A MITEL PRODUCT GUIDE

Unify OpenScape Branch

OpenScape Branch V10

Security Checklist

July 2024

A31003-H81A0-P100-03-76A9

Notices

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

Trademarks

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

Contents

1 Introduction

1.1 History of Change

Date	Version	What
18/03/2011	1.0	Release of OSB V1R4
06/07/2011	2.0	Update to OSB V2R0
16/03/2012	3.0	Update to OSB V7R0
26/03/2012	3.1	Release of OSB V7R0
16/05/2012	3.2	Added RADIUS support & some corrections
16/05/2012	3.3	Release of OSB V7R0 with RADIUS
24/07/2012	7.0	Added login to SSH with PKI
06/11/2012	7.1	Corrections from System Test
04/01/2013	8.0	Release of OSB V8
09/02/2015	8.1	M1 of OSB V8R1
18/11/2015	9	Added V9
17/08/2017	9.1	Update V9R3
21/08/2018	10	Update V9R4
26/02/2019	11	Update V10
04/10/2023	12	Documentation improvements
23/07/2024	13	Rebranded to Mitel layout

1.2 General Remarks

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

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

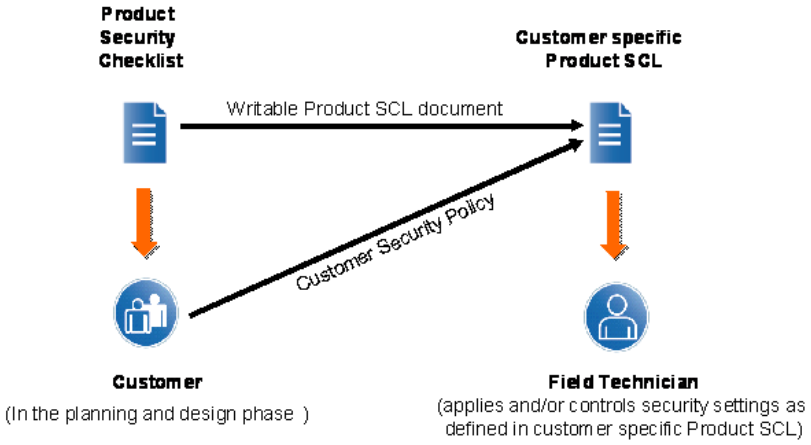
- to adapt these default settings to the needs of the individual customer and the specific characteristic of the solution to be deployed

- to weigh the costs of implementing security measures against the risks of omitting a security measure and to “harden” the systems appropriately.

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

The Security Checklists can be used for two purposes:

1. In the planning and design phase of a particular customer project:
   Use the Security Checklists of every relevant product to evaluate, if all products that make part of the solution can be aligned with the customer’s security requirements – and document in the Checklist, how they can be aligned.
   This ensures that security measures are appropriately considered and included in the Statement of Work to build the basis for the agreement between Unify and the customer: who will be responsible for the individual security measures:
   -
     During installation/setup of the solution
   - During operation
2. During installation and during major enhancements or software upgrade activities:
   The Security Checklists (ideally documented as described in step 1.) are used to apply and/or control the security settings of every individual product.


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 using always the latest version of the Security Checklists of the products that are part of your solution.
  They can be retrieved from the partner portal Unify Business Area (Customer Portal) for OpenScape Branch V10.

- 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.

1.3 Security Strategy for Unify Products

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

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

Product Planning & Design

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

Product Development & Test

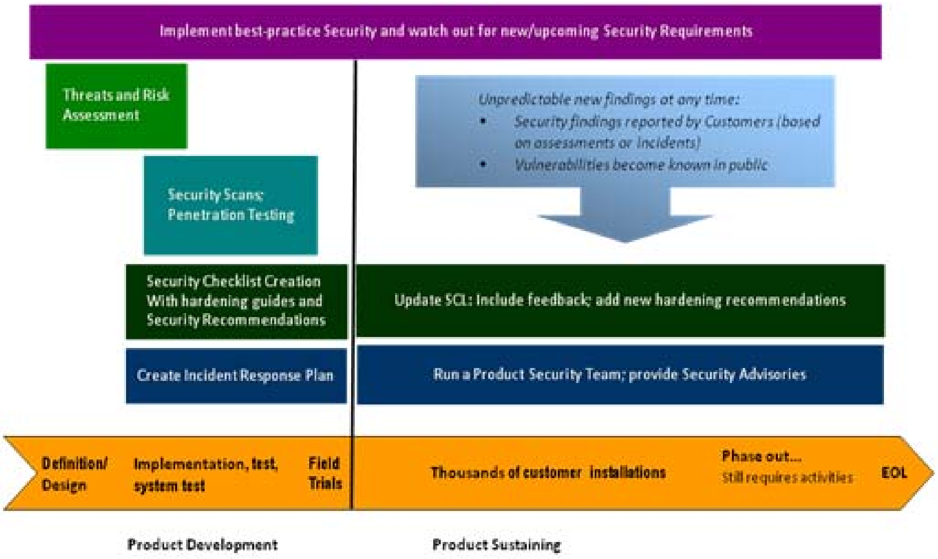
Penetration Tests (Practical Security Assessment) to discover implementation vulnerabilities and to verify the hardening of the default system configuration.

Installation & start of operation

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

Operation & Maintenance

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


Implement best-practice Security and watch out for new/upcoming Security Requirements
Threats and Risk Assessment
Security Scans; Penetration Testing
Unpredictable new findings at any time:
• Security findings reported by Customers (based on assessments or incidents)
• Vulnerabilities become known in public
Security Checklist Creation With hardening guides and Security Recommendations
Update SCL: Include feedback; add new hardening recommendations
Create Incident Response Plan
Run a Product Security Team; provide Security Advisories
Definition/ Design
Implementation, test, system test
Field Trials
Thousands of customer installations
Phase out...
Still requires activities
EOL
Product Development
Product Sustaining

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

The necessary information for that is drawn up in the OpenScape Branch V10 Security Checklist. For OpenScape Branch V10, the Product Security Checklist is this document.

1.4 Security Policies for OSB / SBC

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

As such, the following security policies are applied:

1. **The ability to update 3rd party components with security updates or patches in the field**
   The update of any 3rd party component embedded in the product (including the Operating System) is provided by Unify in the context of regular product maintenance releases (or hotfixes in case of critical updates). The Operating System is based but not identical to a community developed distribution. Even when the community declares a version deprecated this does not necessary means that the OSB/SBC OS is deprecated as the packages and kernel are individually updated by the regular OSB/SBC releases or hotfixes. Applying such security updates in the field is not possible. Instead, customers should stay up-to-date with regard to the product fix and hotfix releases as a whole: this ensures the continuous inclusion of 3rd party component security fixes (if relevant to the product). Also refer to the Mitel Security Policies.

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 Branch V10 and lists their 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:	

	Customer	Supplier
General Remarks		
Open issues to be resolved until		
Date		

2 OpenScape Branch V10 Hardening Procedures in General

The OpenScape Branch is an appliance which provides the functionality of SIP Proxy, Branch Session Border Controller with integrated Media Server. It offers variations with integrated Media Gateway to Analog Trunks (FXO), BRI, PRI and the functionality of Analog Adapter. The interconnection to PSTN can be done by means of the Media Gateway and also by means of SIP Service Providers. It provides the support to a set of features in survivable mode in order to assure continued communications service during the degradation or loss of communication between a remote branch and the headquarters.

The OpenScape Branch can be managed via a local web interface (Local GUI) and via CMP by means of the OSB Assistant. It also offers the access via SSH and SFTP.

In terms of maintenance, it offers the support of alarming via SNMP v3 or SNMPv2 and logging via syslog. It can be integrated to OpenScape Trace Management.

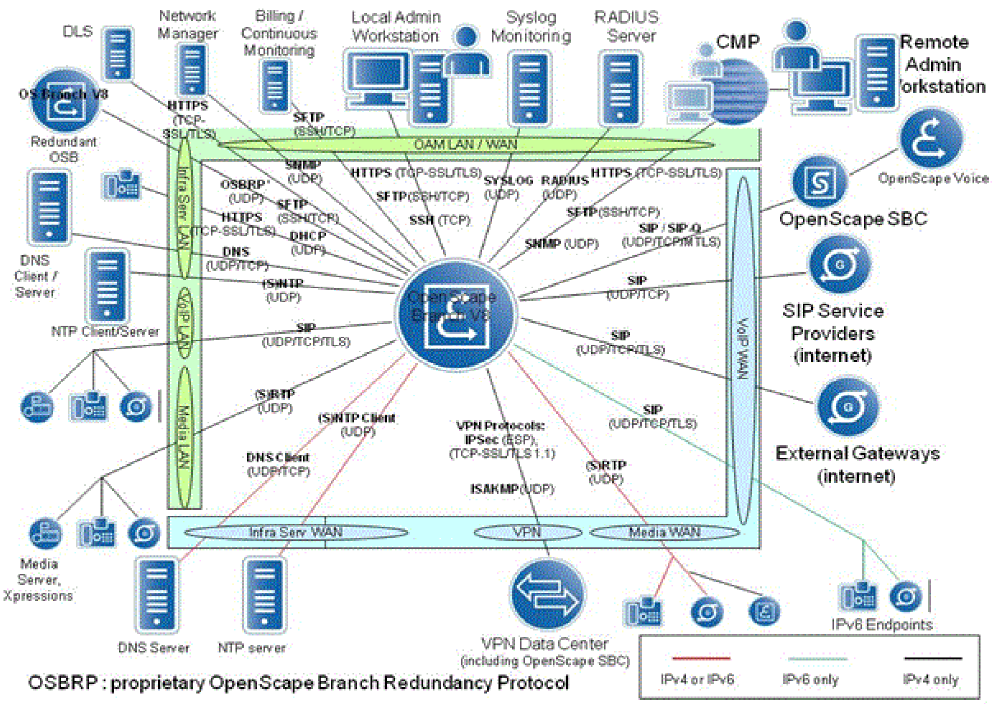
The following network services are supported by the OpenScape Branch:

- DNS server and DNS client
- DHCP server.
- NTP client and NTP server.
- Traffic shapping
- Authentication via RADIUS
- Authentication via PKI
- Digest Authentication
- Firewall
- Message Rate Control
- Denial of Service Mitigation

As a Branch SBC, it supports the following security services:

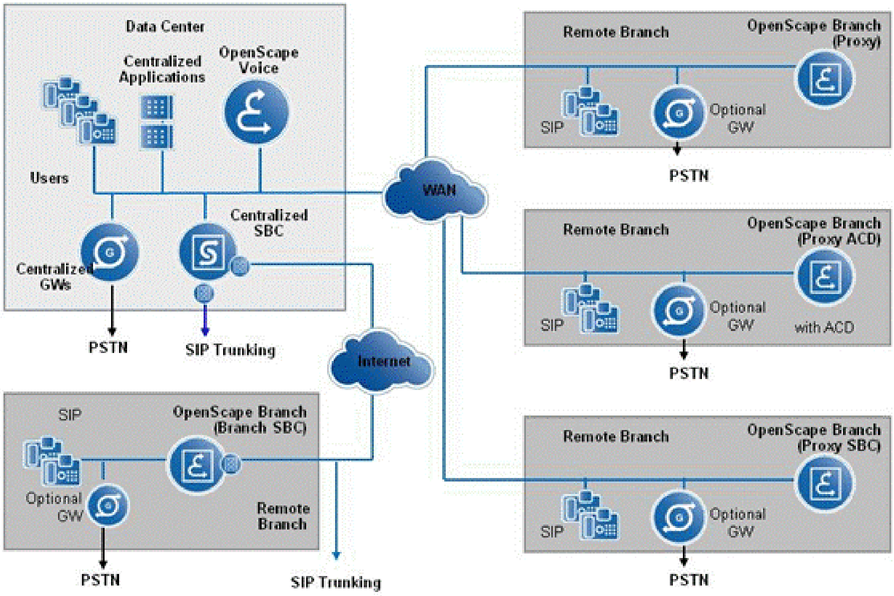
- VPN with IPSec or with OpenVPN.

The following figure presents the network interfaces of the OpenScape Branch:



OSBRP : proprietary OpenScape Branch Redundancy Protocol

The following figure presents the scenarios in which the OpenScape Branch can be deployed:



To tighten security on OpenScape Branch V10, the following measures are recommended :

- Regarding to SNMP

  - SNMPv2 - Changing the SNMP Community Name from the defaults since these are essentially passwords used for data exchange of SNMP trap information.
  - SNMPv3 - configuring the passphrases for the encryption and integrity check
- Changing predefined user account passwords from their defaults as these are well known.
- Changing the system default password policies.
- If the internal firewall is used, ensure it is properly configured.
- Ensure appropriate IP message rate limits are set for normal operation.
- Closing Unused IP Ports – Configure the ports required for operation of the system. If an external firewall is used, ensure that it is properly configured to pass the required traffic towards the system.
- Secure communications to SIP Servers using IPSec tunnels or VPN (OpenVPN) SSL connections in the absence of other mechanisms to secure SIP signalling. Using unsecured transport for SIP signalling provides opportunities for possible eavesdropping and disclosure.
- Use secure transport connections for SIP signalling whenever possible. Using unsecured transport for SIP signalling provided opportunities for possible eavesdropping and disclosure.
- Adopt appropriate media policies for using secure RTP media according to the network peer capability and profile wherever possible. Using unsecured media may lead to eavesdropping.
- Authenticate SIP subscriber by means of Digest Authentication.
- Deviations of the recommended security settings based on customer request shall be documented.
- Use customer PKI issued certificates.
- 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

3 Server Hardening

3.1 Hardware Security Settings

There are no known necessary security hardware settings.

3.2 BIOS Settings

There are no known BIOS security settings required.

3.3 OS Hardening

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

3.4 Changing the SNMP Community Name

SNMPV2 uses the notion of communities to establish trust between managers and agents. Community names are essentially passwords. A community name allows a level of access to MIB data. Data retrieval access levels are read-only (RO). An access level of read-write (RW) is not used.

CL-OSB-SNMP	**Change SNMP Community Name**
Measures	Change default values for Read-Only (RO) community name for SNMP Discovery since SNMP V2 community name is sent in clear text unless other security measures (e.g. VPN) are used for this traffic. By default, the OpenScape Session Border Controller sets the RO community name to "public". It is very important to change this default at installation as it is well known to the general public. See additional setting information below.
References	SNMP V2
Needed Access Rights	root

CL-OSB-SNMP	**Change SNMP Community Name**
Executed OpenScape Branch:	Yes: No:
Customer Comments and Reasons	

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

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

Additional Information for Settings:

From OSB V9R4 and up it is possible to change the SNMP RO community name either via CMP Profile or via Local GUI / OSB 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 Branch boxes via Job Management.

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

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

Changing via Local GUI and OSB Assistant

From OpenScape Branch V9R3 it is possible to change the Community Name from the Local GUI and also from the OSB Assistant.

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

3.5 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-OSB-SNMPv3	**Activate SNMPv3 encryption and 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	
Needed Access Rights	Administrator
Executed OpenScape Branch:	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-1. Notice that MD5 is not considered a secure hash mechanism anymore.
- Auth Password – A passphrase of at least 8 and a maximum of 32 characters shall be configured.
- Priv Protocol – Two options are offered: AES and DES. It is highly recommended to choose AES. Notice that DES is not considered a secure encryption algorithm anymore.
- Priv Password – A passphrase of at least 8 and a maximum of 32 characters shall be configured.

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

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

The following settings are used in SNMPV3 get:

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

3.6 Changing Default Passwords for Accounts

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 **Predefined Accounts**) after the installation completes.

CL-OSB-Passwords	Use non-default OpenScape Branch 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 the pre-defined users, the local passwords shall be changed from their pre-defined values.
References	
Needed Access Rights	administrator IMPORTANT: Access Rights to change "root" password is "root".
Executed OpenScape Branch:	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 **Addendum**, section **Management Security**).

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 8-40 characters long in accordance with the customer’s password policy.

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

In redundant OpenScape Branch deployments, passwords for redundancy users are not synchronized and must be changed in both nodes before redundancy is configured. Also note that for redundancy users only administrators can change password through local gui even on backup node.

> ***NOTICE:*** It is also possible to change the password of the users of a set of selected OpenScape Branch 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.Notice that some of the policy rules do not apply while restoring the user passwords, like password iteration number and password iteration length.

3.7 Change Default Password Policies

Verify if the Password Policies required by the Customer matches to the default policies provided by the OpenScape Branch. If they do not match, the Password Policies must be changed.

CL-OSB-New_Account-Passwords	**Change customer's password policy within the OpenScape Branch**
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	root
Executed OpenScape Branch:	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 OSB, the password policy is automatically synchronized to the backup OSB.

For new users created via Management Portal is recommend to set the change of password in first usage and also set an expiration date accord to the customer password polices.

3.8 Disable Not used Users

In V9R4 and up it is possible to disable via 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.

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

3.9 Perform User Authentication via RADIUS

It is possible to authenticate the users via a RADIUS server. Up to two RADIUS servers can be configured on the OpenScape Branch to perform the user authentication. Every time a user tries to login to OpenScape Branch 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 credentials configured in it.

CL-OSB-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 OSB. A secret must also be configured for each RADIUS server.
References	OpenScape Branch V10 Administrator Documentation [2]
Needed Access Rights	administrator
Executed OpenScape Branch:	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 OSB. 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 OSB will have the same privileges as the pre-defined service user.

The communication between OSB 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 Branch. In order to activate the authentication via the RADIUS server, at least one RADIUS server must be configured in the OpenScape Branch. 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 Branch the physical IP address of each node shall be configured in the RADIUS server (not the virtual IP address).

Regarding to the timeout, it is not recommended to configure a value of 1 or 2 seconds because any network problem would cause the RADIUS authentication to timeout. If the RADIUS authentication times out, the user is locally authenticated.

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

NOTICE: The authentication of users via the su command is performed internally (via Console and SSH only).The OpenScape Branch pre-defined users shall also be configured in RADIUS in order to be able to login to OpenScape Branch when the RADIUS server is reachable. Users which are not pre-defined in OpenScape Branch may also login to OpenScape Branch for all services except SSH and SFTP.

NOTICE: Internal users "assistant" and "redundancy" must not be created on the RADIUS server. It is also possible to enable the RADIUS Accounting. If the Accounting service is enabled, the RADIUS server is informed about the duration of the sessions and it will get the vendor identification. The Ac-counting service may also be separately enabled for CLI (Console access), SSH (and SFTP) and Web.

NOTICE: The Accounting service uses one port higher than the port used for authentication. If the Authentication service uses the default port, the Accounting service will use the port 2116. A secret must be configured for each RADIUS server. This secret is a sequence of 16 characters which is shared between the OpenScape Branch and the RADIUS server. In order to increase security the secret length was fixed to 16 characters.

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

3.10 Perform User Authentication in SSH with PKI

It is possible to authenticate the users in SSH with PKI. In order to be authenticated, the client sends a signed message to the OpenScape Branch. This message is signed with the private key of the client. The OpenScape Branch verifies this message with the public key of the client which is associated to the user in the OpenScape Branch. 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-OSB-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 Branch V10 Administrator Documentation [2]
Needed Access Rights	administrator
Executed OpenScape Branch:	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 Branch. For example, if the External User wants to be able to log in to the OpenScape Branch 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 Branch as the administrator user, a password is not required.The management of the public keys and their association to the user is done in the PKI Configuration section in the Security tab.

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

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

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

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

Perform VoiceMail Password changes

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

OSB-VoiceMail-Passwords	**Use non-default OpenScape Branch passwords**
Measures	Password for Accessing/Retrieving the VoiceMail Messages by User.Verify only digits can be entered for such passwords
References	
Needed Access Rights	administrator

OSB-VoiceMail-Passwords	**Use non-default OpenScape Branch passwords**
Executed OpenScape Branch:	Yes: No:
Customer Comments and Reasons	

4 Securing the OpenScape Branch

4.1 Configuring the Internal Firewall(WAN)

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

CL-OSB-Firewall	**Firewall Protection for the OpenScape Branch - Branch SBC outside or access network (WAN).**
Measures	For the outside network (WAN) of the OpenScape Branch operating as Branch SBC, the OpenScape Branch internal firewall must be used if no other external firewall is used. If an external firewall is used it must be configured to either operate in transparent mode or in a no SIP-NAT mode with dynamic IP address. If the external firewall is operating in no SIP-NAT mode the OpenScape Branch ’Branch behind NAT’ must be enabled. Regardless of the external firewall operation mode, the external firewall must provide equivalent protection as the internal firewall to allow/disallow communication between the Open-Scape Branch and external networks.
References	OpenScape Branch V10 Administrator Documentation[2]
Needed Access Rights	administrator
Executed OpenScape Branch:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

The OpenScape Branch Firewall settings and criteria to be used for the “Allow” setting shall be applied as detailed below for all networks considering IPv4 or IPv6 address types as supported in the network.

Under no circumstances shall “all protocols” be allowed for the OpenScape Branch outside or access network (WAN). Each protocol listed in the configu-ration shall be set to “blocked‟ unless explicit requirements are identified for setting to “allow”.

The OpenScape Branch Firewall settings and criteria to be used 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 WAN interface:

- SIP
- TLS
- RTP/sRTP
- HMGCP, only if OpenScape Branch remote Media Servers are used
- SSH (and SFTP) – this service shall be enabled if the system is remotely administered via CMP.

The following Network Services can be restricted / allowed from being accessed via WAN interface:

- DNS
- SNMP
- FTP
- HTTPS – this service shall be enabled if the system is remotely administered via CMP or Local GUI.
- SSH (and SFTP) – this service shall be enabled if the system is remotely administered via CMP.
- ICMP
- Telnet
- 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 according to customer requirements to allow / block communications from specific network IP addresses on the OpenScape Branch outside network Access network or WAN. The entries in the White / Black list can be made at the subnet level using the CIDR notation.

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

The following IP addresses are defined by IANA as special use:

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

Since these IP addresses are often used for spoofing they shall be added to the blacklist in the firewall if they are not supposed to be used.

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 Branch 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.

If the external firewall is used with no SIP-NAT the following parameters must be configured:

- the External Firewall flag in Firewall Configuration shall be enabled
- if the external firewall is using a static IP address:
  - the external IP address of the external firewall in Firewall Configuration shall be configured

otherwise

the flag Branch behind NAT shall be checked and then the branch uses its "Branch-Name" as "Logical-Endpoint-ID" to be encrypted in the OPTIONS sent to OpenScape SBC.

4.2 Configuring the Internal Firewall (LAN)

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

CL-OSB-Firewall	**Firewall Protection for the OpenScape Branch - Proxy,Proxy-SBC or Branch SBC local network (LAN)**
Measures	For the local network (LAN) of the OpenScape Branch operating as Proxy, Proxy ACD, Proxy-SBC or Branch SBC, the OpenScape Branch internal firewall must be used if no other external firewall is used. If an external firewall is used it must provide equivalent protection as the internal firewall to allow/disallow communication between the OpenScape Branch and the local networks.
References	OpenScape Branch V10 Installation & Upgrade Guide [1]
Needed Access Rights	administrator
Executed OpenScape Branch:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

The OpenScape Branch Firewall settings and criteria to be used 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

Since this firewall is associated to the LAN interface, all remaining protocols shall be allowed by default.

Additionally the internal firewall White/Black list should be configured according to customer requirements to allow / block communications from specific network IP addresses on the OpenScape Branch local network or LAN. The entries in the White / Black list 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 Branch 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.

If the SIP/MGCP/RTP/TCP/TLS is blocked by the configuration the know sersver have to be manually added to the whitelist.

4.3 Changing the Maximum IP Message Rate Threshold

The OpenScape Branch - Branch SBC 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 messages per second. After installation, this value should be adjusted based on the OpenScape Branch 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-OSB-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 Branch V10 Installation & Upgrade Guide[1]
Needed Access Rights	administrator
Executed OpenScape Branch:	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; the “white list” of trusted hosts, identified by their IP addresses, must be considered as exempt from the rate threshold limit.

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

5 Securing the OpenScape Branch Interfaces

5.1 Secure Communication with Servers Using IPSec Tunnels

Configure the OpenScape Branch to use IPSec tunnelling to the Data Center through a VPN Concentrator. When OpenScape Branch 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-OSB-IPSec	**Secure OpenScape Branch 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 and non-SIP communication between OpenScape Branch and servers on the WAN. The usage of IPSec Tunnels assure that OpenScape Branch 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 Branch V10 Administrator Documentation [2]
Needed Access Rights	administrator
Executed OpenScape Branch:	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 Branch IPSec tunnel can be established and used for communication.

The OpenScape Branch will need a Public and a Private IP addresses 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 Branch and OpenScape Voice for this we will have to configure the following:

- OpenScape Branch :

a) A Private (Main IP) and a Public IP (Admin IP) addresses under Network connection

b) IPSec tunnel under Security -> VPN -> IPSec where the:

- Partner: is the VPN concentrator IP�
- Partner Network: OpenScape Voice network information
- ocal: 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 Branch will be the Private (Main) IP address
- VPN concentrator: an IPSec tunnel must be created matching the configuration done in the Open-Scape Branch, such as authentication methods, secrets (passwords) and network addresses.

Note that this feature will only work on non-redundancy OpenScape Branch 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.

5.2 Secure SIP Signalling with Gateways / Trunks

OpenScape Voice Remote Endpoints may be configured to be reachable through the OpenScape Branch to represent and identify remote network servers, e.g., SIP Service Providers or SIP media gateways. UDP, TCP may be used for the signalling 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 Branch and OpenScape Branch Gateways / Trunks representing Media Gateways in the WAN or SIP Service Providers. These connections can be secured using TLS over TCP.

CL-OSB-TLS-Gateway_Trunk	**Secure External Gateways / Trunks Signaling using TLS**
Measures	The OpenScape Branch 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 profiles shall be created with the parameter Minimum TLS version shall be set to TLSv1.2 IMPORTANT: By default the certificate profiles are created with a cipher suite priority which gives preference to ephemeral cipher suites in order to provide Perfect Forward Secrecy. See Handling of Key Material, references and additional information below for installing CA certificates.
References	Refer to the following documents: • OpenScape Branch V10 Installation Guide[1] 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 Branch:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

Within the OpenScape Session Branch Certificate Authority (CA) Certificates may be associated with remote Gateways / Trunks using OpenScape Branch 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 transport security (TLS) for the type of TLS authentication sup-ported and associate with the appropriate CA Certificate profile.

If an unsecured SIP signalling connection is used, the OpenScape Branch 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 Branch is supporting the signalling with the remote Gateway / Trunk, 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 Branch inside or core network (LAN) interface with OpenScape Voice as covered in another section.

NOTICE: The only certificate critical extension which is handled by OpenScape Branch is Basic Constraints. Certificates containing other critical extensions will not be validated by the OpenScape Branch.

5.3 Secure SIP Server VoIP Communications

By default, the OpenScape Branch 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.

If the signaling channel is unsecured the SIP server and OpenScape Branch is vulnerable to “man in the middle” attacks from within the customer’s own network.

The OpenScape Branch supports mutual authentication TLS with OpenScape Voice.

CL-OSB-TLS-Core	**Secure OpenScape server VoIP communications using TLS**
Measures	The OpenScape Branch 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 IMPORTANT: by default the certificate profiles are created with a cipher suite priority which gives preference to ephemeral cipher suites in order to provide Perfect Forward Secrecy. See Handling of Key Material, references and additional information below for installing CA certificates.
References	Refer to the following documents: • OpenScape Branch V10 Installation Guide[1] for installing CA Certificates • OpenScape Voice Design & Planning Manual : Volume 3, Security Reference
Needed Access Rights	administrator
Executed OpenScape Branch:	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 Branch outside or access network (WAN) interface involved in the call. Securing the OpenScape Branch outside or access network (WAN) connections for remote subscribers and remote endpoints is covered in other sections of this document.

5.4 Configure OpenScape Branch - Branch SBC Outside or Access Network (WAN) SIP Signaling IP Ports

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

The OpenScape Branch 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 many security vulnerabilities can be instigated by external attacks to these ports.

It is therefore required that the OpenScape Branch SIP listening ports be changed to other values which do not conflict with other provisioned ports.

CL-OSB-SIP_Ports	**Configure OpenScape Branch 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 required that the OpenScape Branch SIP listening ports be changed to other non-conflicting ports to lessen the threat vulnerability.
References	OpenScape Branch V10 Installation Guide[1].
Needed Access Rights	administrator
Executed OpenScape Branch:	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 Branch 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 Session Border Controller, Remote Gateways and OpenScape Voice interfacing with the OpenScape Branch 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 statically provisioned with the same ‘Contact’ information.

On the OpenScape Branch inside access or branch (LAN) network, OpenScape Branch sends SIP messages to the IP address / port number provided by the phones during registration or as statically provisioned for Gateways / Trunks. Usually, these ports are 5060 (for UDP or TCP) or 5061 (for TLS over TCP), but can sometimes be configurable like the OpenScape Branch above.

On the OpenScape Branch outside or access (LAN) network, the OpenScape Branch sends SIP messages to the OpenScape Voice or to the OpenScape SBC 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 Configure OpenScape Branch Media Stream Security (SRTP)

SIP media sessions (RTP) established through the OpenScape Branch may be encrypted (SRTP). These media sessions establish media streams which traverse the OpenScape Branch which may be passed through virtually untouched. In the case of OpenScape Branch 50i or OpenScape Branch 500i, the integrated Gateway media sessions may be encrypted (SRTP). It is also possible to configure SRTP for FXS Ports in Proxy ATA 24/48.

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.

The following media configurations are supported by the OpenScape Branch 50i / 500i. 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. The following media policies including security key management protocol combinations are possible

- SRTP (SDES)
- SRTP (MIKEY#0)

Additionally to the transmission of media via SRTP, it is also strongly recommended that SIP Signalling is transmitted via TLS as defined in sections Secure SIP Signalling with Gateways / Trunks and Secure SIP Server VoIP Communications. Otherwise the keys are exchanged in clear text messages.

CL-OSB-Media_Security	**Configure OpenScape Branch Media Security for outside or access network (WAN) and inside or branch network (LAN)**
Measures	Identify media security as the preferred profile for media endpoints whenever possible. See additional information below for more information.
References	OpenScape Branch V10 Installation Guide[1].
Needed Access Rights	administrator
Executed OpenScape Branch:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

OpenScape Branch media policies are configured for each Gateway or SIP Service Provider to support the media policy identified above. The media security applied for a call is determined in real time, based upon the OpenScape Branch provisioned media profile for peer gateway or trunk, how the call was routed between the peers and signalling information supplied by the remote peer identifying its support for the desired media profile.

- The OpenScape Branch Gateway / Trunk shall be configured to support media security, identifying the supported media security key negotiation protocol.
- The OpenScape Branch inside or core network (LAN) should be configured to use SRTP with the media security key management protocol used by media peers in the branch.

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

CL-OSB-NTP	**Configure OpenScape Branch 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 Branch configuration
References	OpenScape Branch V10 Installation Guide[1]
Needed Access Rights	administrator
Executed OpenScape Branch:	Yes: No:
Customer Comments and Reasons	

5.6 Activate Digest Authentication to the SIP Subscribers

By default, Digest Authentication is not activated after installation. Even if Digest Authentication is enabled in the OpenScape Voice it does not mean that a SIP Subscriber will be challenged when the OpenScape Branch is operating in survivable mode. So, Digest Authentication shall be enabled in the OpenScape Branch.

CL-OSB-Digest_Authentication_to_SIP_Subscribers	**Activate Digest Authentication to the SIP Subscribers & SIP Endpoints in Survivable Mode**
Measures	Enable Digest Authentication Prerequisite – the connection to OSV must be MTLS so that Digest Authentication can be enabled in OpenScape Branch.
References	• OpenScape Voice Design and Planning Manual: Security Checklist [3] • OpenScape Branch V10 Administrator Documentation [2]
Needed Access Rights	administrator
Executed OpenScape Branch:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

When the feature Digest Authentication is enabled in the OpenScape Branch, the credentials for the subscribers are automatically synchronized with the OpenScape Voice when the SIP Subscriber registers on the OpenScape Voice by using the OpenScape Branch as an outbound proxy.

Due to the synchronization process which only happens when the OpenScape Branch is operating in normal mode, changes to the credentials on the SIP phones and on the OpenScape Voice must be per-formed very carefully in order to guarantee that the credentials are correctly synchronized to the OpenScape Branch.

5.7 Protect LAN Interface for Administration access

A secure web server (HTTPS) is used in the OpenScape Branch for central management CMP or Local GUI provisioning. The network services SSH and SFTP are also used for the administration of OpenScape Branch. 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-OSB-PROT-HTTPS-LGUI	**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 Branch V9 Administrator Documentation [2]
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, White List for the LAN interface.

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

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

1. Login to Local GUI or to CMP / OSB Assistant
2. Open the screen **Security** > **Firewall**
3. Select the LAN Interface and click **Edit**.
4. 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 White list.
5. Select **Block** for HTTPS and SSH network connections.
6. Click **OK** and then click **Apply Changes**.

It is recommended that a secured secondary ssh access be identified in the White List to prevent lockout situations. For example, if by mistake an incorrect IP address is inserted in the administrative access control list or CMP IP address reconfiguration takes place, the OpenScape Branch Web server will be inaccessible. If this should occur, the following steps must be followed.

- Login to OpenScape Branch 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.

NOTICE: These steps cause bypassing the OpenScape Branch firewall rules until the corrective action is completed requiring this maintenance activity to be planned accordingly.

5.8 Protect Against SIP Registration DoS Attacks

The OpenScape Branch 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 providing invalid credentials or uses an invalid identity the sender’s IP address is blacklisted or quarantined for a finite period of time.

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.

Each type of violation uses its own quarantine time interval.

CL-OSB-REG-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 aech type of violation
References	OpenScape Branch V10 Administrator Documentation [2]
Needed Access Rights	administrator
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

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

If the OpenScape Branch 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 Branch is operating in Survivable mode, the decision is based on the configuration of Digest Authentication in the OpenScape Branch. If Digest Authentication is enabled in the OpenScape Branch, 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 Branch, 404 Unknown is responded back and the Source IP is quarantined. If Digest Authentication is disabled in the OpenScape Branch, 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.

5.9 Change Default Certificates for Web Server (HTTPS)

Provisioning in the OpenScape Branch 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 Branch. Some customers may request to change the default certificates which are used by https to a certificate which matches to the company PKI.

CL-OSB-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. 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 Branch V10 Administrator Documentation [2]
Needed Access Rights	administrator, root
Executed OpenScape SBC:	Yes: No:
Customer Comments and Reasons	

Additional Information for Settings:

If an invalid https certificate is loaded onto the OpenScape Branch by mistake, then it will not be possible to communicate with the OpenScape Branch via the CMP or the Local GUI. If such a problem occurs, then the following steps shall be followed to recover previous HTTPS Profile:

- Login to OpenScape Branch via an SSH session from the secured server as the service user
- Increase the user privileges to root: su + <password>.

- Type the CLI command "pmc recover" - This command recovers the previous database with a last valid https certificate.

> ***NOTICE:*** The management of the HTTPS certificates and their association to the HTTPS system profile is done in the Certificate management and PKI Configuration sections in the Security tab, as described in the OpenScape Branch V9 Administrator Documentation [2].

5.10 Disable basic security check over LAN traffic by default

Sipserver applies the SIP messages received over a sanity check for security reasons. This process spends some system performance and delays the message processing.

It is possible to disable the sanity check over LAN traffic by the flag **Disable basic security check over LAN traffic** under **VoIP > General**. This flag is disabled by default, i.e., the sanity check is enabled.

Considering the LAN a controlled environment, it is safe to disable this check over messages coming from the LAN. In order to give to the system more performance, from now, it will be disabled by default in new installations.

In case of system upgrades, the flag "Disable basic security check over LAN traffic" shall be set manually.

6 Administration / Management Security

The OpenScape Branch is managed by using:

- A local instance of OpenScape Branch Assistant that runs on the same server as the external OpenScape Branch application. The client for the local instance of OpenScape Branch Assistant is a standard web browser. The interface from the client to this OpenScape Branch Assistant is protected by HTTPS.

  NOTICE: The local instance of OpenScape Branch Assistant that runs on the OpenScape Branch server is used only to administer the OpenScape Branch server and provides a specialized Graphical User Interface.

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

The OpenScape Branch can also be configured to authenticate users remotely via a RADIUS server (See section Perform User Authentication via RADIUS).

6.1 Local Authentication

6.1.1 PAM Framework

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

Module Type	Module Flag	Module Name	Arguments

password	requisite	pam_passwdqc.so	pw_iteration_nr=3
			retry=3
			match=4
			similar=deny
			passphrase=0
			enforce=everyone
			pw_iteration_length=180
			min=disable, disable,
			disabled,8,8
			max=40
			random=42

password	requisite	pam_unix2.so	**use_authtok nullok**

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

6.1.2 Editing PAM Configuration Files

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

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

1. Log on to OpenScape Branch as administrator or service
2. Increase the user privileges to root :su + <password>
3. Edit password-related file **/etc/pam.d/common-password-pc**
4. Change "pw_iteration_nr=3" to "pw_iteration_nr=4" as follows:
   password requisite pam_passwdqc.so min=disabled,disabled,disabled,8,8 max=40 passphrase=0 match=4 similar=deny random=42 enforce=everyone retry=3 pw_iteration_nr=4 pw_iteration_length=180
5. Save the file
6. Log off

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

6.2 Password Policy

Password Rules & Aging Management

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

7 Virtualization

The OpenScape Branch may be virtualized using supported versions (check the Virtualization Guide to see the supported versions).

7.1 Virtualization Hardening According to VMWare

The primary hardening is for the Hypervisor. The Hardening Guide issued by the VMWare shall be followed.

The Hardening Guide repository at VMWare homepage shall be checked for the most-up-to-date version:

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

8 Addendum

8.1 GDPR

The OpenScape Branch is compliant with GDPR. The OpenScape Branch 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 Policy

8.2.1 Password Rules and Aging Management

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 a CMP Profile or via Command Line Interface.

NOTICE:

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 OSB 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 Branch boxes via Job Management.

Via Command Line Interface

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

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 pass-word 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] IMPORTANT: This parameter is only valid for SSH. For Local GUI and CMP there is no limitation on the number of times a user can try to change a password

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 []

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

8.2.2 Password Aging

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

- By accepting the defaults for accounts creation in /etc/login.defs, which indicate the password aging controls (used by useradd) listed in the table below.

  INFO: Note that 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.

NOTICE: 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.

NOTICE: The root password does not age.

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. Lower versions of PuTTy do not honor this configuration and closes the session by entering the wrong password only once.

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

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

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

auth	**required**	**pam_tally2.so onerr=fail deny=3 unlock_time=60**
auth	include	common-auth
account	include	common-account
account	**required**	**pam_tally2.so**
password	include	common-password
#session	required	pam_loginuid.so
session	optional	pam_radius_auth.so
session	include	common-session
session	required	pam_lastlog.so nowtmp

/etc/pam.d/passwd

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

NOTICE: 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 section Activate Digest Authentication to the SIP Subscribers).

8.3 Pre-defined Accounts

The following 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
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

Management Interface	User	Rights to Change Password	Rights to Reset Password
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

8.4 Handling of Key Material

The OpenScape Branch provides a set of default TLS CA certificates which can be used to establish TLS connections. It is highly recommended that the customer replace these default factory certificates with their own CA Certificates from the Public Key Infrastructure (PKI). 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 Branch typically operates as a TLS server however TLS client operation is also supported.

The OpenScape Branch inside network or branch network interface TLS connection with Gateways typically uses mutual authentication TLS.

The OpenScape Branch outside network or access network interface TLS connection with OpenScape Voice or OpenScape SBC typically uses mutual authentication TLS.

TLS Server Authentication

For a TLS server authenticated connection the following is installed in the OpenScape Branch:

TLS server authentication where the OpenScape Branch 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 its Certificate CA chain

TLS authentication where the OpenScape Branch is the TLS client:

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

Mutual Authentication

For mutual authentication, the following information is installed in the OpenScape Branch:

- 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 its 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 which is used to verify the validity of its own Certificate in its Certificate CA chain
- Remote Client Root CA 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) or Without PFS.
- Encryption with the options Preferred AES_-128
- (default), Required AES_-256
- Mode of operation with the options Preferred GCM (default), CBC only, GCM only

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

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

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

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

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

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

The OpenScape Branch 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 > 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.

It is also possible to use certificates for establishing the VPN connection. In this case a certificate profile shall be created for VPN. The following information is then required:

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

By configuring the tunnel connection the correct certificate profile shall be selected.

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

The maximum number of certificate profiles is defined as follows:

- OSB50, OSB50i, OSB250 – Max Certificate Profiles shall be 5.
- OSB500i, IBM 3250,IBM 3550, Fujitsu RX200, Fujitsu R300 – Max Certificate Profiles shall be 15.

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

- Certificate validation - Enables the validation of the CA chain and CA signature, Validity Period and Critical Extensions
- Revocation status - Enables the verification of revoked certificates according to the CRL of the CA
- Subject authentication - Enables the validation of certificate Subject CN or Subject Alternative Name according to the configured gateway/trunk FQDN or IP Address.

> ***INFO:*** It is possible to upload up to 5 certificate files to a set of selected branches via a CMP Profile.

The procedure to configure and activate Certificates in the OpenScape Branch is described in [2] OpenScape Branch V10 Administrator Documentation (e-Doku or Customer Portal / product information).

#	Interface	Customer requirement for OpenScape Branch credentials	SEN Default credentials	Usage
1	SIP Server (OSV)		SEN 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	SIP Subscriber		SEN default certificate	TLS server authentication is typically supported requiring that at a minimum the customer CA Certificate must be installed

#	Interface	Customer requirement for OpenScape Branch credentials	SEN Default credentials	Usage
3	SIP Service Provider & Gateway (TLS mutual authentication)			If TLS server authentication is used, the OpenScape Branch operating as the TLS client requires the Root CA certificate and intermediate Root CA(s) for each SIP SP remote end-point be installed
4	SIP Service Provider & Gateway (TLS mutual authentication)		SEN default certificate	If TLS mutual authentication is used, the OpenScape Branch 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 end-point.
5	CMP & Local GUI Management		SEN default certificate	The customer CA Certificate must be installed in place of the SEN default.

8.5 Port Table

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

https://apps.g-dms.com/ifm/php/php_ifmdb/scripts/login.php or via Customer 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 Branch 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). For OpenScape

Branch the following reports are predefined: “SCL_OSB_Proxy_V10”, “SCL_OSB_BranchSBC_V10” and “SCL_OSB_SBCProxy_V10”. One can use one of the predefined reports as a template or starting point and modify Entities, SW-Versions, and Interfaces as desired for building the customized report.

3. Select Entities:

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

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

4. Select SW-Version:

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

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

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

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

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

   - To store a report, enter a Filename into the textfield below the Select Interfaces menu .e.g. “SCL_OSB_Proxy_V10”.
   - 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 Branch V10 on one Side of the firewall.

   b) All other SW Versions including the OpenScape Branch V10 (as a peer) shall be put on the other side.

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

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

	Destination / Source Port#	Network / Application Protocol	Default State	configurable	From	To	Description / Function
1	P:0,0	UDP/IPSEC	Open	No	OSB IPSec VPN	VPN Concentrator	VPN tunnel endpoint based on IPSec (IPv4) - IPSecEncapsulating Security Payload
2	D:443	HTTPS/TCP-SSL/TLS	Open	No	Central CMP or Local GUI Web Browser	OSB Web Server	https based CMP management or Web session
3	P:500,500	ISAKMP/UDP	Open	No	OSB IPSec VPN	VPN Concentrator	VPN tunnel endpoint based on IPSec (IPv4) - IPSecInternet Key Exchange
4	S:514, D:500-600	Syslog/UDP	Open	No	OSB	Syslog Server	Syslog Server in OSV-TM
5	P:4500	NAT-T/UDP	Open	No	OSB	Remote Endpoint	VPN tunnel endpoint based on IPSec (IPv4) – NAT traversal
6	P:5060	SIP/UDP	Open	Yes	OSB/LAN Network Interface	LAN Network Interface/ OSB	SIP Signaling / UDP from/to LAN Interface
7	P:5060	SIP/UDP	Open	Yes	OSB/ WAN Network Interface	WAN Network Interface/ OSB	SIP Signaling / UDP from/to LAN Interface
8	P:5060	SIP/TCP	Open	Yes	OSB/LAN Network Interface	LAN Network Interface/ OSB	SIP Signaling / TCP from/to LAN Interface
9	P:5060	SIP/TCP	Open	Yes	OSB/ WAN Network Interface	WAN Network Interface/ OSB	SIP Signaling / TCP from/to LAN Interface
10	P:5060	SIP/TCP-TLS	Open	Yes	OSB/LAN Network Interface	LAN Network Interface/ OSB	SIP Signaling / TCP from/to LAN Interface

	Destination / Source Port#	Network / Application Protocol	Default State	configurable	From	To	Description / Function
11	P:5060	SIP/TCP-TLS	Open	Yes	OSB/ WAN Network Interface	WAN Network Interface/ OSB	SIP Signaling / TCP from/to LAN Interface
12	S: 35000 - 65000, D: 10000 – 49999 29100 – 30099 32768 – 43647 35000 – 65000 5004 – 5059 10000 – 19999 20000 – 20499 55000 – 65000	(S) RTP – (S) RTCP / UDP	Closed	Dynamic	OSB LAN (iGW with SRTP/ G.729)and WAN (Branch SBC and SBC Proxy)	OSB LAN or WAN (S)RTP – (S)RTCP Media Endpoint, OSB peer, OS-SBC	OSB Source port determined dynamically during SIP signaling
13	D: 35000 - 65000, S: 10000 – 49999 29100 – 30099 32768 – 43647 35000 – 65000 5004 – 5059 10000 – 19999 20000 – 20499 55000 – 65000	(S) RTP – (S) RTCP / UDP	Closed	Dynamic	LAN or WAN (S)RTP – (S)RTCP Media Endpoint, OSB peer, OS-SBC	OSB LAN (iGW with SRTP/ G.729)and WAN (Branch SBC and SBC Proxy)	OSB Destination port determined dynamically during SIP signaling

	Destination / Source Port#	Network / Application Protocol	Default State	configurable	From	To	Description / Function
14	S: 10000 - 19999, D: 10000 – 49999 29100 – 30099 32768 – 43647 35000 – 65000 5004 – 5059 10000 – 19999 20000 – 20499 55000 – 65000	(S) RTP – (S) RTCP / UDP	Closed	Dynamic	OSB LAN (iGW without SRTP/ G.729)	OSB LAN (S)RTP – (S)RTCP Media Endpoint, OSB peer, OS-SBC	OSB Source port determined dynamically during SIP signaling
15	D: 10000 - 19999, S: 10000 – 49999 29100 – 30099 32768 – 43647 35000 – 65000 5004 – 5059 10000 – 19999 20000 – 20499 55000 – 65000	(S) RTP – (S) RTCP / UDP	Closed	Dynamic	LAN (S)RTP – (S)RTCP Media Endpoint, OSB peer, OS-SBC	OSB LAN (iGW without SRTP/ G.729)	OSB Destination port determined dynamically during SIP signaling

	Destination / Source Port#	Network / Application Protocol	Default State	configurable	From	To	Description / Function
16	S: 20000 - 20499, D: 10000 – 49999 29100 – 30099 32768 – 43647 35000 – 65000 5004 – 5059 10000 – 19999 55000 – 65000	(S) RTP – (S) RTCP / UDP	Closed	Dynamic	OSB LAN (integrated Media Server)	OSB LAN (S)RTP – (S)RTCP Media Endpoint, OSB peer, OS-SBC	OSB Source port determined dynamically during SIP signaling
17	D: 20000 - 20499, S: 10000 – 49999 29100 – 30099 32768 – 43647 35000 – 65000 5004 – 5059 10000 – 19999 55000 – 65000	(S) RTP – (S) RTCP / UDP	Closed	Dynamic	LAN (S)RTP – (S)RTCP Media Endpoint, OSB peer, OS-SBC	OSB LAN (integrated Media Server)	OSB Destination port determined dynamically during SIP signaling
18	D:123	SNTP / UDP	Open	No	SNTP Client	OSB SNTP	SNTP time query
19	D:22	(S) FTP or SSH/ UDP	Open	Yes	OSB/ OSVTM, CLI, Mass Provisioning, Traffic Tool, Billing Tool	OSB	Secure File Transfer client access / CLI SSH Billing
20	D:22	(S) FTP	Open	Yes	OSB	Billing Tool	Billing

	Destination / Source Port#	Network / Application Protocol	Default State	configurable	From	To	Description / Function
21	S:162 D:162	SNMP / UDP	Open	Yes	OSB SNMP Agent	CMP, Network Management, Alarming	Network Alarming
22	P:1075, 1075	OSB Redundancy /UDP	Open	No	OSB	OSB	Internal OSB redundancy
23	D:22	SSH/UDP	Open	No	OSB/CLI, Mass Provisioning	OSB	CLI SSH & service access
24	D:68	DHCP/UDP	Closed	No	OSB	DHCP Server	DHCP Server only for simplified installation
25	D:2427	SSH/UDP	Open	Yes	OSV	OSB	MGCP Server on OSB
26	S:1024 - 65535	DNS/TCP or UDP	Closed	No	OSB	DNS	DNS Client
27	D:53	DNS/TCP or UDP	Closed	No	SIP Subscriber or Endpoint	OSB DNS Server	DNS Server
28	S:1024 - 65535	RADIUS/ TCP	Closed	No	OSB	RADIUS Server	RADIUS authentication / accounting
29	D:443	SOAP / HTTP / TCP-TLS	Open	Yes	CMP, Web Client	OSB	SOAP via HTTPS with WSDL tunnelled. Also for Local GUI WBM
30	S:10000 - 14999	SOAP/HTTP/ TCP-TLS	Open	Yes	OSB	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
31	P:10000 - 14999	BFCP/ UDP,TCPor TCP-TLS	Closed	Yes	Remote BFCP Endpoint	OSB / Remote BFCP Endpoint	BFCP ports determined dynamically during SIP signaling

9 References

[1] **OpenScape Branch V10 Installation Guide**

(e-Doku or Customer Portal / product information)

[2] **OpenScape Branch V10 Administrator Documentation**

(e-Doku or Customer Portal / product information)

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

(e-Doku or Customer Portal / product information)

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

available via Customer Portal

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