Security Guidelines

AudioCodes One Voice™ Operations Center Product Suite

OVOC

Version 7.4

Table of Contents

List of Figures

List of Tables

This page is intentionally left blank.

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published March-01-2018

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at https://www.audiocodes.com/services-support/maintenance-and-support.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Throughout this manual, unless otherwise specified, the term *device* refers to AudioCodes products. References in this document to “OVOC Voice Quality Package” refer to what was previously known as “SEM”.

Document Revision Record

LTRT	Description
94040	Initial release of the document.
94041	Updating Java Web Start certificates after upgrade; correction to firewall table; updating Java security level on PC; enabling the 'QOEENABLETLS' parameter when working with MP-1xx devices.
94042	Updates for supporting SSL encrypted HTTPS connection between endpoints and OVOC server.
94043	Updated Firewall Configuration Schema and OVOC Maximum Security Implementation diagrams.
94044	Updates to Step 3: Configuring the Firewall and Step 5: Implementing X.509 Authentication.
94046	Replaced the OVOC Maximum Security Implementation diagram and the Firewall diagram. Added firewall tables for OVOC and NOC/OSS.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at https://online.audiocodes.com/documentation-feedback..

1 Introduction

This document provides security guidelines for safeguarding your network and OVOC applications against malicious attacks.

1.1 AudioCodes OVOC Security Solution

The AudioCodes OVOC application provides a comprehensive package of security features that handles the following main security areas:

- **Securing the OVOC server Platform:**
  - Step 1: Implementing Server Security Settings (see Chapter 2)
- **Securing the Application (Identity Management):**
  - Step 2: Defining OVOC Users (see Chapter 3)
- **Securing the Communication:**
  - Step 3: Configuring the Enterprise Firewall (see Chapter 4)
  - Step 4: Configuring SNMP (see Chapter 5)
  - Step 5: Implementing X.509 Authentication (see Chapter 6)

This page is intentionally left blank.

Part I

Securing the OVOC server Platform

2 Step 1: Implementing Server Security Settings

This step describes enhanced security settings that can be implemented using the EMS Server Manager to prevent intrusion to the OVOC server platform. The EMS Server Manager tool has been designed to provide the ability to configure all the required security measures to prevent intruders from accessing and manipulating Operating System level files. The EMS Server Manager tool serves as an interface to the Operating System and therefore discourages users from running Linux commands directly from an OS shell; such actions can expose security vulnerabilities.

2.1 Changing the OS Password

OS Password settings are comprised of the following:

- General password settings: these settings enable you to change the 'Minimum Acceptable Password Length' and 'Enable User Block on Failed Login'. In addition, you can modify settings for a specific user, such as 'User's Password' and 'Password Validity Max Period'.
- Operating System Users Security Extensions: these settings enable you to change the default user password "acems" for accessing the OVOC server platform over an SSH connection terminal. In addition you can configure this passwords validity period, the maximum allowed numbers of simultaneous open sessions and the inactivity time period (days) before the OS user is locked.

Note: The 'Security Event' is raised when a specific user is blocked after reaching the maximum number of login attempts.

To change these settings, refer to Section 'OS User Passwords' in the *One Voice Operations Center Server IOM.*

2.2 Changing Database Default Password

You can change the Oracle Database password. The OVOC server shuts down automatically before changing the Oracle Database password. Refer to Section 'DB Password' in the *OVOC server IOM.*

Note: It is not possible to restore these passwords or to enter the OVOC Oracle Database without them.

2.3 Provisioning SSH Options to access OVOC Server

You can configure the following options for connecting to the SSH terminal connection (for more information, refer to 'Section SSH' in the *One Voice Operations Center Server IOM*):

- Configure SSH Log Level: You can configure the log level of the SSH daemon server. The log files are found at the location '/var/log/secure' (older records are stored in secure.1, secure.2 etc.)
- Configure SSH Banner: The SSH Banner displays a pre-defined text message each time the user connects to the OVOC server using an SSH connection. You can customize this message. By default this option is disabled
- Configure SSH on Ethernet Interfaces: You can allow or deny SSH access separately for each network interface enabled on the OVOC server.
- Configure SSH Allowed Hosts: This option enables you to define which hosts are allowed to connect to the OVOC server through SSH:
  - Allow ALL Hosts (default)
  - Deny ALL Hosts

Note: When this action is performed, the OVOC server is disconnected and you cannot reconnect through SSH. Before you disable SSH access, ensure that you have provisioned alternative connection methods, for example, serial management connection or KVM switch connection.

  - Add Host/Subnet to Allowed Hosts

Note: When adding a Host Name, ensure to verify your remote host name appears in the DNS server database and your OVOC server has an access to the DNS server.

  - Remove Host/Subnet from Allowed Hosts

Note: When you remove either the only existing IP address, Subnet or Host Name in the Allowed Hosts list, there are no remote hosts with access (i.e. for each respective option) to connect to the OVOC server using SSH. When this action is performed, you are disconnected from the OVOC server and may not be able to reconnect through SSH. Therefore, prior to disabling SSH access, ensure that alternative connection methods have been provisioned, for example, serial management connection or KVM switch connection.

2.4 Integrity Testing

Integrity testing is performed to verify whether system file attributes have been modified. You can activate the regular File Integrity tool or the Advanced Intrusion Detection tool as described below. Both these tools are by default enabled.

2.4.1 File Integrity Checker

The File Integrity checker tool periodically verifies whether file attributes were changed (permissions/mode, inode #, number of links, user id, group id, size, access time, modification time, creation/inode modification time). File Integrity violation problOC are reported through OVOC Security Events. The File Integrity checker tool runs on the OVOC server machine. See Section 'File Integrity Checker' in the *One Voice Operations Center Server IOM.*

2.4.2 Software Integrity Checker (AIDE) and Pre-linking

AIDE (Advanced Intrusion Detection Environment) is a file and directory integrity checker. This mechanism creates a database from the regular expression rules that it finds in its configuration file. Once this database is initialized, it can be used to verify the integrity of the files.

Pre-linking is designed to decrease process startup time by loading each shared library into an address for which the linking of needed symbols has already been performed. After a binary has been pre-linked, the address where the shared libraries are loaded will no longer be random on a per-process basis. This is undesirable because it provides a stable address for an attacker to use during an exploitation attempt. See Section 'Software Integrity Checker (AIDE) and Pre-linking' in the *One Voice Operations Center Server IOM*.

2.5 Transferring Files Using SFTP / SCP

Files should be transferred to and from the OVOC server using any SFTP/SCP file transfer application. Refer to the *One Voice Operations Center Server IOM* appendix for such instructions.

All OVOC and device information available for the NMS and other Northbound interfaces including Topology, Performance and Backup data is located in the OVOC server machine under the folder /NBIF. This folder can be accessed using HTTPS browsing by entering the URL https:// <OVOC server IP>/NBIF in your Web browser.

For more information, refer to the *One Voice Operations Center Integration with Northbound Interfaces*.

2.6 Advanced Security Options

2.6.1 Auditd

Auditd is the user space component to the Linux Auditing System that is responsible for writing audit records to the disk. This tool monitors what is happening in your system at the kernel level. For example, it monitors network traffic and access to files.

Using the Auditd option, you can change the auditd tool settings to comply with the Security Technical Information Guidelines (STIG) recommendations.

This option is by default disabled; however, it is highly recommended to enable it. When enabled, these records are saved in the /var/log/audit/ directory on the OVOC server platform. To enable this option, refer to Section 'Auditd Options' in the *One Voice Operations Center Server IOM*.

2.6.2 Network Options

The following network security options provide protection against hackers and intruders. All these options are by default disabled; however it is highly recommended to enable all of these options. To enable these options, refer to Section 'Network Options' in the *One Voice Operations Center Server IOM*.

- Ignore Internet Control Message Protocol (ICMP) Echo requests:

  This option ensures that the OVOC server does not respond to ICMP broadcasts, and therefore such replies are always discarded. This prevents attempts to discover the system using ping requests.

- Ignore ICMP Echo and Timestamp requests:

  This option ensures that the OVOC server does not respond to an ICMP timestamp request to query for the current time. This reduces exposure to spoofing of the system time.

- Disable ICMP Redirect Messages:

  This option disables the sending of ICMP Redirect Messages, which are generally sent only by routers.

- Block ICMP Redirect Messages:

  This option ensures that the OVOC server does not respond to ICMP Redirect broadcasts, and therefore such replies are always discarded. This prevents an intruder from executing a denial of service attack by attempting to redirect traffic from the OVOC server to a different gateway.

Part II

Securing the Application

This part describes the user management on the OVOC servers.

3 Step 2: Defining OVOC Users

OVOC users can be authenticated and authorized either locally on the OVOC server or using a centralized third-party platform. By default, OVOC users are managed locally in the OVOC database.

3.1 Implementing Centralized Identity Management (LDAP and RADIUS)

It is *recommended* to implement an external LDAP server or RADIUS server in your network for authenticating and authorizing the OVOC management users (Web and CLI). This can be done, for example, by using an LDAP-compliant server such as Microsoft Active Directory (AD). When a user attempts to log in to the OVOC, the OVOC server verifies the login username and password with the AD server or RADIUS server.

You can also configure an HTTPS connection with the LDAP server for the LDAP user authentication (see Section 6.4.8).

Note: You must initially connect to the OVOC using the default user 'acems'. Once you have successfully connected with the 'acems' user, you can then change the authentication and authorization for the OVOC server installation settings to RADIUS or LDAP.

3.1.1 Provisioning Administrator and Operator Security Levels

The OVOC determines the user's security level (privileges) based on the user's profile in the AD or RADIUS server. When the user properties custom attribute “Security Level” (specifically defined OVOC attribute) has not been defined on the RADIUS or LDAP server and configured with one of the OVOC Security levels (see Section 3.2.1), then the default security level "Operator" is assigned to the user (refer to Section "LDAP Server" and RADIUS Server" in the *One Voice Operations Center User's* manual). If you wish, you can deny user access or set a different security level to the user by configuring the 'Default Authorization Level on Radius Attribute Absence' or Default Authorization Level on LDAP Group Absence' parameter.

3.2 Implementing Local OVOC Based Identity Management

In case you don’t have an LDAP or RADIUS authentication server in your network, you can manage OVOC users in the OVOC local database using the Users List.

Note: For RADIUS users only: the local users database can be automatically used as a backup if the connection to the RADIUS servers fails after a defined timeout; when the RADIUS connection fails, the user and password are replicated to the local users database and therefore the user can login to the OVOC as a local user. This feature is configured by parameter 'Enable Local Authentication on Radius Timeout' (refer to Section 'Radius Server' *in the One Voice Operations Center User’s Manual*). In addition, when the RADIUS connection fails, the 'Security Alarm' is raised; when all RADIUS servers cannot be reached, this alarm has the "Critical" status.

3.2.1 Provisioning Operator Security

The table below summarizes the Operator Actions and Security Levels for the multi-tenant architecture:

Table 3-1: Provisioning Operator Security

Operator Type	Security Level	Define Operators	Manage Tenants	Manage Global/System Entities/Resources	Manage Tenant Resources	Monitor System Resources	Monitor Tenant Resources
System	Admin	Yes, All levels	Yes	Yes	Yes	Yes	Yes
	Operator	No	No	Yes	Yes	Yes	Yes
	Monitor	No	No	No	No	Yes	Yes
Tenant	Admin	In this tenant network only	No	No	In this tenant network only	No	Yes
	Operator	No	No	No	In this tenant network only	No	Yes
	Monitor	No	No	No	No	No	Yes

3.2.1.1 Resource/Entity Management

The table below shows the actions permitted for each OVOC operator type and security level:

- **Global resources:** Includes OVOC server-related management including the OVOC server License, File Storage, Operating System, Server Backup and Restore and HA configuration.
- **Tenant resources:** Includes the portion of the OVOC server License that is allocated to the tenant.
- **Global entities:** Includes security policy for operators, CA certificate assignment, storage policy, global alarm settings and device backup policy settings.
- **System entities:** Includes system alarms, forwarding rules for system alarms and statistics reports.
- **Tenant entities:** Includes all entities that are accessible for a specific tenant such as all regions, sites, devices, links, call hierarchies and summaries, journal records and alarms. In addition to statistics reports, alarm forwarding rules and threshold and alert rules.

For details of which actions can be performed according to Operator Security level, refer to the documentation of each specific feature in the *One Voice Operations Center User's Manual*.

3.2.1.2 Operator Type

The following operator types can be provisioned:

- **System "Admin":** Global operator with permissions to manage resources for the entire OVOC topology:
  - Define and manage all system tenants

- Define system operators (all levels) or tenant operators (admin, operator and monitor) and attach them to any tenants.
- Manage system entities/resources
- Define and manage global entities/resources
- Manage all tenant specific entities/resources

- **System "Operator":** Operator with permissions for viewing and performing operations on all devices:
  - Manage system entities/resources
  - Define and manage global entities/resources which can be view and managed by all other tenants.
  - Manage all tenants' specific entities/resources except security-related entities, include moving device between tenants.
- **System "Monitor":** Viewing only:
  - Monitor all tenants specific entities/resources
  - Monitor system entities/resources
  - Monitor global entities/resources
- **Tenant "Admin":** The Tenant Admin can manage resources for the tenant network only:
  - Define tenant operators (Admin, Operator and Monitor)
  - Delete tenant operators only if he attached to attach to all tenants as the deleted operator
  - Manage only tenant specific entities/resources, including moving device between attached tenants and tenant license pool management.
  - Monitor global entities
- **Tenant "Operator":** The Tenant Operator has operator privileges for the Tenant network only:
  - Manage tenant specific resources, will not be aware in any way to other tenants entities/resources or system entities/resources, include moving devices between attached tenants and tenant license pool management
  - Monitor global entities
- **Tenant "Monitor":** The Tenant Monitor has Monitor privileges for devices that are defined in the specific tenant network.
  - Monitor tenant specific resources
  - Monitor global entities

Note: Multi-tenancy is not supported when users are stored in the RADIUS or the LDAP AD server.

This page is intentionally left blank.

Part III

Securing the Communication

This part describes how to secure the connections between the OVOC clients and servers.

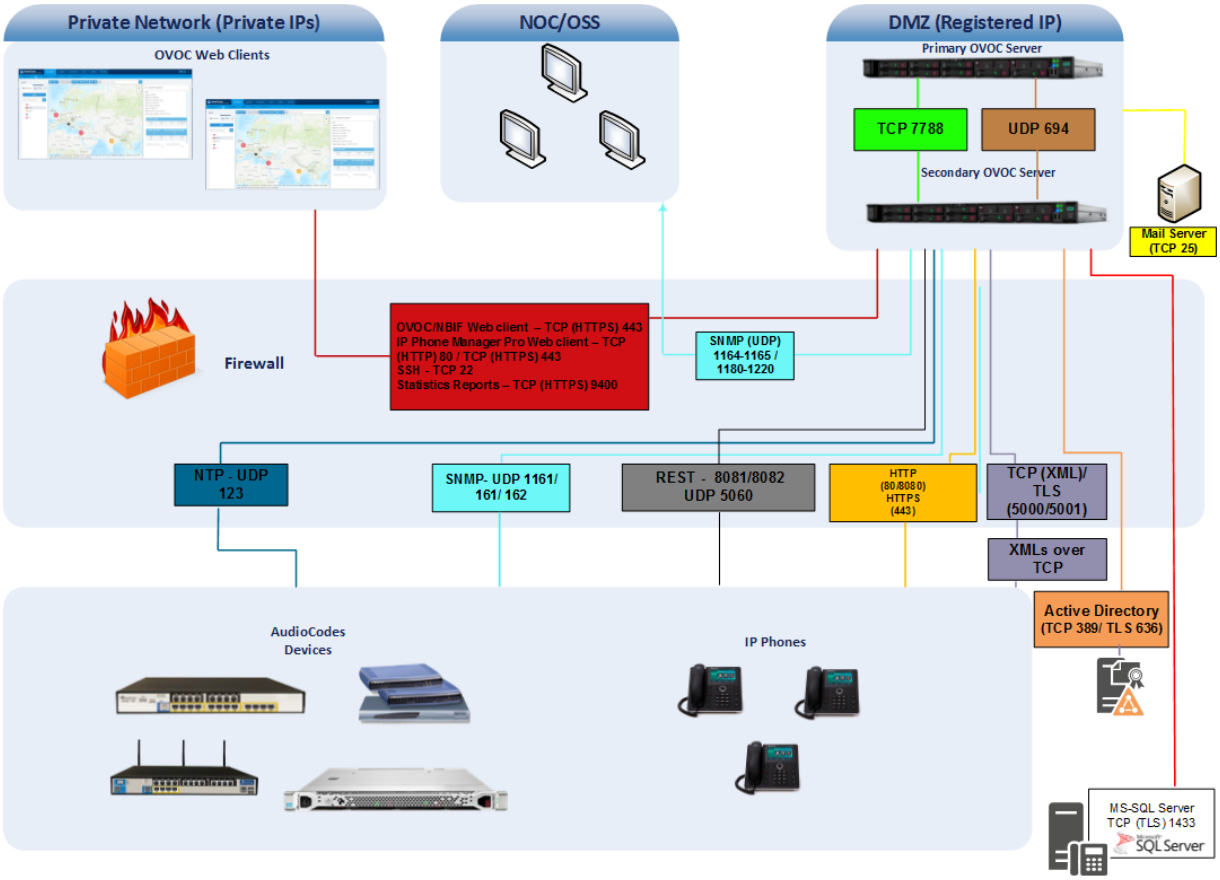
4 Step 3: Configuring Enterprise Firewall

The OVOC interoperates with firewalls, protecting against unauthorized access by crackers and hackers, thereby securing regular communications. You need to define rules in your firewall to manage the secure communications for all OVOC interfaces that connect to the OVOC server. Each of these network interfaces processes use different communication ports which should be secured appropriately.

By default, all ports are open on the OVOC server side. When installing the OVOC server, you need to configure its network and open the ports in your Enterprise LAN according to your site requirements; based on the firewall configuration rules (representing these port connections) that are described in the table below. For some of the firewall rules shown in the table below, the port numbers shown are default numbers, such ports can be reconfigured by users.

The table below shows the firewall configuration schema for all OVOC connections.

Figure 4-1: Firewall Configuration Schema



Note: The above figure displays images of devices. For the full list of supported products, refer to the *OVOC Release Notes*.

The table below shows the firewall configuration according to the highest level of security that can be implemented on the OVOC server platform.

Note: Some of these port connections shown in the table below are non-secure (indicated in the column 'Secured Connection" below).

Table 4-1: High Security Firewall Configuration

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
OVOC Clients and OVOC server					
TCP/IP client ↔ OVOC server	TCP	✓	22	SSH communication between OVOC server and TCP/IP client. Initiator: client PC	OVOC server side / Bi-directional.
OVOC and NBIF Client ↔ OVOC server	TCP (HTTPS)	✓	443	HTTPS for OVOC/NBIF clients. Initiator: Client	OVOC server side / Bi-directional.
OVOC server and Devices					
Device (Behind NAT) ↔ OVOC server	UDP	✓	1161	Keep-alive – SNMPv3 trap listening port (used predominantly for devices located behind a NAT). Initiator: AudioCodes device	OVOC server side / Receive only.
Device (Not Behind NAT) ↔ OVOC server	UDP	✓	162	SNMPv3 trap listening port on the OVOC that is used when the device is not located behind a NAT. Initiator: AudioCodes device	OVOC server side / Receive only.

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
Device ↔ OVOC server (Trap Manager)	UDP	✓	161	SNMPv3 Trap Manager port on the device that is used to send traps to the OVOC. Initiator: OVOC server	MG side / Bi-directional
Device↔ OVOC server (NTP Server)	UDP (NTP server)	×	123	NTP server synchronization. Initiator: MG (and OVOC server, if configured as NTP client) Initiator: Both sides	Both sides / Bi-directional
Device ↔ OVOC server	TCP (HTTPS)	✓	443	HTTPS connection for files transfer (upload and download) and REST communication. Initiator: OVOC server	OVOC server side / Bi-directional
Endpoints (IP Phones)					
OVOC server ↔ IP Phone Manager Pro	TCP (HTTPS)	✓	443	HTTPS connection between the OVOC server and the IP Phone Manager Pro Web page. Initiator: client browser.	OVOC server side / Bi-directional.
				HTTPS connection used by endpoints for downloading firmware and configuration files from the OVOC server. Initiator: Endpoints	

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
OVOC server ↔ Endpoints (IP Phones)	TCP (HTTPS)	✓	8082	HTTPS REST updates (encryption only without SSL authentication). It is recommended to use this connection when managing more than 5000 IP Phones. In this case, you should change the provisioning URL port from 443 to 8082 in the phone's configuration file. Initiator: Endpoint	OVOC server side / Bi-directional
OVOC Voice Quality Package TLS					
AudioCodes Devices ↔ OVOC Voice Quality Package server	TCP (TLS)	✓	5001	XML based Tomcat TLS secured communication for control, media data reports and SIP call flow messages. Initiator: AudioCodes device	OVOC server side / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
Statistics Reports					
Statistics Reports client page ↔ Tomcat server	TCP (HTTPS)	✓	9400	HTTPS connection that is used for generating Statistics Reports. Initiator: Client's Web browser (Statistics Report page).	OVOC server side / Bi-directional
MS-SQL Server					
OVOC Voice Quality Package server ↔ Lync MS-SQL Server	TCP (TLS)	✓	1433	Connection between the OVOC server and the MS-SQL Lync server. This port should be configured with SSL. Initiator: Skype for Business MS-SQL Server	Lync SQL server side / Bi-directional
LDAP Active Directory Server					
OVOC Quality Package server ↔ Active Directory LDAP server (Skype for Business user authentication with OVOC Quality Package)	TCP (TLS)	✓	636	Connection between the OVOC Quality Package server and the Active Directory LDAP server with SSL configured. Initiator: OVOC server	Active Directory server side/ Bi-directional
OVOC server ↔ Active Directory LDAP Server (OVOC users authentication)	TCP (TLS)	✓	636	Connection between the OVOC server and the Active Directory LDAP server with SSL configured. Initiator: OVOC server	Active Directory server side/ Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
RADIUS Server					
OVOC server ↔ RADIUS server	UDP	×	1812	Direct connection between the OVOC server and the RADIUS server (when OVOC user is authenticated using RADIUS server). Initiator: OVOC server	OVOC server side / Bi-directional
OVOC HA					
Primary OVOC server ↔ Secondary OVOC server (HA Setup)	TCP	×	7788	Database replication between the servers. Initiator: Both servers	Both OVOC servers / Bi-directional
	UDP	×	694	Heartbeat packets between the servers. Initiator: Both servers	
Mail and Syslog Servers					
OVOC server ↔ Mail Server	TCP	×	25	Trap Forwarding to Mail server Initiator: OVOC server	Mail server side / Bi-directional
OVOC server ↔ Syslog Server	TCP	×	514	Trap Forwarding to Syslog server. Initiator: OVOC server	Syslog server side /Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
RFC 6035					
OVOC Quality Package Server ↔ Endpoints	UDP	×	5060	SIP Publish reports sent to the OVOC Quality Package server from the endpoints, including RFC 6035 SIP PUBLISH for reporting device voice quality metrics. Initiator: Endpoint	OVOC Quality Package server / Bi-directional

Table 4-2: Firewall Configuration: NOC/OSS ⟶ OVOC

Source IP Address Range	Destination IP Address Range	Secured Connection	Protocol	Source Port Range	Destination Port Range
NOC/OSS	OVOC	✓	SFTP	1024 - 65535	20
		✓	SSH	1024 - 65535	22
		×	Telnet	1024 - 65535	23
		×	NTP	123	123
		✓	HTTPS	N/A	443
		✓	SNMP (UDP) Set for Active alarms Resync feature.	N/A	161

Table 4-3: Firewall Configuration: OVOC ⟶ NOC/OSS

Source IP Address Range	Destination IP Address Range	Secured Connection	Protocol	Source Port Range	Destination Port Range
OVOC	NOC/OSS	×	NTP	123	123
		✓	SNMP (UDP) Trap	1024 – 65535	162
		✓	SNMP (UDP) port for Active alarms Resync feature.	1164 - 1165	-
		✓	SNMP (UDP) port for alarm forwarding.	1180-1220	-

5 Step 4: Securing SNMP Interface Access (OVOC)

This chapter describes the guidelines for implementing SNMP for the connection with AudioCodes devices.

5.1 Securing Trap Forwarding over SNMPv3

The SNMPv3 protocol can be used for securing traps that are generated on devices, IP Phones. The SNMP connection must be configured on both the OVOC and on the devices/IP Phones.

- For configuring SNMPv3 in the OVOC, refer to the *One Voice Operations Center User's* manual.

  Note that when you add the device to the OVOC, in the SNMPv3 settings, it is recommended to set the following for maximum security:

  - Security Level parameter to 'Authentication and Privacy'
  - Authentication Protocol parameter to 'SHA'
  - Privacy protocol to 'AES_128'.
- For configuring SNMPv3 on devices, refer to the *One Voice Operations Center User's Manual*, Appendix *Prepare Devices for Interoperability Automatic Provisioning.*

5.1.1 Prefer SNMPv3 over SNMPv2

Use SNMP Version 3 (SNMPv3) (and not SNMPv1 and SNMPv2c), if possible. SNMPv3 provides secure access to the device using a combination of authentication (MD5 or SHA-1) and encryption (DES or AES-128) of packets over the network.

This page is intentionally left blank.

6 Step 5: Implementing X.509 Authentication

X.509 certificates can be used to authenticate a connection between an OVOC client and the OVOC servers (Apache and Tomcat); between the OVOC server and external third-party servers in the Enterprise network (Active Directory LDAP server and MS-SQL Monitoring server) and between the OVOC server and AudioCodes' devices. The certificates may be implemented for one or more of the SSL connections described in the table below.

Note:

- The OVOC Apache and Tomcat servers and their clients can use the same certificate files.
- The Active Directory and server Skype for Business MS-SQL Monitoring servers use Microsoft certificates.

6.1 Types of Certificates

The above connections can be implemented using the following types of certificates:

- **Default Certificates:**

  AudioCodes self-signed certificates are by default installed on the OVOC server and used by default for the OVOC and NBIF clients TLS (HTTPS) connections. For securing the connection with AudioCodes devices over TLS (HTTPS), these Certificates need to be taken from the OVOC server directory and loaded to the AudioCodes devices.

- **Custom Certificates:**

  Custom certificates can be generated and imported to the OVOC server. These certificates are generally signed by the Enterprise's external CA. If Enterprises use their own organizational certificate Infrastructure (PKI) for enhanced security, then these certificates can be deployed using the EMS Server Manager utility menu option 'Server Certificate Updates'. This option enables you to generate the private keys, the Certificate Signing Requests and import the files received from the CA to the OVOC server.

Warning: When implementing a TLS (HTTPS) connection with AudioCodes devices, the default OVOC AudioCodes device certificates must be loaded to AudioCodes devices (see Section 6.4.6). In addition, when replacing default certificate files with custom certificate files (see Section 0); these certificate files should also be loaded to the AudioCodes devices.

6.2 Recommended Workflow

The section describes the recommended workflow for implementing X.509 authentication.

6.2.1 OVOC Client and Servers

1. Setup HTTPS connections using default certificates
2. Implement custom server certificates (overriding default certificates) using the EMS Server Manager Server Certificates Update option (see Section 0).

Note: Before you replace the default certificates with custom certificates, it is recommended to setup all of the HTTPS connections with the default certificate deployment to verify that these connections are working as required.

6.2.2 AudioCodes Devices

1. Setup the default HTTPS connection on the OVOC server and the AudioCodes devices
2. Implement custom certificates (overriding default certificates) using the EMS Server Manager (see Section 0).

Note: Before you replace the default certificates with custom certificates, it is recommended to setup all of the HTTPS connections with the default certificate deployment to verify that these connections are working as required.

6.2.3 Endpoints

Setup the endpoint connections for REST updates and statutes sent from the IP Phones and for downloading firmware and configuration files. Connection with endpoints is encryption only without SSL authentication.

6.2.4 Third-party Vendor Server Connections

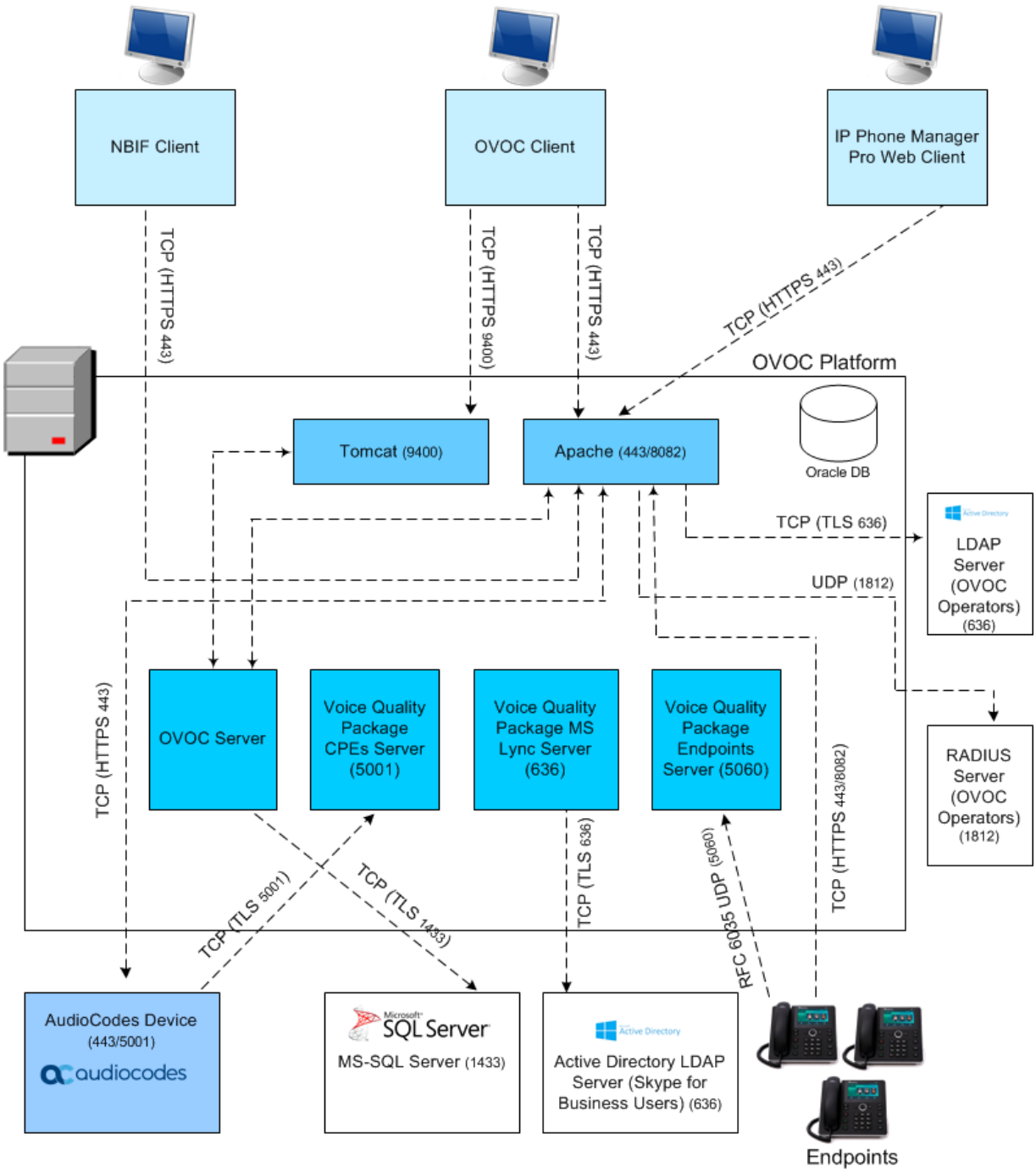
Setup the SSL connections with the Microsoft Skype for Business Active Directory and MS-SQL servers. These connections are secured using Third-party certificates.

Setup the RADIUS server connection. This connection is secured by a RADIUS secret password and other RADIUS parameters.

6.3 HTTPS/SSL/TLS Security Implementation Diagram

The figure below shows the maximum security that can be implemented in the OVOC environment.

Figure 6-1: OVOC Maximum Security Implementation



6.4 Enabling HTTPS/SSL/TLS Connections

The OVOC installation and the AudioCodes device are installed with default certificates as described above. Apart from the connection with AudioCodes devices, all other connections are by default secured over HTTPS and therefore need to be enabled to run over HTTPS.

Note: For browser and Java version compatibility, refer to the *IOM manual*.

The following connections are described in this section:

Table 6-1: OVOC Connections

Connection Type	Reference
OVOC HTTPS client ↔ OVOC server (Apache and Tomcat servers).	Section 6.4.1
Statistics Reports client page ↔ Tomcat server	Section 6.4.2
OVOC IP Phone Manager Pro browser ↔ OVOC Apache Server	Section 6.4.3
OVOC server ↔ Endpoints (IP Phones)	Section 6.4.4
OVOC server ↔NBIF Client	Section 6.4.5
OVOC server ↔ AudioCodes devices	Section 6.4.6
OVOC Voice Quality Package ↔ AudioCodes devices	Section 6.4.7
Third-Party Vendor Server Connections	
OVOC server ↔ Active Directory LDAP server- User authentication and authorization	Section 0
OVOC server ↔ RADIUS server- User authentication and authorization	Section 6.4.8.2
OVOC server ↔ Microsoft Active Directory LDAP Server Skype for Business	Section 6.4.8.3
OVOC server ↔ Skype for Business MS-SQL Server Skype for Business Server	Section 6.4.8.4

6.4.1 OVOC Web Client

The OVOC Web client connection is by default enabled over HTTPS through port 443 using AudioCodes default self-signed certificate.

6.4.2 Statistics Reports Page

The connection to the Statistics Reports Web page is by default enabled over HTTPS through port 9400.

6.4.3 OVOC IP Phone Manager Pro Web Client

The connection to the IP Phone Manager Pro Web page is by default enabled over HTTPS through port 443. This is managed by the EMS Server Manager option 'IP Phone Management Server and NBIF Web pages Secured Communication' (refer to Section 'IP Phone Manager Pro and NBIF Web pages Secured Communication' in theIOM manual). This connection is secured using the AudioCodes self-signed certificate. In addition, in the IP Phone Manager Pro configure the following:

- 'Secure (HTTPS) communication from the IPP Manager to the Devices' (Setup tab > System Settings). When configured, this parameter secures (HTTPS) requests from the IP Phone Manager Pro to the phone. Communications and REST actions such as Restart, Send Message will be performed over HTTPS. This parameter is not relevant when using an SBC proxy.
- 'Devices Status: Open IP Phone web administrator using HTTPS' (Setup tab > System Settings). When configured, this parameter opens the HTTPS Web page seamlessly without prompting whether the page is secure to open.

6.4.4 Endpoints

An HTTPS connection between the endpoints and the IP Phone Manager Pro is implemented as follows:

- REST connection for alarms and statuses: This connection is implemented over SSL (encryption only without SSL authentication) using the AudioCodes self-signed certificate, where the default AudioCodes certificates are used to encrypt the data. If you replace the default AudioCodes server certificates on the OVOC server with custom certificates, this does not affect the HTTPS connection between the endpoints and the OVOC server i.e. data is still encrypted using the default certificates.
- Download configuration and firmware files to the endpoints over HTTPS through port 443 (see Section 6.4.3).
- In the IP Phone Manager Pro Web, configure the parameter 'Secure (HTTPS) communication from the Devices to the IP Phone Manager Pro (requires generating configuration files)' (Setup tab > System Settings). When configured, this parameter secures HTTPS requests sent from the phone to the IP Phone Manager Pro. Communications and REST updates such as keep-alive, alarms and statuses between the phone and the server will be performed over HTTPS. In addition, the downloading of firmware and configuration files is also secured. This parameter also applies when an SBC proxy is implemented.

6.4.5 NBIF Client

Connection between the NBIF client and the OVOC server is by default secured over HTTPS over using AudioCodes default self-signed certificate. This is managed by the EMS Server Manager option 'IP Phone Manager Pro and NBIF Web pages Secured Communication' in the EMS Server Manager.

Logging into the OVOC client from a NBIF client requires a user name and password. This ensures that only authorized tenants can access this folder. The default user is "nbif" and the default password "pass_1234". This password can be changed using the "Change HTTP/S Authentication Password for NBIF Directory" option in the EMS Server Manager (refer to Section 'Change HTTP/S Authentication Password for NBIF Directory' in the *IOM manual*).

6.4.6 AudioCodes Devices

The OVOC server and AudioCodes device connection is by default over HTTP and should be secured over HTTPS for the purpose of files upload/download and REST communication.

➢ **To secure the connection between the OVOC server and the device over HTTPS:**

1. When adding devices to OVOC, select the "Enable HTTPS Connection" check box in the Device Details or set the Connectivity parameter to "HTTPS" in the Tenant Details.
2. Copy default OVOC AudioCodes device certificates from the /home/acems/boardCertFiles directory on the OVOC Server directory (see example below) to an external location and then load them to the AudioCodes devices.

```
 [root@vmware-low-219boardCertFiles]# pwd
/home/acems/boardCertFiles
[root@vmware-low-219 boardCertFiles]# ll
total 12
-rw-r--r-- 1 acems dba 615 Dec  3 15:53 board_cert.pem
-rw-r--r-- 1 acems dba 887 Dec  3 15:53 board_pkey.pem
-rw-r--r-- 1 acems dba 704 Dec  3 15:53 root.pem
```

   Refer to section "Installing Custom Certificates on AudioCodes Devices" in the *IOM manual.*
3. Configure HTTPS parameters on the AudioCodes device (using the device's Web server). Refer to Section "Configuring HTTPS Parameters on the Device" in the *IOM manual.*
4. Implement Two-Way Authentication with X.509 Certificates (see Section 6.4.6.1).
5. (Optional) Disable TLS Version 1.0.

   By default, the TLS connection with AudioCodes devices (port 443) is secured over TLS version 1.0. If you wish to secure this connection over a higher TLS version (TLS version 1.1 or version 1.2), then you can disable TLS version 1.0 using the procedure described in the *IOM manual* Section "Disabling TLS Version 1.0".

6.4.6.1 Implement Two-Way (Mutual) Authentication with X.509 Certificates

You should use two-way authentication over HTTPS between the device and OVOC. This prevents unauthorized access to both the OVOC and the device. Configuration is required on both OVOC and the AudioCodes device for the deployment of this setup.

➢ **To setup the two-way authentication on the AudioCodes device:**

1. Configure the following parameters:
   - For Media Gateway and SBC devices:
     - Enable the *AUPDVerifyCertificates* parameter.
   - For MP-1xx devices:
     - Enable *AUPDVerifyCertificates*
     - Set *ServerRespondTimeout* to *10000*
     - When working with TLS, enable *QOEENABLETLS*

Refer to Section “Installing Custom Certificates on AudioCodes Devices” in the *IOM manual*.

➢ **To setup the two-way authentication on the OVOC server:**

1. Ensure that HTTPS is enabled on the device when adding to OVOC.
2. Set the HTTPS Authentication option “Set Mutual Authentication” using the EMS Server Manager-refer to Section 'HTTPS Authentication' in the IOM manual).

6.4.7 OVOC Voice Quality Package and AudioCodes Device Communication

The XML-based communication for OVOC Voice Quality Package connection with AudioCodes devices is by default non-secured. If you wish to secure this connection over TLS, you must configure the SEM – AudioCodes devices communication' option in the EMS Server Manager. This setting secures the connection over port 5001 instead of port 5000 (you can also configure this option to open both ports 5000 and 5001, refer to Section "OVOC Quality Package - AudioCodes Devices Communication" in the IOM manual). The connection is then secured using the AudioCodes self-signed certificate.

6.4.8 Third-party Vendor Server Connections

This section describes how to authenticate the following third-party vendor server connections:

- Active Directory LDAP Server User Authentication (see Section 0).
- RADIUS Server Connection (see Section 6.4.8.2).
- Active Directory Server (Skype for Business Users) SSL Connection (see Section 6.4.8.3).
- Skype for Business MS-SQL SSL Connection (see Section 6.4.8.4).

6.4.8.1 Active Directory LDAP Server User Authentication

This section describes how to secure the connection between the OVOC server and an LDAP server for LDAP user-based authentication. This connection is secured using Microsoft certificates. When these certificates are loaded to OVOC, the /opt/ssl/keystore.jks directory is updated.

➢ **Do the following:**

1. Open the Software Manager (System > Configuration > File Manager), then click **Add > Add Auxiliary File**, select File Type 'Certificate' and add the required certificate file.
2. Open the Authentication page (**System** tab > **Administration** > **Security** > **Authentication**.
3. From the Authentication Type drop-down list, select **LDAP**.
4. Select the SSL check box and then from the Certificate drop-down list, select the Certificate file that you loaded in step 1.
5. If you wish to use the LDAP credentials to login to AudioCodes devices using Single Sign-on, select check box "Use LDAP Credentials for Device Page Opening". When configured, the LDAP credentials are used to login to AudioCodes devices over Single Sign-on instead of the HTTP/S credentials defined in the device settings or in the tenant's SNMP profile.

For more information, refer to the *One Voice Operations Center User's Manual*. When this file is loaded

6.4.8.2 RADIUS Server Authentication

This section describes how to secure the connection between the OVOC server and a RADIUS server for RADIUS-based authentication. You can centrally configure authentication of OVOC operators using a RADIUS (Remote Authentication Dial-In User Service) server. If the connection to the RADIUS servers fails, the local operators database can be automatically used as a backup after a defined timeout, i.e., if the RADIUS connection fails, the user and password are replicated to the local users database so the operator can log in to the OVOC as a local user (configured by parameter 'Enable Local Authentication on Radius Timeout' and dependent on the timeout value defined in 'RADIUS Auth Retransmit Timeout (msec)').

When the RADIUS-authenticated operator logs into the OVOC, they're assigned one of the OVOC security levels, for example 'Operator'. If it's not defined on the RADIUS server, the OVOC by default allows access for the RADIUS-authenticated operator, with 'Operator' permission.

➢ **Do the following:**

1. Open the Authentication page (**System** tab > **Administration** > **Security** > **Authentication**.
2. From the Authentication Type drop-down list, select **RADIUS**.
3. Configure the parameters:
   - 'RADIUS retransmit timeout' (Default: 3000 milliseconds). If this timeout expires, local authentication is performed.
   - 'RADIUS auth number of retries' (Default: 1)

   Note that these parameters will be used for each RADIUS Server.
4. Select the **Enable display of RADIUS reply message** option. Default: Cleared.
5. From the 'Default Authentication Level' dropdown, select either **Operator** (default), **Amin**, **Monitor** or **Reject**.
6. For each of the three RADIUS servers, define the server's IP address, port and secret. At least one server must be provisioned. 'Server Secret' defines the shared secret (password) for authenticating the device with the server. Must be cryptically strong. Also

used by the server to verify authentication of RADIUS messages sent by the device (i.e., message integrity). See the device's manual for more information.

7. If you wish to use the RADIUS credentials to login to AudioCodes devices using Single Sign-on, select check box “Use RADIUS Credentials for Device Page Opening”. When configured, the RADIUS credentials are used to login to AudioCodes devices over Single Sign-on instead of the HTTP/S credentials that are defined in the device settings or in the tenant’s SNMP profile.

Note: If an operator tries to log in to RADIUS and it's inaccessible, a local login to the OVOC is attempted and 'Authentication Type' is automatically switched to **OVOC** (local authentication). When the connection is re-established, the operator must manually switch back authentication mode.

For more information, refer to the *One Voice Operations Center User’s Manual*.

6.4.8.3 Active Directory Server (Skype for Business Users) – OVOC Voice Quality Package

This section describes how to secure the connection between the OVOC and the Skype for Business Active Directory server for managing Skype for Business users using the OVOC Voice Quality Package. This connection is secured using Microsoft certificates. When these certificates are loaded to OVOC, the /opt/ssl/keystore.jks directory is updated.

➢ **Do the following:**

1. Open the Software Manager (System > Configuration > File Manager), then click **Add > Add Auxiliary File**, select File Type ‘Certificate’ and add the required certificate file.
2. Open the Active Directory Settings page (**Users** tab > **Active Directories**) and then click **Edit**.
3. Select the ‘Enable SSL’ check box and then from the Certificate file drop-down list, select the certificate file that you loaded in step 1.

For more information, refer to the *One Voice Operations Center User’s Manual*.

6.4.8.4 OVOC and Skype for Business MS-SQL SSL Connection-– Voice Quality Package

This section describes how to secure the connection between the OVOC server and the Skype for Business MS SQL Monitoring server for monitoring using the OVOC Voice Quality Package. This connection is secured using Microsoft certificates. When these certificates are loaded to OVOC, the /opt/ssl/keystore.jks directory is updated.

➢ **Do the following:**

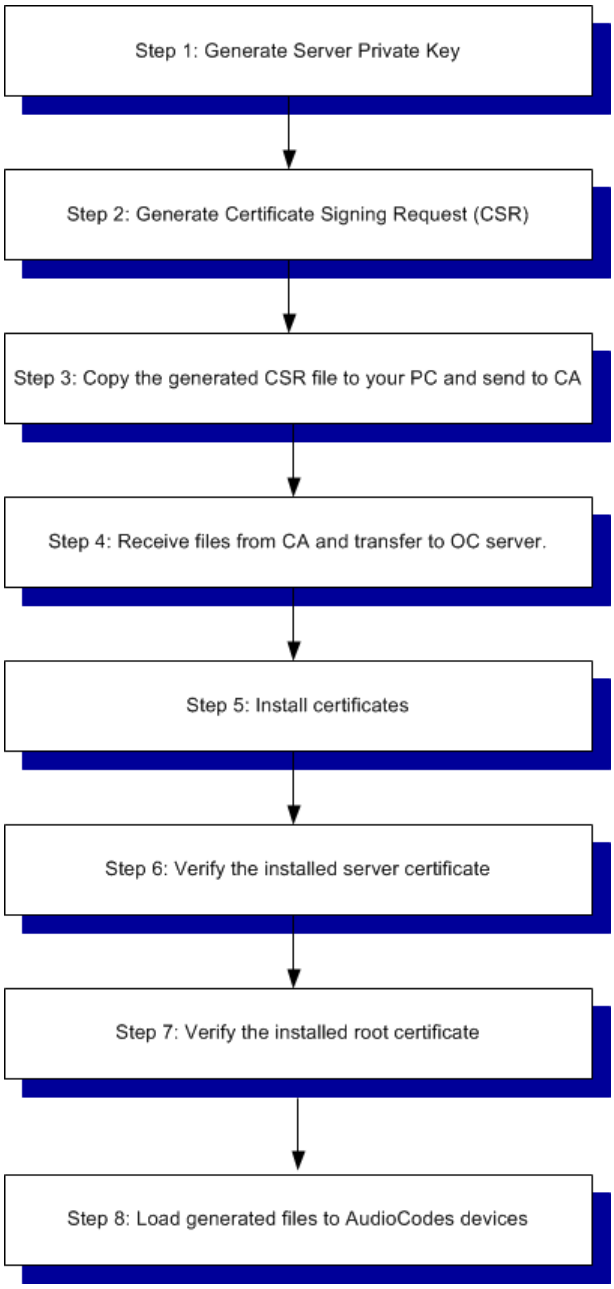
1. Open the Software Manager (System > Configuration > File Manager), then click **Add > Add Auxiliary File**, select File Type ‘Certificate’ and add the required certificate file.
2. Open the Lync Device Details screen (Network tab > Topology), select the Skype for Business device and then click **Edit**.
3. From the SSL drop-down list, select **Using Certificate** and then from the Certificate File drop-down list, select the certificate file that you loaded in step 1.

   For more information, refer to the *One Voice Operations Center User’s Manual*.

6.5 Generating Custom OVOC Server Certificates

Default SSL certificates can be replaced by custom certificates using the Server Certificates Update menu option in the EMS Server Manager (refer to Section 'Server Certificates Update' in the IOM manual). The figures below illustrate the workflow process for deploying the new custom server certificates using this menu option.

Figure 6-2: Server Certificate Deployment Workflow



- **Step 1:** Generate the Server Private Key according to selected required bits.
- **Step 2:** Generate the Certificate Signing Request (CSR) with the private key password generated in step 1 and personal/corporate identification details.
- **Step 3:** Copy the CSR to your PC and send to the desired root CA for signing.
- **Step 4:** Copy the certificate files that you receive back from the root CA to the OVOC server.
- **Step 5:** Install the certificate files

  HA systems must be uninstalled, and then you must perform this procedure separately on both server machines (as stand-alone machines.
- **Step 6 & 7:** Run verification procedures to verify that the certificates have been installed.
- **Step 8:** Load the generated files to AudioCodes devices.

  For securing connection with AudioCodes devices, you must also load the generated files to the AudioCodes devices as described in Section 6.4.6.

Note:

- If you did not generate the Certificate Signing Request using the EMS Server Manager:
  - √ Follow the workflow procedures for step 4 onwards.
  - √ You need to create the /home/acems/server_certs directory (refer to Step 4 in the Server Certificates Update procedure in the *IOM manual* for details).
- The root certificate should be named root.crt and that the server certificate should be named server.crt. If you received intermediate certificates then rename them to ca1.crt and ca2.crt.
- Make sure that all certificates are in PEM format (refer to Appendix “Verifying and Converting Certificates” in the *IOM manual*).

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: www.audiocodes.com

Document #: LTRT-94046