AudioCodes One Voice Operations Center (OVOC)

OVOC

Security Guidelines

Version 7.8

audiocodes

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: October-02-2020

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 website at https://www.audiocodes.com/services-support/maintenance-and-support.

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 website at https://online.audiocodes.com/documentation-feedback.

Stay in the Loop with AudioCodes

Related Documentation

Document Name
Mediant 500 MSBR User's Manual
Mediant 500L MSBR User's Manual
Mediant 500L Gateway and E-SBC User's Manual

Document Name
Mediant 800B Gateway and E-SBC User's Manual
Mediant 800B MSBR User's Manual
Mediant 1000B Gateway and E-SBC User's Manual
Mediant 1000B MSBR User's Manual
Mediant 2600 E-SBC User's Manual
Mediant 3000 User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
Migration from EMS and SEM Ver. 7.2 to One Voice Operations Center
One Voice Operations Center IOM Manual
One Voice Operations Center Product Description
One Voice Operations Center User's Manual
Device Manager Pro Administrator's Manual
One Voice Operations Center Alarms Monitoring Guide
One Voice Operations Center Performance Monitoring Guide
One Voice Operations Center Security Guidelines
One Voice Operations Center Integration with Northbound Interfaces
Device Manager for Third-Party Vendor Products Administrator's Manual
Device Manager Agent Installation and Configuration Guide
ARM User's Manual

Document Revision Record

LTRT	Description
94051	Added Sections: Step 6: Implementing HTTP Tunnel Overlay (Cloud Architecture); Enterprise Firewall with Cloud Architecture Updated Section: Implement Two-Way (Mutual) Authentication with X.509 Certificates for Enterprise Device Connections; Firewall table and Figure; HTTPS Security Figure
94052	Updated Section: Step 1: Implementing Server Security Settings; Securing Trap Forwarding over SNMPv3; Connecting OVOC to Managed Devices without Cloud Architecture; OVOC Security Solution; Enabling HTTPS/SSL/TLS Connections; Defining OVOC Users and sub-sections; Implementing Local OVOC Database Authentication and sub-sections; Firewall Configuration Schema and NAT Firewall Settings; Device Manager Connections Added Sections: NTP and Clock Synchronization; Step 7: Northbound Interface Connections; Step 8: Setting Up NAT Connections; Firewall Rules for NAT Configuration Options; Privacy Mode; Security Fix Backporting Removed Section: Implementing Local Database Authentication; Prefer SNMPv3 over SNMPv2 Moved Section: Configure Cloud Architecture Mode (HTTPS Overlay Network)
94053	Updated Section: Establishing Connections for Device Manager Devices Added Section: Managing Microsoft Teams Phones; Inbuilt Features; HTTP X-Header Security Tags

Table of Contents

This page is intentionally left blank.

1 Introduction

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

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 on page 3
- Securing the Application (Identity Management):
  - Step 2: Defining OVOC Users on page 10
- Securing the Communication:
  - Step 3: Configuring Enterprise Firewall on page 20
  - Step 4: Securing SNMP Interface Access (OVOC) on page 33
  - Step 5: Implementing X.509 Authentication on page 34
  - Step 6: Setting Up Northbound Interface Connections on page 46
  - Step 7: Managing Device Connections on page 47

Securing the OVOC Server Platform

2 Step 1: Implementing Server Security Settings

This step describes enhanced security settings that can be implemented using the OVOC Server Manager to prevent intrusion to the OVOC server platform. The OVOC 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 OVOC 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. In addition, each OVOC release version includes the latest security updates for the RPM packages that are available in the official CentOS/RHEL repositories (see Backporting Security Fixes below).

This Section describes the following actions that can be performed in the OVOC Server Manager to enhance security:

- Changing the OS Password on the next page
- Changing Database Default Password on page 5
- Provisioning SSH Options to Access OVOC Server on page 5
- Integrity Testing on page 6
- Transferring Files Using SFTP / SCP on page 6
- Advanced Security Options on page 7
- NTP and Clock Synchronization on page 8

Inbuilt Features

The OVOC Server includes the following inbuilt features:

- Backporting Security Fixes below
- HTTP X-Header Security Tags on the next page

Backporting Security Fixes

Security scans may reveal that the available version for RedHat/CentOS httpd upstream packages is higher than the installed version. This may be due to the RedHat/CentOS Security scans not taking backporting into account. In this regard, when AudioCodes detects a specific vulnerability, it incorporates the related fix not only in the latest upstream version, but also in older versions i.e. backports the fix to the older version, distributed by RedHat/CentOS and makes these updates available to the AudioCodes software distribution list.

Each OVOC release version includes the latest security updates for the RPM packages that are available in the official CentOS/RHEL repositories – including kernel, openssl, PHP and other components. Although these packages do not include the latest available upstream version, they are not necessarily vulnerable to all the vulnerabilities listed in RedHat/CentOS security scan reports.

For more information on Security Backporting, refer to:

https://access.redhat.com/security/updates/backporting/

HTTP X-Header Security Tags

The OVOC Server embeds the following security tags in X-headers for HTTP responses to OVOC clients:

- **HTTP 401 Unauthorized**: these responses from the OVOC server to managed AudioCodes devices now includes the standard "www-authenticate" header with "Basic" scheme.
- OVOC Server HTTP X-header responses from the OVOC server to all OVOC clients include the following tags for enhanced security:
    - **x-frame-options**: prevent hijack attacks attempts to clicks (click-jacking) that are designated for the original server and send them to another server. This ensures that content is not embedded into other sites.
    - **X-XSS-Protection**: prevent Cross-Site scripting attacks that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks.
    - **set X-Content-Type (Options nosniff)**: protect against MIME sniffing vulnerabilities by ensuring that the MIME types advertised in the Content-Type headers are not changed and are interpreted as deliberately configured.

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.

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.*

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 'OVOC DB Password' in the *OVOC IOM*.

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

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

> ⚠ 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

> ⚠ 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

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.

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.

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*.

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. Refer to Section 'Software Integrity Checker (AIDE) and Pre-linking' in the One Voice Operations Center Server IOM.

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 Guide*.

Advanced Security Options

This section includes the following advanced security configuration options:

- Auditd below
- Network Options below

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.

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.

NTP and Clock Synchronization

Network Time Protocol (NTP) is used to synchronize the time and date of the OVOC server (and all its components) with other devices in the IP network You can configure the OVOC server to either obtain its NTP clock from an external source or from its own server. Consequently OVOC clients and subnets can synchronize with one of these clock sources. If the OVOC server is configured as a Stand-alone server, then you can configure the clients and subnets which are authorized to synchronize with the OVOC clock (see below).

- It is recommended to configure the OVOC server to synchronize with an external clock source because the OVOC server clock is less precise than other NTP devices. For example, for OVOC cloud deployments, it is recommended to configure the AWS/Azure IP address or Domain Name as the NTP clock source.
- Configure the same NTP server clock source on both the OVOC server and the managed AudioCodes device (Setup menu > Administration tab > Time & Date).

- **Restrict Access to NTP Clients:** If you have configured the OVOC server as an NTP server, then you can configure NTP rules to authorize which clients are permitted to synchronize with the OVOC system NTP clock (see Section "Restrict Access to NTP Clients" in the *OVOC IOM*).
- **Authorizing Subnets:** When the OVOC server is configured as an NTP server, you can configure NTP rules to authorize which subnets can connect to synchronize with the OVOC system clock (see Section Authorizing Subnets to Connect to OVOC in the *OVOC IOM*).
- **Activate DDoS Protection:** You can activate DDos protection to prevent Distributed Denial of Service attacks on the OVOC server. For example, attacks resulting from security scans. This is relevant for both when the OVOC server is configured as a Stand-alone clock source and when an external clock source is used.

Securing the Application

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.

Authenticating OVOC Users with External User Databases

It is recommended to use an external databases for securing OVOC users using one of the following platforms:

- LDAP Server
- Microsoft Azure
- RADIUS Server

When a user attempts to log in to OVOC, the login user name and password are validated, and if successful, OVOC then determines the user's OVOC security level based on the custom OVOC attribute on the external platform. If one of the OVOC Security levels has not been defined (see Provisioning Operator Security on page 14), .the parameter 'Default Operator Type and Security Level' (LDAP and Azure) and Default Auth level (RADIUS) in the Authentication page determines behavior:

- If a security level has been defined on the external platform for this parameter, the user is logged in with this security level
- If this parameter is set to "Reject", then the user will not be able to login.

External Authentication and Multi-Tenancy

Both the LDAP and Microsoft Azure user authentication types support multi-tenancy. When System or Tenant operators login to OVOC they view only elements belonging to their tenants. For LDAP, a single authentication server is used.

⚠ Multi-tenancy is not supported for RADIUS server user authentication.

Microsoft Azure

If you already have centralized user authentication using Microsoft Azure Active Directory, it's recommended to implement it for OVOC operators as well.

➢ **Do the following:**

1. Open the Authentication page (System > Administration > Security > Authentication) and from the 'Authentication Type' drop-down, select AZURE.

2. View the read-only 'Security Azure Hostname' field. It defines the name of the Azure AD host in the cloud. It allows OVOC to access Azure AD in the cloud.
3. From the 'Azure AD Path Type File' drop-down, select Organizations (default) or Tenant.
   - If you choose 'Tenant', the field 'Azure Tenant ID' is activated - see the next step. A string must be configured for it (mandatory).
   - If you leave at the default (Organizations), OVOC will be able to access Azure AD in the enterprise network if a standard service is purchased.
4. View the 'Azure Tenant ID' field. It will be read-only if Organizations is selected in the preceding step. The preceding figure shows 'Azure Tenant ID' as a read-only field defined with the string tenant-Id. If a new tenant ID is purchased, the OVOC first accesses the cloud via the 'Security Azure Hostname' field and then (via the 'Azure Client ID' field) a specific Azure AD in the enterprise's network.
5. In the 'Azure Client ID' field, enter the ID of the Azure AD client.
6. In the 'Azure Client Secret' field, define the shared secret (password) to allow the OVOC application access to the specific Azure AD (OVOC authentication). Must be cryptically strong. The OVOC will then be capable of accessing the Azure AD.
7. Under the "Authentication Level Settings" section, set the names for the Authentication Groups.
8. Under the section 'Endpoints Groups Authorization Level Settings', configure the 'Tenant Endpoints Group User Group Name' parameter.
9. Under the section 'GW / SBC / MSBR Authentication', select the option Use AD Credentials for Device Page Opening for the OVOC to sign operators in to AudioCodes devices using the same credentials they used to sign in to the OVOC. The AudioCodes device will then perform authentication with the Azure AD and login to the AudioCodes device will be attempted with same AD user name / password instead of the HTTP/S credentials that are defined in the device settings or in the tenant’s SNMP profile.
10. Click **Submit**.

■ Logging in as an Azure User with Multi Factor Authentication:

➢ To log in as an Azure user with Multi-Factor Authentication:

1. Point your browser to the OVOC server's IP address: https://<IP Address>. You only need to enter its IP address; the rest of the URL is automatically added. Logging in can optionally be performed using FQDN rather than IP address.
2. Enter your Username and Password and then click Login.
3. During the Azure authentication process, the server detects that Multi Factor Authentication is required and opens an additional window (Microsoft window) in which the operator performs MFA authentication.

4. Enter your Microsoft password and click Sign in. An SMS is sent to your cellular phone including a code. (this is one of the methods employed). The MFA method is configured in the Azure Active Directory.

5. Enter the 'Code' and then click Verify.

The GUI by default displays the Dashboard.

LDAP Server

If you already have centralized user authentication via an LDAP server, it's recommended to implement it for OVOC operators as well. This connection is secured using Microsoft certificates, which are saved to the /opt/ssl/keystore.jks directory on the OVOC server.

➢ **Do the following:**

1. In the OVOC, open the Authentication page (**System** > **Administration** > **Security** > **Authentication**).
2. From the 'Authentication Type' drop-down, select **LDAP**.
3. Configure the 'LDAP Authentication Server IP'.
4. Configure the 'LDAP Authentication Server Port'.
5. Configure the 'LDAP Connectivity DN' parameter using an Active Directory Service Account (mandatory), for example, MyServiceAccount@domain.
6. Configure the 'LDAP Connectivity Password' as required.
7. In the 'LDAP Server Number of Retries' field, enter the number of login attempts the operator can make before they're suspended. When the number is reached, the operator is blocked. Only the 'system' operator whose security level is 'Administrator' can then unblock them. Default: 3 attempts.
8. Configure the 'User DN Search Base' as required.
9. Select the 'SSL' option to secure the connection with the LDAP server over SSL; the 'Certificate' drop-down is activated.

⚠ Make sure you load the SSL certificate file, required by the LDAP Active Directory platform, to the OVOC Software Manager.

10. From the 'Certificate' drop-down, select the certificate file to secure the connection with the LDAP server over SSL.
11. In the "Authorization Level Settings" section, enter the required names of the Authentication Groups.
12. Under the screen section 'GW / SBC / MSBR Authentication', select the option "Use AD Credentials for Device Page Opening" to enable OVOC operators to login to AudioCodes devices using the LDAP server credentials instead of the HTTP/S credentials that are defined in the device settings or in the tenant’s SNMP profile.

13. Click **Submit**.

RADIUS Server

If you already have centralized user authentication via an RADIUS (Remote Authentication Dial-In User Service)server, it's recommended to implement it for OVOC operators as well.

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 'Radius Transmit Timeout' and dependent on the timeout value defined in 'RADIUS auth number of retries' .

➢ **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)

> 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 the required value,.
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.

> 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*.

Combined Authentication Mode

When the Combined Authentication Mode is enabled and an operator attempts to log in to the external server, however it's unavailable, OVOC connects to the local database with the same operator credentials.

For example, if the local user database is configured as the first order and the local user does not exist, OVOC attempts to connect to the external database LDAP or RADIUS with the same user credentials. When the RADIUS,or LDAP or Microsoft Azure Authentication Types and the "Combined Authentication Mode" are both configured, the Fixed License Pool and Floating License functionality are supported (using the local database credentials).

➢ To enable the Combined Authentication Mode:

- Under Combined Authentication Mode, select the Enable combined authentication option, the 'Authentication Order' drop-down is enabled from which External First or Local First can be selected.
  - **External First:** If the Azure server is unavailable when the externally authenticated operator attempts to log in, OVOC connects with the same operator credentials to the local (OVOC) operators database.
  - **Local First:** If the operator is not found in the local (OVOC) operators database, OVOC connects with the same operator credentials to the external authentication server.

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 networ	No	No	In this tenant networ	No	Yes

Operator Type	Security Level	Define Operators	Manage Tenants	Manage Global/System Entities/Resources	Manage Tenant Resources	Monitor System Resources	Monitor Tenant Resources
		k only			k only		
	Operator	No	No	No	In this tenant network only	No	Yes
	Monitor	No	No	No	No	No	Yes
	Mon-itoring Links	No	No	No	No	No	Links Only
Endpoints Group (Tenant)	Admin or Operator	No	No	No	Only for endpoints in the managed Group	Yes	Yes
UMP Operator (System)	Operat-or	No	Yes	Yes	Yes	Yes	Yes

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 phone deployments, Endpoint groups can be defined to manage specific phones in a site i.e. for upgrades (see also Operator Type below).

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”: Operator with Viewing only permissions:
    - Monitor all tenants specific entities/resources
    - Monitor system entities/resources
    - Monitor global entities/resources
- UMP Operator used for managing the connection with the Microsoft Teams Office 365 platform as part of the AudioCodes Live Teams Cloud solution.
- 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 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
- Tenant "Monitoring Links": The Monitoring Links has privileges for the managed links only:
  - Sites defined as link destinations and devices defined as source/destination to the links.
  - Assigned links in the Network screen
  - Alarms and events for the assigned link entities
  - Statistics for assigned links
  - Notifications for tasks and alarms only for the assigned links
- Endpoints Group Tenant operator used for managing Tenant Endpoints Groups. When defining Tenant operator (with "Admin" or "Operator" permissions), ensure to select the check box "Restrict Endpoints Actions Except for these Groups".

Privacy Mode

“Privacy” mode can been enabled by System operators to hide the following OVOC data from Tenant and System operators:

- Masking of gateway and SBC phone numbers
- Hiding of existing User/URI reports or schedulers
- Hiding of existing user tables and statistics
- Hiding of User/URI reports and their respective schedulers
- Hiding of new Calls/SIP Ladder
- For Skype for Business call:
  - Partial masking for Phone CDRs
  - Full masking for CDR URIs
  - Full masking for MDRs

- Full masking for Conference CDRs.

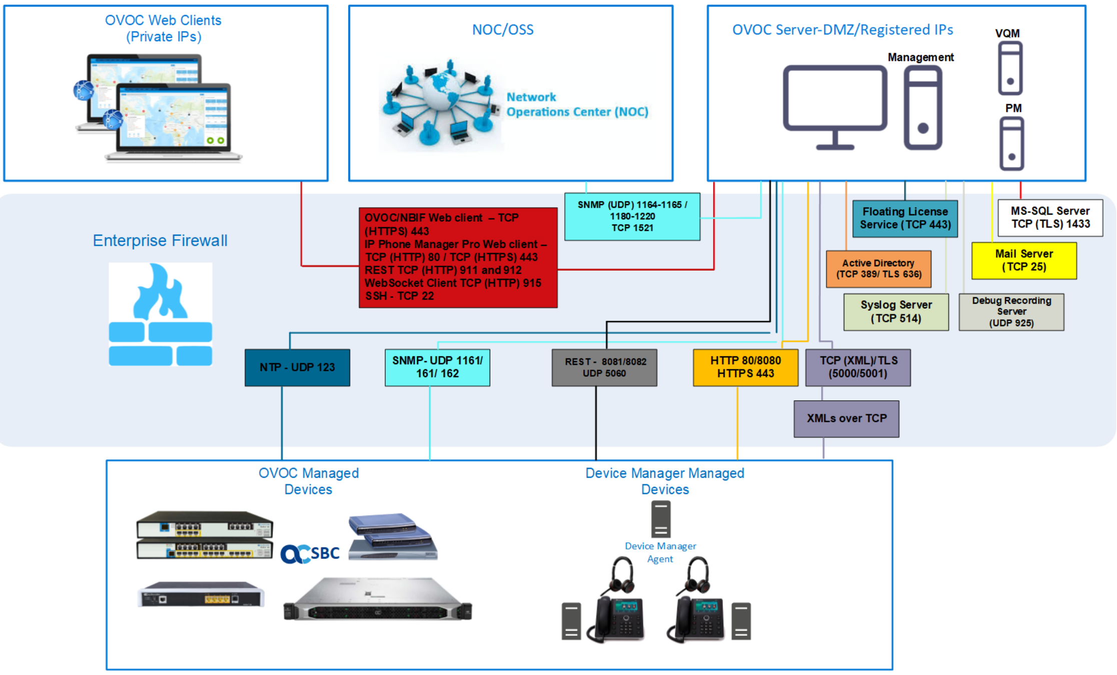
Securing the Communication

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


OVOC Web Clients
(Private IPs)
NOC/OSS
Network
Operations Center (NOC)
OVOC Server-DMZ/Registered IPs
VQM
Management
PM
Enterprise Firewall
OVOC/NBIF Web client – TCP (HTTPS) 443
IP Phone Manager Pro Web client – TCP (HTTP) 80 / TCP (HTTPS) 443
REST TCP (HTTP) 911 and 912
WebSocket Client TCP (HTTP) 915
SSH - TCP 22
SNMP (UDP) 1164-1165 / 1180-1220
TCP 1521
Floating License Service (TCP 443)
MS-SQL Server TCP (TLS) 1433
Active Directory (TCP 389/ TLS 636)
Mail Server (TCP 25)
Syslog Server (TCP 514)
Debug Recording Server (UDP 925)
NTP - UDP 123
SNMP- UDP 1161/ 161/ 162
REST - 8081/8082 UDP 5060
HTTP 80/8080 HTTPS 443
TCP (XML)/TLS (5000/5001)
XMLs over TCP
OVOC Managed Devices
SBC
Device Manager Managed Devices
Device Manager Agent

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 recommended firewall configuration according to the highest level of security that can be implemented on the OVOC server platform.

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

Table 4-1: Recommended Firewall Port Configuration

Connection Type	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: 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: device	OVOC server side / Receive only.
Device ↔ OVOC server (Trap Manager)	UDP	√	161	SNMPv3 Trap Manager port on the device that is used to send traps to the	MG side / Bi-directional

Connection Type	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				OVOC. Initiator: OVOC server	
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
Devices					
OVOC server ↔ Device Manager Pro	TCP (HTTPS)	√	443	HTTPS connection between the OVOC server and the Device Manager Pro Web page. Initiator: client browser	OVOC server side / Bi-directional.
				HTTPS connection used by devices for downloading firmware and	

Connection Type	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				configuration files from the OVOC server. Initiator: Device	
OVOC server ↔ Devices (used for backward compatibility)	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 devices configuration file. Initiator: Device	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: Endpoint	OVOC server side / Bi-directional

Connection Type	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
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
RADIUS Server					

Connection Type	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
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 Type	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
		×	TCP connection for Data Analytics DB Access Initiator: DB Access	N/A	1521

Source IP Address Range	Destination IP Address Range	Secured Connection	Protocol	Source Port Range	Destination Port Range
			client This port is open when the "Data Analytics" Voice Quality feature license has been purchased and the feature has been enabled		

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
NOC/OSS	OVOC	×	NTP	123	123
		√	SNMP (UDP) Trap	1024-65535	162
		√	SNMP (UDP) Set for Active alarms Resync feature	1164-1165	-
		√	SNMP (UDP) port for alarm forwarding	1180-1220	-

Firewall Rules for Cloud Architecture Mode

When the OVOC server is deployed in a public cloud and the Cloud Architecture feature is enabled (see Configure Cloud Architecture (HTTPS Tunnel Overlay) on page 47), all proprietary connections between SBC devices and the OVOC server are bundled into an HTTP/S tunnel overlay network over ports 80/443, therefore these ports must be open on the Enterprise firewall. Configuring other Enterprise firewall rules for SBC and OVOC server connections is not necessary.

- For maximum security, Its advised to implement this connection over HTTPS port 443 with one-way authentication.
- Mutual authentication is not supported for this mode.
- AudioCodes and custom certificates can be used to secure the connection between SBC devices and the OVOC server.

Firewall Rules for NAT Configuration Options

The table below describes the ports to open on Enterprise or Cloud firewall deployments for devices managed behind a NAT for the different configuration options as described in Step 7: Managing Device Connections on page 47.

Table 4-4: Firewall Rules for NAT Configuration

Configuration Option	Ports to Configure	Port side / Flow Direction
SBC Devices		
Cloud Architecture Mode (Device > OVOC)	■ TCP HTTP 80 ■ TCP HTTPS 443	OVOC server side / Bi-directional
OVOC Server NAT Mode (OVOC > Devices)	SNMP UDP port 1161	OVOC server side / Receive only
	SNMP UDP port 162	OVOC server side / Receive only
	TCP 5000	OVOC server side / Bi-directional
	TCP 5001 (Voice Quality Management over TLS)	OVOC server side / Bi-directional
	NTP 123 NTP server port (configure the OVOC server's Public IP address as the NTP server)	Both sides / Bi-directional
Phones		
Device Manager Agent	TCP HTTPS Port 443	OVOC server side / Bi-

Configuration Option	Ports to Configure	Port side / Flow Direction
		Directional

Firewall Rules for Service Provider Cluster Mode

This table is applicable for the Management Server when Service Provider Cluster mode is enabled.

Table 4-5: OVOC Service Provider Cluster Mode

Connection Type	Ports to Configure	Access	Secured	Port side / Flow Direction
OVOC Clients and OVOC Server				
HTTP/REST	80	Public (MGMT)	×	OVOC Management server side / Bi-directional
	443	Public (MGMT)	√	OVOC Management server side / Bi-directional
REST	911	Private (MGMT)	×	OVOC Management server side / Bi-directional
Floating License	912	Private (MGMT)	×	OVOC Management server side / Bi-directional
Websocket	915	Private (MGMT)	×	OVOC Management server side / Bi-directional
OVOC Server and Managed Devices				
SNMP / Traps	1161	Public (MGMT)	√ (v3)	OVOC Management server side / Bi-

Connection Type	Ports to Configure	Access	Secured	Port side / Flow Direction
				directional
SNMP	161	Public (MGMT)	√ (v3)	OVOC Management server side / Bi-directional
SNMP Traps	162	Public (MGMT)	√ (v3)	OVOC Management server side / Bi-directional
NTP	123	Public (MGMT)	×	OVOC Management server side / Bi-directional
PM Server and Managed Devices				
HTTPS REST connection used for polling managed devices.	443	Public (MGMT)	√	OVOC Management server side / Send only
Voice Quality Package and SIP Publish				
Voice Quality Package	5001	Public (MGMT)	√	OVOC Management server side / Receive only
SIP 6035	5060	Public (MGMT)	×	OVOC Management server side / Receive only
Phones				
IPP Files	8080	Public (MGMT)	×	OVOC Management server side / Bi-directional
IPP REST	8082	Public	√	OVOC

Connection Type	Ports to Configure	Access	Secured	Port side / Flow Direction
		(MGMT)		Management server side / Bi-directional
External Servers				
Skype for Business	1433	Skype For Business Server	√	OVOC Management server side / Bi-directional
LDAP	636	LDAP Server	√	OVOC Management server side / Bi-directional
RADIUS	1812	On RADIUS Server	✘	OVOC Management server side / Bi-directional
Mail Server (forwarding)	25	Mail Server	✘	OVOC Management server side/ Bi-directional
Syslog Server	514	Syslog Server	✘	OVOC Management server side / Bi-directional
Dedicated Cluster Node Ports				
Akka platform used for inter-process communication	2551..2555	Private (All) Required access from cluster servers	✘	OVOC Management server side/ Bi-directional
Java Database Connectivity (JDBC) used for communication with the PM server	1521	Private (MGMT)	✘	OVOC Management server side / Bi-directional

Connection Type	Ports to Configure	Access	Secured	Port side / Flow Direction
				Accessed only from other PM/VQM servers
Kafka platform used for inter-process communication	9092	Private (All) Required access from cluster servers	✗	OVOC Management server side / Bi-directional
ZooKeeper	2181	Private (All) Required access from cluster servers	✗	OVOC Management server side / Bi-directional

5 Step 4: Securing SNMP Interface Access (OVOC)

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

Securing Trap Forwarding over SNMPv3

The SNMPv3 protocol can be used for securing traps that are generated on devices. The SNMP connection must be configured on both OVOC and on the devices. 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 Section "Automatic Detection" in the *OVOC User's Manual*.

⚠

- It is recommended to use SNMP Version 3 (SNMPv3) (and not SNMPv1 and SNMPv2c). 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.
- For Cloud platforms (Microsoft Azure and Amazon AWS) SNMP is by default disabled for security reasons. To enable it, in the managed SBC devices Web interface, set parameter 'Disable SNMP' to **No** (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP Community Settings**).

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.

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

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 OVOC 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.

When implementing a TLS (HTTPS) connection with AudioCodes devices, the default OVOC AudioCodes device certificates must be loaded to AudioCodes devices (see Connecting OVOC to Managed Devices without Cloud Architecture on page 40 and Securely Connecting OVOC to SBC Devices with Cloud Architecture on page 48). In addition, when replacing default certificate files with custom certificate files (see Generating Custom OVOC Server Certificates); these certificate files should also be loaded to the AudioCodes devices.

Recommended Workflow

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

OVOC Client and Servers

1. Setup HTTPS connections using default certificates

2. Implement custom server certificates (overriding default certificates) using the OVOC Server Manager Server Certificates Update option (see Generating Custom OVOC Server Certificates on page 44).

> ⚠ 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.

Devices

Setup the endpoint connections for REST updates and statutes sent from end user devices and for downloading firmware and configuration files. Connection with devices is over SSL without certificate authentication.

External 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. See
- Setup the RADIUS server connection. This connection is secured by a RADIUS secret password and other RADIUS parameters: Refer to Step 2: Defining OVOC Users on page 10 for setting up user authentication and to the *Northbound Integration Guide* for setting up the RADIUS client and server.
- Data Analytics API: If you have purchased a license to use the Data Analytics API from Northbound Interfaces, see Data Analytics API on page 46

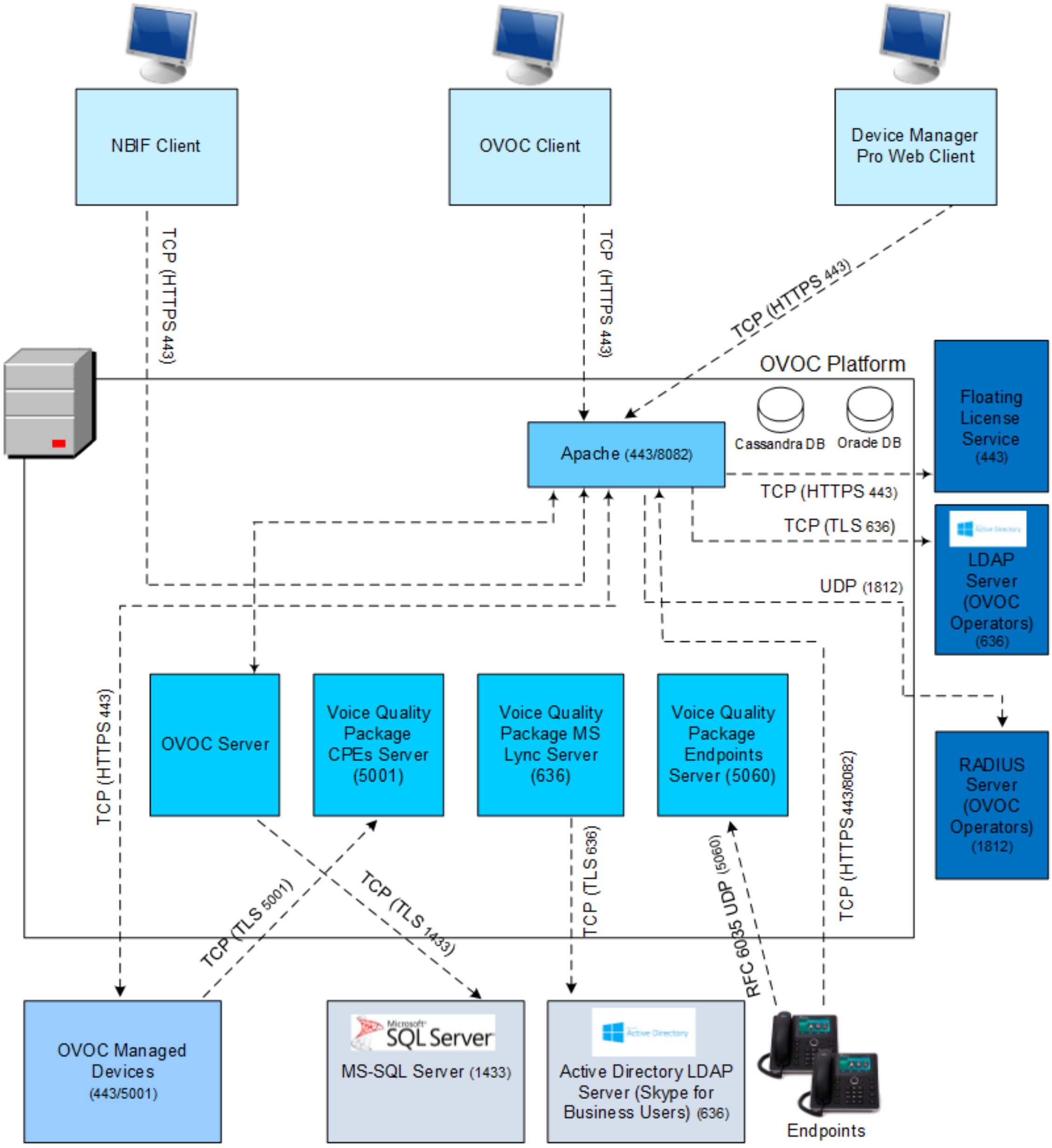
Enabling HTTPS SSL TLS Connections

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.

> ⚠ For browser and Java version compatibility, refer to the *One Voice Operations Center IOM manual*.

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

Figure 6-1: OVOC Maximum Security Implementation


NBIF Client
OVOC Client
Device Manager Pro Web Client
TCP (HTTPS 443)
TCP (HTTPS 443)
TCP (HTTPS 443)
OVOC Platform
Apache (443/8082)
Cassandra DB
Oracle DB
Floating License Service (443)
TCP (HTTPS 443)
TCP (TLS 636)
LDAP Server (OVOC Operators) (636)
UDP (1812)
RADIUS Server (OVOC Operators) (1812)
TCP (HTTPS 443)
OVOC Server
Voice Quality Package CPEs Server (5001)
Voice Quality Package MS Lync Server (636)
Voice Quality Package Endpoints Server (5060)
TCP (HTTPS 443/8082)
TCP (TLS 5001)
TCP (TLS 1433)
TCP (TLS 636)
RFC 6035 UDP (5060)
OVOC Managed Devices (443/5001)
SQL Server
MS-SQL Server (1433)
Active Directory LDAP Server (Skype for Business Users) (636)
Endpoints

This version supports TLS versions 1.0, 1.1. and 1.2

The following connections are described in this section:

Table 6-1: OVOC Connections

Connection Type	Reference
OVOC HTTPS client ↔ OVOC Apache server	OVOC Web Client on the next page
OVOC Device Manager Pro browser ↔ OVOC	Device Manager Pro Web Client on the next page

Connection Type	Reference
Apache Server	
OVOC server ↔NBIF client	NBIF Client on page 46
OVOC server ↔ OVOC Managed Devices	OVOC and Floating License Service Connections on page 43
OVOC Voice Quality Package ↔ Endpoints	OVOC Voice Quality Package and Enterprise Device Communication on page 41
Third-Party Vendor Server Connections	
OVOC server ↔ Active Directory LDAP server- User authentication	LDAP Server on page 12
OVOC server ↔ RADIUS server- User authentication	RADIUS Server on page 13
OVOC server ↔ Microsoft Azure- User Authentication	Microsoft Azure on page 10
OVOC server ↔ Microsoft Active Directory LDAP Server Skype for Business	Active Directory Server (Skype for Business Users) – OVOC Voice Quality Package on page 42
OVOC server ↔ Skype for Business MS-SQL Server Skype for Business Server	OVOC and Skype for Business MS-SQL SSL Connection–– Voice Quality Package on page 42

OVOC Web Client

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

Device Manager Pro Web Client

The connection to the Device Manager Pro Web page is by default enabled over HTTPS through port 443. This is managed by the OVOC 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 the IOM manual). This connection is secured using the AudioCodes self-signed certificate. In addition, in the Device Manager Pro configure the following:

- ‘Secure (HTTPS) communication from the Device Manager to the Devices’ (Setup tab > System Settings). When configured, this parameter secures requests from the Device Manager Pro to the device over HTTPS. 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 Device Manager 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.
- Device Management Agent: to secure the connection between the Device Management Agent and the Device Manager over HTTPS:
  - Install the OVOC server certificate on the Windows server running the Device Management Agent
  - In the Device Manager Agent Web interface, enter the IP address of the OVOC server as follows:

    https://<OVOC Server_IP address

> To fully secure this connection, the Device Manager service key must also be configured in the Agent Web interface. This key can be taken from the Device Agents page in the Device Manager web (Setup &gt; System &gt; Device Agents). For more information, refer to the Device Manager Agent Installation and Configuration Guide.

- Jabra Integration Service: to secure the connection between the managed device and the Device Management Agent over HTTPS, configure the IP address of the OVOC server as follows:

    https://<OVOC Server_IP address

  For more information, refer to the Device Manager for Third-Party Vendor Products manual.

Device Manager Connections

The HTTPS connection between devices and the Device Manager Pro is managed 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 devices over HTTPS through port 443 (see Device Manager Pro Web Client on the previous page).

- "Secure (HTTPS) communication from the Device Manager to the Devices" (default not enabled): Sends secured (HTTPS) requests from the Device Manager Pro server to the phones. If this option is selected, communications and REST actions such as Restart, Send Message, etc. are performed over HTTPS. This parameter is not relevant when using an SBC HTTPS (OVOC Services) proxy server.

> ⚠ This parameter is relevant for the direct connection between the devices and the Device Manager Pro and does not affect the Device Manager Agent connection which is always secured over HTTPS.

- "Secure (HTTPS) communication from the Devices to the Device Manager" (default not enabled): Sends secured (HTTPS) requests from the phones to the Device Manager Pro server. If this option is selected, communications and REST updates such as keep-alive, alarms and statuses between the phones and OVOC server are performed over HTTPS. This parameter is also relevant for loading firmware and configuration files, and when using an SBC HTTPS (OVOC Services) proxy server.

> ⚠ This parameter is relevant for the direct connection between the devices and the Device Manager Pro and does not affect the Device Manager Agent connection which is always secured over HTTPS.

- Devices Status: Open Device Web Administrator using HTTPS (default not enabled): The browser immediately opens the device's Web interface, over HTTPS, without prompting that there is a problem with the website's security certificate and that it is not recommended to continue to the website.
- Only allow devices added by the administrator into OVOC:
  - Phones that were not added by the network administrator will be blocked by the OVOC.
  - If a device's Mac Address is not listed in the 'Manage Users & Devices' page, it is blocked by OVOC. OVOC must be restarted for the parameter to take effect.

Implement Two Way Mutual Authentication for Device Connections

It is recommended to use two-way authentication over HTTPS between the device and the OVOC. This prevents unauthorized access to both OVOC and the device. This setup requires the installation of trusted root certificates on both the device and the OVOC server. These certificates can be generated using the OVOC Server Manager option "Trust Store Configuration" (see Generating Custom OVOC Server Certificates on page 44).

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

1. In the OVOC Web interface, ensure that device and tenant connections are enabled for HTTPS (default).

2. Configure the IPP HTTPS Authentication option 'Set Mutual Authentication' using the OVOC Server Manager-(refer to Section 'IPP HTTPS Authentication' in the IOM manual).

Connecting OVOC to Managed Devices without Cloud Architecture

The OVOC server and AudioCodes device connection is by default over HTTPS and is secured for the purpose of files upload/download and REST communication and for Single Sign-on from the Device page in the OVOC Web interface. This section describes how to configure the connection between the OVOC server and managed devices when the "Cloud Architecture feature" ,see Configure Cloud Architecture (HTTPS Tunnel Overlay) on page 47 is disabled.

> ⚠ Single Sign-on to devices Web interface is not supported for devices deployed behind a NAT (see Establishing Connections for OVOC Managed Devices on page 47)

➢ To connect OVOC to managed devices when the Cloud Architecture feature is disabled:

1. In the OVOC Web interface, ensure that device and tenant connections are enabled for HTTPS (default).
2. Copy default OVOC 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 devices (refer to section “Installing Custom Certificates on AudioCodes Devices” in the IOM manual).

```
 [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
```

3. Configure HTTPS parameters on the device. Refer to Section "Configuring HTTPS Parameters on the Device" in the IOM manual.
4. Implement Two-Way Authentication with X.509 Certificates (see Implement Two Way Mutual Authentication for Device Connections on the previous page).
5. (Optional) Disable TLS Version 1.1 (refer to Section 'TLS Version 1.1' in the *OVOC IOM*).
6. (Optional) Edit the SSL Cipher Suites Configuration String (refer to Section 'Edit the SSL Cipher Suites Configuration String' in the *OVOC IOM*).
7. In the OVOC Web interface Configuration page(**System** menu >**Administration** tab > **OVOC Server** folder > **Configuration** > **General Settings** tab), configure the SBC Devices Communication parameter to either "IP Based" (default) or "Hostname Based"- FQDN host name that is specified in the OVOC server certificate file used to authenticate the connection with the Active Directory Domain Controller.

⚠ If you configure the "Hostname Based" option ensure , you must also configure the parameter "Verify Certificate SubjectName" on the managed device (**Setup** Menu > **Signaling & Media** tab > **Quality of Experience** folder > **Quality of Experience Settings**).

Implement Two-Way (Mutual) Authentication with X.509 Certificates for Enterprise Device Connections

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. In the OVOC Web interface, ensure that device and tenant connections are enabled for HTTPS (default).
2. Set the SBC HTTPS Authentication option “Set Mutual Authentication” using the OVOC Server Manager (refer to *Section 'SBC HTTPS Authentication' in the IOM manual*).

⚠ This option is not supported for devices that are deployed behind a NAT.

OVOC Voice Quality Package and Enterprise 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 OVOC 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.

Microsoft Connections

This section describes how to authenticate the following Microsoft connections:

- Active Directory Server (Skype for Business Users) SSL Connection (see Active Directory Server (Skype for Business Users) – OVOC Voice Quality Package below)
- Skype for Business MS-SQL SSL Connection (see OVOC and Skype for Business MS-SQL SSL Connection–- Voice Quality Package below)

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.
4. You can authenticate the Active Directory connection using either the IP address of the Active Directory Domain Controller (default) or it's FQDN host name. To configure the latter option, in the Active Directory Details screen,select the **View Certificate Subject Name** check box. In this case, the OVOC server is an SSL client that verifies the FQDN specified in the Certificate file used to authenticate the connection with the Active Directory Domain Controller.

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

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 MS Lync/Skype 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.

4. From the Connection Mode drop-down list, select whether you wish to connect to the MS-SQL Server using the MS-SQL password or the Microsoft Windows password .

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

OVOC Floating License Connections

Connection between SBC devices and OVOC is established over SNMP and the functionality of the Floating License service is managed over the TCP/HTTPS REST connection. The following connections are managed:

- OVOC Floating License Connections above
- OVOC Managed Devices and Floating License Application Connection below

OVOC and Floating License Service Connections

The connection between OVOC and AudioCodes Floating License service (Cloud Mode) is secured over TCP HTTPS port 443 by an AudioCodes provided certificate (one-way authentication by OVOC), which is automatically installed (version 7.4.3000 and later). This certificate must not be replaced using the Server Certificates Update option in the OVOC Server Manager or deleted or modified in any way (only in the event of a clean installation or upgrade of OVOC) and must only be used for the HTTPS connection to the Floating License service.

This connection is also secured using an AudioCodes provided shared secret password (Product Key string) that should be configured in the Floating License Key field in the Device Floating License page in the OVOC Web. You can find the Product Key in the License Summary screen (System menu, Administration tab, License > Summary) in the OVOC Web.

The Floating License Server Status is displayed in the OVOC Server Manager. For more information, refer to the OVOC IOM.

OVOC Managed Devices and Floating License Application Connection

Connection between SBC devices and OVOC is managed as follows:

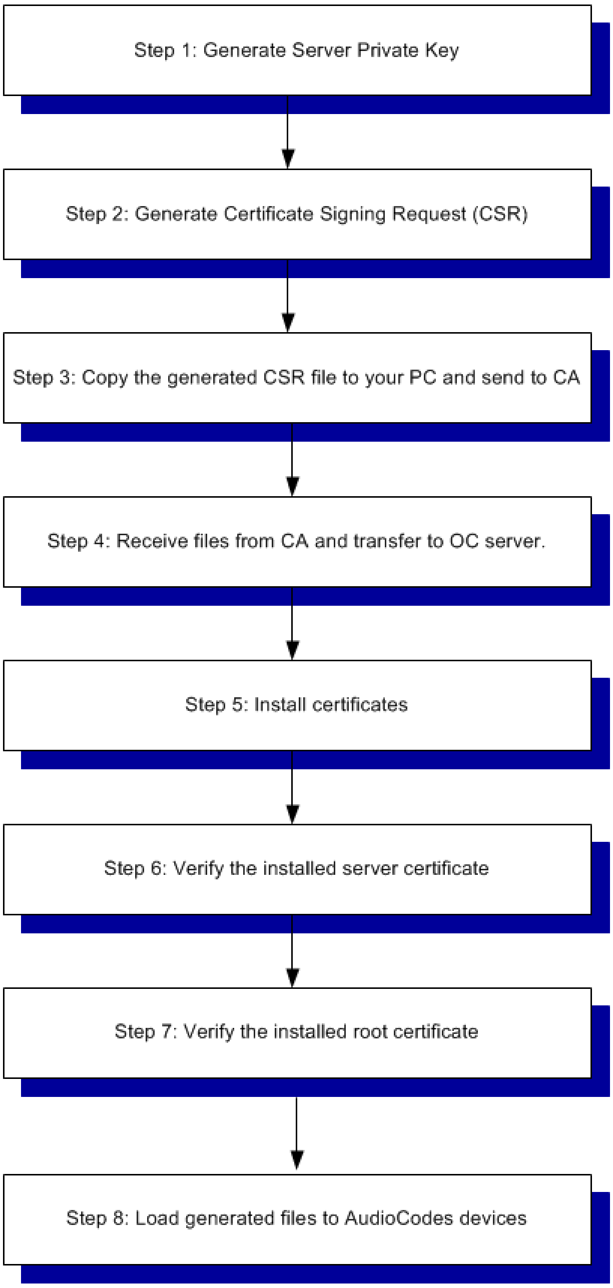
- The initial connection is established over SNMP and all OVOC initiated updates, such as Operator user or password changes are sent to the managed devices over SNMP.
- All SBC device initiated requests are sent over REST HTTPS port 443 and the Floating License application process on OVOC replies over this connection (HTTPS server). This connection is secured by default using the OVOC devices certificate (taken from the OVOC installation directory and installed on the managed devices). In addition, a Floating License OVOC Operator must be defined for managing this REST connection and the feature must be enabled on all devices that you wish to manage. This operator is defined in the OVOC Web Device Floating License page (System > Administration > License > Device Floating License).

- A proxy server is implemented for the connection between OVOC and the AudioCodes Floating License Service and can be configured using the OVOC Server Manager option "Proxy Settings".

Generating Custom OVOC Server Certificates

Default SSL certificates can be replaced by custom certificates using the Server Certificates Update menu option in the OVOC 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 Server Private Key
Step 2: Generate Certificate Signing Request (CSR)
Step 3: Copy the generated CSR file to your PC and send to CA
Step 4: Receive files from CA and transfer to OC server.
Step 5: Install certificates
Step 6: Verify the installed server certificate
Step 7: Verify the installed root certificate
Step 8: Load generated files to AudioCodes devices

- **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 AudioCodes devices as described in either of the following procedures:
  - Connecting OVOC to Managed Devices without Cloud Architecture on page 40
  - Securely Connecting OVOC to SBC Devices with Cloud Architecture on page 48

> - If you did not generate the Certificate Signing Request using the OVOC 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).

7 Step 6: Setting Up Northbound Interface Connections

This section describes key issues for connecting to external NOC systems. For more information, refer to the *Northbound Integration Guide*.

- Syslog messages and emails sent from the OVOC server to a northbound interface are not secured.
- Single sign-on is not supported for devices located behind a NAT, unless the Cloud Architecture feature is enabled, in which case, SBC device connections can be secured over an HTTP/S Tunnel Overlay network (see).
- An SSH connection from the OVOC server to the device is not supported.

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 OVOC Server Manager option ‘DeviceManagerPro andNBIFWebpages Secured Communication’ in the OVOC 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 OVOC Server Manager (refer to Section ‘Change HTTP/S Authentication Password for NBIF Directory’ in the *IOM* manual).

Northbound User Authentication

It is recommended to authenticate user connections from Northbound interfaces with one of the following external authentication servers:

- LDAP Server (see LDAP Server on page 12)
- Microsoft Azure (see Microsoft Azure on page 10)
- RADIUS Server (see RADIUS Server on page 13)

For details on setting up a RADIUS server and client, refer to the *Northbound Integration Guide*.

Data Analytics API

When the Data Analytics feature is enabled in the OVOC Server Manager (refer to *OVOC IOM*), the connection with the OVOC server is established with user "Analytics" over port 1521 (non-secure connection, see Step 3: Configuring Enterprise Firewall on page 20).

8 Step 7: Managing Device Connections

When the connections between the OVOC server and the managed devices traverse a firewall or NAT, direct connections cannot be established (both for OVOC > Device connections and for Device > OVOC connections). OVOC provides methods for overcoming this issue. These methods can be used for both initial setup and Second-Day management:

- Establishing Connections for OVOC Managed Devices below
- Establishing Connections for Device Manager Devices on page 49

For configuration of the different firewall rules for each configuration option, see Firewall Rules for NAT Configuration Options on page 28

Establishing Connections for OVOC Managed Devices

- When OVOC is deployed behind a firewall or NAT in the cloud or in a remote network, it cannot establish a direct connection with managed devices using its private IP address. Consequently, the following methods can be used to overcome this issue:
  - For OVOC Cloud deployments: Configure the OVOC server public IP address.
  - For OVOC deployments in a remote public network: Configure the IP address of the NAT router.

  See Configure OVOC Server with Public or NAT IP Address on page 49
- When devices are deployed behind a firewall or NAT in the cloud or in a remote network, they cannot connect establish a direct connection with the OVOC server. Consequently, the following methods can be used to overcome this issue:
  - Automatic Detection below
  - Configure Cloud Architecture (HTTPS Tunnel Overlay) below

⚠
- All of the above options requires a configured WAN interface on the managed AudioCodes devices.
- Single Sign-on to OVOC devices Web interface is only supported for the Cloud Architecture option.

Automatic Detection

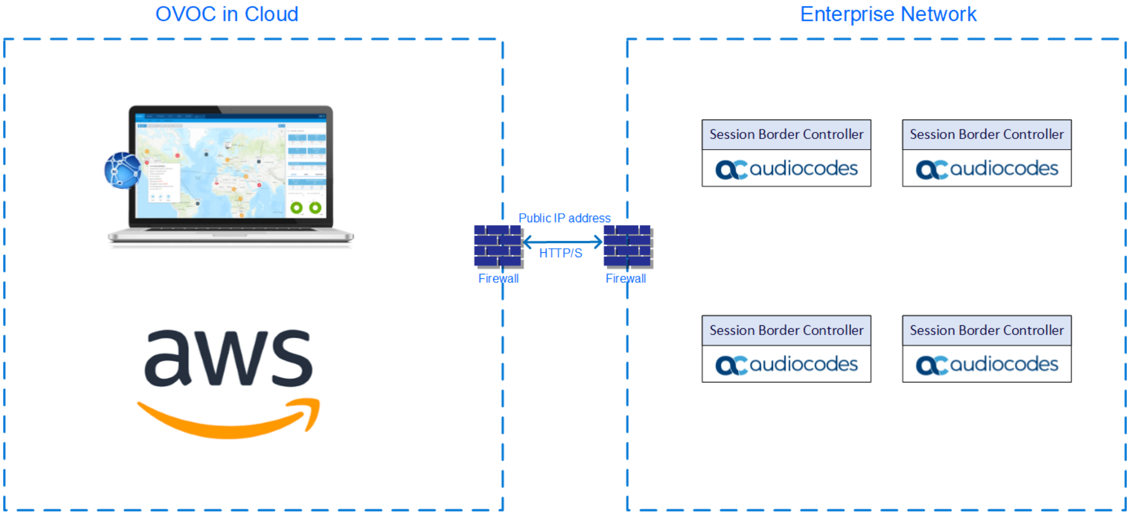
Devices are connected automatically to OVOC through sending SNMP Keep-alive messages. Refer to Section "Adding AudioCodes Devices Automatically" in the *OVOC User's Manual*.

Configure Cloud Architecture (HTTPS Tunnel Overlay)

When OVOC-managed devices are deployed in a public cloud and managed devices are either deployed either in the Cloud or in a remote enterprise network, an automatic mechanism can be enabled to secure the OVOC server and Device communication through binding to a dedicated HTTPS tunnel through a generic WebSocket server connection. This mechanism binds proprietary OVOC server > SBC device connections including SNMP, HTTPS, syslog and debug recording into an HTTPS tunnel overlay network. This eliminates the need for administrators to manually manage firewall rules for these connections and to lease third-party VPN services. Using this configuration, Single Sign-on to managed devices can be performed from the Devices Page link in the OVOC Web interface for devices managed behind a NAT. The figure below illustrates the OVOC Cloud Architecture.

This mode is only available on the Amazon AWS platform.

Figure 8-1: Cloud Architecture



Securely Connecting OVOC to SBC Devices with Cloud Architecture

This section describes how to securely connect SBC devices to the OVOC server when the HTTP Tunnel Overlay Cloud Architecture feature is enabled.

➢ To secure the connection between OVOC and devices over HTTPS with tunnel overlay:

1. In the OVOC Web interface, ensure that device and tenant connections are enabled for HTTPS (default).
2. Copy default OVOC 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 (refer to section “Installing Custom Certificates on AudioCodes Devices” in the IOM manual).

```
 [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
```

3. Configure HTTPS parameters on the device. Refer to Section "Configuring HTTPS Parameters on the Device" in the *IOM* manual.

4. In the OVOC Web interface, ensure that the SBC Devices Communication parameter is set to "IP Based" (System menu >Administration tab > OVOC server folder > Configuration).

> ⚠ If this parameter is set to "Hostname Based" and the Cloud Architecture feature is enabled in the OVOC Server Manager, then the connected SBC devices cannot be managed for this OVOC instance.

5. Enable the option "Enable Cloud Architecture" in the OVOC Server Manager (refer to Section "Configuring Cloud Architecture Mode"in the *IOM* manual).

6. Ensure port 443 is open on the Enterprise firewall.

Configure OVOC Server with Public or NAT IP Address

The OVOC server can be configured with the public IP address of the OVOC deployment platform. For example, when OVOC is deployed in the AWS or Azure Cloud, the public IP address for accessing these platforms over the internet is configured. Managed devices may be remotely deployed either in the cloud or in a remote enterprise network.

- Refer to Section "Configure OVOC Server with Public IP Address" in the *OVOC IOM.*
- For Configuration of firewall rules, see Firewall Rules for NAT Configuration Options on page 28

> ⚠
> - Single Sign-on to the SBC devices Web interface is not supported for this configuration option.
> - When the "Cloud Architecture" mode is enabled, this option does not appear in the "Network Configuration" menu.

Establishing Connections for Device Manager Devices

When phones are deployed behind a firewall or NAT and connect to OVOC over the public internet, they can always reach OVOC; they send keep-alive message to the OVOC per hour (either directly or via Device Manager Agent). This mechanism is used for both initial setup and Second-Day Management.

In the other direction, OVOC cannot establish a direct connection with the phones to perform actions such as Device Reset and Configuration and Firmware file updates. This issue can be resolved by using the following:

- Device Manager Agent for both initial setup and Second-day management for managing Microsoft Lync/Skype for Business phones, Polycom Trio devices, Polycom VVX devices and Spectralink 8440 (see Configure Device Manager Agent below).

> Refer to *Device Manager for Third-Party Vendor Products Administrator's Manual* and the *Device Manager Agent Installation and Configuration Guide*. For managing Jabra devices, the Jabra Integration Service and the Device Manager Agent are used. Refer also to both of the above manuals.

- For Microsoft Teams phones deployments, the Device Manager Agent is used for initial setup; however, a dedicated mechanism is used for Second-day management (see Managing Microsoft Teams Phones below).

Configure Device Manager Agent

The Device Manager Agent is deployed locally in the enterprise network on a Microsoft Windows server and enables secured HTTPS communication with encryption between OVOC and managed phones. It enables network administrators to initiate actions directly to phones traversing a NAT | Firewall in a local enterprise network, from a global cloud network. The Agent listens to OVOC at predefined intervals and checks if there are actions required to run on the devices in the network. Actions are aggregated per tenant and run on each device in the network. The actions include checking statuses, updating firmware, resetting the device, configuration updates and sending SIP messages. For more information, Refer to Section "Managing Devices Behind NAT" in Device Manager Agent Installation and Configuration Guide.

Managing Microsoft Teams Phones

Microsoft Teams phones do not have REST server capabilities; they cannot receive REST commands such as Device Reset and configuration and firmware files updates. Instead when the Device Manager Pro performs such actions on the Teams phones (PUT and POST only), the commands are embedded in the HTML response in the Keep-alive messages that are sent from the Teams phones at one minute intervals. See example HTML Keep-alive response below.

```
{
  "requests":[
   {
    "method":"PUT",
    "path":"\/rest\/v1\/command\/ResetGracefulHandler",
    "body":{
      "sessionId":"f0144216",
      "emsUserName":"elic@audiocodesipprnd.onmicrosoft.com",
      "emsUserPassword":"81c11125567a212da873582b82e3efb6",
      "schedulePeriod":""
    }
```

International Headquarters

1 Hayarden Street,

Airport City

Lod 7019900, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

200 Cottontail Lane

Suite A101E

Somerset NJ 08873

Tel: +1-732-469-0880

Fax: +1-732-469-2298

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

Website: https://www.audiocodes.com/

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-94053

audiocodes