A MITEL
PRODUCT
GUIDE

Unify OpenScape Session Border Controller

OpenScape SBC V11

Security Checklist

July 2024

A31003-S53B0-P101-02-76A9

Mitel

Notices

Trademarks

Contents

1 Introduction

1.1 History of Changes

Date	Version	What
2023-10-03	1.0	Initial version V11
2024-07-04	2.0	Updates and enhancements

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 each 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

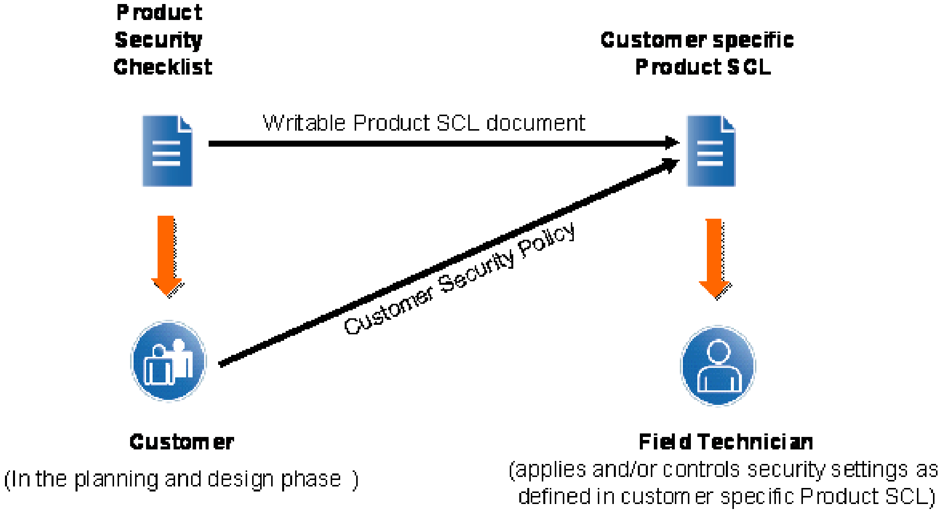
basis for the agreement between Unify and the customer: who will be responsible for the individual security measures:

- During installation/setup of the solution
- During the solution's operation

2. During installation and during major enhancements or software upgrade activities:

   - The Customer specific Product Security Checklists are used by the field technician to apply and/or control the security settings of each individual product.

Figure: Usage of Security Checklists (SCL)


Product Security Checklist
Customer specific Product SCL
Writable Product SCL document
Customer Security Policy
Customer
(In the planning and design phase)
Field Technician
(applies and/or controls security settings as defined in customer specific Product SCL)

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 always using the latest version of the Security Checklists of the products that are part of your solution.
  They can be retrieved from the Unify Partner Portal by locating the OpenScape Session Border Controller V11 product.
- We encourage you to provide feedback in any cases of unclarity, or problems with the application of this checklist.

Please contact the Mitel Product Security Office (obso@atos.net).

1.3 Security Strategy for Unify Products

Reliability and security are key requirements for all products, services and solutions delivered by Unify. These requirements are supported by a comprehensive security software development lifecycle that applies to all new products or product versions being developed from their design phase until the end of life of the product.

Unify products 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 and includes:

Product Planning & Design

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

Product Development & Test

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

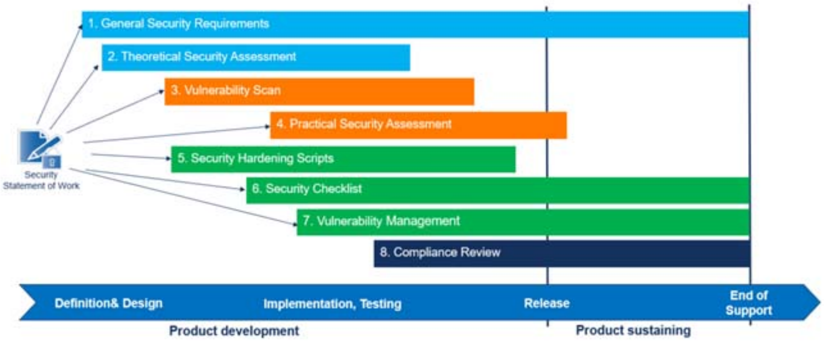
Installation & start of operation

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

Operation & Maintenance

Proactive Vulnerability Management is publised at Mitel Security Advisories to identify, analyze and resolve security vulnerabilities that emerge after products have been released, and to deliver guidance, e.g. Security Advisories published for customers to make informed decisions on how to mitigate or close these vulnerabilities.

Figure: Unify Baseline Security Policy - from Design to EOL


1. General Security Requirements
2. Theoretical Security Assessment
3. Vulnerability Scan
4. Practical Security Assessment
5. Security Hardening Scripts
6. Security Checklist
7. Vulnerability Management
8. Compliance Review
Security Statement of Work
Definition& Design
Implementation, Testing
Release
End of Support
Product development
Product sustaining

For more information about the Unify product security strategy we refer to the relevant Security Policies.

Unify has adopted the security principles security by design and security by default. However, security default cannot by achieved in all cases or a risk-based approach is more suitable for certain measures. The Product Security Checklist provides the necessary foundation to customize the security settings based on the specific customer security requirements.

The Security Checklist is a living document that integrates feedback and new security aspects during the whole product sustaining phase (see Figure 2). To maintain the Unify product at the security level accomplished at installation time it will be necessary to apply new security enhancements to the product during its life time. Additional security measures for the operation and maintenance phase of the product as described above in this chapter should also be applied.

1.4 Security Policies for OpenScape SBC and OpenScape Branch

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 upon, but not identical to, a community developed distribution. Even when the community declares a version deprecated this does not necessarily mean that the SBC/SBC OS is deprecated as the packages and kernel are individually updated by the regular SBC/SBC releases or hotfixes. Customers should stay up to date regarding 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 Unify's Security Policy - Vulnerability Intelligence Process.
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 Customer Deployment - Overview

This Security Checklist covers the product OpenScape Session Border Controller V11 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 OpenScape Session Border Controller V11 R1 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 SBC can be managed via a local web interface (Local GUI) and via the Unify Common Management Platform (CMP) by means of the SBC Assistant. It also supports administrative access via SSHv2 and SFTP.

In terms of maintenance, the OpenScape SBC supports alarming via SNMP v3 or SNMPv2 [PG1] [FS2] and logging via syslog. It can also be integrated to OpenScape Trace Management.

The following network services are supported by the OpenScape SBC:

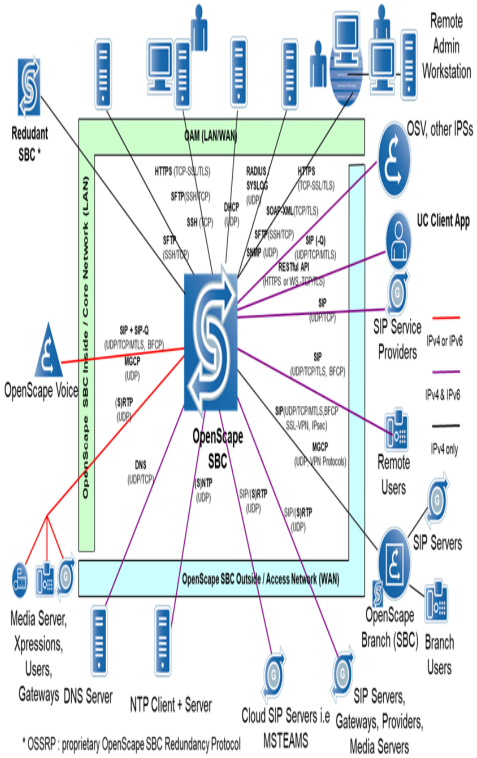
- DNS server and DNS client
- DHCP server
- NTP client and NTP server
- Traffic shaping
- User Authentication by RADIUS
- User Authentication via PKI
- SIP Digest Authentication
- Firewall
- Message Rate Control
- Denial of Service Mitigation

As an OpenScape SBC, it supports the following security services:

- VPN with IPSec or with OpenVPN

Figure 3 presents the network interfaces of the OpenScape SBC:

Figure: OpenScape SBC Interfaces and Protocols



The following figures show some of the possible deployment options of the OpenScape SBC.

Figure: OpenScape SBC Deployment

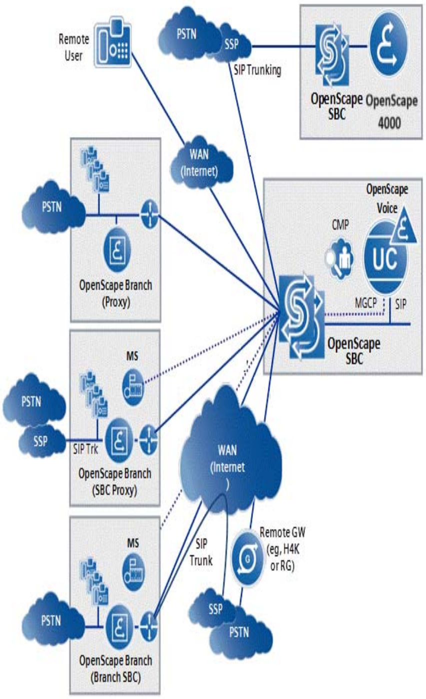


Figure: OpenScape SBC Single Arm Deployment for MS TEAMS Overview

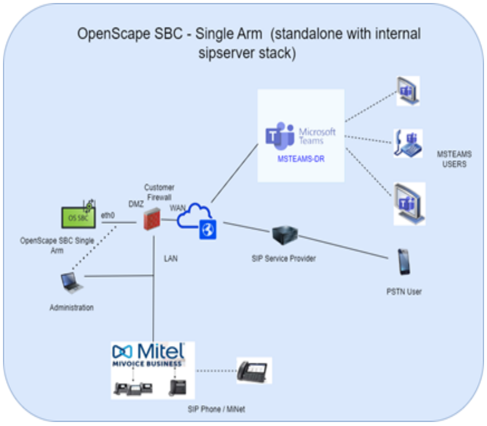
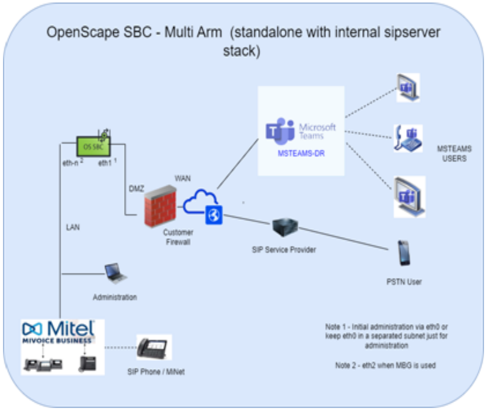


Figure: OpenScape SBC Multi Arm Deployment for MS TEAMS Overview


OpenScape SBC - Multi Arm (standalone with internal sipserver stack)
OS SBC
eth-n 2
eth1 1
DMZ
WAN
LAN
Customer Firewall
Microsoft Teams
MSTEAMS-DR
MSTEAMS USERS
SIP Service Provider
PSTN User
Administration
Mitel MIVOICE BUSINESS
SIP Phone / MiNet
Note 1 - Initial administration via eth0 or keep eth0 in a separated subnet just for administration
Note 2 - eth2 when MBG is used

Recommended measures for OpenScape SBC secure deployments are provided in the following chapters.

The customer should always ensure that only up-to-date software is installed. The newest versions of Unify software are available on the Unify Software Server. It is also recommended to ensure to that any 3rd party software versions and patches (if applicable) are kept up to date. The customer should also consider any hardware manufacturer advisories as well as Unify security advisories [2].

Generally the latest software version released should be installed for all components of the solution.

To tighten security on OpenScape SBC V11 R1, the following measures are recommended:

- Place the OpenScape SBC in the customer's DMZ behind the firewall
- Use SNMPv3 - configure the passphrases for the encryption and integrity check
  - If using SNMPv2 - Changing the SNMP Community Name from the defaults since these are essentially passwords used for data exchange of SNMP trap information.
- Always change predefined user account passwords from their defaults as these are well known.
- Change the system default password policies.
- If the internal firewall is used, ensure it is properly configured.
- Ensure IP message rate limits are set appropriately for normal operation for the customer.
- Close all unused IP Ports – Configure the ports required for operation of the system only. If an external firewall is used, ensure that it is properly configured to only pass the required traffic towards the system.
- Secure communications to SIP Servers using IPsec tunnels or VPN (OpenVPN) TLS connections in the absence of other mechanisms to secure SIP signaling.

- 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 according to the network peer capability and profile wherever possible. Using unsecured media may lead to eavesdropping.
- Authenticate SIP subscriber by means of Digest Authentication.
- Deviations of the recommended security settings based on customer request should be documented.
- Use customer PKI issued certificates. Make a note of their expiration.
- 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.
- Protect Local GUI interface for Web Server access and restrict HTTPS access from specific IPs.

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

3 Server Hardening

Each server the OpenScape SBC runs on must be hardened. For an OpenScape SBC cluster each server must be hardened individually. General requirements for all systems, which run communication clients and applications:

- The operating system version is supported for the communication software (see sales information). Unnecessary software is removed.
- Current security updates are installed (see chapter OpenScape SBC V11 R1 Hardening Procedures in General).
- The access to the system is protected by passwords according to the password rules in 10.2 .
- Hardware Security Settings

There are no known necessary security hardware settings. Customer should verify with their server vendor for any recommendations from them.

3.1 Bios settings

Preventing the possibility of booting from a USB device.

3.1.1 BIOS password protection

Accessing the server BIOS allows for the changing of the boot order of the server. Once changed an intruder may use tools that are bootable from CD-ROM or USB device that allow a user to change the administrator password, install files or retrieve sensitive information. To prevent this access to the server's BIOS needs to be protected with a strong password.

CL-SBC-BIOS-PW	**BIOS password protection**
Measures	A strong BIOS password needs to be set to avoid changing of settings (i.e., boot order) in the BIOS setup.
References	N/A
Needed Access Rights	Administrator

CL-SBC-BIOS-PW	BIOS password protection
Executed	Yes: No:
Customer Comments and Reasons	

INFO: BIOS passwords should be set in accordance with company security policies. This security policy can be found in the Addendum.

3.1.2 Boot order

When the boot order sequence in the BIOS setup is set incorrectly an intruder may use tools that are bootable from CD-ROM or USB device which allows them to change the administrator password, install files or retrieve sensitive information. To prevent this, the boot order must be set correctly.

CL-SBC-BIOS-BOOT	BIOS boot order
Measures	Set boot order in BIOS to **NOT** boot from removable media.
References	N/A
Needed Access Rights	Administrator
Executed	Yes: No:
Customer Comments and Reasons	

INFO: BIOS will need to be configured to boot from external device for initial OS installation, but once installed then the boot sequence should be configured to not allow boot from external sources.

3.2 OS Hardening

For products that are delivered as hardware or software appliances the operating system is delivered and installed as an integral part of the application load. Operating systems hardening is integral part of the product development. Hardening is performed according to baseline security requirements and industry best practices.

For applications that do not include the operating system as part of their product delivery in general customers provide the operating system and are responsible for operating system hardening.

Where Unify applications deliver hardening measures (e.g., scripts), they should be included in the security checklist, and it is recommended that customers are applying them during installation. OpenScape SBC is deployed with a customized version of openSUSE Leap 15.5.

OpenScape SBC is deployed with a customized version of openSUSE Leap 15.5.

An OS specific password policy should be implemented - please see Addendum. Sources for customer specific certificates, see in Addendum.

3.3 Clean Customer Deployment

The installation files are already cleaned, so only necessary applications are installed. Installation of aditional applications are not recommeded.

3.4 Single Arm Configuration

When deployed in a single arm configuration the OpenScape SBC should be deployed in a DMZ with a three leg firewall configuration, with the customer network isolated from the WAN and DMZ.

- 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 from the customer LAN.

3.5 Changing the SNMP Community Name

Recommendation is to migrate SNMP services to SNMPV3.

If SNMPv2 is still used, then the below measures must be implemented.

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-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 SBC sets the RO community name to "public". It is very important to change this default at installation as it is well known. ee additional setting information below.
References	SNMP v2
Needed Access Rights	root
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

NOTICE: In a redundant system, the Community Name is automatically synchronized to the Backup node. It is possible to backup & restore the configured Community Name.

The SNMP community string shall contain 20-32 alphanumeric characters or special characters ~ ! @ # $ % ^ & * ( ) +.

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 V11 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

It is possible to change the Community Name for the SNMP Discovery process 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. The profile can be applied to a set of selected OpenScape SBC boxes via Job Management.

An Alarm Manager log in WARN level is generated when the SNMP community string is changed.

Changing via the Local GUI and OpenScape Session Border Controller Assistant

From OpenScape SBC V9R3 it is possible to change the Community.

Name from the Local GUI and from the SBC Assistant.

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

3.6 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-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 passphrase shall be configured for encryption and another one for integrity check.
References	N/A
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 – It is highly recommended to choose SHA - 256. Notice that MD5 is not considered a secure hash mechanism anymore.
- Auth Password – a passphrase of at least 15 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 15 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.

SNMP Gets are disabled by default, when enabled it allows read access of several internal MIBs. To prevent unauthorized access to SNMP Gets the administrator needs to configure the username, security level, authentication protocol, authentication password and private password.

The following settings are used in SNMPV3 get:

- Read-only user - A username with at least 8 and a maximum 32 characters shall be configured.
- Authentication pass - passphrase of at least 15 and a maximum of 32 characters shall be. Per configuration the minimum is 8, however 15 is recommended.
- Encryption pass - passphrase of at least 15 and a maximum of 32 characters shall be configured. Per configuration the minimum is 8, however 15 is recommended.

Regarding MIBs, currently the ability to walkthrough several MIBs is allowed.

To disable the MIBs that should not be accessed a change in the /etc/init.d/snmpdx has 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>"
```

3.7 Changing Default Passwords

After the installation for each account, a default password is available. Since the default passwords are publicly available, it is required that all pre-defined passwords be changed for “root”, “administrator”, “service”, “guest”, “assistant”, “ACD”, “CDR” and” redundancy” (see Addendum, section Default Accounts) after the installation completes.

CL-SBC-Passwords	**Use non-default OpenScape SBC passwords**
Measures	During the installation, all accounts are created with predefined 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 theirpre-defined values.
References	
Needed Access Rights	administrator IMPORTANT: Access Rights to change "root" password is "root".
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 the Addendum.

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

```
passwd user
```

Where “user” is: "root", “administrator”, “service”, “guest”, “assistant”, "ACD", "cdr", “redundancy”.

Passwords should be 15-40 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 SBC boxes by means of CMP Profiles which are applied with Job Management.

NOTICE: The user passwords can be backed up and restored to a file. Passwords are stored in an encrypted format see pam.d in chapter Privileged Access Management (PAM) Framework. Notice that some of the policy rules do not apply while restoring the user passwords, like password iteration number and password iteration length.

3.8 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-SBC-Password Policies	**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

CL-SBC-Password Policies	**Change customer’s password policy within the OpenScape Session Border Controller**
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

The procedures to manage the password policy are described in Section 6 Administration/Management Security.

In a redundant SBC, the password policy is automatically synchronized to the backup SBC.

For new users created via CMP or local GUI is recommend setting the change of password in first usage and set an expiration date according to the customer password polices.

3.9 Disable Unused Accounts

Since OpenScape SBC V9R4 and up it is possible to disable via the Common Management Portal the user accounts that are not used, this is not valid for root, and redundancy users. If there is only one administrator or service user, they also can’t be disabled. It is recommended that unused accounts are disabled.

CL-SBC-Disable Not Used Accounts	**Disable accounts for not used users**
Measures	All not user accounts must be disabled.
References	OpenScape SBC V11 Administrator Documentation
Needed Access Rights	administrator
Executed Server 1:	Yes: No:
Customer Comments and Reasons	

3.10 Authentication via RADIUS

It is possible to authenticate the users via a RADIUS server. Up to two RADIUS servers can be configured on the OpenScape SBC to perform the user authentication. Every time a user tries to login to OpenScape SBC via Web, via SSH, via SFTP or via Console a request will be sent to the RADIUS server asking for the authentication of the user. The RADIUS server will accept or reject the user authentication by comparing the provided credentials with the configured credentials.

CL-SBC-RADIUS	**User Authentication via RADIUS**
Measures	The user authentication is performed by a RADIUS server. The IP address of up to two RADIUS can be configured in the SBC. A secret must also be configured for each RADIUSserver.
References	OpenScape SBC V11 Administrator Documentation
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information about the Functionality:

If the RADIUS server is reachable the authentication will be performed on the RADIUS server. If the RADIUS server is not reachable the users will be locally authenticated in the SBC. So, even if the predefined users are managed via RADIUS it is required to change their passwords from predefined value.

The users which are not locally configured on the SBC will have the same privileges as the pre-defined service user.

The communication between SBC and the RADIUS server is performed by means of the protocol EAP and the encryption algorithm is MD5.

Additional Information for Settings:

The authentication of users via the RADIUS server may be enabled in the OpenScape SBC. To activate the authentication via the RADIUS server, at least one RADIUS server must be configured in the OpenScape SBC. Server redundancy is possible by configuring 2 RADIUS servers.

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

In case of redundant OpenScape SBC the actual IP address of each SBC node shall be configured in the RADIUS server (not the virtual IP address).

Regarding timeout configuration, it is not recommended to configure a value of less than 2 seconds as a brief network problem could cause the RADIUS authentication to timeout. If the RADIUS authentication times out, the user is locally authenticated.

The authentication via the RADIUS server is separately enabled for CLI (Console access), SSH (and SFTP) and Web access.

INFO:

The authentication of users via the “ su” command is performed internally (via Console and SSH only). The OpenScape SBC pre -defined users must also be configured in RADIUS to be able to log into the OpenScape SBC when the RADIUS server is reachable. Users which are not pre-defined in OpenScape SBC may also login to OpenScape SBC 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 informed of the duration of the sessions and vendor identification. The Accounting service may also be separately enabled for CLI (Console access), SSH (and SFTP) and Web.

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.

To increase security, the secret length was fixed to 16 characters. It can consist of upper or lower case letters, digits, or special characters. Special characters can be any of the following set: ~!@#$%^&*()_+|\=-'{}[]:"';<>?/.,

INFO: For access via SSH, it is not possible to login with users that 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.

3.11 User Authentication via 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
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.

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

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	OpenScape SBC V11 A dminist rator Documentation
Needed Access Rights	Administrator

CL-OS_SBC-PUSH-NOT	Configure Push Notification
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 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	OpenScape SBC V11 Administrator Documentation
Needed Access Rights	Administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

3.14 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		

3.15 Hardening for Unify Phone conections

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.

3.15.1 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 SBC V11 Administrator Documentation
Needed Access Rights	Administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

4 Virtualization

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

4.1 Virtualization Hardening

We recommend hardening the virtualization infrastructure according to security guidelines provided by the virtualization vendor. As an alternative, best practice standards like the Benchmarks issued by the Center of Internet Security (CIS) may be considered.

The OpenScape SBC can be virtualized using supported versions. (Check the Virtualization Guide to see the supported versions and configurations).

5 Securing the OpenScape Session Border Controller Interfaces

5.1 Configuring the Internal Firewall (WAN)

The OpenScape Session Border Controller must be protected against attacks by by placing the SBC behind a customer firewall.

CL-SBC-Firewall-WAN	**Firewall Protection for the OpenScape Session Border Controller outside or access network (WAN).**
Measures	For the OpenScape SBC outside network (WAN) when 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 protection to allow/disallow communication between theOpenScape SBC and external networks.
References	OpenScape SBC V11 Administrator Documentation
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”.

The OpenScape Session Border Controller Firewall settings and criteria for the “Allow” setting shall be applied as detailed below for all networks:

The following VoIP protocols can be restricted/allowed from being accessed via W AN interface

- 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
- FC00::/7 – Private Use

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.

5.2 Configuring the Internal Firewall (LAN)

The OpenScape SBC must be protected against attacks by using an external firewall.

CL-SBC-Firewall-LAN	**Firewall Protection for the OpenScape Session Border Controller local network (LAN).**
Measures	For the OpenScape SBC local network (LAN) the external firewall used must provide protection to allow/disallow communication between the OpenScape SBC and the local networks.
References	OpenScape SBC V11 Administrator Documentation
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:

The following VOIP protocols can be restricted / allowed from being accessed via LAN interface:

- DNS
- SNMP
- HTTPS
- SSH (and SFTP)
- NTP
- SIP
- MGCP
- RTP
- ICMP
- TLS

The following protocols cannot be restricted on the LAN interface since they are essential to OpenScape Branch functionality: ICMP.

The following protocols cannot be enabled in the LAN interface:

- FTP
- Telnet

Additionally, the internal firewall White/Blacklist should be configured according to customer requirements to allow / block communications from specific network IP addresses on the OpenScape SBC local network or LAN. The entries in the White / Blacklist can be made at the subnet level using the CIDR notation.

INFO: The rules which are defined in the internal firewall are valid for TCP and UDP.

If the internal firewall is configured to block incoming traffic for a certain service, it will block new incoming connections. However, if the connection is started by the OpenScape SBC the incoming flow will be allowed for that service and for the peer party to which the connection had been established. This exception is valid for both transport types UDP and TCP.

5.3 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-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 SBC V11 Installation & Upgrade Guide
Needed Access Rights	administrator
Executed	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 packets 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 “whitelist” to values for the specific customer configuration.

5.4 Secure Communication with Servers Using IPSec Tunnels

Configure the OpenScape SBC to use IPsec tunnelling to the Data Center through a VPN Concentrator. When OpenScape SBC and OpenScape Voice are separated via a WAN connection the usage of IPsec Tunnels will ensure that SIP, Voice (RTP) and MGCP messages are transported into a secure connection between both ends.

CL-SBC-IP sec	**Secure OpenScape SBC communications on the outside or access network (WAN) to the Data Center using IPsec tunnels**
Measures	Verify that IPsec can be used to encrypt SIP andnon-SIP communication between OpenScape SBC and servers on the WAN. The usage of IPsec Tunnels assure that OpenScape SBC will have a Private IP address that is only known by the OpenScape Voice for SIP, Voice (RTP) and MGCP communication so these messages will be encrypted for other parties that try to read the information unduly.
References	OpenScape SBC V11 Administrator Documentation
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

After installation and configuration of VPN server supporting the IPsec tunnel in the Data Center, verify that the OpenScape SBC IPsec tunnel can be established and used for communication.

The OpenScape SBC will need a Public and a Private IP address for the IPsec configuration:

Under no circumstances, any other party besides the OpenScape Voice will know this Private IP as this one will be used to encrypt the messages transmitted in the WAN over the IPsec tunnel.

A VPN concentrator will establish the connection between the OpenScape SBC and OpenScape Voice for this we will have to configure the following:

OpenScape SBC:

- A Private (Main IP) and a Public IP (Admin IP) address under Network connection
- IPsec tunnel under Security -> VPN -> IPsec where the:
  - Partner: is the VPN concentrator IP
  - Partner Network: OpenScape Voice network information
  - Local: Public (Admin) IP address
  - Local network: Private (Main) IP address
  - Encryption information that matches the configuration made in the VPN concentrator
  - OpenScape Voice: under the endpoint configuration, the Signaling IP address of OpenScape SBC will be the Private (Main) IP address
  - VPN concentrator: an IPsec tunnel must be created matching the configuration done in the OpenScape SBC, such as authentication methods, secrets (passwords) and network addresses.

INFO: Note that this feature will only work on non-redundant OpenScape SBC Systems.

In addition, if more than one VPN concentrator is used (in case of geo- separated OpenScape Voice system for example) several IPsec tunnels can be created and established simultaneously.

5.5 Secure SIP Server VoIP Communications

By default, the OpenScape SBC interface with the SIP server (OpenScape Voice) or with the centralized Session Border Controller (OpenScape SBC) uses TCP transport for SIP signaling. Information is sent in clear text which can be easily sniffed in the customer’s network. The SIP signaling connection should be secured using TLS 1.2 or higher.

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 SBC platform and OpenScape SIP server come with a set of default 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). The certificate profile which is configured in System TLS Certificate shall be set with the parameter Minimum TLS version as TLSv1.2. This configuration is performed under: **Security** > **General** > **Certificate management** > **Certificate profile** > **TLS version**, by selecting the **TLS V1.2** option. 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 Certificate Handling, references and additional information below for installing CA certificates.
References	Refer to the following documents: • *OpenScape SBC V11 Installation Guide for installing CA Certificates* • *OpenScape Voice Design & Planning Manual: Volume 3, Security Reference*
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.

5.5.1 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 SBC SIP listening ports be changed to other values which do not conflict with other provisioned ports.

CL-SBC-SIP_Ports	**Configure OpenScape Session Border Controller Outside or Access Network (WAN) ports required for VoIP communication**
Measures	Since SIP listening ports are well known in the network many security vulnerabilities can be instigated by external attacks to these ports. It is recommended that the OpenScape SBC SIP listening ports be changed to other non-conflicting ports to lessen the threat vulnerability.
References	OpenScape SBC V11 Installation Guide
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 SBC outside access or WAN network, OpenScape SBC 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 SBC 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).

Refer to Port Table for more information.

5.5.2 Secure SIP Signaling with Remote Users

OpenScape Voice Remote Subscribers registering through the Session Border Controller are recommended to use SIP signaling secured using TLS between the OpenScape SBC and Remote Subscribers.

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-SBC-TLS-USERS	**Secure SIP signaling for remote users**
Measures	The OpenScape SBC 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). The certificate profile which is configured in System TLS Certificate shall be set with the parameter Minimum TLS version as TLSv1.2. This configuration is performed under: **Security** > **General** > **Certificate management** > **Certificate profile** > **TLS version**, by selecting the **TLS V1.2** option. 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	Refer to the following documents: • *OpenScape SBC V11 Installation Guide for installing CA Certificates* • *The administration documentation for the SIP Gateway / Trunk should be referenced to install CA certificates and configure SIP endpoints to use TLS*
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

INFO: The use of TLS avoids opening 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).

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.

5.5.3 Secure SIP Signaling with Gateways / Trunks

OpenScape Voice Remote Endpoints may be configured to be reachable through the OpenScape SBC to represent and identify remote network servers, e.g., SIP Service Providers or SIP media gateways. UDP, TCP may be used for the signaling transport however information is sent in clear text which can be easily sniffed in a network. For TCP transport, TLS may be used to secure the connection.

It is highly recommended that SIP signaling be secured between the OpenScape SBC and OpenScape SBC Gateways / Trunks representing

Media Gateways in the WAN or SIP Service Providers. These connections can be secured using TLS over TCP.

Each of the application / client mentioned above must be setup individually for secured transmission.

CL-SBC-TLS-Gateway & Trunks	**Secure External Gateways / Trunks Signaling using TLS**
Measures	The OpenScape SBC 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).
References	Refer to the following documents: • *OpenScape SBC V11 Installation Guide for installing CA Certificates* • *The administration documentation for the SIP Gateway / Trunk should be referenced to install CA certificates and configure SIP endpoints to use TLS*
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
  - Minimum TLS version to be supported (set to TLSv1.2)
  - Cipher suites selection by means of the parameters: Perfect Forward Secrecy, Encryption and Mode of operation

-
- Configure the Gateway / Trunk SIP signaling for the type of TLS and associate with the appropriate CA Certificate profile.

If an unsecured SIP signaling connection is used, the OpenScape SBC 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 SBC is supporting the signaling with the remote Gateway / Trunk, failure to follow these procedures may provide a false sense of security.

> ***INFO:*** TLS is established on a hop-by-hop basis. To apply end-to-end signaling security, equivalent measures must be applied to the OpenScape SBC inside or core network (LAN) interface with OpenScape Voice as covered in another section.

> ***INFO:*** The only certificate critical extension which is handled by OpenScape SBC is Basic Constraints. Certificates containing other critical extensions will not be validated by the OpenScape SBC.

5.5.4 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-SBC-Media_Security	**Configure OpenScape SBC Media Security for outside or access network (WAN) and inside network (LAN)**
Measures	Identify media security as the preferred profile for media endpoints whenever possible. See additional information below for more information.
References	OpenScape SBC V11 Installation Guide
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-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 SBC configuration.
References	Refer to the following documents: • *OpenScape SBC V11 Installation Guide*
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

5.5.5 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 using unknown to OpenScape-Voice user identities.

Voice user identities.Each type of violation uses its own quarantine time interval.

CL-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 V11 Administrator Documentation
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.

If the OpenScape SBC is operating in Normal mode, the decision of adding the IP address of the offending computer is based on the responses provided by the OpenScape Voice.

If the OpenScape SBC is operating in Survivable mode, the decision is based on the configuration of Digest Authentication in the OpenScape SBC. If Digest Authentication is enabled in the OpenScape SBC, a 403 Prohibited is sent back when the Max Retries in reaction to a challenge (401 Unauthorized) is reached and the IP address of the offending computer is added to the quarantine list. If the Subscriber DN does not exist in the OpenScape SBC, 404 Unknown is responded back, and the Source IP is quarantined. If Digest Authentication is disabled in the OpenScape SBC, no control of registration is performed.

Once a violator for the respective detection mechanism is determined, the IP message source IP address is quarantined for the specified time interval. The quarantine time interval may be adjusted. Note that a too small value may prevent a potential attacker from moving on and insufficient DoS protection while a too large value may prevent legitimate SIP users which have been incorrectly configured from being reinstated into service in a timely manner.

5.5.6 Limiting SIP Message Rates in any SIP interface by time interval

The SBC/BCF has two mechanisms to prevent TDoS attacks, the first mechanism considers the number of SIP requests received from any IP in any interface during certain interval (i.e 10s). If the number of SIP request is above of the defined limit the SBC will start responding with response code 503. If the number of requests or any other network packet is above the configured limit (message rate) then the DoS mechanism will be triggered, and the source IP is blocked and put in quarantine for a configurable timer.

CL-SBC-MSG-Rate Limit by time	**SIP Message Rate Limiting by Time**
Measures	The main problem in this TDoS mechanism is if the attack is done in a sustainable rate to trigger the time limit mechanism but not the message rate limit in this case the SBC will have degradation of the SIP services. The remediation for this case is to use an external commercial service to protect against DDoS attacks.
References	OpenScape Session Border Controller V11 Administrator Documentation
Needed Access Rights	administrator
Executed	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

The Message Rate limiting by time is available on the OpenScape SBC Function’s WAN and LAN network interfaces. However as the LAN interface is considered more secure the mechanism described in **Configuring the Internal Firewall (WAN)** is only applicable to the WAN interface.

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-SBC-MSG Rate Limit	**SIP Message Rate Limiting**
Measures	If message rate limiting is used, the OpenScape Session Border Controller 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 message rate profile. commercial service to protect against DDoS attacks.
References	OpenScape Session Border Controller V11 Administrator Documentation
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 signaling. Whenever a SIP message arrives on the OpenScape Session Border Controller destination address, the message source IP address and port are logged against the destination address. If the received message exceeds the message rate threshold logged for the source address, then the message is 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.

5.5.7 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, both for making calls and accessing features, must depend on SIP application-level authentication through 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* or the vendors’ call control documentation.

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

5.5.8 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_SBC-Information Filtering	**SIP Message Filtering Debug Informations**
Measures	On Security General Settings enable the flags: • Warning Info on Error responses removal • Internal Names and additional headers removal
References	OpenScape Session Border Controller V11 Administrator Documentation
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

6 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 TDoS 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 Controller using the Domain based Routing (alphanumeric video) have a separated netwrok realm for the video calls. In addition, the trust level should be set to minimum for this domain.
References	OpenScape Session Border Controller V11 Administrator Documentation
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

As described in chapter 5.4.1 it is recommended that the OpenScape SBC SIP listening ports be changed to other values which do not conflict with other provisioned ports.

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).

7 Administration

The OpenScape Session Border Controller is managed using:

- 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 SBC Assistant that runs on the OpenScape SBC server is used only to administer the OpenScape SBC server and provides a specialized Graphical User Interface.

The Common Management Portal (CMP) by means of the OpenScape SBC Assistant is used to authenticate the user or “assistant” against the OpenScape SBC. The “assistant" password must be synchronized between the OpenScape SBC Assistant and the OpenScape SBC.

The OpenScape SBC can also be configured to authenticate users remotely via a RADIUS server (See section Perform User Authentication via RADIUS).System Access Protection – Authorization.

7.1 System Access Protection-Authorization

7.1.1 Change Default Certificates for Web Server (HTTPS)

Provisioning in the OpenScape SBC is performed by means of a web interface. An administrator can access the provisioning interface either directly by means of the Local GUI or by means of the central management CMP. In both cases, HTTPS is used to communicate with the Web server in the OpenScape SBC. Some customers may request to change the default certificates which are used by HTTPS to a certificate which matches to the company PKI.

CL-SBC-HTTPS-PKI	Replace HTTPS default certificates by PKI
Measures	If PKI is required for the customer also for HTTPS, the HTTPS profile shall be modified. 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. This configuration is performed under: **Security** > **General** > **Certificate management** > **Certificate profile** > **TLS version**, by selecting the **TLS V1.2** option. 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 V11 Administrator Documentation
Needed Access Rights	Administrator, root
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

7.1.2 Protect LAN Interface for Administration Access

A secure web server (HTTPS) is used in the OpenScape SBC for central management CMP or Local GUI provisioning. The network services SSH and SFTP are also used for the administration of OpenScape SBC. The access to Local GUI, to SSH and to SFTP shall be protected in such a way that only one of a few computers can have access to them.

CL-SBC-PROT-HTTPS LOCAL GUI	Protect the Local GUI, SSH and SFTP, only allow provisioning CMP and predefined IP addresses
Measures	The CMP provisioning interface IP address and the Local GUI, SSH and SFTP provisioning IP address must be identified and placed in the administrative access control list. The certificate profile which is used for the System HTTPS shall be configured with the Minimum TLS version set to TLS V1.0.
References	OpenScape Session Border Controller V11 Administrator Documentation
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

The IP address of the Central CMP and of the computers which shall be granted access to Local GUI, SSH and SFTP must be identified. These IP addresses must be provisioned identifying HTTPS access as allowed within the security tab, firewall section, Whitelist for the LAN interface.

The IP addresses shall be added for both HTTPS port (port 443) and SSH/SFTP port (port 22).

To add the IP addresses and ports to the LAN Firewall, please follow these steps:

- Login to Local GUI or to CMP / SBC Assistant
- Open the screen **Security** > **Firewall**
- Select the LAN Interface and click **Edit**
- Add the IP address or subnet / Logical-Endpoint-ID of the administration computer(s) and the CMP server with the ports 443 and 22 to the Whitelist.
- Select **Block** for the HTTPS and SSH network connections
- Click **OK** and then click **Apply Changes**

It is recommended that a secured secondary SSH access be identified in the Whitelist 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 reconfiguration takes place, the OpenScape SBC Web server will be inaccessible. If this should occur, the following steps must be followed:

- Login to OpenScape SBC via an SSH session from the secured server as the service user.

- 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 or Local GUI to correct the mistake which also reapplies the firewall rules.

> ***INFO:*** These steps cause bypassing the OpenScape SBC firewall rules until the corrective action is completed requiring this maintenance activity to be planned accordingly.

7.2 System Access Protection-Authentication

For Password based Authentication, refer to Privileged Access Management (PAM) Framework.

For Certificate based Authentication, refer to User Authentication via SSH with PKI.

7.2.1 Privileged Access Management (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.

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:

- Log on to OpenScape SBC as administrator or service
- Increase the user privileges to root :su + <password>
- Edit password-related file `/etc/pam.d/common-password-pc`
- 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
  ```
- Save the file
- Log off

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

A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. The product password policies are mandated by technical means. OpenScape SBC technically supports the password policies depicted in chapter 8.1.1.1. There for every password rule a default value and a range of values that can be configured for that rule are given. If the default values don’t fit with the customer’s password policy, the values the customer wants to be configured shall be depicted in chapter 8.1.2

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.

INFO: Changing these parameters does not affect any new user or current password. Any password syntax rule changes take effect the next time a user’s password is changed.

Via CMP Profile

The most significant password policy parameters can be changed by means of an SBC profile in CMP namely: Password Aging Max Days, Min Three Class Length, Min Four Class Length, Password Iteration Number and Password Iteration Length. It is possible to apply the profile to a set of selected OpenScape SBC boxes via Job Management.

Via Command Line Interface

There are several supported parameters which can be used to modify the behavior of pam_passwdqc. The table below lists and describes each; defaults are in brackets. Some parameters are NOT allowed to be changed (such that security would be lessened) and some parameters have stricter limitations than standard PAM. As the settings are just edited using a standard editor, it will be possible to make some of these settings invalid, so care and proper testing is needed to verify any changes made.

8.2.1.1 Password rules supported by OpenScape SBC

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 []

8.2.1.2 PW Policy agreed for customers deployment

These are the customer PW/PIN rules for the PW Policy on OpenScape SBC level. Please implement them as default values. Filling the below table with customer specific values is only necessary if:

- The customer PW Policy is different from the default values.

	Password	PIN
Minimal length		
Minimal number of upper-case letters		
Minimal number of numerals		
Minimal number of special characters		
Maximal number of repeated characters		
Maximal number of sequential characters		

	Password	PIN
Change interval		
Maximum number of erroneous login attempts		
Password History		

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.

> ***INFO:*** Changing these parameters does not affect any existing users. The following commands must be executed to change those users.

  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.

> ***INFO:*** The root password does not age.

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.soauth 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.soaccount 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.soauth required pam_tally2.so onerr=fail
deny=3 unlock_time=60auth include common-auth
account include common-accountaccount 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-authauth requisite pam_tally2.so onerr=fail
deny=3 unlock_time=60account include common-accountaccount
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)).

8.2.4 Default Accounts

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

User	Assistant	Local GUI	ssh/sftp	Groups
guest	No access	Read only	No access	user
assistant	Read and Write	No access	sftp only	assistant, sshlogin
administrator	No access	Read and Write	ssh (Read only)	User, sshlogin
service	No access	Read and Write	ssh/sftp (Read and Write)	www, user, admin, sshlogin, assistant
root	No access	Read and Write	No access [1]	root

User	Assistant	Local GUI	ssh / sftp	Groups
ACD	No access	Read only (Read and Write for ACD parameters)	sftp only	user, sshlogin
cdr	No access	No Access	sftp only	cdr, sshlogin
redundancy	No access	No access	sftp only	user,sshlogin

[1] Root privileges via ssh can be obtained by using sudo

For the accounts below, the Management Interface grants rights to change and reset the password :

Management Interface	User	Rights to Change Password	Rights to Reset Password
CMP (Assistant)	assistant	guest, assistant, administrator, service, ACD, cdr, redundancy	guest, assistant, administrator, service, root, ACD, cdr, redundancy
Local GUI	administrator and service	guest, assistant, administrator, service, ACD, cdr, redundancy	guest, assistant, administrator, service, root, ACD, cdr, redundancy
	service	guest, assistant, administrator, service, ACD, cdr, redundancy	None
	root	guest, assistant, administrator, service, root, ACD, cdr	guest, assistant, administrator, service, root, ACD, cdr, redundancy
	guest and ACD	Own password	None
CLI (ssh)	root (via su command)	guest, assistant, administrator, service, root, ACD, cdr, redundancy	None
	service (via sudo)	guest, assistant, administrator, service, root, ACD, cdr, redundancy	None

8.3 Certificate Handling

The OpenScape SBC provides a set of default TLS CA certificates which can be used to establish TLS connections. It is highly recommended that the customer replaces these default factory certificates with their own CA Certificates from the Public Key Infrastructure (PKI). TLS connections are supported using either server authentication or mutual authentication.

Remote Gateways and Trunks addressing SIP servers, SIP trunking gateways, or SIP service providers using TLS connections may be supported using either server or mutual authentication. The OpenScape SBC typically operates as a TLS server however TLS client operation is also supported.

The OpenScape SBC outside network interface for TLS connection with Gateways typically uses mutual authentication TLS (MTLS).

The OpenScape SBC inside network or access network interface for TLS connection with OpenScape Voice or OpenScape SBC typically uses mutual authentication TLS (MTLS).

8.3.1 TLS Server Authentication

Install the following for a TLS server authenticated connection in the OpenScape SBC.

TLS server authentication where the OpenScape SBC is the TLS server:

- Server Certificate
- 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

TLS server authentication where the OpenScape SBC is in the TLS client:

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

8.3.2 TLS Mutual Authentication

For TLS mutual authentication, install the following information in the OpenScape Session Border Controller,

In the OpenScape SBC:

- Local Server Certificate
- Server intermediate CA Certificates (if any)
- Server public key (in the 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
- Client intermediate CA Certificate (if any)
- Client public key (in the 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

The cipher suites can be configured per certificate profile by means of three parameters:

- Perfect Forward Secrecy with the options Preferred PFS (default) orWithout PFS
- Encyption with the options Preferred AES-128
- Required AES-256 (default)
- 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

Cipher suites are hardcoded and cannot be changed.

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 SBC 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:
  - 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.

8.3.3 Credentials used for OpenScape SBC

While OS SBC provides default certificates it is strongly recommended that customer specific certificates are installed instead immediately upon the installation process prior to the system being deployed in the customer’s DMZ.

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

#	Interface	Customer requirement for OpenScape Session Border Controller credentials	Unify Default credentials	Usage
1	SIP Server (OSV)		Unify default certificate	TLS mutual authentication: requires at a minimum both local client and server Certificates be installed as well as the Root CA Certificate for the OpenScape Voice server.
2	Remote Users		Unify default certificate	TLS server authentication is typically supported requiring that at a minimum the customer CA Certificate must be installed.
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.

8.4 Port Table

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

Partner Portal

To get all necessary Security Checklist Port Table information you should select the appropriate data category according to the stakeholder 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_V11*. 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 V11 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 V11 on one Side of the firewall.
   b) All other SW Versions including the OpenScape SBC V11 (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 Interface/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 Interface/ OS-SBC	SIP Signaling / TCP for Access Realm (outside network)

	Destination / Source Port#	Network / Application Protocol	Default State	configurable	From	To	Description / Function
7	P:5060	SIP/TCP	Open	Yes	OS-SBC/ Core Realm Network Interface	Core Realm Network Interface / 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 Interface/OS-SBC	SIP Signaling / TCP secured by TLS for Access Realm (outside network)
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

	Destination / Source Port#	Network / Application Protocol	Default State	configurable	From	To	Description / Function
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
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

	Destination / Source Port#	Network / Application Protocol	Default State	configurable	From	To	Description / Function
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
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 SBC Administrator Documentation and Server Guideline**

available via e-Doku or Partner Portal (SEBA)/ product information

[2] **Unify Security Advisories and Product Security Policies**

Unify Security Advisories

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

available via SEBA Partner Portal

[5] **Center of Internet Security – Security Benchmarks**

Center of Internet Security