has rights to changing password (see Changing Default Passwords for Accounts) or reset password of: guest, assistant, administra-tor, service, redundancy
3	administra-tor			- Read-Write Local GUI access only, i.e., no central CMP interface support - user, sshlogin group membership - ssh read-only access / no sftp - Has rights to changing password (see Changing Default Passwords for Accounts) or reset password of: guest, assistant, administra-tor, service, redundancy

#	User Name	PW Policy config-ured	Unify Default PW (to be changed immedi-ately)	Description
4	service			- Read-Write Local GUI access only, i.e., no central CMP interface support - Read-Write CLI (ssh) access (via sudo)- user, admin, sshlogin, assistant group membership - Read-Write ssh / sftp - Has rights to change password (see Changing Default Passwords for Accounts) of: guest, assistant, administrator, service, redundancy
5	root			- Read-Write Local GUI access only, i.e., no central CMP interface support - Read-Write CLI (ssh) access - root group membership - No ssh / No sftp (privileges can be ob-tained via su command) - Has rights to change password (see Changing Default Passwords for Accounts) or reset password of: guest, assistant, administra-tor, service,, redundancy, root (via su command)
6	redun-dancy			- No Local GUI or central CMP interface access - user, sshlogin group membership - no ssh access / sftp only

8.4 Handling of Key Material

The OpenScape Session Border Controller provides a set of default TLS Certificate Authority (CA) certificates which can be used to establish TLS connections. It is highly recommended that the customer replace these default factory certificates with their own CA Certificates from the Public Key Infrastructure (PKI). Refer to the OpenScape Session Border Controller Administrator Documentation [2] regarding the procedures.

SIP servers using TLS connections to interface with the OpenScape Session Border Controller’s inside or core network may be supported using server or mutual authentication.

Remote subscriber TLS connections on the OpenScape Session Border Controller outside or access network are supported using server authentication where the OpenScape Session Border Controller operates as the TLS server.

Remote Endpoints addressing SIP servers, SIP proxy servers, SIP trunking gateways, or SIP service providers using TLS connections on the OpenScape Session Border Controller outside or access network may be supported using either server or mutual authentication.

The OpenScape Session Border Controller inside or core network interface with OpenScape Voice typically uses a TLS connection with mutual authentication TLS.

CA certificates used in the establishment of TLS connections used for other protocols may be replaced or added to the configuration as required.

8.4.1 TLS Server Authentication

Install the following when the OpenScape Session Border Controller is the TLS server:

Install the following when the OpenScape Session Border Controller is the TLS server:

- Server Certificate provided by the CA
- Server intermediate CA certificates (if any)
- Server public key (in the Server Certificate file)
- Private key
- Server Root CA Certificate (optional) is used to check the validity of its own Certificate and Certificate CA chain

Install the following when the OpenScape Session Border is the TLS client:

- Private key
- Server Root CA Certificate which is used to validate the CA chain of the received server certificate

8.4.2 TLS Mutual Authentication

For TLS mutual authentication, install the following information in the OpenScape Session Border Controller. Install both client and server certificates since either connection peer may establish the TLS connection requiring mutual authentication:

- Local Server Certificate provided by the CA
- Server intermediate CA Certificates (if any)
- Server public key (in the Local Server Certificate file)
- Private key

- Local Server Root CA Certificate is optional and is used to check the validity of its own Certificate and Certificate CA chain
- Local Client Certificate provided by the CA (if different from the Local Server Certificate)
- Client intermediate CA Certificate (if any)
- Client public key (in the Local Client Certificate file)
- Local Client Root CA Certificate is optional and is used to verify the validity of its own Certificate and Certificate CA chain
- Remote Client Root CA Certificate which is used to validate the CA chain of the received client certificate
- Remote Server Root CA Certificate which is used to validate the CA chain of the received server certificate

8.4.3 HTTPS Certificates

The OpenScape Session Border Controller also allows the customization of HTTPS certificates. A certificate profile can be created for HTTPS which will contain the following information:

- Local Server Certificate
- Server intermediate CA certificates (if any)
- Local key

The certificate profile for HTTPS shall be selected at **Security >General >Certificate Management**.

8.4.4 Certificate Profiles

Certificate profiles may be defined to allow associating one or more certificates with network interfaces having similar secure connection requirements.

Certificate key files and Diffe-Hellman parameter files may be uploaded and referenced during certificate profile creation.

Each named profile can be associated with a network interface supporting the following configuration:

Validation

The validation of certificates can be configured per certificate profile by means of the following parameters:

- Certificate validation - Enables the validation of the CA chain and CA signature, Validity Period and Critical Extensions
- Revocation status - Enables the verification of revoked certificates according to the CRL of the CA.

- Subject authentication - Enables the validation of certificate Subject CN or Subject Alternative Name according to the configured gateway/trunk FQDN or IP Address.

Renegotiation

- Identify the type of verification to be performed

TLS Version

- TLS v1.2 with optional TLS v1.0 fallback

Cipher Suites

Cipher suites can be configured per certificate profile by means of 3 parameters:

- Perfect Forward Secrecy with the options Preferred PFS (default) or Without PFS
- Encryption with the options Preferred AES-128 (default), Required AES-256
- Mode of operation with the options Preferred GCM (default), CBC only, GCM only.

The following table presents the sequence of cipher suites according to the configuration:

Preferred Forward Security	Encryption	Mode of Operation	Cipher suites
Preferred PFS	Preferred AES-128	Preferred GCM	ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDH-ECDSA-AES128-GCM-SHA256:ECDH-RSA-AES128-GCM-SHA256:ECDH-ECDSA-AES128-SHA256:ECDH-RSA-AES128-SHA256:ECDH-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-GCM-SHA384:ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES256-SHA384:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA:
Preferred PFS	Preferred AES-128	CBC Only	ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDH-ECDSA-AES128-SHA256:ECDH-RSA-AES128-SHA256: ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES256-SHA384:AES128-SHA:AES256-SHA: :DES-CBC3-SHA
Preferred PFS	Preferred AES-128	GCM Only	ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDH-ECDSA-AES128-GCM-SHA256:ECDH-RSA-AES128-GCM-SHA256:ECDH-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-GCM-SHA384:AES128-GCM-SHA256:AES256-GCM-SHA384

Preferred Forward Security	Encryption	Mode of Operation	Cipher suites
Preferred PFS	Required AES-256	Preferred GCM	ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDH-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-GCM-SHA384:ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES256-SHA384:AES256-GCM-SHA384:AES256-SHA
Preferred PFS	Required AES-256	CBC Only	ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES256-SHA384:AES256-SHA
Preferred PFS	Required AES-256	GCM Only	ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDH-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-GCM-SHA384:AES256-GCM-SHA384
Without PFS	Preferred AES-128	Preferred GCM	ECDH-ECDSA-AES128-GCM-SHA256:ECDH-RSA-AES128-GCM-SHA256:ECDH-ECDSA-AES128-SHA256:ECDH-RSA-AES128-SHA256:ECDH-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-GCM-SHA384:ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES256-SHA384:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA:AES256-SHA:DES-CBC3-SHA
Without PFS	Preferred AES-128	CBC Only	ECDH-ECDSA-AES128-SHA256:ECDH-RSA-AES128-SHA256:ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES256-SHA384:AES128-SHA:AES256-SHA:DES-CBC3-SHA
Without PFS	Required AES-128	GCM Only	ECDH-ECDSA-AES128-GCM-SHA256:ECDH-RSA-AES128-GCM-SHA256:ECDH-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-GCM-SHA384:AES128-GCM-SHA256:AES256-GCM-SHA384

Preferred Forward Security	Encryption	Mode of Operation	Cipher suites
Without PFS	Required AES-256	Preferred GCM	ECDH-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-GCM-SHA384:ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES256-SHA384:AES256-GCM-SHA384:AES256-SHA
Without PFS	Required AES-256	CBC Only	ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES256-SHA384:AES256-SHA
Without PFS	Required AES-256	GCM Only	ECDH-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-GCM-SHA384:AES256-GCM-SHA384

The certificates can be signed with SHA-1 (SHA-128) and SHA-2 (SHA-256, SHA-384 and SHA-512).

The Minimum TLS Version can be set to TLS V1.0, TLS V1.1 and TLS V1.2. If Minimum TLS Version is set to TLS V1.0, the TLS V1.2 is offered but fallback to TLS V1.0 is accepted. For security reasons SSLv2 and SSLv3 are not supported anymore.

The OpenScape Session Border Controller also allows the customization of HTTPS certificates. A certificate profile can be created for HTTPS which will contain the following information:

- Local Server Certificate
- Server intermediate CA certificates (if any)
- Local key

The certificate profile for HTTPS shall be selected at **Security > General > Certificate Management > System Certificate**.

It is possible to set the Minimum TLS Version.

The cipher suites can also be configured for the HTTPS certificate profiles by means of the parameters Perfect Forward Secrecy, Encryption and Mode of Operation.

The uploaded and created certificates and keys are automatically propagated to the pair node in case of redundant OSBs.

The validation of certificates can be configured per certificate profile by means of the following parameters:

- Certificate Verification – which defines the level of validation:
  a) **None** – no verification is performed on the certificate.
  b) **Trusted** – Certificate Authority Validation and Validity Period
  c) **Full** – Certificate Authority Validation, Validity Period, Revocation Status, Critical Extensions and Certificate Subject Authentication.
- Revocation Status – it is possible to enable/disable the verification of the revocation status. If the Certificate Verification is set to

Trusted or **Full** the Revocation Status flag is enabled by default. The Revocation Status checkbox is greyed out if the Certificate Verification is set to **None**.

- Identity Check – it is possible to enable/disable the verification of the Common Name and Subject Alternate Name in the certificate. If the Certificate Verification is set to **Full** the Identity Check flag is enabled by default. The Identity Check checkbox is greyed out if the Certificate Verification is set to **None** or **Trusted**.

INFO: It is possible to configure up to 10 certificate profiles, each containing a certificate

8.4.5 Certificate Downloading / Default Credentials

INFO: The downloaded certificate files and created keys are automatically propagated between redundant OpenScape Session Border Controller nodes.

#	Inter-face	Customer require-ment for Open-Scape Session Border Control-ler cre-dentials	Unify Default creden-tials	Usage
1	SIP Server (OSV)		Unify default certificate	TLS mutual authentication: requires at a minimum both local client and server Certifi-cates be installed as well as the Root CA Certificate for the OpenScape Voice server.
2	Remote Users		Unify default certificate	TLS server authentication is typ-ically supported requiring that at a minimum the customer CA Certificate must be installed.

#	Interface	Customer requirement for OpenScape Session Border Controller credentials	Unify Default credentials	Usage
3	SIP Service Provider Remote Endpoint(TLS server authentication)			If TLS server authentication is used, the OpenScape Session Border Controller operating as the TLS client requires the Root CA certificate and intermediate Root CA(s) for each SIP SP remote endpoint be installed.
4	SIP Service Provider & Gateway (TLS mutual authentication)		Unify default certificate	If TLS mutual authentication is used, the OpenScape Session Border Controller requires installation of both a customer local client and server CA certificate (unless both are the same) as well as the Root CA certificate and intermediate Root CA(s) for each SIP SP remote endpoint.
5	CMP & Local GUI Management		Unify default certificate	The customer CA Certificate must be installed in place of the Unify default.

DTLS Server Authentication

- DTLS V1.0
- DTLS V1.2 and DTLS V1.0 fallback

Cipher Suites

The following table presents the list of supported of cipher suites:

Pre-ferred For-ward Security	Encryption	Mode of Opera-tion	Cipher suites
Pre-ferred PFS	Preferred AES-128	Preferred GCM	ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA384: ECDH-ECDSA-AES128-GCM-SHA256: ECDH-RSA-AES128-GCM-SHA256: ECDH-ECDSA-AES128-SHA256: ECDH-RSA-AES128-SHA256: ECDH-ECDSA-AES256-GCM-SHA384: ECDH-RSA-AES256-GCM-SHA384: ECDH-ECDSA-AES256-SHA384: ECDH-RSA-AES256-SHA384: AES128-GCM-SHA256: AES256-GCM-SHA384: AES128-SHA: AES256-SHA: DES-CBC3-SHA

Verification of the supported Ciphers and DTLS version with Chrome Browser and FireFox browserIn call direction from SIP to Circuit and from Circuit to SIP.

8.5 Port Table

For latest updates of the OpenScape Session Border Controller port tables refer to the Interface Management Database (IFMDB) directly:

https://apps.g-dms.com/ifm/php/php_ifmdb/scripts/login.phpor via Customer Portal.

To get all necessary Security Checklist Port Table information you should select the appropriate data category according to the stake-holder and then navigate to the report generation section. Perform the following actions to create a customized report:

1. Choose “Firewall Scenario Report”
2. Select Generic Scenarios:
   a) Choose “select all” to include all generic solutions which are to be considered in the report followed by the right-most arrow to continue.
   b) Or, select the appropriate “OSV Solution Vx” which the OpenScape Session Border Controller is a member to get a more

"solution specific" report, followed by the right-most arrow to continue.

c) Or, select a predefined report selection followed by the right-most arrow to continue, proceeding to step 6). An example is *SCL_SBC_V10*. One can use one of the predefined reports as a template or starting point and modify Entities, SW-Versions, and Interfaces as desired for building the customized report.

3. Select Entities:

   a) Choose "Select all released" to consider all possible released entities for the report however this will include entities which have no communication possibilities with the OpenScape Branch.

   b) Or, select only those entities which are present in the network or have OpenScape SBC communication possibilities of interest and are to be considered in the report.
   For internal testing, "select all" is possible however unreleased Entities would also be shown for the next selection.

4. Select SW-Version:

   a) Choose "Select latest Release" for the most recent software versions to be considered.

   b) For internal testing, "select latest" is possible however unreleased SW versions would also be shown for the next selection. This can be narrowed to a more manageable number by choosing the other options, "select latest", "select all Released", "select latest Released".

5. Select Interfaces:
   Here product specific information must be selected by the user.

   a) With "select all" many undefined or unused interfaces will be included in the report.

   b) A better choice would be to select individual interfaces of interest. The user may elect to store this report in the IFMDB which can be retrieved at a later time under "select generic scenarios in the Field below the menu.

   • To store a report, enter a Filename into the textfield below the Select Interfaces menu .e.g. "OSV SBC v10 SCL".

   • Steps 1 through 5 are stored as a reference or starting point for generating future reports.

6. Select left & right side of Firewall:

   a) Put OpenScape SBC v10 on one Side of the firewall.

   b) All other SW Versions including the OpenScape SBC v10 (as a peer) shall be put on the other side.

7. Select information to be shown in the report:
   Suggest keeping it as is for port table view.

8. Available report styles:
   The recommended report style for Security checklists is AF005P.
   The description is Firewall Scenario port table.

	Destination / Source Port#	Network / Application Protocol	Default State	configurable	From	To	Description / Function
1	D:443	HTTPS/TCP-SSL/TLS	Open	No	Central CMP or Local GUI Web Browser	OS-SBC Web Server	https based CMP management or Web session
2	S:514, D:500-600	Syslog/UDP	Open	No	OS-SBC	Syslog Server	Syslog Server in OSV-TM
3	P:4500	NAT-T/UDP	Open	No	OS-SBC IPSec VPN	Remote Endpoint	VPN tunnel endpoint based on IPSec (IPv4) – NAT traversal
4	P:5060	SIP/UDP	Open	Yes	OS-SBC/ Access Realm Network Interface	Access Realm Network Interface/OS-SBC	SIP Signaling / UDP for Access Realm (outside network)
5	P:5060	SIP/UDP	Open	Yes	OS-SBC/ Core Realm Network Interface	Core Realm Network Inter-face/OS-SBC	SIP Signaling / UDP for Core Realm (inside network, e.g., OpenScape Voice, HiPath 4K)
6	P:5060	SIP/TCP	Open	Yes	OS-SBC/ Access Realm Network Interface	Access Realm Network Inter-face/ OS-SBC	SIP Signaling / TCP for Access Realm (outside network)
7	P:5060	SIP/TCP	Open	Yes	OS-SBC/ Core Realm Network Interface	Core Realm Network Inter-face / OS-SBC	SIP Signaling / TCP for Core Realm (inside network, e.g., OpenScape Voice, HiPath 4K)
8	P:5061	SIP/TCP-TLS	Open	Yes	OS-SBC/ Access Realm Net-work Interface	Access Realm Network Inter-face/OS-SBC	SIP Signaling / TCP secured by TLS for Access Realm (outside network)

	Destination / Source Port#	Network / Application Protocol	Default State	configurable	From	To	Description / Function
9	P:5061	SIP/TCP-TLS	Open	Yes	OS-SBC/ Core Realm Network Interface	Core Realm Network Interface/OS-SBC	SIP Signaling / TCP secured by TLS for Core Realm (inside network, e.g., OpenScape Voice, HiPath 4K)
10	S: 10000-49999, D: 10000 - 49999 10000 - 49999 29100 - 29131 29100 - 30099 32768 - 43647 35000 - 65000 5010 - 5059 55000 - 65000	(S) RTP – (S) RTCP / UDP	Closed	Yes	OS-SBC Access or Core Realm	Access or Core Realm (S)RTP – (S)RTCP Media End-point, OS-SBC peer	OS-SBC Source port determined dynamically during SIP signaling
11	D: 10000-49999, S: 10000 - 49999 10000 - 49999 29100 - 29131 29100 - 30099 32768 - 43647 35000 - 65000 5010 - 50595 5000 - 65000	(S) RTP – (S) RTCP / UDP	Closed	Yes	Access or Core Realm (S)RTP – (S)RTCP Media End-point, OS-SBC peer	OS-SBC Access or Core Realm	OS-SBC Destination port determined dynamically during SIP signaling
12	D:123	SNTP / UDP	Open	No	Access Realm SNTP Client	OS-SBC SNTP	SNTP time query

	Destination/ Source Port#	Network/ Application Protocol	Default State	configurable	From	To	Description/Function
13	D: 22	(S) FTP or SSH/ TCP	Open	No	OS-SBC/ Core Realm OSVTM, CLI, Mass Provi-sioning, Traffic Tool	OS-SBC	Secure File Transfer client access / CLI SSH
14	S: 162 D:162	(S) RTP – (S) RTCP / UDP	Open	Yes	OS-SBC Core Realm SNMP Agent	CMP, Network Management,Alarming	Network Alarming
15	P:1075,1075	OSB Redundancy / UDP	Open	No	OS-SBC Core Realm	OS-SBC Core Realm	Internal OS-SBC redundancy
16	D:22	SSH / TCP	Open	No	OS-SBC/ Core Realm CLI, Mass Provi-sioning	OS-SBC	CLI SSH and service access
17	D:2427	MGCP / UDP	Closed	Yes	OSV	OS-SBC Core Realm	MGCP server on OS_SBC Core realm
18	S:1024, 65535	DNS / TCP or UDP	Closed	No	OS-SBC	DNS	DNS Client
19	S:1024, 65535	RADIUS/TCP	Closed	No	OS-SBC	RADIUS Server	RADIUS authentication / accounting

	Destination / Source Port#	Network / Application Protocol	Default State	configurable	From	To	Description / Function
20	D:443	SOAP/HTTP/TCP-TLS	Open	Yes	CMP, Web Client	OS-SBC	SOAP via HTTPS with WSDL tunneled. Also for Local GUI WBM
21	S:10000 - 14999	SOAP/HTTP/TCP-TLS	Open	Yes	OS-SBC	CMP,Web Client	SOAP via HTTPS to access Assistant for Simplified Installation and License Management - Secure Web client for Assistant access - the server uses listening port 4709
22	S:10000 - 14999	BFCP / UDP, TCP or TCP-TLS	Closed	Yes	Core or Access Realm Remote BFCP Endpoint / OS-SBC	OS-SBC Core or Access Realm / Remote BFCP Endpoint	BFCP ports determined dynamically during SIP signaling

9 References

[1] **OpenScape Session Border Controller V10 Installation Guide**

(e-Doku or Partner Portal / product information)

[2] **OpenScape Session Border Controller V10 Administration Documentation**

(e-Doku or Partner Portal / product information)

[3] **OpenScape Voice V10 Security Checklist, Planning Guide**

(e-Doku or Partner Portal / product information)

[4] **Interface Management Database (IFMDB)**

(available via SEBA Partner Portal)

http://www.unify.com/us/partners/partner-portal.aspx

[5] **Support of Operating System Updates for Server Applications**

http://wiki.unify.com/images/archive/c/c0/20110429131918!Security_Policy_-_Support_of_Operating_System_Updates_for_Server_Applications.pdf

[6] **Security Policy-Vulnerability Intelligence Process**

http://wiki.unify.com/images/archive/c/ce/20131110234526!Security_Policy_-_Vulnerability_Intelligence_Process.pdf