A MITEL
PRODUCT
GUIDE

OpenScape Voice V10

Security Checklist

07/2024

A31003-H80A0-P101-03-76A9

Mitel

Notices

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

Trademarks

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

Contents

History of Changes **5**

1 Introduction **7**
1.1 General Information 7
1.2 Update and Feedback 8
1.3 Customer Deployment - Overview 9

2 Hardening Measures **11**

3 Server Hardening **13**
3.1 Notes on IPSec 13
3.2 Hardware Security Settings 13
3.3 BIOS Settings 14
3.3.1 BIOS Password 14
3.3.2 Boot Order 15
3.4 Operating System Hardening 15
3.4.1 Password Management 15
3.4.1.1 Password Protecting GRUB 15
3.4.1.2 Changing Predefined Passwords for Administrator Accounts 17
3.4.1.3 Protection against Toll Fraud 19
3.4.1.4 Change Predefined Passwords for Application Accounts 20
3.4.1.5 Change Default Password Policies for New Accounts 21
3.4.2 Remote SSH Access and FIPS Compliance 23
3.4.2.1 Standard SSH profile 23
3.4.2.2 Optimal SSH profile 24
3.4.2.3 Modify SSH Configuration 24
3.4.3 Change Denial of Service (DoS) Thresholds 24
3.4.4 Allow IPsec Fragmentation 26
3.4.5 Turn on IPsec Between Servers 28
3.4.6 Transport Layer Security (TLS) Certificates 29
3.4.6.1 Change the Default TLS Certificates 29
3.4.6.2 Enable Certificate Expiration Verification 30
3.4.6.3 Review Certificate Revocation List Settings 31
3.4.6.4 Certificate Verification Configuration Level Definitions for Unattended Mode 31
3.4.6.5 Enable TLSv1.2 Perfect Forward Secrecy (PFS) 33
3.4.7 Baseline Information 36
3.4.7.1 Set User-ID (SUID) / Set Group ID (SGID) Files 36
3.4.8 Remote Syslog 39
3.4.9 IPv6 40

3.5 Securing the Administrative Interface 43
3.5.1 Administration via SNMP 43
3.5.1.1 SNMP Community String 43
3.5.1.2 Configure Secure SNMP Trap Destinations 45
3.5.2 Administration via SOAP 46
3.5.2.1 Configure TLS 47
3.5.2.2 Enable TLS Certificate Validation 48
3.5.2.3 Enable Certificate Revocation List Checking 49
3.5.2.4 Enable Certificate Identity Checking 50

3.5.2.5 Configure IPSec if TLS is not Supported by a SOAP Client . . . 51
3.5.2.6 Adding Authorization to SOAP . . . 52
3.5.2.7 Firewalling the SOAP Clients . . . 55
3.6 Securing the Billing Interface . . . 55
3.7 Securing the IMM or iRMC Access . . . 56
3.8 Securing the Signaling Interface . . . 57
3.8.1 Securing SIP Services - Securing SIP Signaling Manager on OSV . . . 57
3.8.1.1 Enable Authentication Services . . . 57
3.8.1.2 Activate Authentication of SIP Subscribers and SIP Endpoints behind Proxies and SBCs . . . 58
3.8.1.3 Enable TLS Certificate Validation . . . 59
3.8.1.4 Enable Certificate Revocation List Checking . . . 60
3.8.1.5 Enable TLS Identity Checking . . . 60
3.8.2 Secure Configuration for SIP Subscribers . . . 61
3.8.2.1 Activate MTLS for SIP Subscribers . . . 61
3.8.2.2 Activate TLS Signaling for SIP Subscribers . . . 62
3.8.2.3 Restrict/Allow registering and making calls via Central SBC . . . 63
3.8.2.4 Activate Digest Authentication to SIP Subscribers . . . 64
3.8.3 Secure Configuration for SIP Endpoints . . . 65
3.8.3.1 Activate MTLS Signaling for SIP Endpoints . . . 65
3.8.3.2 Activate Digest Authentication to SIP Endpoints . . . 66
3.8.3.3 Tell the OSV that a SIP Endpoint is a Central SBC . . . 67
3.8.3.4 Never Trust Proxies and SBCs . . . 68
3.8.3.5 Use Aliases with Ports . . . 70
3.8.4 Securing MGCP Services . . . 71
3.8.4.1 Securing Media Servers . . . 71
3.8.5 Securing CSTA Services . . . 71
3.8.5.1 Enable TLS Certificate Validation . . . 71
3.8.5.2 Enable Certificate Revocation List Checking . . . 72
3.8.5.3 Enable Certificate Identity Checking . . . 73
3.8.5.4 Configure TLS on CSTA Clients . . . 74
3.8.5.5 Configure IPSec if TLS is not Supported by a CSTA Application . . . 76
3.8.5.6 Firewalling the CSTA Applications . . . 76
3.8.6 Restrict IPMI to Internal Networks . . . 77
3.8.7 Change the Default Passwords for the IMM/iRMC Card . . . 77
3.8.8 Deactivate Clear-Text Administration / Activate Encrypted Communication - RX200S6 Platforms . . . 78
3.8.9 Deactivate Clear-Text Administration / Activate Encrypted Communication - x3550 M3 and x3550 M4 platforms . . . 79
3.8.10 Disable Weak Ciphers for IMM . . . 81
3.9 Features . . . 82
3.9.1 Prevent fraud using 3 way calling . . . 82
3.9.2 MLPP . . . 82
3.9.3 DA Challenging . . . 83
3.9.4 CSTA Control . . . 84
3.9.5 NG911 Emergency calling . . . 84
3.9.6 Foreign Domains support . . . 85
3.10 Secure SIP Trunks . . . 86
3.11 Security Patches . . . 88
3.12 Integrity of SW load and Patch sets . . . 88
3.13 Virus Protection . . . 88

4 References . . . 91

History of Changes

Issue	Date	Changes
3	09/2021	Minor edit in chapter: 3.4.6.5 Enable TLSv1.2 Perfect Forward Secrecy (PFS)
2	08/2020	Added chapter 3.9.6 Foreign Domains support
1	10/2019	Initial Release

1 Introduction

CAUTION

It is of vital importance that security measures outlined in this document are executed.

1.1 General Information

Information and communication and their seamless integration in Unified Communications and Collaboration (UCC) are important and valuable assets for an enterprise and are the core parts of their business processes. Therefore, they have to be adequately protected. Every enterprise may require a specific level of protection, which depends on individual requirements for availability, confidentiality, integrity and compliance of the IT and communication systems being used.

Unify attempts to provide a common standard of features and settings of security parameters within the 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 accordingly.

As a basis for that, the Security Checklists are published. They support the customer and the service both directly and indirectly, as well as those wanting to maintain it themselves, to agree on the settings and to document the decisions that are made.

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 of the products that form a part of the solution can be aligned with the customer’s security requirements. 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. The customer will be responsible for the individual security measures:
   - during installation and 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 the previous step) are used to apply and/or control the security settings of every individual product.

1.2 Update and Feedback

By their nature, security-relevant topics are prone to continuous changes and updates. New findings, corrections and enhancements of this checklist are being included as soon as possible. Therefore, we recommend always using the latest version of the Security Checklists of the products that are part of your solution. They can be retrieved from the partner portals at the relevant product information site.

We encourage you to provide feedback on anything that is not clear or about problems with the application of this checklist.

Please contact the OpenScape Baseline Security Office (obso@unify.com).

1.3 Customer Deployment - Overview

This Security Checklist covers the product OpenScape Voice V9 and lists the security relevant topics and settings in a comprehensive form.

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

2 Hardening Measures

The information in this document is intended to support the service technicians, re-sellers, and consultants in the examination and setting of the required security measures in the software and at the hardware for OpenScape Voice.

The current security settings are to be confirmed by the customer by means of signature in the delivery of OpenScape Voice.

Deviations of the security settings on customer request are to be documented.

This manual addresses the hardening issues related to the following:

- Hardware security settings
- BIOS settings
- Operating System hardening
- Securing interfaces
- Patches

3 Server Hardening

3.1 Notes on IPSec

IPSec, when listed in subsequent chapters, should be configured with SHA2 and make use of X.509 certificates.

3.2 Hardware Security Settings

There are no necessary security hardware settings known now for any of the OpenScape Voice supported hardware platforms.

Precondition: OpenScape Voice has been installed / updated according to the OSV Installation Manual. In the table below, enter the manufacturer name and model number on which OpenScape Voice is installed.

CL-OSV-Hardware Platform	**Hardware Platform**
Measures	Enter the manufacturer name and model number on which OpenScape Voice is installed.
Hardware Platform	
Needed Access Rights	n/a
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

Enter one of:

- IBM x3550 M3, IBM x3550 M4
- Fujitsu RX200 S6, Fujitsu RX200 S7

3.3 BIOS Settings

3.3.1 BIOS Password

Access to the BIOS allows changing the boot order of the server. Once changed an intruder may use tools that are bootable from CD-ROM or USB device that allow a user to change the administrator password or install files.

To prevent this from happening, the BIOS needs to be password protected.

NOTE: BIOS passwords should be set in accordance with company security policies.

Change the administrator password to access the BIOS according to the instructions in your server's documentation guides.

- IBM: http://www-947.ibm.com/support/entry/portal/Documentation
  - x3550 M3: Installation and User's Guide
  - x3550 M4: Installation and User’s Guide
- Fujitsu: http://ts.fujitsu.com/support/manuals.html - manuals are listed under Industry Standard Server products.
  - RX200 S6: D3031 BIOS Setup Utility (Reference Manual)
  - RX200 S7: D3032 BIOS Setup Utility for PRIMERGY RX200 S7 (Reference Manual)

CL-OSV-BIOS	**Use non-default BIOS password**
Measures	Change the administrator password to access the BIOS according to the instructions in your server's documentation guides.
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.3.2 Boot Order

CL-OSV-Boot-Order	Only boot from disk
Measures	On a non-virtual OSV, change boot order to only boot from disk.
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.4 Operating System Hardening

The OpenScape Voice V10 operates on a SuSE Linux Enterprise Server Version 12 (SLES 12) operating system.

3.4.1 Password Management

3.4.1.1 Password Protecting GRUB

By default the Linux boot loader configuration is password free. After system installation/upgrade the boot loader should be configured with a password in order to properly secure the OSV.

CL-OSV-GRUB-Password	Add Password for GRUB
Measures	Add a password for the GRUB boot loader. ***NOTE:*** This must be performed on all OSV nodes.
References	
Needed Access Rights	Root
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

How to set a password for GRUB:

1. Login as sysad via SSH and locally switch user to root.
2. Command line for setting up a fresh OSV boot_loader, according to installed loads and with current security active:
   `/unisphere/srx3000/srx/bin/install_bootloader.sh <`primary or secondary according to which load is active`> '/dev/sda' 2 3 12 'none' '' '/dev/sda'`
   Which load is active can be checked with `/unisphere/srx3000/srx/bin/sync8k -v invocation`.
3. Start grub and generate an md5sum value for your password using the grub tools as follows:

   ```
   root@grt910an1:[/]# grub2-mkpasswd-pbkdf2
   Password: **********
   Reenter password: **********
   PBKDF@ hash of your password is
   grub.pbkdf2.sha512.10000.9CA4611006FE96BC77A...
   ```

   (encrypted password is a place holder for the MD5 encrypted password).
4. Exit grub and edit the /boot/grub/menu.lst file:

   ```
   vi /boot/grub2/grub.cfg
   ```

5. Paste at the end of the file the password directive with the set superusers command as follows:

   ```
   set superusers="root"
   password_pbkdf2 root
   grub.pbkdf2.sha512.10000.9CA4611006FE96BC77A...
   ```

6. Save and close the file (:wq).
7. When trying to edit the grub settings you will be prompted for username and password.

8. Enter `root` and the password you typed during the `grub2-mkpasswd-pbkdf2` command. If the credentials are correct, you can edit the grub settings.

NOTE: The GRUB password protection instructions only protect the grub modification and the loading of custom linux images. It does not protect the actual boot process.

NOTE: Don’t use the standard SuSE script `grub2-mkconfig` for updating GRUB because it will damage the configuration.

3.4.1.2 Changing Predefined Passwords for Administrator Accounts

NOTE: The 'solid' user account does not carry a password and does not require a change of password because only the root user is permitted to login to the Solid account. Log in as the 'solid' user from user accounts other than the root account is not allowed and will receive an "incorrect password" response.

During the installation, all administrator accounts are created with default passwords which are generally known. These passwords must be changed upon deployment.

CL-OSV-Passwords-Admin-Accounts	Change Predefined Passwords for Administrator Accounts
Measures	Change default passwords for the following accounts: • "root" default account for the Linux Operating System • "srx" default account used by the OSV application related processes • "sysad" default account for System Administrators • "superad" default account for System Administrators with special rights • "hipatham" default account for HiPath Accounting Manager • "hipathcol default account for HiPath Collector • "cdr" default account used by the Call Detail Recording process on OSV • "secad" default account for System Security Administrators • "dbad" default for Database Administrators "webad" default for Web Server Administrator (for Simplex configurations only)
References	OSV V10 Service Manual: Installation and Upgrades, Installation Guide, Chapter “Installation” for additional information regarding passwords.
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

For an OpenScape Voice cluster, these passwords must be changed on each node individually.

Users "sysad", "superad", "secad", "dbad" and "webad" have **90** day expiry limits set on their passwords.

Login to the system as root and enter the following command:

```
root# passwd user
```

Passwords should be 15-36 characters long in accordance with the customer's password policy.

Affects on Other Products

The "srx" account is used by the OpenScape Voice Assistant to log in to OpenScape Voice and therefore, the new password needs to be entered on the Common Management Platform (CMP) as well.

To do this, login to the Common Management Platform (CMP) and navigate to:

Configuration > OpenScape Voice > Select Switch > Switches > Select Switch and Edit > Mark "**Enable Password(s)**", modify password(s) for "**srx**" and **Save**.

For other products like, e.g., billing services using the "cdr" account, logging in via SSH/SFTP using any of the accounts mentioned in the previous table would need to be changed as well.

3.4.1.3 Protection against Toll Fraud

Toll fraud is the unauthorized use of a phone system that causes considerable financial losses to a company. The actions listed in this section must be applied to protect against unauthorized access to the OpenScape Voice system.

Securing Mailboxes

The CLIP-No-Screening feature for one-number-services (ONS) can be used to spoof an internal number and make fraudulent high-cost long distance calls.

Attackers usually make short test calls during off-hours in their attempt to get access to the mailbox. These calls are a sign that the phone system is under attack.

Mailboxes which are able to establish outgoing calls pose an even higher risk to the system.

Follow the instructions below to secure the mailboxes of your OpenScape Voice system:

- Keep the number of unused mailboxes to a minimum.
- Frequently monitor any unused mailboxes.
- Do not use default passwords.
- Apply a strong password/PIN policy to all mailboxes.
- Update the passwords/PINs frequently.
- Keep all common Voice access numbers confidential.

These numbers include dialable numbers outside of the system, that provide remote access to the mailboxes.

- Allow only a small number of password attempts and lock the service/device/mailbox when this number is reached.
- Deploy a firewall.
- Grant minimum permissions possible.
- Perform software updates regularly, especially when security fixes are available.

3.4.1.4 Change Predefined Passwords for Application Accounts

Use the assistant to change the password of the solid database accounts.

CL-OSV-Passwords-Application-Accounts	**Change Predefined Passwords for Application Accounts**
Measures	Change default passwords for solid users: • "dba" • "rtp" "sym" (for **Simplex** configuration Applications only)
References	OSV V10 Service Manual: Installation and Upgrades, Installation Guide, Chapter: “Installation” for additional information regarding passwords.
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

These passwords can be changed via the OpenScape Voice Assistant as follows:

Login to the Common Management Platform (CMP) and navigate to:

Configuration > OpenScape Voice > Select switch > Administration > General Settings > Database

Use the assistant to change the password of the solid database accounts.

3.4.1.5 Change Default Password Policies for New Accounts

Attention:

In order to prevent a potential collision between customer defined user accounts and OSV system accounts it is necessary to observe the following account restrictions:

- The account names and IDs listed below are reserved for OSV system accounts
- The group names and IDs listed below are reserved for OSV system accounts

In the event a customer defined account conflicts with an OSV system account ID (or group ID) listed below then the following action should be taken:

- Remove (and/or redefine) the conflicting customer defined account.
- Remove (and/or redefine) the conflicting customer defined group.

The following tables summarize the reserved system accounts and groups for the Openscape Voice Server.

Account Name	Account ID
haldaemon	501
sym	502
cdr	1001
srx	1522
solid	5000
superad	10000
sysad	10001
secad	10010
dbad	10011
reserved	10012
webad	10013

Table 1 Reserved OSV System Account IDs

Group Name	Group ID
rtpgrp	911
reserved	912
sym	913
dba	3020
cdrusers	3021

Table 2 *Reserved OSV Group IDs*

Group Name	Group ID
seclog	10001
reserved	10002

Table 2 Reserved OSV Group IDs

Any questions should be addressed to your next level of support.

The customer's password policy has to be installed in case the customer creates new administrator accounts that are allowed to log in via SSH or SFTP.

CL-OSV-Passwords_New_Accounts	**Change Default Password Policies for New Accounts**
Measures	Ensure the customer's password policy has been applied to the system, preferably by using the /etc/pam.d mechanism.
References	
Needed Access Rights	Administrator
Executed	Yes No
Customer Comments and Reasons	

Additional Information for Settings

If the customer has no password policy, make sure that new user accounts have a minimum password length of 15 characters, a password history of no less than 5 and the character requirements defined.

To set the password history and minimum password length modify the "password:" line in the **/etc/security/pam_pwcheck.conf** configuration file as follows:

```
password:  minlen=15 maxlen= remember=5  use_cracklib
use_authtok use_first_pass
```

For minimum password length also modify /etc/login.defs as follows:

```
PASS_MIN_LEN 15
```

The default password age should be set to 60 days.

After 60 days, the user will be prompted to change his password. There is a 30 day grace period to do so before the account is locked.

To set the password age:

```
passwd -x 60 -w 14 -n 1 -i 30 <userid>
```

The default password character requirements are two Upper case letters, two Lower case, one Numeric character (two for a JITC system) and at least one special character (two for a JITC system). Also a limitation of three repeats for the same character class exists. For a JITC system there must be at least 15 characters.

To set the password minimum character requirements, minimum difference, and password retries modify the "password requisite" line in the:

/etc/security/common-password-pc configuration file:

```
password requisite pam_cracklib.so retry=3 difok=4
maxclassrepeat=3 minlen=8 dcredit=-1 ucredit=-2 lcredit=-2
ocredit=-1
```

3.4.2 Remote SSH Access and FIPS Compliance

Following an initial V10 installation the remote access configuration of the OpenScape server via SSH meets the industry standard of FIPS compliance. Following an upgrade, however, the previous customer SSH configuration is generally preserved in order to maintain backward compatibility. It is therefore possible that the remote SSH configuration is not in compliance with industry accepted security best practices.

There are three distinct SSH configuration scenarios that should be observed on the OpenScape Voice Server, as shown:

1. Backward compatible – previous SSH configuration, potentially weak
2. Standard profile - FIPS compatible, minimal vulnerability
3. Optimal profile – FIPS compliant, JITC (DoD) compliant (recommended)

Unify recommends configuring SSH remote access using the “Optimal” profile and relying on the “Standard” profile for backward compatibility, if at all possible. The following summarizes the recommended profiles based on the encryption ciphers and message authentication codes that are found in `/etc/ssh/sshd_config and /etc/ssh/ssh_config`

3.4.2.1 Standard SSH profile

Ciphers:

```
aes128-ctr
aes192-ctr
aes256-ctr
aes128-cbc
aes192-cbc
aes256-cbc
3des-cbc
```

MACs:
```
hmac-sha1
hmac-sha2-256
hmac-sha2-512
```

3.4.2.2 Optimal SSH profile

Ciphers:
```
aes128-ctr
aes192-ctr
aes256-ctr
```

MACs:
```
hmac-sha1
hmac-sha2-256
hmac-sha2-512
```

NOTE: FIPS compatibility requires the removal of weaker encryption options like “blowfish” and “arcfour”.

3.4.2.3 Modify SSH Configuration

1. Modify `/etc/ssh/sshd_config` and `/etc/ssh/ssh_config` configuration files to comply with one of the profiles above, by using a text editor to set the appropriate Ciphers and MACs entries in the files.
2. Restart ssh daemon
   `systemctl restart sshd`

3.4.3 Change Denial of Service (DoS) Thresholds

During the installation, a large amount of data must be transferred to and from the server from software servers and between nodes of the cluster, etc. In order not to impede this process, the threshold for detection of a denial of service attack has been intentionally set at 200,000 messages per second. After installation, this value should be reduced.

A default white list is automatically generated at startup, based on the following node.cfg entries: Each partner on the admin, signaling and billing interfaces, and snmp_servers.

CL-OSV-DoS_Thresholds	**Change DoS Thresholds**
Measures	Change the default packet rate that will trigger a denial of service lockout.
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

Denial of Service thresholds are provisionable from the CLI. The following are the defaults and provisionable ranges:

- Block Period: 1 to 2048 seconds, with default of 60 seconds.
- Rate Threshold: 1 to 256,000 packets per second, with a default of 200,000 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 an SBC or proxy can create heavier amounts of packet traffic and need to be taken into account when setting the rate threshold value and the “white list” of trusted hosts, which is the list of IP addresses that are exempt from the rate threshold limit.

After installation, and bring up is complete and verified, for normal operation of the OpenScape Voice system, Unify recommends the rate threshold value be set to 200 packets per second (CLI:6,1,1,6,3) for a clustered deployment and 2000 packets per second for an integrated simplex deployment. Use Option 2 to display the Rate Thresholds and option 1to modify the Rate Thresholds.

The administrator must take care that trusted servers are included in the “white list” of trusted hosts (CLI:6,1,1,6,2). Use option 3 to display a list of all trusted hosts.

The “white list” should include the IP addresses of:

- External administration servers, for example, external OpenScape Voice Assistant.
- Trusted high traffic servers, for example, media servers, PSTN gateways, session border controllers, SIP voice mail servers, peer SIP switches and proxies in the network.

- Billing servers, billing clients, license servers, and other servers which routinely transfer files to/from the OpenScape Voice system.

The OpenScape Voice IP addresses used for communication between the nodes of the OpenScape Voice cluster are automatically added to the “white list” during installation, and can also be added manually, if necessary.

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.

3.4.4 Allow IPsec Fragmentation

NOTE: Unify recommends using strong keys for IPsec.

If remote branch offices are connected to the data center by way of VPN or IPsec tunnel, the routers doing that may require an MTU lower than the default of 1500. This is most noticeable when SIP keysets are deployed at the remote branch offices, as they exchange large amounts of data in a message that normal endpoints would not transmit. Many customer routers that establish this tunnel use ICMP (type 3) packets to determine what the maximum packet size is that can be reliably transmitted. The firewall in the OpenScape Voice must be opened to respond to these kinds of ICMP packet challenges. If these (type 3) ICMP packets are being dropped, these settings will allow safely opening the firewall to permit the traffic.

CL-OSV-Allow IPsec Fragmentation	**Allow IPsec Fragmenatation**
Measures	Change default ICMP types to allow IPsec fragmentation between SIP endpoints (by way of VPN tunnel on remote router).
References	
Needed Access Rights	Administrator
Executed	Yes Ⓝ No Ⓝ
Customer Comments and Reasons	Ⓝ

Additional Information for Settings

To enable ICMP message type 3 on OpenScape Voice:

- Modify the ICMPDefaultTypes parameter string to include message type 3 (CLI: 1,1,3):

```
Configuration Parameters (methods):
browseParameterNames ...........1
getParameter....................2
modifyParameter ................3
Selection (default: 2): 3

modifyParameter:
name : hiQ/Security/Filt/ICMPDefaultTypes

modifying variable parameters:
current value: 0, 8
value <max length: 2047>: 0,3,8
input value was: "0,3,8"
Do you want to execute this action? (default: yes) :

executing method modifyParameter...
Ok.
```

- Restart the Security Manager on each node (CLI: 98):

```
CLI> procStopProcess "SecMgr1"
```

...wait a few seconds for it to shut down.

```
CLI> procStartConfiguredProcess "SecMgr1"
```

Menu commands are:

5…1…8 (to stop) and then 6 (to start)

- Create ICMP packet filter rule(s) for remote host, subnet, or all hosts (CLI: 6,8,3,1):

```
Packet Filter Rule Name <Max Length 63 (max length: 63)> (def: )
: SUBNET789_SIP1_FRAGMENT_ALLOWED
Description <Max Length 63 (max length: 63)> (def: ):
Allow ipsec fragmentation with remote SIP subnet
Remote FQDN <Max Length 63 (max length: 63)> (def: ):
Remote IP Address <Max Length 15 (max length: 15)> (def:):
<remote subnet for SIP endpoints>
Remote NetMask <Max Length 15 (max length: 15)> (def:
255.255.255.255) :
255.255.255.0
<remote subnet mask for SIP endpoints>
Transport Protocol <1=icmp, 2=udp, 3=tcp, 4=all, 5=esp, 6=ah,
7=sctp> (default: 4): 1
Direction <1=incoming, 2=outgoing, 3=bothways (default: 1): 1
Action <1 = Allow, 2 = Drop> (default: 1): 1
Do you want to execute this action <y/n> (default: yes):
Operation successful
```

3.4.5 Turn on IPsec Between Servers

NOTE: Unify recommends using strong keys for IPsec.

After the installation of all servers and connected devices and a functional test has been completed, ensure that you have defined IPsec policies and activated IPsec communication to any server that communicates over insecure protocols (such as SNMP, MGCP, CSTA).

CL-OSV-IPsec_Between_Servers	**Turn on IPsec Between Servers**
Measures	Verify that IPsec is used to encrypt all non-secure communication between the OpenScape Voice and its associated servers.
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

Add Secure Endpoints for all associated servers that appoint IPsec natively through their OS. Refer to the *OSV V10 Service Manual: Installation and Upgrade*s, section *IPSec Configuration,* for additional information.

Refer to the guidelines from those associated servers as to how to configure IPsec on their side. Typically, this is done at an OS level. The OS supplier usually provides guidelines as to how to configure IPsec for their products.

Use IPsec for the following servers:

- Media Servers (to protect the MGCP protocol). This includes an OpenScape Branch deploying an on-board media server.
- OpenScape UC Servers (to protect the CSTA protocol).
- Transfer of logging files.
- Common Management Platform server (to protect SNMP traffic).

Affects on Other Products

The IPsec credentials must be entered on the peer server as well.

NOTE: OpenScape Voice uses "strongSwan" to establish IPsec connections. From V9R1 onwards, OSV platform supports IKE version 2 as well. Until then IPSec capabilities were provided through the “ipsec-tools” package, known as “raccoon”. With this enhancement the following are supported as well: IKE version 2, PFS group 14 (2048 bit) and Hmac SHA512.

3.4.6 Transport Layer Security (TLS) Certificates

3.4.6.1 Change the Default TLS Certificates

OpenScape Voice comes with a default self-signed TLS Server Certificate. Even when not integrated in a PKI infrastructure, the default TLS certificate of OSV should be replaced with a new TLS certificate.

CL-OSV-TLS_Certificates	**Change the Default TLS Certificates**
Measures	Create new root and server certificates for the OpenScape Voice solution.
References	Refer to the following manual: *OpenScape Solution Set V10 Certificate Management and Transport Layer Security (TLS) Administration Guide*
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

Creating your own root certificate means that the root CA certificate must be installed in the trusted Root CA store of all products that need to establish a TLS connection to OpenScape Voice. This includes, but is not limited to:

- Phones
- Proxies
- Gateways
- Voice Mail Servers, etc.

3.4.6.2 Enable Certificate Expiration Verification

OpenScape Voice supports alarming the pending expiration of certificates. Because of TLS Session Renegotiation, TLS connections for which the certificate expires after a connection was set up, will be terminated as soon as the TLS session is renegotiated. It is therefore important not to ignore these certificate expiration warnings. The monitored certificates can be viewed in the Common Management Platform (CMP) by logging in and navigating to:

Configuration > OpenScape Voice > Administration > Certificate Management > Certificate Monitoring

CL-OSV-Enable-TLS-Certificate-Expiration	**TLS Certificate Expiration**
Measures	Enable TLS Certificate Expiration Monitoring by logging in to the CMP, navigating to: **Configuration > OpenScape Voice > Administration > Certificate Management > General Settings** Ensure that the Certificate Store points to the directory or directories which have certificates that need to be monitored. and that there is sufficient warning time (e.g. 60 days for first warning and re-issue the warning every week).
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.4.6.3 Review Certificate Revocation List Settings

OpenScape Voice supports verification of revocation status of received certificates by downloading the Certificate Revocation Lists (http only) of the certificate issuers. This feature should be turned on in order to ensure that OpenScape Voice does not accept TLS connection requests from products that have configured a certificate which was revoked by the certificate's issuer.

CL-OSV-Review-CRL-Settings	**Review CRL Settings**
Measures	Review TLS Certificate Revocation List download settings by logging in to the CMP, navigating to: **Configuration > OpenScape Voice > Administration > Certificate Management > General Settings** The CRL store should point to /usr/local/ssl/crls. Ensure also that CRL updates are downloaded frequently enough.
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.4.6.4 Certificate Verification Configuration Level Definitions for Unattended Mode

The Certificate Verification Process supports 3 levels of certificate verification in all Unify products that perform unattended certificate verification for TLS. OSV supports these three levels as a configuration option with the values “None”, “Trusted” and “Full” as described below.

IMPORTANT: It is strongly recommended that the default self-signed TLS server certificate is replaced with a new TLS server certificate and that the certificate verification level be set to either “Trusted” or “Full”.

The configuration options are:

- **None** - No authentication of the remote entity is performed. The remote entity is not checked at all or any potential errors during the check are ignored. This is the default setting since both Trusted and Full require administrative steps by configuring the associated CA certificate(s).
- **Trusted** - the certificate (including certificate chain) provided by the remote entity is checked:
  - for integrity
    * The certificate is signed with a commonly known and cryptographically strong hash algorithm (to prevent from unintentional acceptance of forged/fake certificates or fingerprints) including SHA-1, SHA-256, SHA-384, SHA-512 and excluding MD5 or earlier MD variants (MD4, MD2)
    * Gereral Security Requirements for State-of-the-Art Cryptographic Hash Functions apply.

    NOTE: Acceptance of SHA-1 is deprecated; products may also no longer accept SHA-1 certificates in case their validity goes beyond January 2017 (a date which is in sync with e.g. Google's or Microsoft's plans); detailed phase-out requirements for the acceptance of SHA-1 certificates is still to be determined.

  - that it is trusted:
    * The chain of trust for the digital signature provided by the remote entity ends up in one of the (root) CA-certificates, which are pre-configured for that interface on the product.
  - that all certificates in the chain are not expired (i.e. current date/time is within the certificate's given validity period)
  - that none of the certificates in the chain is revoked.

    NOTE: Revocation checks are done using OCSP (Online Certificate Status Protocol) or are based on CRL (Certificate Revocation Lists). They are controlled via independent configuration items and apply to both Full and Trusted mode.

- **Full** - the certificate (including certificate chain) provided by the remote entity is checked against the same criteria as in Trusted mode, plus:
  - Identity check - verify the end entity's identity (this check should be configurable and 'on' by default

- Check the correct use of all critical extensions (e.g. Basic constraints, Key Usage, Extended Key Usage). If an extension is marked critical and is not recognized, the certificate must be rejected.
- Check the correct use of known extensions not marked as critical (e.g. Basic constraints, Key Usage, Extended Key Usage)

3.4.6.5 Enable TLSv1.2 Perfect Forward Secrecy (PFS)

If perfect forward secrecy is required, the OSV supported cipher suites should be restricted to TLS V1.2 ciphers only and ephemeral Diffie-Hellman keys (DHE or EDH), such as ECDHE (elliptic curve) and DHE (RSA).

However DHE (based on finite fields) should not be used because of the LogJam vulnerability. Also, ECDHE is faster than DHE.

For OpenScape Voice the supported cipher suites are configured via the RTP parameters:

```
SSL/MutualAuth/Client/SupportedCiphers
SSL/MutualAuth/Server/SupportedCiphers
SSL/CSTAMutualAuth/Server/SupportedCiphers
SSL/EndPoint/Server/SupportedCiphers
SSL/Soap/Server/SupportedCiphers
```

(See the OpenSSL man page for www.openssl.org/docs/ssl/SSL_CTX_set_cipher_list.html, SSL_set_cipher_list and www.openssl.org/docs/apps/ciphers.html for further information).

The default value of the SupportedCiphers RTP parameters (colon separated list of ciphers) is:

```
EECDH+ECDSA+AES128:
EECDH+AES128:
ECDH+AES128:
EECDH+ECDSA+AES256:
EECDH+AES256:
TLSv1.2+FIPS:
kRSA+FIPS:
!eNULL:
!aNULL:
!DSS:
!EDH
```

Which results in the following list of cipher suites:

```
ECDHE-ECDSA-AES128-GCM-SHA256:
ECDHE-ECDSA-AES128-SHA256:
ECDHE-ECDSA-AES128-SHA:
ECDHE-RSA-AES128-GCM-SHA256:
```

```
ECDHE-RSA-AES128-SHA256:
ECDHE-RSA-AES128-SHA:
ECDH-RSA-AES128-GCM-SHA256:
ECDH-ECDSA-AES128-GCM-SHA256:
ECDH-RSA-AES128-SHA256:
ECDH-ECDSA-AES128-SHA256:
ECDH-RSA-AES128-SHA:
ECDH-ECDSA-AES128-SHA:
ECDHE-ECDSA-AES256-GCM-SHA384:
ECDHE-ECDSA-AES256-SHA384:
ECDHE-ECDSA-AES256-SHA:
ECDHE-RSA-AES256-GCM-SHA384:
ECDHE-RSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA:
ECDH-RSA-AES256-GCM-SHA384:
ECDH-ECDSA-AES256-GCM-SHA384:
ECDH-RSA-AES256-SHA384:
ECDH-ECDSA-AES256-SHA384:
AES256-GCM-SHA384:
AES256-SHA256:
AES128-GCM-SHA256:AES128-SHA256:
AES256-SHA:
AES128-SHA:DES-CBC3-SHA
```

CL-OSV-TLSV1.2	**Set the minimum TLS version to TLSV1.2**
Measures	Set RTP parameter value of SSL/TLSVersion to TLSV1.2 ***NOTE:*** This is already the default value for new installations.
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

CL-OSV-No-DHE	**Disable DHE ciphers**
Measures	Add !DHE to the value of the RTP parameters: SSL/MutualAuth/Client/SupportedCiphers SSL/MutualAuth/Server/SupportedCiphers SSL/CSTAMutualAuth/Server/SupportedCiphers SSL/EndPoint/Server/SupportedCiphers SSL/Soap/Server/SupportedCiphers
References	
Needed Access Rights	Administrator
Executed	Yes ☐ No ☐
Customer Comments and Reasons	☐

CL-OSV-pFS	**Only allow pFS cipher suites**

Measures	To only use perfect forward secrecy, use ECDHE or DHE. But since DHE should be disabled (see above), use ECDHE only.
	E.g. if the supported ciphers list is (PFS + fallback to non-PFS; GCM; AES-256):
	`ECDHE-ECDSA-AES256-GCM-SHA384:`
	`ECDHE-RSA-AES256-GCM-SHA384:`
	`ECDH-ECDSA-AES256-GCM-SHA384:`
	`ECDH-RSA-AES256-GCM-SHA384:`
	`AES256-GCM-SHA384`
	only keep the lines with ephemeral DH, i.e. remove the last 3 lines by setting the RTP parameter value (see previous measure) to:
	`ECDHE-ECDSA-AES256-GCM-SHA384:`
	`ECDHE-RSA-AES256-GCM-SHA384`

References	
Needed Access Rights	Administrator
Executed	Yes ☐ No ☐
Customer Comments and Reasons	☐

NOTE: The Elliptical Curve for ECDHE cipher suits can be configured with the RTP parameter `SSL/XX/XX/ECparam`. Default is `secp256r1`. (another supported value is secp384r1)

with

```
XX/XX =
MutualAuth/Client
MutualAuthServer
CSTAMutualAuth/Server
EndPoint/ServerSoap/Server
```

NOTE: If DHE (and EDH) is removed (see 2nd last measure) there is no need to configure the RTP parameters:
`SSL/XX/XX/SupportedDH`
`SSL/XX/XX/DHPath`

with

```
XX/XX =
Soap/Server
MutualAuth/Client
MutualAuthServer
CSTAMutualAuth/Server
EndPoint/Server
```

3.4.7 Baseline Information

This section contains baseline information for the SUID files and the SGID files on the OSV system.

3.4.7.1 Set User-ID (SUID) / Set Group ID (SGID) Files

This section contains all the files with SUID/SGID permissions on the OSV. This also includes the Symphonia and Media Server files as well.

If desirable, this can be used by System Administrators for baseline verification of all the SUID/SGID files on the OSV system. No action needs to be taken.

OSV Applications
/usr/bin/hiQIDS
/usr/bin/rcp.orig
/usr/bin/rsh.orig
/usr/local/bin/DNMP
/usr/local/bin/NRF
/usr/local/bin/SecMgr
/usr/local/bin/XcmSnd
/usr/local/bin/execRtp
/usr/local/bin/oplog_dload
/usr/local/bin/oplog_install
/usr/local/bin/oprtt_install
/usr/local/bin/oprtt_priocntl
/usr/local/bin/pcm_rb
/usr/local/bin/psr
/usr/local/bin/soaSF
/usr/local/bin/soapServer
/usr/local/bin/sptToolLaunch
/usr/local/bin/srxctrl_rid
/usr/local/bin/submgtSchedule
/usr/local/bin/sudo
/usr/local/bin/ttud
/usr/local/bin/userFaillog
/usr/local/bin/visudo
/usr/local/bin/RtpAudGetFileSize
/usr/local/bin/RtpAudGetProcSize
/usr/local/bin/RtpExecv
/usr/local/bin/RtpLogSolid
/usr/local/bin/RtpNetSnmp
/usr/local/bin/RtpSecEvtCheck.bin
/usr/local/bin/RtpSecEvtRotate.bin
/usr/local/bin/RtpSnmpCheck
/usr/local/bin/RtpSolid
/usr/local/bin/RtpSolidAcc
/usr/local/bin/RtpSolidAccess
/usr/local/bin/RtpSolidUserAdm
/usr/local/bin/SrxSecEvtFilter
/usr/local/bin/nativeMgcpUnit

OSV Applications
/usr/local/bin/nativeRTPunit
/usr/local/bin/fe_client
/usr/local/bin/fe_ctl
/usr/local/bin/ttudDaemon
/usr/local/bin/rdmount
/usr/local/bin/rdumount
/enterprise/mediaserver/application_host/bin/nativeRTPunit-x86
/enterprise/mediaserver/application_host/bin/nativeRTPunit-x86_64
/enterprise/mediaserver/application_host/bin/nativeMgcpUnit
/enterprise/mediaserver/application_host/bin/nativeRTPunit

Linux Distribution
/bin/mount
/bin/ping6
/bin/ping
/bin/su
/bin/umount
/usr/bin/at
/usr/bin/chage
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/crontab
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/opiepasswd
/usr/bin/opiesu
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/vlock
/usr/bin/wall
/usr/bin/write
/usr/sbin/getbulk
/usr/sbin/getmany
/usr/sbin/getnext
/usr/sbin/getone
/usr/sbin/gettab
/usr/sbin/inform

Table 3 Linux Expected SUID/SGID executables

Linux Distribution
/usr/sbin/mgrtool
/usr/sbin/postdrop
/usr/sbin/postqueue
/usr/sbin/trapsend
/usr/sbin/utempter
/usr/sbin/zypp-refresh-wrapper
/sbin/arping6
/sbin/mount.nfs
/sbin/unix_chkpwd
/sbin/unix2_chkpwd
/usr/lib/PolicyKit/polkit-explicit-grant-helper
/usr/lib/PolicyKit/polkit-grant-helper-pam
/usr/lib/PolicyKit/polkit-read-auth-helper
/usr/lib/PolicyKit/polkit-revoke-helper

Table 3 Linux Expected SUID/SGID executables

3.4.8 Remote Syslog

OpenScape Voice supports remote syslog logging, where a subset of syslog log records is sent to an external server. This prevents attackers from hiding their tracks, by deleting or modifying log records on OpenScape Voice.

CL-OSV-Syslog	Configure Remote Syslog
Measures	Use the script `loghost_configuration.pl -Help` to configure remote syslog, if needed.
References	
Needed Access Rights	Root
Executed	Yes  No 
Customer Comments and Reasons	

3.4.9 IPv6

OpenScape Voice supports IPv6 messages for SIP and MGCP signaling messages and for some OAMP functions. IPv6 creates new vulnerabilities that need to be addressed.

CL-OSV-IPv6	IPv6 Hardening
Measures	• Disable IPv6 stack on Ethernet ports where not used. • Disable autoconfiguration (stateless and statefull). • If during Path MTU Discovery a "Packet Too Big" message is received requesting a next-hop MTU that is less than the IPv6 minimum link MTU, then the product shall ignore the request for the smaller MTU and shall include a fragment header in the packet. • Don't use Flow Label. • Don't use DHCP. • Don't set overwrite flag in the neighbor advertisement message. • When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache does not contain the target's entry, the advertisement shall be silently discarded. • When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache entry is in the INCOMPLETE state when the advertisement is received and the link layer has addresses and no target link-layer option is included, the product shall silently discard the received advertisement. • When address resolution fails on a neighboring address, the entry shall be deleted from the product's neighbor cache. • Disable redirect function. • Disable router advertisement. • The product shall have a configurable rate-limiting parameter for rate limiting the ICMP error messages it originates. The following items are from https://www.suse.com/documentation/sles-12/singlehtml/book_hardening/book_hardening.html: • Disable IP source routing. • Disable ICMP Redirect Acceptance.

CL-OSV-IPv6	**IPv6 Hardening**
References	
Needed Access Rights	Root
Executed	Yes  No 
Customer Comments and Reasons	

3.5 Securing the Administrative Interface

3.5.1 Administration via SNMP

The SNMP interface is used to support Alarm Notification (traps), Alarm Management and Performance Monitoring (statistics) by third party surveillance systems.

OSV supports SNMPv1 and SNMPv2c for SNMP Set and Get operations and supports SNMPv1, SNMPv2c and the more secure SNMPv3 for sending traps.

3.5.1.1 SNMP Community String

SNMPv1 and SNMPv2c use the notion of communities to establish trust between managers and agents. Community strings are essentially passwords. A community string allows a level of access to Management Information Base (MIB) data. Access levels are read-only (RO) for data retrieval and read-write (RW) for data modification. Thus an SNMP Manager requires at least two community strings or passwords.

CL-OSV-SNMP_Community_String	**Change SNMP Community String**
Measures	Change default values for RO and RW community strings.
References	Refer to the OSV IUG, sections titled: • “SNMP Community Names on OpenScape Voice” • “Changing the Community String for the Emanate Master Agent” Navigate to menu 6 > 1 > 9 > 2 to display the SNMP configuration for verification purposes
Needed Access Rights	Root

CL-OSV-SNMP_Community_String	Change SNMP Community String
Executed	Yes No
Customer Comments and Reasons	

Additional Information for Settings

The OpenScape Voice sets by default the RO community name to "SENread" and the RW community name to "SENsnmp". It is very important to change these default values at the time of installation as they could be well known to the general public.

The OpenScape Voice provides the capability to modify the SNMP RO and RW community names via the CLI (CLI: 6,1,9). Use Option 1 to display the current SNMP configuration and Option 2 to modify the SNMP configuration.

NOTE: V1 and V2 of the SNMP protocol sends the community names in clear text. To prevent sniffing the community name, the interface between the SNMP agent and the SNMP server needs to be secured via IPsec.

Affects on Other Products

Any server (with exception of the Survival Authority) using SNMP to retrieve information from OpenScape Voice or to set information in OpenScape Voice has to also change the read and write community names.

SNMP Community Names on OpenScape Voice V9

NOTE: Avoid using any UNIX special characters (e.g., ampersand (&), semi colon (;), etc.) when changing the SNMP community string as these characters may cause translation errors.

NOTE: To change the SNMP community name string to meet site security requirements, it is *strongly recommended* that you contact your next level of support before attempting the following procedures.

Changing the Community String for the Emanate Master Agent

In V5 (and later releases), you may change community strings with the use of Cli. In order to use startCli, follow the procedure below:

1. Login to CLI as: **sysad**

   Node1:/home/sysad (62> **startCli**

2. Navigate to menu 6 > 1 > 9 > 2

3. Change the read-only/read-write community strings as shown below:

```
SNMP Management (methods):
        Display SNMP Configuration.....................1
        Modify SNMP Configuration......................2
        Return.................................99
        Selection (default: 1): 2
        *** Modify SNMP community String ***
        Enter Read-only SNMP community String: <Any ASCII
string (max length: 64)> (default: SENread):
        Enter Read-write SNMP community String: <Any ASCII
string (max length: 64)> (default: SENSnmp):
        Do you want to execute this action? <y/n> (default:
yes):
        Checking connection with grd404n1.
        Checking connection with grd404n2.
        Backing up original configuration file.
        Copying new configuration file to grd404n1.
        Copying new configuration file to grd404n2.
        Please wait. Applying new configuration on grd404n1.
        Please wait. Applying new configuration on grd404n2.
        Validating new configuration
        Done.
```

4. Navigate to menu 6 > 1 > 9 > 2 to display the SNMP configuration for verification purposes.

3.5.1.2 Configure Secure SNMP Trap Destinations

OSV supports sending SNMP Traps via SNMPv2c or SNMPv3 with the latter being the more superior from a security perspective.

The protocol can be configured on a per trap destination basis via the CMP.

CL-OSV-SNMP_Trap_Destinations	**Secure SNMP Trap Destinations**
Measures	Configure the security settings for each trap destination by logging in to the CMP, navigating to: **Configuration > OpenScape Voice > Administration > General Settings > EZIP > Servers** Enter the security settings for each trap destination server. Use the more secure version v3 with preference if supported by the remote trap receiver. Otherwise, use version v2c. When using version v2c, enter the community String expected by the trap receiver in the Security Name field. Avoid having to use the default string 'public'. When using version v3, enter the Security Name, Security Level, Auth Protocol, Privacy Type and passwords. Avoid having to use the default Security Name SNMPv3User. Also SHA is preferred for authentication and AES is preferred as privacy type. A setting of **NoAuthNoPriv** is basically a non-secure setting equivalent to using SNMPv2c.
References	
Needed Access Rights	Root
Executed	Yes  No 
Customer Comments and Reasons	

3.5.2 Administration via SOAP

The OpenScape Voice allows configuration changes to be made via the SOAP interface. SOAP Applications should use one of two mechanisms to secure this interface:

- Secure the connection between the SOAP client and the SOAP server via IPsec. This allows connecting to the TCP SOAP server ports.

- Secure the connection between the SOAP client and the SOAP server by connecting to the TLS SOAP server ports.

NOTE: The OpenScape Voice firewall must be opened to allow SOAP clients other than the Assistant to connect.

NOTE: TLS V1.2 with fallback to TLS V1.0 is supported for SOAP.

3.5.2.1 Configure TLS

SOAP Clients that support Mutual TLS (i.e. possess a TLS Certificate usable for TLS Client Authentication) should connect to OpenScape Voice via Mutual TLS.

CL-OSV-Secure_SOAP_Signaling_via_TLS	**Secure SOAP Signaling via TLS**
Measures	Secure SOAP Clients that support establishing TLS connections with TLS.
References	*OSV V10 Service Manual: Installation and Upgrades*
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

To verify the starting port for SOAP TLS, login to the Common Management Platform (CMP) and navigate to:

Configuration > OpenScape Voice > Administration > General Settings > RTP

Verify that the value of the RTP parameter `Srx/Subp/StartingPortWithTLS` is set to a valid port number and that `Srx/Subp/NumberOfInstancesWithTLS` is set to an appropriate value (usually 1).

The default secure server ports are 8757 to 8760.

When changing any of the above RTP parameters, the SoapServer process on each node needs to be restarted (CLI: 98)

CLI> **procStopProcess "soapServer01"**

...wait a few seconds for it to shut down.

CLI> **procStartConfiguredProcess "soapServer01"**

In a duplex configuration also:

CLI> **procStopProcess "soapServer02"**

...wait a few seconds for it to shut down.

CLI> **procStartConfiguredProcess "soapServer02"**

The menu commands are:

5…1…8 (to stop the process)

5…1…6 (to start the process))

3.5.2.2 Enable TLS Certificate Validation

Using TLS becomes really meaningful, only when the certificates that are received from partners are screened for content. Verification of received certificates is normally done by a person inspecting the certificates received from a web-site. Browsers help in this matter by warning if certificates are not fulfilling standard verification procedures. With the Mutual TLS connections established between the OSV and other TLS Clients/Servers which present TLS Certificates to it, this kind of attended certificate verification is not possible. Proper rules need to be set up in OSV in order to provide what is called an Unattended Certificate Verification.

CL-OSV-Validate_TLS_for_SOAP_Server	**Activate certificate validation for all TLS SOAP server ports**
Measures	Set the Certificate Validation Level to Full (or at least Trusted) by logging in to the CMP, navigating to: **Configuration > OpenScape Voice > Administration > General Settings > SOAP/XML Client > TLS Settings** See referenced guide on information whether to set the Level to Full or Trusted.
References	*OpenScape Solution Set V10 Certificate Management and Transport Layer Security (TLS) Administration Guide*
Needed Access Rights	Administrator

CL-OSV-Validate_TLS_for_SOAP_Server	**Activate certificate validation for all TLS SOAP server ports**
Executed	Yes No
Customer Comments and Reasons	

3.5.2.3 Enable Certificate Revocation List Checking

OpenScape Voice supports verification of certificates by downloading the Certificate Revocation Lists (http only) of the certificate issuers. This feature should be turned on in order to ensure that OpenScape Voice does not accept TLS connection requests from products that have configured a certificate which was revoked by the certificate's issuer.

NOTE: CRL Checking applies to the Trusted and Full Certificate Validation Levels.

CL-OSV-Check_CRL_for_SOAP_Server	**Enable CRL Checking for certificates received on TLS SOAP Server ports**
Measures	Check the Enable CRL Checking box by logging in to the Common Management Platform (CMP), navigating to: **Configuration > OpenScape Voice > Administration > General Settings > SOAP/XML Client > TLS Settings**
References	*OpenScape Solution Set V10 Certificate Management and Transport Layer Security (TLS) Administration Guide*
Needed Access Rights	Administrator
Executed	Yes No
Customer Comments and Reasons	

3.5.2.4 Enable Certificate Identity Checking

OpenScape Voice supports verifying the identity of the TLS peer in a mutually authenticated TLS connection. This is called identity checking and it involves verifying that the information in the Subject Alternative Name or Common Name field of the received certificate matches the IP address of the TLS peer or translates to the IP address of the TLS peer after DNS resolution in case these fields contained an FQDN.

NOTE: Identity Checking only applies to the Full Certificate Validation Level.

CL-OSV-Enable_Identity_Checking	**Enable Certificate Identity Checking**
Measures	Check the Enable Identity Checking box by logging in to the Common Management Platform (CMP), navigating to: **Configuration > OpenScape Voice > Administration > General Settings > SOAP/XML Client > TLS Settings**
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.5.2.5 Configure IPSec if TLS is not Supported by a SOAP Client

SOAP Clients that do **not** support TLS can connect to OpenScape Voice via TCP with a secure IPsec connection. The unsecure SOAP Server ports are 8767-8770.

CL-OSV-Secure_SOAP_Signaling_via_IPsec	**Secure SOAP Signaling via IPsec**
Measures	Secure TCP SOAP Clients (such as the Common Management Platform) with IPsec. ***NOTE:*** The communication between the OpenScape Voice Server and the Common Management Platform can also be secured using TLS.
References	*V10*
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

The ports can be checked using the CLI or the Display of Rtp parameters using the OpenScape Voice Assistant:

- Srx/Subp/Port for the first available port
- Srx/Subp/NumberOfInstances for the number of available ports

When changing any of the above RTP parameters the soapserver process on each node needs to be stopped and started. Expert Cli examples follow:

CLI> **procStopProcess "soapServer01"**

...wait a few seconds for it to shut down.

CLI> **procStartConfiguredProcess "soapServer01"**

In a duplex configuration, be sure to restart the process in node2. Expert Cli examples follow;

CLI> **procStopProcess "soapServer02"**

...wait a few seconds for it to shut down.

CLI> **procStartConfiguredProcess "soapServer02"**

From the Cli Menu, make the following selections:

5…1…8 (to stop the process)

5…1…6 (to start the process)

Additional Information for Settings

Refer to Section 3.4.5, “Turn on IPsec Between Servers”, on page 28.

3.5.2.6 Adding Authorization to SOAP

The SOAP server must be set up to authorize SOAP clients for limited access to the SOAP server. Before activating this authorization mechanism, verify that the IP address of the application with Super Administrator rights is entered.

If that IP address is not entered, OSV will effectively block all SOAP access once authorization is enabled, because at the point of activation of Authorization, no clients are configured yet. The OSV Assistant should be the application with Super Administrator rights, so first ensure that your current working Common Management Platform's IP address is entered as the IP Address of the application with Super Administrator rights.

CL-OSV-Verify_Super_Administrator	**Verify that the IP Address of the SOAP Application with Super Administrator Rights is set**
Measures	Verify the correct IP address is entered in the RTP parameter Srx/Subp/SuperUserIpAddress by logging in to the Common Managemente Platform (CMP), navigating to: **Configuration > OpenScape Voice > Administration > General Settings > RTP**
References	OpenScape Voice V10, Administrator Manual, SOAP/XML Client Management
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

CL-OSV-Enable_SOAP_Authorization	**Enable SOAP Authorization checks**
Measures	Enable SOAP Authorization checks by logging in to the Common Management Portal (CMP), navigating to: **Configuration > OpenScape Voice > Administration > General Settings > RTP** Verify that the Value for the RTP Parameter `Srx/Subp/Authorization` is set to RtpTrue. Modify it if it is currently set to RtpFalse.
References	OpenScape Voice V10, Administrator Manual, SOAP/XML Client Management
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

After this, the SOAP APIs accessed by SOAP clients can be limited by defining the role played by an individual SOAP Client. It is possible to assign more than one role to a Client Profile. One or more of the following roles can be assigned to a SOAP client:

- Super Administrator (access to all APIs)
- System Administrator
- Network Administrator
- BG Administrator
- CAC Administrator
- Calea Administrator
- Executive Assistant Administrator

CL-OSV-Enable_Client_Roles	**Enable Client Roles**
Measures	Enable the OSV SOAP Server to verify which SOAP APIs a SOAP client is authorized to use by logging in to the CMP, navigating to: **Configuration > OpenScape Voice > Administration > General Settings > SOAP/XML Client > Clients** Set the Client Roles enabled checkbox.
References	OpenScape Voice V10, Administrator Manual, How to Activate SOAP/XML Clients
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Authorization can then be added for each SOAP client via the OpenScape Voice Assistant. SOAP clients are identified via their IP address.

CL-OSV-Add_Client_Profiles	**Add Client Profiles for all SOAP clients**
Measures	Add a client profile for each SOAP client except the Super Administrator defined in CL-OSV-Verify_Super_Administrator by logging in to the Common Management Platform (CMP), navigating to: **Configuration > OpenScape Voice > Administration > General Settings > SOAP/XML Client > Clients > Add...** Add IP address and role for the SOAP client. Allow Access and set the required transport type to TLS if the SOAP Client supports it.
References	OpenScape Voice V10, Administrator Manual, How to Activate SOAP/XML Clients
Needed Access Rights	Administrator

CL-OSV-Add_Client_Profiles	Add Client Profiles for all SOAP clients
Executed	Yes  No 
Customer Comments and Reasons	

3.5.2.7 Firewalling the SOAP Clients

By default, OpenScape Voice blocks all admin traffic via the firewall. To allow a SOAP client to connect, the firewall must be opened for the SOAP client.

NOTE: The firewall is already opened for all SOAP Clients which were added using the authorization mechanism (Section 3.5.2.6, “Adding Authorization to SOAP”).

CL-OSV-Firewalling_SOAP_Clients	Firewall the SOAP Clients
Measures	Open firewall for authorized SOAP Clients
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.6 Securing the Billing Interface

Billing files can be pushed or pulled, securely by OpenScape Voice to a billing server or from a billing client. The transfer of these files must be done using SFTP.

CL-OSV-Billing_Interface	Secure the Billing Interface
Measures	Turn on SFTP for pushing billing files to a billing server.
References	*OSV V10 Service Manual: Installation and Upgrades*
Needed Access Rights	Administrator

CL-OSV-Billing_Interface	Secure the Billing Interface
Executed	Yes No
Customer Comments and Reasons	

Additional Information for Settings

Turn on SFTP for pushing billing files to a billing server. When a billing client pulls billing files from OpenScape Voice, it must be configured to set up an SFTP session using the "cdr" account's credentials.

Login to the Common Management Platform (CMP) and navigate to:

Configuration > OpenScape Voice > Select switch > Administration > General Settings > CDR > General tab > Set the CDR Delivery Method to SPush > Enter username and password for Primary and possibly backup billing server > Save

3.7 Securing the IMM or iRMC Access

The Intel IMM card is used by the and IBM x3550 platforms for remote access. The iRMC card is used by the FTS RX200 platform for remote access.

CL-OSV-Secure_Remote_access	Securing IMM or iRMC Access
Measures	• Restrict IPMI to Internal Networks • Encrypt Traffic • Utilize Strong Passwords • Require Authentication • Deactivate Weak Ciphers for IMM
References	
Needed Access Rights	Administrator
Executed	Yes No
Customer Comments and Reasons	

3.8 Securing the Signaling Interface

3.8.1 Securing SIP Services - Securing SIP Signaling Manager on OSV

3.8.1.1 Enable Authentication Services

By default, Digest Authentication is not activated after installation. This allows a hacker to register a phone using the phone number of any subscriber, and thus fake their identity. This may be avoided by assigning a unique login, password, and realm to each subscriber.

CL-OSV-Clean-Authentication	**Enable Clean Authentication**
Measures	Turn on Clean Authentication for SIP signaling: Login to the Common Management Platform (CMP) and navigate to: **Configuration > OpenScape Voice > Administration > Signaling Management > Authentication > General** and check the Clean Authentication box.
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

Clean Authentication can also be provisioned from the CLI.

NOTE: With clean authentication the OSV identifies SIP endpoints only by contact header or bottom via header (and not top via header), i.e. the RTP parameter `Srx/Sip/AuthTraverseViaHdrs is RtpTrue`)

3.8.1.2 Activate Authentication of SIP Subscribers and SIP Endpoints behind Proxies and SBCs

OpenScape Voice has a system-wide setting with which SIP subscribers and SIP endpoints communicating with OpenScape Voice through a trusted SIP proxy are not authenticated, regardless of any configured digest authentication settings on the SIP Subscribers or SIP Endpoints. Configuring a SIP Proxy as a trusted entity (see Section 3.8.3.4, “Never Trust Proxies and SBCs”) is definitely not recommended. This system-wide setting is not a recommended setting either.

CL-OSV-Authentication_Behind_trusted_Endpoints	**Activate Authentication of SIP Subscribers and SIP Endpoints behind Trusted Endpoints**
Measures	Not needed in **OpenScape Voice**, if Clean Authentication is enabled (Section 3.8.1.1, “Enable Authentication Services”), the RTP parameter below is set correctly Enforce authentication of SIP Subscribers and SIP Endpoints behind SIP Proxies by logging in to the Common Management Portal (CMP) navigating to: **Configuration > OpenScape Voice > Administration > General Settings > RTP** Verify that the Value for the RTP Parameter `Srx/Sip/AuthTraverseViaHdrs` is set to RtpFalse. Modify it if it is currently set to RtpTrue.
References	*OSV V10 Service Manual: Installation and Upgrades*, chapter: “Activate Authentication of SIP Subscribers and SIP Endpoints behind Trusted Endpoints”
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

Authentication of SIP Subscribers and SIP Endpoints behind SIP Proxies and SBCs can also be done via the CLI.

3.8.1.3 Enable TLS Certificate Validation

Using TLS only becomes really meaningful when the certificates received from partners are screened for content. Verification of received certificates is normally done by a person inspecting the certificates received from a web-site. Browsers help in this matter by warning if certificates are not fulfilling standard verification procedures. With the Mutual TLS connections established between the OSV and other TLS Clients/Servers which present TLS Certificates to it, this kind of attended certificate verification is not possible. Proper rules need to be set up in OSV in order to provide what is called an Unattended Certificate Verification.

CL-OSV-Validate_TLS_for_SIP_Server	**Activate certificate validation for the Mutual TLS SIP server and client ports**
Measures	Set the Certificate Validation Level to Full (or at least Trusted) by logging in to the Common Management Platform (CMP), navigating to: **Configuration > OpenScape Voice > Administration > Signaling Management > TLS Settings > SIP** Different levels can be entered for the cases where OSV acts as TLS Server (OSV receives a request for a TLS session) or as TLS Client (OSV initiates the TLS session) for the Mutually authenticated TLS Session. See referenced guide on information whether to set the Level to Full or Trusted.
References	*OpenScape Solution Set V10 Certificate Management and Transport Layer Security (TLS) Administration Guide*
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.8.1.4 Enable Certificate Revocation List Checking

OpenScape Voice supports verification of certificates by downloading the Certificate Revocation Lists (http only) of the certificate issuers. This feature should be turned on in order to ensure that OpenScape Voice does not accept TLS connection requests from products that have configured a certificate which was revoked by the certificate's issuer.

NOTE: CRL Checking applies to the Trusted and Full Certificate Validation Levels.

CL-OSV-Check_CRL_for_SIP_Server	**Enable CRL Checking for certificates received on TLS SIP Server and client ports**
Measures	Check the Enable CRL Checking box by logging in to the Common Management Platform (CMP), navigating to: **Configuration > OpenScape Voice > Administration > Signaling Management > TLS Settings > SIP**
References	*OpenScape Solution Set V10 Certificate Management and Transport Layer Security (TLS) Administration Guide*
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.8.1.5 Enable TLS Identity Checking

OpenScape Voice supports verifying the SIP identity of the TLS peer in a mutually authenticated TLS connection. This is called SIP identity verification and it involves verifying that the information in the Common Name field of the received certificate matches one of the aliases configured on OpenScape Voice for the SIP endpoint representing the top-VIA header field of the received SIP request. In case of failure, a “403 Forbidden” is returned denying access to the OpenScape Voice for the request originator.

NOTE: SIP Identity Checking only applies to the Full Certificate Validation Level.

CL-OSV-Enable_Identity_Checking_for_SIP_Server	**Enable Certificate Identity Checking for certificates received on TLS SIP Server and client ports.**
Measures	Check the Enable Identity Checking box by logging in to the Common Management Platform (CMP), navigating to: **Configuration > OpenScape Voice > Administration > Signaling Management > TLS Settings > SIP**
References	*OSV V10 Service Manual: Installation and Upgrades*
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.8.2 Secure Configuration for SIP Subscribers

3.8.2.1 Activate MTLS for SIP Subscribers

Security Discussion:

Although phones are secured using Digest Password Authentication and TLS encrypted communications, no certificates are used for the phones.

MTLS offers to the switch the capability of requiring a valid device certificate to be deployed on the SIP Subscriber devices. This has to be seen in addition to the digest authentication which can be viewed more as a 'user' authentication,

I.e. the certificate authorizes the phone to connect to the OSV and the digest authentication authorizes the user (represented by his phone number) to register with the OSV and make calls through it.

CI-OSV-Sub-MTLS	**Configure SIP subscriber for TLS with mutual authentication**
Measures	Use the CMP set subscriber transport type to MTLS ***NOTE:*** The MTLS phones need to be configured with a valid certificate. If the phone is connected with the OSV via SBC, the SBC needs to be configured for subscriber MTLS, and if the phone is connected via OSB, the OSB needs to be configured for subscriber MTLS support
References	*OpenScape SBC V10, Administrator Documentation*
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.8.2.2 Activate TLS Signaling for SIP Subscribers

By default, SIP subscribers are generated using SIP signaling in clear-text via TCP or UDP. Signaling should be encrypted using TLS provided the SIP subscriber supports it.

NOTE: TLS V1.2 with fallback to TLS V1.0 is supported for SIP over TLS by default.

CL-OSV-TLS_Signaling_for_SIP_Subscribers	**Activate TLS Signaling for SIP Subscribers**
Measures	Set SIP Subscribers to TLS using the OpenScape Voice Assistant - branch offices and main office
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

The turn on TLS for SIP Signaling to the Subscribers setting can be controlled on a per subscriber basis.

To Set SIP Subscribers to TLS using the OpenScape Voice Assistant, login to the Common Management Platform (CMP) and navigate to:

Configuration > OpenScape Voice > Select switch > Business Group > Select Business Group > Select Branch Office > Members > Subscribers > Select Subscriber, click Edit > Connection tab > Set Transport Protocol to TLS > Save

3.8.2.3 Restrict/Allow registering and making calls via Central SBC

OpenScape Voice allows all configured SIP subscribers to register as a remote user via a centralized SBC (if they know the registrar address of the SBC and the DA parameters). This setting is not recommended.

The system administrator can control remote subscriber access to the OpenScape Voice via the "Registration via Central SBC Allowed' attribute/flag. See also Section 3.8.3.3, “Tell the OSV that a SIP Endpoint is a Central SBC”.

CL-OSV-SBC_Remote_Users	**Restrict/Allow registering and making calls via Central SBC**
Measures	Set the 'Registration via Central SBC Allowed' flag appropriately only for subscribers which are allowed to register remotely via the SBC by logging in to the Common Management Platform (CMP), navigating to: **Configuration > OpenScape Voice > Select switch > Business Group > Select Business Group > Select Branch Office > Members > Subscribers > Select Subscriber, click Edit > Connections tab > Check Registration via Central SBC Allowed > Save**
References	See below.
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

In order to control remote subscriber access via a Central SBC, the endpoint attribute 'Central SBC' MUST be set for those SIP endpoints that represent central SBCs. See also Section 3.8.3.3, “Tell the OSV that a SIP Endpoint is a Central SBC”.

3.8.2.4 Activate Digest Authentication to SIP Subscribers

CL-OSV-Activate_DA_For_SIP_Subscribers	**Activate Digest Authentication for SIP Subscribers**
Measures	Assign user name, individual password, and realm to each SIP subscriber using the customer's password policy. Login to the Common Management Platform (CMP) and navigate to: **Configuration > OpenScape Voice > Select switch > Business Group > Select Business Group > Select Branch Office > Members > Subscribers > Select Subscriber, click Edit > Security tab > Set Realm, User Name and Password > Save**
References	See below.
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.8.3 Secure Configuration for SIP Endpoints

3.8.3.1 Activate MTLS Signaling for SIP Endpoints

By default, SIP endpoints are generated using SIP signaling in clear-text via TCP or UDP. Signaling should be encrypted using mutual TLS provided the SIP endpoint supports it.

NOTE: It is recommended that you set the transport type for SIP endpoints that are configured with valid certificates to MTLS. This together with proper certificate checking allows OSV to prevent man-in-the-middle attacks on communication between 2 SIP endpoints by configuring the endpoints for TLS with mutual authentication.

NOTE: TLS V1.2 with fallback to TLS V1.0 is supported for SIP over TLS by default.

CL-OSV-MTLS_Signaling_for_SIP_Endpoints	**Activate MTLS Signaling for SIP Endpoints**
Measures	Turn Signaling to the Endpoints. This setting can be controlled on a per Endpoint basis.
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

Set SIP Endpoints to MTLS using the OpenScape Voice Assistant. Login to the Common Management Platform (CMP) and navigate to:

Configuration > OpenScape Voice > Select switch

Endpoints can be created in business groups and globally.

To set an endpoint in the business group to MTLS navigate to:

Business Group > Select Business Group > Select Branch Office > Members > Endpoints > Select Endpoint, click Edit > SIP tab > Set Transport Protocol to MTLS > Save

To set a global endpoint to MTLS navigate to:

Global Translation and Routing > Endpoint Management > Endpoints > Select Endpoint, click Edit > SIP tab > Set Transport Protocol to MTLS > Save

3.8.3.2 Activate Digest Authentication to SIP Endpoints

SIP Endpoints that are not secured via MTLS must be provisioned for digest authentication.

CL-OSV-Activate_DA_For_SIP_Endpoints	**Activate Digest Authentication for SIP Endpoints**
Measures	Activate Digest Authentication if the SIP Endpoint is not configured for Mutual Authenticated TLS.
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

Login to the Common Management Platform)CMP) and navigate to:

Configuration > OpenScape Voice > Select switch

Endpoints can be created in business groups and globally. To set digest authentication for an endpoint in the business group navigate to:

Business Group > Select Business Group > Select Branch Office > Members > Endpoints > Select Endpoint, click Edit > SIP tab / Security / Add … or Edit > Set Local and Remote Realm, User Name and Password > Save

NOTE: Local is used for challenges received from the peer endpoint and Remote is used for creating challenges towards the peer endpoint.

To set digest authentication for a global endpoint navigate to:

Global Translation and Routing > Endpoint Management >Endpoints > Select Endpoint, click Edit > SIP tab / Security / Add … or Edit > Set Local and Remote Realm, User Name and Password > Save

NOTE: Local is used for challenges received from the peer endpoint and Remote is used for creating challenges towards the peer endpoint.

3.8.3.3 Tell the OSV that a SIP Endpoint is a Central SBC

OpenScape Voice allows all configured SIP subscribers to register as a remote user via a centralized SBC (if they know the registrar address of the SBC and the DA parameters). This setting is not recommended.

In order to control remote subscriber access via a Central SBC, the endpoint attribute 'Central SBC' MUST be set for those SIP endpoints that represent central SBCs.

With this setting, the subscriber flag 'Registration via Central SBC Allowed' controls whether a subscriber is granted or disallowed access to the OpenScape Voice (see Section 3.8.2.3, “Restrict/Allow registering and making calls via Central SBC”).

CL-OSV-SBC_Remote_Users	**Tell the OSV that a SIP Endpoint is a Central SBC**
Measures	Check the "Central SBC" endpoint attribute by logging in to CMP, navigating to: • For the BG-related endpoints: **Configuration > OpenScape Voice > Select switch > Business Group > Select Business Group > Select Branch Office > Members > Endpoints > Select Endpoint, click Edit > Attributes tab > Check Central SBC > Save** • For the system-wide endpoints: **Configuration > OpenScape Voice > Select switch > Global Translation & Routing > Endpoint Management > Endpoints > Select Endpoint, click Edit > Attributes tab > Check Central SBC > Save**
References	
Needed Access Rights	Administrator

CL-OSV-SBC_Remote_Users	**Tell the OSV that a SIP Endpoint is a Central SBC**
Executed	Yes  No 
Customer Comments and Reasons	

3.8.3.4 Never Trust Proxies and SBCs

When configuring SIP Proxies and SBCs on OpenScape Voice (any Sip Endpoint which has the SIP Proxy endpoint attribute set), never set any of the ports of the SIP proxy or the SBC itself to Trusted. Trusted settings are only to be used for SIP endpoints which do not support digest authentication or which have mutually authenticated TLS connections (e.g. gateways, voice mail, SSPs on SBCs...).

IMPORTANT: Toll fraud attacks are possible when SIP Proxies or SBCs are set to Trusted.

CL-OSV-Do-Not-Trust-SIP-Proxies-And-SBCs	**Never set port(s) of SIP Endpoints which have the SIP Proxy endpoint attribute set (applies to proxies and SBCs) to Trusted.**
Measures	Verify that none of the SIP Endpoints which have the SIP Proxy endpoint attribute set (proxies and SBCs) have their port set to Trusted. Ports of remote endpoints on SBCs may have to be set to trusted if the SSP does not support digest authentication. However additional security measures must be considered on the SBC in order to protect against toll fraud.
References	*OSV V10 Administration Guide*, chapter: “How to Set Security Settings for Endpoints”
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

Trusted ports are configured in OpenScape Voice Assistant. Login to the Common Management Platform and navigate to:

Business Group > Members > Endpoints
or
Global Translation and Routing > Endpoint Management > Endpoints

For the SIP Endpoint representing a SIP Proxy or an SBC:

1. Select Endpoint by ticking the box in front of the Name
2. Click on the Edit button
3. Open the SIP tab on the SIP Endpoint dialog and navigate to the Security area.
4. Click Add/Edit to open the SIP Configuration dialog.
5. Verify that the Trusted Entity check box is not set and that no digest authentication credentials are entered.
6. Click OK

For all other SIP Endpoints:

If the SIP Endpoint supports digest authentication, don't mark it as a Trusted Entity - instead specify the local and remote digest authentication credentials:

1. Select Endpoint by ticking the box in front of the Name
2. Click on the Edit button
3. Open the SIP tab and navigate to the Security area.
4. Click Add/Edit to open the SIP Configuration dialog.
5. Verify that the Trusted Entity check box is not set.
6. Specify the local and remote digest authentication credentials.
7. Click OK.

If the SIP Endpoint does not support digest authentication, mark it as a Trusted Entity and specify the port(s) used by the trusted SIP Endpoint.

NOTE: You should never use the **All Ports Trusted** setting.

---

1. Select Endpoint by ticking the box in front of the Name
2. Click on the Edit button
3. Open the SIP tab and navigate to the Security area.
4. Click Add/Edit to open the SIP Configuration dialog.
5. Check the Trusted Entity check box.
6. Specify the port(s) used by the trusted SIP Endpoint.
7. Click OK.

3.8.3.5 Use Aliases with Ports

SBCs often are configured with a single core IP address with ports used to represent Remote Subscribers, Remote Endpoints and the port for the SBC itself. When configuring the SIP Endpoints on OpenScape Voice representing the remote endpoints and the SBC itself, never configure an alias with just the IP address.

It is recommended to use aliases with ports for all SIP endpoints – not just the SBC's. OpenScape Voice will accept messages from any port of the specified IP address if used as alias without port specification.

CL-OSV-Use-Aliases-With-Ports	**When configuring the alias(es) for a SIP Endpoint in OpenScape Voice, use IP addresses or FQDNs with port specification. Aliases are used to identify the sender of messages received by the OpenScape Voice. These messages are always sent from a specific port.**
Measures	Ensure that the aliases configured for OpenScape Voice SIP Endpoints have ports specified (even if they are the default port).
References	*OSV V10 Administration Guide*, chapter: "Aliases"
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

Aliases are specified in OpenScape Voice Assistant. Login to the Common Management Platform (CMP) and navigate to:

Business Group > Members > Endpoints > Add or Edit > Aliases;
or
Global Translation and Routing > Endpoint Management > Endpoints Add or Edit > Aliases

3.8.4 Securing MGCP Services

3.8.4.1 Securing Media Servers

Media Servers communicate via the MGCP protocol which only supports the UDP transport type.

CL-OSV-Media_Servers	**Securing Media Servers**
Measures	Secure Media Servers with IPsec.
References	*OSV V10 Service Manual: Installation and Upgrades*
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

Please refer to OSV Service Manual: Installation and Upgrades, Appendix titled, “Configuring IPSec for MGCP Connections.”

3.8.5 Securing CSTA Services

3.8.5.1 Enable TLS Certificate Validation

Using TLS becomes really meaningful, only when the certificates that are received from partners are screened for content. Verification of received certificates is normally done by a person inspecting the certificates received from a web-site. Browsers help in this matter by warning if certificates are not fulfilling standard verification procedures. With the Mutual TLS connections established between the OSV and other TLS Clients/Servers which present TLS Certificates to it, this kind of attended certificate verification is not possible. Proper rules need to be set up in OSV in order to provide what is called an Unattended Certificate Verification.

CL-OSV-Validate_TLS_for_CSTA_Server	**Activate certificate validation for all TLS CSTA Applications**
Measures	Set the Certificate Validation Level to Full (or at least Trusted) by logging in to the Common Management Platform, navigating to: **Configuration > OpenScape Voice > Administration > Signaling Management > TLS Settings > CSTA tab** See referenced guide on information whether to set the Level to Full or Trusted
References	*OpenScape Solution Set V10 Certificate Management and Transport Layer Security (TLS) Administration Guide*
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.8.5.2 Enable Certificate Revocation List Checking

OpenScape Voice supports verification of certificates by downloading the Certificate Revocation Lists (http only) of the certificate issuers. This feature should be turned on in order to ensure that OpenScape Voice does not accept TLS connection requests from products that have configured a certificate which was revoked by the certificate's issuer.

NOTE: CRL Checking applies to the Trusted and Full Certificate Validation Levels.

CL-OSV-Check_CRL_for_CSTA_Server	**Enable CRL Checking for certificates received from TLS CSTA Applications**
Measures	Check the Enable CRL Checking box by logging in to the Common Management Platform (CMP), navigating to: **Configuration > OpenScape Voice > Administration > Signaling Management > TLS Settings > CSTA tab**
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.8.5.3 Enable Certificate Identity Checking

OpenScape Voice supports verifying the identity of the TLS peer in a mutually authenticated TLS connection. This is called identity checking and it involves verifying that the information in the Subject Alternative Name or Common Name field of the received certificate matches the IP address of the TLS peer or translates to the IP address of the TLS peer after DNS resolution in case these fields contained an FQDN.

NOTE: Identity Checking only applies to the Full Certificate Validation Level.

CL-OSV-Enable_Identity_Checking	**Enable Certificate Identity Checking**
Measures	Check the Enable Identity Checking box by logging in to the Common Management Platform (CMP), navigating to: **Configuration > OpenScape Voice > Administration > Signaling Management > TLS Settings > CSTA tab**
References	*OpenScape Solution Set V10 Certificate Management and Transport Layer Security (TLS) Administration Guide*
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.8.5.4 Configure TLS on CSTA Clients

Configure a TLS client certificate on CSTA applications that support TLS with Mutual Authentication. The TLS Client certificate must be valid (Valid From, Valid To) and the Common Name or Subject Alternate Name must contain the IP address of the CSTA application. Refer to the CSTA client's documentation to find instructions on how to install the TLS certificate.

The Root CA that issues the TLS client certificate must be entered in the Trusted Root CA store on OpenScape Voice.

CL-OSV-Install_RooT_CA_for_CSTA_Application	**Install the Root CA for the certificate issued by a CSTA TLS Client in OSV's Trusted Root CA Store**
Measures	The Root CA certificate (in PEM format) needs to be appended to the trusted Root CA store for CSTA client certificates on OpenScape Voice. The location is stored in the RTP parameter SSL/CSTAMutualAuth/Server/CertificatesPath and the store itself is the file with name stored in the RTP parameter SSL/CSTAMutualAuth/Server/SupportedCertificates.
References	*OSV V10 Service Manual: Installation and Upgrades*, See section Configuring -OpenScape -Voice for IPSec-based CSTA Connections
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

NOTE: This will prevent a man-in-the middle attack and prevents eaves-dropping as the signalling traffic is encrypted.

Additional Information for Measures:

Via CLI (CLI: 1,1)

Use Option 2 to verify the value for RTP parameters:

`SSL/CSTAMutualAuth/Server/CertificatesPath`

`SSL/CSTAMutualAuth/Server/SupportedCertificates.`

then use SFTP to transfer the new Root CA certificate on the OSV and then use SSH to login to OSV and append the new ROOT CA to the appropriate file.

3.8.5.5 Configure IPSec if TLS is not Supported by a CSTA Application

CL-3	Securing the TCP CSTA Applications
Measures	Secure CSTA applications that only support TCP with IPSec.
References	OSV Service Manual: Installation and Upgrades, Appendix titled, “Configuring IPSec for CSTA Connections.”
Needed Access Rights	Administrator
Executed	Yes No
Customer Comments and Reasons	

3.8.5.6 Firewalling the CSTA Applications

By default, OpenScape Voice blocks all traffic to the CSTA TCP and TLS port via the firewall. To allow a CSTA application to connect, the firewall must be opened for the SOAP client.

CL-1	CSTA Application Access Control
Measures	The OpenScape Voice firewall must be configured to allow access to the CSTA Server TCP and/or TLS port from the IP address. Access to the CSTA Server TCP port should only be granted if the CSTA application does not support TLS with Mutual Authentication.
References	*OSV V10 Service Manual: Installation and Upgrades*
Needed Access Rights	Administrator
Executed	Yes No
Customer Comments and Reasons	

NOTE: *This will prevent access from unauthorized CSTA Applications.*

3.8.6 Restrict IPMI to Internal Networks

Restrict IPMI traffic to trusted internal networks. Traffic from IPMI (usually UDP port 623) should be restricted to a management VLAN segment with strong network controls. Scan for IPMI usage outside of the trusted network and monitor the trusted network for abnormal activity.

3.8.7 Change the Default Passwords for the IMM/ iRMC Card

By default, the IMM/iRMC card is shipped with well known and well documented default passwords.

CL-OSV-_Passwords_IMM/ iRMC	**Change the Default Passwords for the IMM/iRMC Card**
Measures	Change default passwords.
References	Refer to *OpenScape Voice V10 Service Manual: Installation and Upgrades*, section titled, “Changing the User ID and Password for the IMM/iRMC Account.”
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

Change the User ID and Password to the user name and password configured for the IMM/iRMC on the specified node. This must be complete for each node of the cluster.

IMPORTANT: : Failure to complete this update for each cluster configuration will result in Communication Failure alarms and could cause a failure event resulting in one of the nodes in the cluster being shutdown.

3.8.8 Deactivate Clear-Text Administration / Activate Encrypted Communication - RX200S6 Platforms

Overview

The iRMC User's Guide can be used as another reference for this procedure. To find the latest version of this document go to:

http://manuals.ts.fujitsu.com/

At this URL a '**Quick Access**' feature can be employed by entering irmc in the *Search by product* parameter field. This typically results in 'Integrated Remote Management Controller (iRMC)' being displayed for selection.

After selecting 'Integrated Remote Management Controller (iRMC)' click the arrow to the right of the *Search by product* parameter field. The next window presented will provide download options for iRMC User manuals. Be sure to select the manual appropriate to your server configuration.

The iRMC can be configured with a default CA Certificate, a self-signed Certificate, or a Certificate can be uploaded to the iRMC.

The procedure requires an rsa ip parameter from each node or node in the case of a simplex (or Low Cost) system.

NOTE: The node.cfg rsa ip parameter should only be changed by using the IFgui Update tool. For more details on the IFgui Update tool refer to the OSV Service Manual: Installation and Upgrades, Appendix titled, “Updating the Node.cfg File (Also Known as EZIP)”.

An example of node.cfg query to resolve the rsa ip parameter of a node follows. This snapshot example is from a duplex V6 OSCV running ps12E05;

To resolve the node 1 IP (*rsa_1_ip*);

```
root@bocast4a:[/etc/hiq8000] #116
# grep -i rsa_1_ip node.cfg
rsa_1_ip: 10.235.54.20
root@bocast4a:[/etc/hiq8000] #117
#
```

To resolve the node2 IP (*rsa_2_ip*);

```
root@bocast4a:[/etc/hiq8000] #117
# grep -i rsa_2_ip node.cfg
rsa_2_ip: 10.235.54.21
root@bocast4a:[/etc/hiq8000] #118
#
```

Procedure for the RX200S6 platform

a) Log into the iRMC by starting a Web browser and navigating to either

   HTTPS://<iRMC_address>

   Or, if HTTPS is not enabled, you will have to navigate to

   HTTP://<iRMC_address>

   where <iRMC_address> is the IP address that is specified in node.cfg by the rsa_1_ip parameter.

   Hint: Remember to repeat the procedure for node 2 of a duplex system.

b) Log in using the username/password configured for the IMM.

c) To upload a CA certificate or use a default certificate, select **iRMC S2** then the **Certificate Upload** option in the left-hand pane. Select one of the options presented for the Certificate.

d) To generate a self-signed Certificate, select the **iRMC S2** then the **Generate Certificate** option in the left-hand pane. Populate the applicable fields, and click the Create button.

e) Once a Certificate is configured, select **Network Settings** then **Ports and Services** in the left-hand pane. The *Force HTTPS* box should be checked and the *Telnet* Enabled box should be unchecked. If you had to change either of these, click the **Apply** button.

f) For an OSV cluster, you will have to repeat the same actions using the IP address specified in node.cfg by the *rsa_2_ip* parameter.

3.8.9 Deactivate Clear-Text Administration / Activate Encrypted Communication - x3550 M3 and x3550 M4 platforms

Overview

The IBM Integrated Management Module User's Guide can be used as another reference for this procedure. To find the latest version of this document or the IBM white paper *Transitioning to UEFI and IMM*, go to:

http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-5079770&brandind=5000008

or complete the following steps:

NOTE: Changes are made periodically to the IBM Web site. Procedures for locating firmware and documentation might vary slightly from what is described in this document.

---

1. Go to http://www.ibm.com/systems/support/.
2. Under **Product support**, click **System x**.
3. From the **Product family** list, select your server and click **Go**.
4. Under **Support & downloads**, click **Documentation**.
5. Under **Product usage**, select the **Integrated Management Module User's Guide - IBM Servers** link.

The IMM can be configured with a self-signed Certificate or a Certificate can be uploaded to the IMM.

The procedure requires an rsa ip parameter from each node or node in the case of a simplex (or Low Cost) system.

NOTE: The node.cfg rsa ip parameter should only be changed by using the IFgui Update tool. For more details on the IFgui Update tool refer to the OSV Service Manual: Installation and Upgrades, Appendix titled, “Updating the Node.cfg File (Also Known as EZIP.)

An example of node.cfg query to resolve the rsa ip parameter of a node follows. This snapshot example is from a duplex V6 OSCV running ps12E05;

To resolve the node 1 IP (*rsa_1_ip*);

```
root@bocast4a:[/etc/hiq8000] #116
# grep -i rsa_1_ip node.cfg
rsa_1_ip: 10.235.54.20
root@bocast4a:[/etc/hiq8000] #117
#
```

To resolve the node2 IP (*rsa_2_ip*);

```
root@bocast4a:[/etc/hiq8000] #117
# grep -i rsa_2_ip node.cfg
rsa_2_ip: 10.235.54.21
root@bocast4a:[/etc/hiq8000] #118
#
```

Procedure for the x3550 M3 and x3550 M4 platforms

a) Log into the IMM by starting a Web browser and navigating to either:

   HTTPS://<IMM_address>

   Or, if HTTPS is not enabled, you will have to navigate to:

   HTTP://<IMM_address>

   where <IMM_address> is the IP address that is specified in node.cfg by the *rsa_1_ip* parameter.

b) Log in using the username/password configured for the IMM.

c) To generate a self-signed CA certificate or import/upload a Signed Certificate, select **IMM Control** then the **Security** option in the left-hand pane. Select one of the options presented in the section titled **HTTPS Server Certificate Management**.

   - Set the *HTTPS Server* drop-down box to *Disabled* and click the **Save** button to the right of the box. The Certificate options should then be displayed.

d) After the Certificate has been generated or imported, use the drop-down box to set the *HTTPS Server Configuration for Web Server* option to *Enabled* and click the **Save** button to the right of the box.

e) Select **IMM Control** then **Network Protocols** in the left-hand pane. In the Network Protocols display scroll down to the Telnet Protocol. Select *Disable* from the drop down menu list for the *Telnet connection count*. Scroll to the bottom of the window and select the **Save** button (located in the bottom right hand corner).

f) For an OSV cluster, you will have to repeat the same actions using the IP address specified in node.cfg by the *rsa_2_ip* parameter.

3.8.10 Disable Weak Ciphers for IMM

IMPORTANT: Ensure that the latest IMM version recommended by Unify is installed.

For all IBM server types, except IBM x3550 M4, apply High Security Mode (needs minimum firmware version 1.42) as follows:

1. Navigate as follows:

   IMM Control > Security > Cryptography Management

2. Select: **High Security Mode**

3. After configuration change, restart the IMM for the configuration to take effect.

3.9 Features

3.9.1 Prevent fraud using 3 way calling

When the initiator of a 3-way conference leaves the conference, the call between the remaining 2 parties stays up. This allows for call fraud.

If e.g. an employee in the US creates a conference with his phone, his cell phone and a party in China, he can leave the conference and continue the US-China long distance call being charged to his company.

CL-OSV-ConfDrop	**Drop conference when initiator leaves**
Measures	Set `Srx/Main/LCSLastHomeDnConfDrop` parameter to "true so that a Server based conference (=LCS) is dropped if the remaining participants are only externals.
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.9.2 MLPP

The MLPP feature allows for termination of existing calls to free up resources for new more important calls to succeed.

CL-OSV-MLPP	Configure MLPP with Caution
Measures	Review MLPP configuration: • Assign the feature and maximum allowed precedence level only to users which require the ability to prioritize their calls, possibly at the expense of preempting other busy or establishing calls for a called destination. • Make sure that subscribers using the Precedence and Preemption feature are authenticated properly since weak authentication can lead to unauthorized access and possibly preempting other user calls. • Define Precedence and Preemption authentication PINs responsibly, e.g. don't assign one 'global' PIN or no PIN at all. • If CAC related session resource management is used (network preemption), ensure adequate network session resources are configured to support expected call traffic, otherwise higher precedence calls may preempt other lower precedence calls if inadequate network session resources are available.
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.9.3 DA Challenging

OpenScape Voice can be configured not to challenge certain SIP messages (such as SUBSCRIBE, NOTIFY, PUBLISH and INFO messages) when digest authentication is activated. This feature should not be used.

CL-OSV-Challenge	Configure Remote Syslog
Measures	Confirm that the RTP parameter is turned off. However, if it has to be on, then make sure that the subscribers are configured with TLS or MTLS to prevent insertion of unchallenged messages into an existing dialog. RTP Parameter example: `Srx/Sip/BypassDA`
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.9.4 CSTA Control

OSV functions can be controlled via the CSTA interface. (e.g. to authenticate SIP trunk calls from the PSTN to the mobile network via a custom CSTA application.) The interface between OSV and CSTA application needs to be secure since an administrator that gains authorized access to the OSV may cause severe disruptions.

CL-OSV-CSTA	Check CSTA configuration
Measures	
References	Section 3.8.5, “Securing CSTA Services”
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.9.5 NG911 Emergency calling

Next Generation 911 (NG911) is the future of emergency telecommunications. In conventional 911 routing there is typically, what is called an E911 Selective Router inside the Emergency Services Network (ESN) that is responsible for routing the emergency calls to the appropriate Public Safety Answering Points (PSAPs).

CL-OSV-NG911	Configure NG911
Measures	• OSV acts as a client and opens up HTTP/HTTPS connections for LoST server queries. In order to guarantee data integrity HTTPS must be used.
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.9.6 Foreign Domains support

With the introduction of Foreign Domains support for Video SIP URI dialing it is possible for unknown entities to make calls reaching OSV from a domain that is not known and as such not trusted.

By default such calls are blocked from an SBC so in a typical deployment there is nothing to be done.

However in order to support Video SIP URI dial-in from anywhere, it is needed that an OSSBC is used and that it allows and routes video calls from foreign domains to OSV.

CL-OSV-Foreign Domains	Configure Foreign Domains
Measures	• When you want to allow such calls to arrive to OSV (for example, to allow for video dial-in use cases) make sure the correct configuration is applied on the OSSBC. Such calls should be arriving from a specific and dedicated IP and port (proper configuration of OSSBC). • On OSV make sure that these calls are routed only to specific destinations and routing is not possible for foreign domains • On OSV create an endpoint with an alias of that IP and port. Assign the **Support Foreign Peer Domains** endpoint attribute to that endpoint. • Create an endpoint profile to be used by that endpoint and create a class of service and traffic type that will be assigned for these calls. Route these calls only to specific endpoints such as video conferences equipment depending on the use case.
References	
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

3.10 Secure SIP Trunks

It is strongly recommended that the customer install a customer-premises Session Border Controller (SBC) on SIP trunk peer-to-peer connection of carrier-based SIP Service Provider (SSP) that provide access to the Public Switched Telephone Network (PSTN), even when the SSP says it is not necessary. The benefits include:

1. Security:

   There are only limited security options available without an SBC. Even "SIP aware" firewalls have compatibility issues and do not provide the same level of security as an SBC. No customer would open their data network to their Internet Service Provider (ISP); similarly, no customer should think it is okay to open their UC network up to a SIP trunk provider.

2. Functionality:

   SIP trunk providers often restrict traffic to a limited IP address range. Without an SBC to proxy this traffic, audio problems can occur when SIP calls are directed to devices that are outside of this range. This can happen with teleworkers, VPN users, and devices in other countries/subnets.

3. Serviceability:

   VoIP service support needs to have a demarcation for validating SIP trunk call functionality. VoIP technicians almost never have access to a customer's data network or data firewall. Without an SBC, the VoIP technician needs to work with the customer's IT department on all issues related to SIP trunking. IT skills vary greatly, especially when it comes to VoIP, so getting the right person to take responsibility and actually run the necessary traces to trouble shoot a SIP trunk problem can take days resulting in customer frustration.

CL-OSV-SIP_Trunks	**Secure the SIP Trunks**
Measures	Secure the SIP Trunk
References	Refer to the Installation and Administration documentation for the SBC model and version that is being installed. Note: Use only an SBC model and version that is listed in the OpenScape Solution Set product compatibility guide.
Needed Access Rights	Administrator
Executed	Yes  No 
Customer Comments and Reasons	

Additional Information for Settings

It is strongly recommended that a customer-premises SBC be used on all carrier-based SIP trunk interfaces even when it is not essential to provide connectivity to the SSP. A customer-premises SBC also allows VoIP service technicians to quickly diagnose and resolve SIP trunk issues including any nuances of the SSP' SIP signaling that cannot be readily handled by OpenScape Voice that may be encountered during the life of the installation. Without an SBC, the options on how to deal with SIP signaling issues are severely limited, and worse, the options to block VoIP attacks that may be initiated by outsiders gaining access via the SSP network from reaching the OpenScape Voice server are also limited.

When there is no customer-premises SBC, the OpenScape Voice server becomes the first line of defense against VoIP attacks. Such attacks are not typically captured by traditional data firewalls, even when using a data firewall that claims support for SIP traffic. On the other hand, SBCs are specifically designed to protect the customer's SIP communications server (i.e., the OpenScape Voice server) against such attacks.

Customer's that choose not to install a customer-premises SBC on their SIP trunks acknowledge and accept the consequences resulting from this decision, which include the possibility of experiencing significant performance impact on OSV (including the possibility of outages) in the event of an outside attack is waged via the SIP trunk.

3.11 Security Patches

All OpenScape Voice security patches are delivered with the product. Any new security patches for the OpenScape Voice will be delivered to the customer via technical support.

3.12 Integrity of SW load and Patch sets

OSV SW loads and patch sets are downloaded from the Software Supply Server SWS (https://sw-download.unify.com/SWSIntranet/SWSIntra.aspx). The associated readme file on SWS contains MD5 checksums of each file being downloaded. It s strongly recommend that the installer calculates the MD5 checksum of the received downloaded files and compares them with the checksum listed in the readme file.

3.13 Virus Protection

Unify has tested the OpenScape Voice server with various anti-virus scanner products. Unify strongly advises against running an anti-virus scanner of other intrusion detection system on the OpenScape Voice server itself. The following are the reasons for this:

- Although the server is already a low-profile target for viruses, worms and other intruders because it is Linux-based and not Windows-based, its firewall configurations and carefully controlled administrative access minimize its susceptibility.

- Running such scanners can cause a significant increase in server CPU usage, invalidating other capacity calculations. A corporate policy that requires virus scanners on all computers is probably not appropriate to enforce on this type of specialized server ; it is recommended that a waiver be sought from such a policy.

Instead, it is more appropriate to scan the software prior to installation and make use of an IDS (such as Tripwire) to monitor the server for changes to the critical files.

CL-OSV-Virus	**n Virus Scanner**
Measures	
References	
Needed Access Rights	Administrator
Executed	Yes ☐ No
Customer Comments and Reasons	

4 References

1. OpenScape Voice, Service Manual: Installation and Upgrades, Installation Guide
   (e-Doku or partner portal / product information)
2. Support of Virus Protection Software for Server Applications
3. Interface Management Database (IFMDB)
   available via partner portals
   https://www.mitel.com/login
4. Software Supply Server - SWS