Reference Guide

AudioCodes Family of Media Gateways and Session Border Controllers (SBCs)

Security Guidelines

SIP Media Gateways and SBCs

Version 7.2

audiocodes

Table of Contents

<div style="border:1px solid blue; background:#e0e0e0; padding:10px;">

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: January-13-2021

</div>

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.

Stay in the Loop with AudioCodes

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.

Document Revision Record

LTRT	Description
30208	Initial document release for Version 7.2.
30209	Corporate logo and URLs updated.
30211	Network port assignment updated.
30212	Screenshots and paths of Web-based management tool updated for 7.2.252; secure SIP chapter updated.
30213	Changing default ports and disabling telnet recommendations; SSH enabled b default
30215	LDAP section promoted.
30218	SSL 3.0 removed and TLS 1.3 added; cross-reference fixed; classification last rule deny removed

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.

1 Introduction

This document provides recommended security guidelines for safeguarding your network and your AudioCodes device against malicious attacks.

> **Note:**
>
> - This document provides only recommended security guidelines; your network architecture may require additional and/or different security measures.
>
> - The document includes partial configuration; for detailed configuration, refer to the device's *User's Manual*.
>
> - The document may refer to AudioCodes products not included in Version 7.2. See the *Release Notes Ver. 7.2* for a list of the supported products.

1.1 Security Threats

AudioCodes devices are commonly located at the demarcation point between safe (*trusted*) and unsafe (*un-trusted*) networks. A typical example of an un-trusted network would be a SIP trunk connected to an Internet Telephony Service Provider (ITSP) network; the trusted network would be the internal LAN. The figure below illustrates this basic concept of trusted and un-trusted networks.

Figure 1: Trusted and Un-trusted Networks
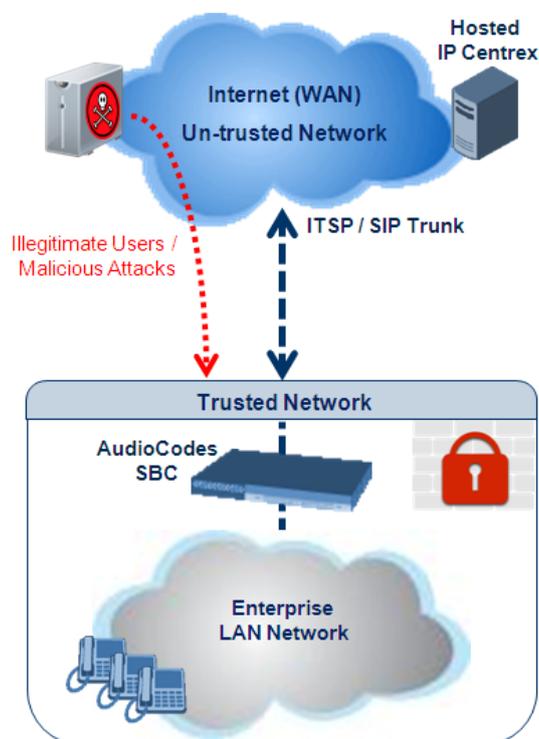
Attacks on your network from the un-trusted network may include the following:

- **Denial of Service (DoS) attacks:** Malicious attacks designed to cripple your VoIP network by overloading it with calls or service requests.

- **Overload events:** In addition to purposeful DoS attacks, non-malicious periods of intense activity can also cause an increase in call signaling rates that exceed what your infrastructure can support, resulting in network conditions that are similar in effect

to DoS attacks. Successful attacks resulting in contact center downtime can result in lost revenue and diminished customer satisfaction.

■ **Network abuse and fraud:** Malicious intrusion or service theft may take the form of an unauthorized user gaining access to your VoIP network by mimicking an authorized user or seizing control of a SIP proxy and initiating outbound calls to the PSTN for free. Another possibility is using a compromised endpoint to redirect or forward calls for eavesdropping.

■ **Viruses and malware:** Computer viruses, worms, Trojan horses, and other malware can infect user agent phones and SIP-based ACD infrastructure - just as they can computers and servers - and degrade performance or completely disrupt service. As devices become more sophisticated with distinct operating systems, malware also serves as a way to subjugate devices and launch DoS attacks that piggyback encrypted links.

■ **Identity theft:** Phishing and "man-in-the-middle" can be used to acquire caller identification information to gain unauthorized access to services and information. Theft by phone (or service theft), whereby access to your corporate phone system is attempted by users posing as legitimate ones can sky-rocket your corporation's phone bill.

■ **Eavesdropping:** The ability to listen to or record calls is easier on VoIP networks than on PSTN. This is a concern not only because of personal privacy violations, but also because sensitive information can be compromised and exploited.

■ **Spam over Internet Telephony (SPIT):** The delivery of unsolicited calls or voicemails can inundate networks, annoy subscribers, and diminish the usefulness of VoIP networks.

These threats can exist, for example, at the following main IP network border points:

■ **Interconnect:** SIP trunks to ITSPs, using SIP signaling for inbound and outbound calls.

■ **Trusted access:** Private, managed IP networks that connect service providers' residential, enterprise, or mobile subscribers (as part of an emerging federation of trusted networks).

■ **Un-trusted access:** Unmanaged Internet for connections to work-at-home agents or inbound callers.

1.2   AudioCodes Security Solution

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

■ **Securing the Service:** Secures the call services it provides by implementing separation and defense of different network entities (e.g., SIP Trunk, softswitch, and users). This is accomplished by the following:

- Physical separation of networks

- SRDs for each SIP entity (user agent)

- IP Groups for each SIP entity (user agent)

■ **Securing the Device:**

- Management - ensuring that only authorized users can access the device's management interface

- Defense against attacks on the device regarding SIP signaling and media (RTP)

Due to the vast number and types of potential attacks (some described in the previous section), security of your trusted VoIP network should be your paramount concern. The device provides a rich set of features to support perimeter defense for protecting your trusted network from the un-trusted ones. However, the device's security features and capabilities are only effective if implemented correctly. Improper use of the device for perimeter defense may render the overall security solution ineffective, thereby exposing your network to multiple threats.

The benefits of an IP-based telephony network are quite clear, but so are the threats and security implications that need to be addressed. The IP borders of the IP telephony network are the attack points and it is the AudioCodes security solutions that are designed to help safeguard your trusted network from such threats.

This page is intentionally left blank.

2   Separate Network Traffic

This chapter provides recommendations for separating network traffic.

2.1   Identify Trusted and Un-trusted Networks

It is crucial that you identify the trusted network (i.e., your local LAN) and the un-trusted network (i.e., public Internet – WAN) in the environment in which the device is deployed. There may be multiple un-trusted networks in a single deployment environment. For example, far-end WAN users and a SIP trunk with an ITSP may represent two un-trusted networks.

Once identified, you need to handle the un-trusted networks with extreme caution in order to safeguard your trusted network from malicious attacks from them. One of the main precautions is to separate your trusted network from the un-trusted network, using different logical configuration entities such as SRDs etc. The precautions and security guidelines are described in detail in subsequent sections.

2.2   Implement Physical Network Separation using Ethernet Port Groups

For the devices mentioned in the note above, you can physically separate the network traffic by Ethernet ports, using Ethernet Groups. Each Ethernet Group can include up to two physical Ethernet ports. The Ethernet Device defines the VLAN per Ethernet Group. The Ethernet Device is then assigned to the network interface as an Underlying Device. The following procedure provides an example of assigning different ports per traffic type.

1. Assign ports to different Ethernet Groups in the Ethernet Groups table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Groups**):

Figure 2-1: Assigning Ports to Ethernet Groups

INDEX ⬍	NAME	MODE	MEMBER 1	MEMBER 2
0	GROUP_1	Single	GE_4_1	--
1	GROUP_2	Single	GE_4_2	--
2	GROUP_3	Single	GE_4_3	--

2. Configure VLAN IDs per Ethernet Group in the Ethernet Devices table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Devices**):

Figure 2-2: Assigning VLANs to Ethernet Groups

INDEX ⬍	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING
0	1	GROUP_1	vlan 1	Untagged
1	2	GROUP_2	vlan 2	Untagged
2	3	GROUP_3	vlan 3	Untagged

3. Assign the Ethernet Devices (VLANs) to the different traffic network interfaces in the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**):

Figure 2-3: Assigning Ethernet Devices (VLANs) to IP Interfaces

INDEX ⇕	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	O+M+C	OAMP	IPv4 Manual	10.15.7.96	16	10.15.0.1	0.0.0.0	0.0.0.0	vlan 1
1	RTP	Media	IPv4 Manual	10.15.7.9	16	10.15.0.1	0.0.0.0	0.0.0.0	vlan 2
2	SIP	Control	IPv4 Manual	10.15.7.99	16	10.15.0.1	0.0.0.0	0.0.0.0	vlan 3

3   Implement Layer 3/4 (Network) Firewall

This section discusses Layer 3/4 (Network) firewall recommendations. By default, there are no firewall rules and this exposes the device to security risks. Therefore, configuring firewall rules is highly recommended to protect the device from external attacks.

3.1   Block Unused Network Ports

It is highly recommended that you disable network ports that are not used in your deployment. For example, if you are not using Trivial File Transfer Protocol (TFTP) in your network, then you should disable this network port application.

3.2   Define VoIP Traffic Firewall Rules

For packets whose source IP addresses are known, it is recommended to define VoIP firewall rules that allow receipt of calls or packets from this network and block all calls from elsewhere. These rules can be defined per source IP address, port, protocol, and network IP interface. If an incoming packet is received from an invalid source (as defined in the firewall), the call or packet is discarded.

Below is a list of recommended guidelines when configuring the VoIP firewall:

■   **Add firewall rules per network interface:** It is recommended to define firewall rules for packets from source IP addresses received on the OAMP interface and each SIP Control (SIP) interface (defined in the Multiple Interface table). A less recommended alternative is to define a single rule that applies to all interfaces (by setting the 'Use Specific Interface' parameter to 'Disable').

■   **Define bandwidth limitation per rule:** For each IP network interface, it is advised to define a rate-limiting value (byte rate, burst bytes and maximum packet size). Bandwidth limitation prevents overloading (flooding) of your network and thereby, helps in preventing attacks such as DoS on your device (on each network).

■   **Define rules as specific as possible:** Define the rules as detailed as possible so that they block only the intended traffic.

■   **Add an ICMP firewall rule:** ICMP is typically used for pinging. However, malicious attackers can send over-sized (floods) ICMP packets to a specific network address. Therefore, it is recommended to define a rule for limiting these packets.

■   **Add a rule to block all traffic:** You must define a firewall rule that blocks **all** incoming traffic (i.e., block all protocol traffic from all source IP addresses and ports for all interfaces). This rule must be the **last** rule listed in the table, so that rules above it that allow specific traffic are valid (otherwise, all traffic is blocked).

> **Warning:** If the 'Prefix Length' field on the Firewall Settings page is set to "0", the rule will apply to **all** IP addresses, regardless of whether an IP address is specified in the 'Source IP' field. Thus, if you need to apply a rule to a specific IP address, ensure that you also set the 'Prefix Length' field to a value other than "0".

The Layer 3-4 VoIP traffic firewall rules are configured in the Firewall table (**Setup** menu > **IP Network** tab > **Security** folder > **Firewall**). The table below shows a configuration example of firewall rules:

Configuration Example of Firewall Rules in the Firewall Table

Parameter	Index Rule				
	1	**2**	**3**	**4**	**5**
Match					
Source IP	12.194.231.76	12.194.230.7	0.0.0.0	192.0.0.0	0.0.0.0
Prefix Length	16	16	0	8	0
Start Port / End Port	0-65535	0-65535	0-65535	0-65535	0-65535
Protocol	Any	Any	icmp	Any	Any
Use Specific Interface	Enable	Enable	Disable	Enable	Disable
Interface Name	WAN	WAN	None	Voice	None
Action					
Byte Rate	0	0	40000	40000	0
Burst Bytes	0	0	50000	50000	0
Action Upon Match	Allow	Allow	Allow	Allow	Block

- **Rules 1 and 2:** Typical firewall rules that allow packets ONLY from specified IP addresses (e.g., proxy servers). Note that the prefix length is configured.

- **Rule 3:** A more "advanced" firewall rule - bandwidth rule for ICMP, which allows a maximum bandwidth of 40,000 bytes/sec with an additional allowance of 50,000 bytes. If, for example, the actual traffic rate is 45,000 bytes/sec, then this allowance would be consumed within 10 seconds, after which all traffic exceeding the allocated 40,000 bytes/sec is dropped. If the actual traffic rate then slowed to 30,000 bytes/sec, the allowance would be replenished within 5 seconds.

- **Rule 4:** Allows traffic from the LAN voice interface and limits bandwidth.

- **Rule 5:** Blocks all other traffic.

4 Secure Management Access

This section provides guidelines to secure access to the device's management interface.

4.1 Change Default Management User Login Passwords

To secure access to the device's Web management interface, please adhere to the following recommended guidelines:

■ The device is shipped with a default **Security Administrator** access-level user account whose username is "Admin" and password is "Admin". This user has full read-write access privileges to the device. It is recommended to change the default password to a hard-to-hack string. You can change the username and password on the Local Users table (**Setup** menu > **Administration** tab > **WEB & CLI** folder > **Local Users**):

Figure 4: Changing Default Password of Security Administrator User

■ The device is shipped with a default **Monitor** access-level user account whose username is "User" and password is "User". This user only has read access privileges to the device. The read access privilege is also limited to certain Web pages. However, this user can view certain SIP settings such as proxy server addresses. Therefore, to prevent an attacker from obtaining sensitive SIP settings that could result in possible call theft etc., either delete this user account or change its default login password to a hard-to-hack string. This is done in the Local Users table (**Setup** menu > **Administration** tab > **WEB & CLI** folder > **Local Users**):

Figure 5: Changing Password of Monitor User Level

INDEX ⬍	USERNAME	PASSWORD	STATUS	PASSWORD AGE	SESSION LIMIT	SESSION TIMEOUT	BLOCK DURATION	USER LEVEL
0	Admin	*	Valid	0	5	60	60	Security Admi
1	User	*	Valid	0	2	15	60	Monitor

■ If you have deployed multiple devices, use a unique password for each device.

■ Change the login password periodically (for example, once a month).

4.2 Implement LDAP-based User Authentication and Authorization

It is highly recommended that you implement a third-party, LDAP server in your network for authenticating and authorizing the device's management users (Web and CLI). This can be done by using an LDAP-compliant server such as Microsoft Active Directory (AD). When a user attempts to log in to one of the management platforms, the device verifies the login username and password with AD. The device can also determine the user's management access level (privileges) based on the user's profile in the AD. This is configured in the LDAP pages located under **Setup** menu > **IP Network** tab > **RADIUS & LDAP** folder.

An alternative to using an LDAP server is to use a RADIUS server, as discussed in the next section.

4.3 Implement RADIUS-based Management User Authentication

It is highly recommended that you implement a third-party, RADIUS server in your network for authenticating Web / Telnet management users and thereby, preventing unauthorized access. RADIUS allows you to define different passwords for different interface users, with centralized management of the password database. When RADIUS is used, logging into the Web / Telnet interfaces is performed through the RADIUS server. The device verifies the authenticity of the user name and password with the RADIUS server.

An alternative is to use an LDAP server, as discussed in the previous section.

RADIUS functionality is enabled on the Authentication Server page (**Setup** menu > **Administration** tab > **WEB & CLI** folder > **Authentication Server**):

Figure 6: Enabling RADIUS for Web User Authentication

- ■ 'Enable RADIUS Access Control': select **Enable**.

- ■ 'Use RADIUS for Web/Telnet Login': select **Enable**.

RADIUS authentication servers (IP address, port and 'secret' password for authenticating the device with the RADIUS server) are configured in the RADIUS Servers table (**Setup** menu > **IP Network** tab > **RADIUS & LDAP** folder > **RADIUS Servers**).

Figure 7: Configuring RADIUS Servers for Management User Authentication

INDEX ⬍	IP ADDRESS	AUTHENTICATION PORT	ACCOUNTING PORT	SHARED SECRET
0	10.6.7.7	1645	1646	*

4.4   Implement Two-Way Authentication with X.509 Certificates

It is recommended to use two-way authentication (in addition to HTTPS) between the device's Web server and the management station (i.e., computer) accessing it. Authentication is performed and connection to the Web interface is subsequently allowed only if the following conditions are met:

■   The management station possesses a client certificate from a Certification Authority (CA).

■   The CA certificate is listed in the device's Trusted Root CA Store.

Otherwise, the connection is rejected. Therefore, this prevents unauthorized access to the Web management tool.

> **Note:**
>
> • Implementation of two-way authentication requires a third-party security equipment vendor, CA server, and security administrator personnel. These should create certificates and deploy them to all the computers in the organization.
>
> • The device is supplied with a working TLS configuration consisting of a unique self-signed server certificate. Replace this certificate with one provided by your security administrator. For more information, refer to the *User's Manual*.

➢   **To configure client-server, two-way authentication using X.509 certificates:**

1.   Install a client certificate on the management station (your network administrator should provide you with a certificate).

2.   Install your organization's CA certificate on the management station.

3.   Open the TLS Contexts table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).

4.   In the TLS Contexts table, add a new TLS Context or select the required TLS Context row, and then click the **Trusted Root Certificates** link located at the bottom of the TLS Contexts page.

5.   Click the **Import** button, browse to and select the Root CA certificate file (in base64-encoded PEM format), and then click OK to import the file:

Figure 8: Importing CA Certificate to CA Store
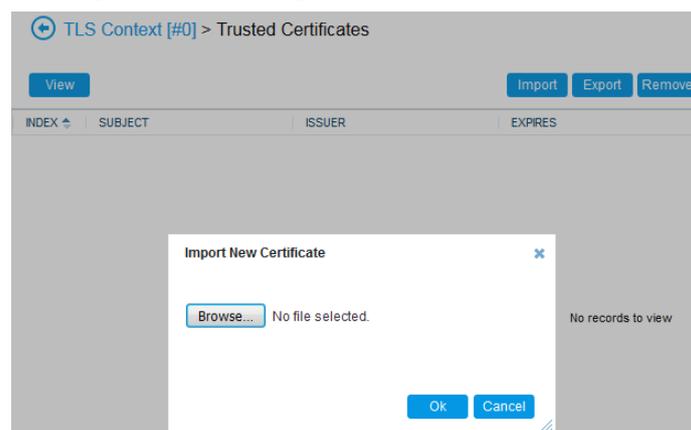
6. Since X.509 certificates have an expiration date and time, the device must be configured to use Network Time Protocol (NTP) to obtain the current date and time. Without the correct date and time, client certificates cannot operate.

7. Ensure that client certificates for HTTPS connections are required, by configuring the 'Require Client Certificates for HTTPS connection' parameter to **Enable** on the Web Settings page (**Setup** menu > **Administration** tab > **WEB & CLI** folder > **Web Settings**):

Require Client Certificates for HTTPS connection Enable

4.5   Secure HTTP Access using HTTPS

It is recommended to allow access to the Web interface through HTTPS **only**. In addition, it is recommended to block port 80. This is done on the Web Settings page (**Setup** menu > **Administration** tab > **WEB & CLI** folder > **Web Settings**), by configuring the 'Secured Web Connection (HTTPS)' parameter to **HTTPS Only** (reset device for setting to take effect):

Figure 9: Securing Access to Web Interface using HTTPS

Secured Web Connection (HTTPS)   HTTPS Only
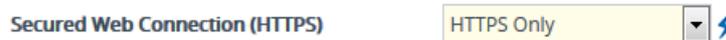
4.6   Secure Telnet Sessions

It's recommended to disable access through Telnet, but if you do require the use of Telnet and your management software provides a secure Telnet application, then use a secured Telnet connection (i.e., Transport Layer Security / TLS). TLS protects Telnet traffic from network sniffing. This is done on the CLI Settings page (**Setup** menu > **Administration** tab > **WEB & CLI** folder > **CLI Settings**):

Figure 10: Securing Telnet with TLS

Embedded Telnet Server   Enable Secured

Telnet Server TCP Port   25

■   'Embedded Telnet Server': **Enable Secured**.

■   'Telnet Server TCP Port': Change the default TCP port (if required). The configuration is applicable for access from the LAN.

4.7   Secure CLI Sessions by SSH

It is recommended to employ Secure SHell (SSH) for accessing the device's CLI. SSH is the de-facto standard for secure CLI. SSH 2.0 is a protocol built above TCP, providing methods for key exchange, authentication, encryption, and authorization. By default, SSH uses the same username and password as the Telnet and Web server.

SSH is enabled on the CLI Settings page (**Setup** menu > **Administration** tab > **WEB & CLI** folder > **CLI Settings**):

Figure 11: Securing SSH (CLI) Sessions

SECURE SHELL (SSH)	
Enable SSH Server	Enable
Server Port	23

■   'Enable SSH Server': **Enable**.

■   'Server Port': If necessary, you may change the default TCP port used for SSH, although this is not recommended. Note that this is applicable for access from the LAN.

For additional security, you can configure a public key for RSA key negotiation (instead of or in addition to using a username and password) when accessing through SSH.

4.8   Define Web, Telnet, and SSH Authorized Access List

Allow only user-defined LAN IP addresses to access the Web, Telnet, and SSH based management interfaces. The device denies access from undefined IP addresses. To do this, configure allowed IP addresses on the Access List page (**Setup** menu > **Administration** tab > **WEB & CLI** folder > **Access List**):

Figure 12: Authorized IP Addresses for Accessing Web / Telnet / SSH Interfaces

Access List

Add an authorized IP address

[   ]   **Add New Entry**

DELETE ROW	AUTHORIZED IP ADDRESS
1 ☐	10.13.2.3

> **Note:**
>
> • The first authorized IP address in the list must be your computer's (terminal) IP address; otherwise, access from your computer will be denied.
>
> • The Web / Telnet / SSH authorized access list concerns OSI Layer 5 (Session). However, you can also add firewall rules for Layer 3 (Network) and Layer 4 (Transport) with bandwidth limitation to limit access to management interfaces (see Section 3.1).

4.9 Secure SNMP Interface Access

This section discusses recommended security guidelines relating to Simple Network Management Protocol (SNMP).

4.9.1 Prefer SNMPv3 over SNMPv2

It is recommended to use SNMP Version 3 (SNMPv3) instead of SNMPv1 and SNMPv2c, if possible. SNMPv3 provides secure access to the device using a combination of authentication (MD5 or SHA-1) and encryption (DES, 3DES, AES-128, AES-192, or AES-256) of packets over the network. It is also recommended that you periodically change the SNMPv3 authentication and privacy keys.

SNMPv3 users are configured in the SNMPv3 Users table (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP V3 Users**), as shown in the figure below:

Figure 13: SNMPv3 Users

INDEX ⇕	USER NAME	AUTHENTICATION PROTOCOL	PRIVACY PROTOCOL	AUTHENTICATION KEY	PRIVACY KEY	GROUP
0	JoeD	MD5	3DES	*	*	Read-Write

4.9.2 Secure SMNPv2 Access

If you are using SNMPv2, change the community strings from their default values as they can easily be guessed by hackers. The default read-write community string is "private" and the read-only is "public".

In addition, by default, the SNMPv2 agent accepts SNMP Get and Set requests from any IP address if the correct community string is used in the request. Therefore, to enhance security with SNMPv2, implement Trusted Managers. A Trusted Manager is an IP address (management station) from which the SNMP agent accepts and processes Get and Set requests. It is also recommended that you periodically change these SNMP community string values.

■ SNMPv2 community strings are configured on the SNMP Community Settings page (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP Community Settings**):

Figure 14: SNMPv2 Community Strings

READ-WRITE COMMUNITY STRINGS

Read-Write 1   snmpv2user john

Read-Write 2

Read-Write 3

Read-Write 4

Read-Write 5

■   SNMPv2 management stations are configured in the SNMP Trusted Managers table (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP Trusted Managers**):

Figure 15: SNMPv2 Trusted Managers

DELETE	TRUSTED MANAGERS IP ADDRESS	
☐	SNMP Trusted Manager 1	10.3.2.1
☐	SNMP Trusted Manager 2	0.0.0.0
☐	SNMP Trusted Manager 3	0.0.0.0
☐	SNMP Trusted Manager 4	0.0.0.0
☐	SNMP Trusted Manager 5	0.0.0.0

4.10   Secure LDAP Communication

If you are using LDAP-based login management (username-password) or LDAP-based SIP routing in your deployment, it is recommended to employ TLS for secure device communication with the LDAP server. This ensures that the device encrypts the username and password sent to the LDAP server.

TLS for LDAP communication is configured in the LDAP Servers table (**Setup** menu > **IP Network** tab > **RADIUS & LDAP** folder > **LDAP Servers**):

Figure 16: Configuring Secure LDAP Server Communication

■   'Use TLS': Select **Yes**.

■   'TLS Context': Select the TLS Context (configured in the TLS Contexts table).

This page is intentionally left blank.

5   Secure SIP using TLS (SIPS)

It is crucial that you implement the TLS-over-TCP protocol to best secure the device's SIP signaling connections. TLS provides encryption and authentication of SIP signaling for your VoIP traffic, preventing tampering of calls. Use it whenever possible for far-end users and ITSPs.

The device's TLS feature supports the following:

- **TLS:** TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3

- **DTLS:** DTLS 1.0 and DTLS 1.2

- **Cipher:** TLS cipher suites for server and client roles (per OpenSSL syntax)

- **Authentication:** X.509 certificates

- **Certificate revocation checking:** OCSP (CRLs are currently not supported)

- Receipt of wildcards ('*') in X.509 Certificates when establishing TLS connections. These wildcards can be part of the CN attribute of the Common Name field or the DNSName attribute of the Subject Alternative Name field.

Recommended security guidelines for ensuring TLS for SIP signaling are described in the subsequent subsections.

5.1   Use Strong Authentication Passwords

Always use strong authentication passwords, which are more difficult to detect than weak ones. A strong password typically includes at least six characters with a combination of upper and lower-case letters, numbers and symbols.

5.2   Use TLS Version 1.1 and/or 1.2

It is recommended to use the highest TLS version possible that is supported by **all** your network entities to achieve the best communication security, based on cryptographic algorithms. The device accepts only connections that adhere to the specified TLS version.

It is also recommended **not** to configure the device to use any TLS version (**Any TLS 1.x**). However, if some network entities use a lesser TLS version and some use a higher TLS version (e.g., TLS 1.3), then you need to configure the device to use any version.

The TLS version is configured for TLS Contexts in the TLS Contexts table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**), using the 'TLS Version' parameter. The example below assumes that the highest TLS versions supported by the network entities are 1.1 and 1.2.

Figure 17: Configuring TLS Version

5.3 Use TLS for SIP Interfaces and Block TCP/UDP Ports

Each port can be vulnerable to attacks. Therefore, it is highly recommended that your SIP interfaces use **only** TLS. When configuring your SIP Interfaces, define the TLS port number, but set the UDP and TCP ports to zero ("0"). This configuration blocks (disables) the UDP and TCP ports. In other words, to disable UDP and TCP ports, you must define SIP Interfaces. In addition, to increase security, define only SIP Interfaces that are necessary.

SIP Interfaces are configured on the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**). The figure below shows an example of a SIP Interface configured for the Voice network interface (LAN) where the UDP and TCP ports set to "0".

Figure 18: SIP Interface using only TLS Port
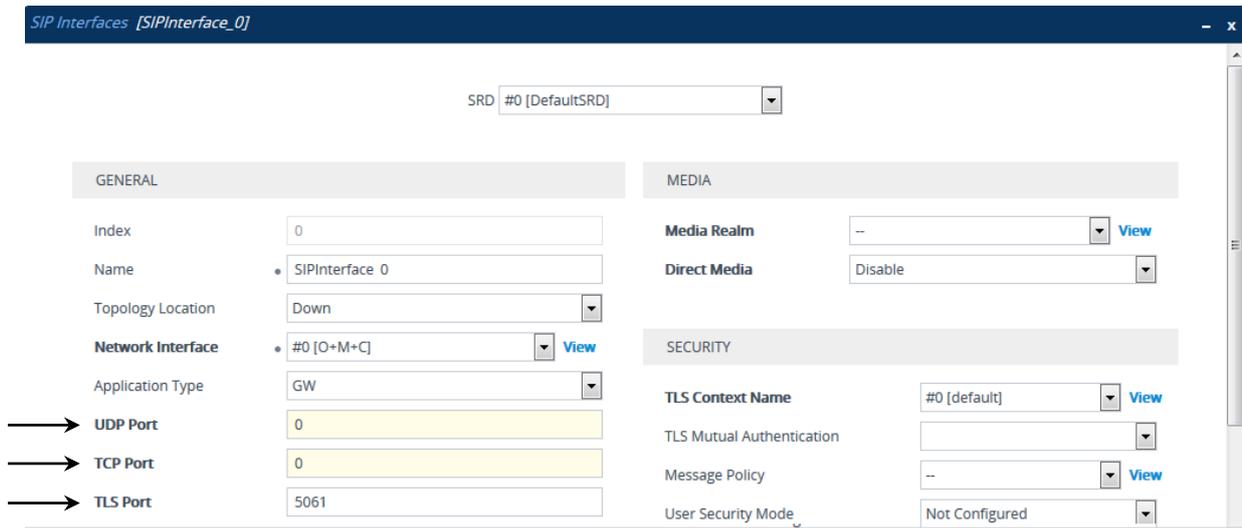
5.4 Use TLS for Routing Rules

It is recommended that your routing rules use TLS only as the transport type. This is configured in the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**), by configuring the 'Destination Transport Type' parameter to **TLS**:

Figure 19: IP-to-IP Routing Rule using SIP over TLS

5.5   Implement X.509 Certificates for SIPS (TLS) Sessions

It is highly recommended to implement the X.509 certificate authentication mechanism for enhancing and strengthening TLS. X.509 is an ITU-T standard for Public Key Infrastructure (PKI).

The device supports the configuration of multiple TLS certificates, referred to as TLS Contexts. TLS Contexts are assigned to Proxy Sets and/or SIP Interfaces, thereby enabling specific calls to use specific TLS certificates.

The device is shipped with a working TLS configuration (TLS Context ID 0), consisting of a unique Self-Signed Server Certificate. Self-Signed Certificate is the simplest form of an X.509 Certificate that is issued by the device itself without the use of any certificate signer (CA). The Self-Signed Certificate consists of the Public Key of the device that is signed by the Private Key of the device itself. However, use of this certificate is **strongly discouraged**. The Self-Signed Certificate is typically used in testing environments or for a low-scale deployment where solution security may be sacrificed in favor of simplified configuration procedures. The Self-Signed Certificate does not utilize CA trust relationships and its authenticity cannot be reliably verified. Instead, you should establish a PKI for your organization (provided by your security administrator) and use certificates signed by genuine CAs.

In a typical PKI scheme, Certificates are issued by a CA and provide an attestation by the CA that the identity information and the public key belong together. Each party has a list of Trusted Root Certificates – certificates of the CAs (or their roots) that are well-known and trusted by the party. When the certificate from the other party is received, its signing entity (CA) is compared with the Trusted Root Certificates list and if a match is found, the certificate is accepted.

The device uses the following files to implement X.509 PKI:

■ **Private Key File:** This file contains a private key that is used to perform decryption. It is the most sensitive part of security data and should never be disclosed to other entities.

■ **Certificate File:** This file contains a digital signature that binds together the Public Key with identity information. The Certificate may be issued by a CA or self-signed (issued by the device itself, which is not recommended – see above).

■ **Trusted Root Certificate File:** This file is the certificate of the Trusted Root CA used to authorize certificates received from remote parties, based on the identity of the CA that issued it. If the root certificate of this CA matches one of the Trusted Root Certificates, the remote party is authorized.

5.6 Use an NTP Server

It is recommended to implement a third-party NTP server so that the device receives the correct current date and time. This is necessary for validating certificates of remote parties. It is also recommended to enable the device to authenticate and validate messages received from the NTP server. Authentication is done using an authentication key with the MD5 cryptographic hash algorithm. NTP messages that are received without authentication are ignored.

The NTP server is configured on the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date** home icon):

Figure 5-20: NTP Server and Authentication Configuration

NTP SERVER	
Enable NTP	Enable
Primary NTP Server Address (IP or FQDN)	0.0.0.0
Secondary NTP Server Address (IP or FQDN)	
NTP Update Interval	Hours: 24 Minutes: 0
NTP Authentication Key Identifier	0
NTP Authentication Secret Key	••••••

6   Implement LDAP-based Conditional Call Routing

It is recommended that you implement a third-party, LDAP server in your network for determining whether a call from a specific source is permitted to be routed to its destination. This setup uses Call Setup rules, configured in the Call Setup Rules table, to define a condition-based script that queries an LDAP server for the caller's number (for example) in a specific LDAP attribute. If the number exists, the device routes the call to the destination; otherwise, the call is dropped. The device executes a Call Setup rule upon the receipt of an incoming call (dialog) at call setup, if a matching routing rule exists in the IP-to-IP Routing table, before the <device> routes the call to its destination.

For configuring the LDAP server for LDAP-based routing, use the LDAP-related items located under the **RADIUS & LDAP** folder (**Setup** menu > **IP Network** tab > **RADIUS & LDAP** folder).

For configuring Call Setup rules, use the Call Setup Rules table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Call Setup Rules**). The below Call Setup rule example routes the incoming call only if the source number of the incoming call exists in the AD server. The device queries the AD server for the attribute record, "telephoneNumber" whose value is the same as the received source number (e.g., "telephoneNumber=4064"). If such an attribute is found, the device routes the call to the destination as specified in the IP-to-IP Routing table. If the query fails (i.e., source number doesn't exist in AD server), the device rejects the call.

Figure 6-1: Call Setup Rule for Conditional LDAP-based Routing

Note: Make sure that you implement secure LDAP communication, as discussed in Section Secure LDAP Communication.

This page is intentionally left blank.

7   Define SIP Message Blacklist/Whitelist

It is recommended to configure SIP message policy rules for blocking (blacklist) unwanted incoming SIP messages or allowing (whitelist) receipt of desired messages. This allows you to define legal and illegal characteristics of a SIP message.

SIP message policy is helpful against VoIP fuzzing (also known as robustness testing), which sends different types of packets to its "victims" for finding bugs and vulnerabilities. For example, the attacker might try sending a SIP message containing an oversized parameter or too many occurrences of a parameter.

Each SIP message policy rule can be configured with, for example, maximum message length, header length, body length, number of headers, and number of bodies. Each rule is then set as a blacklist or whitelist.

The SIP message policy rules are configured in the Message Policies table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Policies**). Below shows a configured policy that defines maximum SIP messages to 32,768 characters, maximum header length to 512 characters, and bodies to 1024 characters. Invalid requests are rejected. Only INVITE and BYE requests are permitted.

Figure 7-1: Configured Message Policy Rule

INDEX ⇕	NAME	MAX MESSAGE LENGTH	MAX HEADER LENGTH	MAX BODY LENGTH	SEND REJECTION
0	Malicious Signature DB Pr	-1	-1	-1	Policy Drop
1	MessagePolicy_1	32768	512	1024	Policy Reject

This page is intentionally left blank.

8   Monitor and Log Events

It is highly recommended that you log and monitor device events (including device operations and calls). The importance of monitoring device events is that you can quickly detect unauthorized access and subsequently take counter measures to effectively terminate the attacker before any potential damage is done to your network.

8.1   Implement Dynamic Blacklisting of Malicious Activity (IDS)

It is important to configure the Intrusion Detection System feature (IDS) to enable the device to detect malicious attacks targeted on the device (e.g., DoS, SPAM, and Theft of Service). It is crucial to be aware of any attacks to ensure that the legitimate call service is maintained at all times. If any user-defined attacks are identified, the device can do the following:

■ Block (blacklist) remote hosts (IP addresses / ports) considered as malicious. The device automatically blacklists the malicious source for a user-defined period after which it is removed from the blacklist.

■ Send SNMP traps to notify of the malicious activity and/or whether an attacker has been added to or removed from the blacklist.

The IDS configuration is based on IDS Policies, where each policy can be configured with a set of IDS rules. Each rule defines a type of malicious attack to detect and the number of attacks (alarm threshold) during an interval (threshold window) before an SNMP trap is sent. Each policy is then applied to a target under attack (SIP Interface) and/or source of attack (Proxy Set and/or subnet address).

For configuring IDS, use the tables under the **Intrusion Detection** folder (**Setup** menu > **Signaling & Media** tab > **Intrusion Detection** folder).

Below is an example of an IDS rule for identifying DoS attacks from ITSP:

1. IDS Policy "ITSP DoS" configured (highlighted):

Table 8-1: Configured IDS Policy Name in IDS Policy Table

INDEX ⬍	NAME	DESCRIPTION
0	DEFAULT_FEU	Default policy for FEU
1	DEFAULT_PROXY	Default policy for proxies
2	DEFAULT_GLOBAL	Default policy for global scope
3	ITSP DoS	Denial of Service

2. IDS Rules configured for "ITSP DoS" IDS policy:

Table 8-2: Configured Rules in IDS Rule Table

INDEX ⬍	REASON	THRESHOLD SCOPE	THRESHOLD WINDOW	MINOR-ALARM THRESHOLD	MAJOR-ALARM THRESHOLD	CRITICAL-AL THRESHOLD	DENY THRESHOLD	DENY PERIOD
0	Malformed message	Global	30	10	15	30	-1	-1
1	Connection abuse	Global	20	-1	70	-1	-1	-1
2	Authentication failure	Global	1	-1	5	-1	-1	-1

3. IDS Policy assigned to a specific SIP interface and subnet:

Table 8-3: Applying IDS Policy to Elements in IDS Match Table

INDEX ⬍	SIP INTERFACE ID	PROXY SET ID	SUBNET	POLICY
0	3			ITSP DoS
1			10.33.0.0/16	ITSP DoS

8.2 Enable Syslog

The device supports generation and reporting of Syslog messages and SNMP traps to external logging servers. It is crucial that you enable one or both these features (preferably Syslog) so that you can monitor events on your device. In addition, as the device does not *retain* logged reports (SNMP is limited), it is recommended that you ensure that your Syslog server saves all logged events for future analysis and reference.

Syslog configuration is done on the Syslog Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Logging Settings**):

Figure 2: Enabling Syslog Server

SYSLOG

⟶ **Enable Syslog** ● Enable

⟶ **Syslog server IP** 10.8.7.5

⟶ Syslog Server Port 514

8.3   Enable Logging of Management-Related Events

Through Syslog you can log and monitor management-related events to help you detect and identify unauthorized management-related activities such as:

■ Unauthorized Web login attempts (attempts to access the Web interface with a false or empty user name or password)

■ Access to restricted Web pages such as the page on which firewall rules are defined

■ Modifications to parameter values (for example, deletion of firewall rules, allowing future unauthorized access)

■ Modifications to "sensitive" parameters - changes made to important parameters such as IP addresses

■ Unauthorized SIP messages (logged SIP messages)

This is configured on the Syslog Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Logging Settings**):

Figure 3: Enabling Logging of Management Events to a Syslog Server

ACTIVITY TYPES TO REPORT	
Select All	☐
Parameters Value Change	☐
Auxiliary Files Loading	☐
Device Reset	☐
Flash Memory Burning	☐
Device Software Upgrade	☐
Non-Authorized Access	☐
Sensitive Parameters Value Change	☐
Login and Logout	☐
CLI Activity	☐
Action Executed	☐

8.4 Enable Call Detail Records

Call Detail Records (CDR) provide vital information on SIP calls made through the device. This information includes numerous attributes related to the SIP call such as port number, physical channel number, source IP address, call duration, and termination reason. The device can be configured to generate and report CDRs for various stages of the call (beginning, initial connection, and end of the call). Once generated, the CDR logs are sent to a user-defined logging server.

This is configured on the Advanced Parameters page (**Troubleshoot** menu > **Troubleshoot** tab > **Call Detail Record** folder > **Call Detail Record Settings**):

Figure 4: Enabling CDR Generation

SYSLOG CDR REPORTS	
CDR Server IP Address	10.15.8.1
CDR Report Level	Start & End & Connect Call
Media CDR Report Level	End Media
CDR Syslog Sequence Number	Enable

> **Note:** Syslog must be enabled for the CDR feature.

9 SBC-Specific Security Guidelines

This section provides basic SBC security guidelines that should be implemented in your network deployment.

> **Note:** This section is applicable only to AudioCodes Session Border Controllers (SBC).

9.1 General Guidelines

It is crucial that you separate trusted from un-trusted networks:

■ Separate un-trusted networks from trusted networks, by using different SRDs, IP Groups, SIP Interfaces, and SIP Media Realms (with limited port range).

■ Similarly, separate un-trusted networks from one another. In particular, far-end users must be separated from the ITSP SIP trunk, using a different SRD, IP Group, SIP interface, and Media Realms. This separation helps in preventing attacks targeted on far-end user ports from affecting other users.

■ For un-trusted networks, use strict classification rules over vague rules. For example, if the ITSP's proxy IP address, port and host name are known, then use them in the classification rules. This ensures that all other potentially malicious SIP traffic is rejected.

■ Unclassified packets must be discarded (rejected).

9.2 Secure Media (RTP) Traffic using SRTP

It is recommended to use Secured RTP (SRTP) for encrypting the media (RTP and RTCP) path and thereby, protecting the VoIP traffic. The device supports SRTP according to RFC 3711. SRTP performs a Key Exchange mechanism (according to RFC 4568). This is done by adding a 'crypto' attribute to the SDP. This attribute is used (by both sides) to declare the supported cipher suites and to attach the encryption key. If negotiation of the encryption data is successful, the call is established. The device's SRTP feature supports various suites such as AES_CM_128_HMAC_SHA1_32.

■ **Globally (all calls):** Media Security page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Security**) by setting the 'Media Security' parameter to **Enable**.

Figure 5: Enabling SRTP Globally

Media Security   ● Enable ▼ ⚡

■ **Per specific calls using IP Profile:** SRTP is enforced on the SBC legs of an IP Profile (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**). For each IP Profile associated with a leg, configure the 'SBC Media Security Mode' parameter to **SRTP**. This enforces the SBC legs to negotiate only SRTP media lines; RTP media lines are removed from the incoming SDP offer \ answer.

Figure 6: Enabling SRTP per SBC Leg using IP Profiles

SBC Media Security Mode   SRTP ▼

9.3 Implement SIP Authentication and Encryption

It is paramount that your network implements authentication and encryption to secure the network and ensure integrity and confidentiality of sensitive communications over un-trusted networks. Some of the main authentication and encryption guidelines are discussed in the subsequent sections.

9.3.1 Authenticating Users as an Authentication Server

Instead of relying on external, third-party authentication servers, the device can be configured to act as an Authentication server, performing authentication and validation challenges with SIP user agents. The SIP method (INVITE or REGISTER) on which it challenges can be defined. If the message is received without an Authorization header, the device challenges the client by sending a 401 or 407 SIP response. The client then resends the request with an Authorization header containing its username and password. The device validates the SIP message and if it fails, the message is rejected and the device sends a 403 "Forbidden" response. If the SIP message is validated, the device verifies identification of the UA by checking whether the username and password received from the user is correct. The usernames and passwords are obtained from the User Information table. If after three attempts the UA is not successfully authenticated, the device sends a 403 "Forbidden" response. The device can also perform authentication on behalf of its UAs with an external third-party server.

To setup the SBC as an Authentication server, you need to do the following:

1. Configure the following parameters for the User-type IP Group of the UAs (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**):

Figure 7: Configuring SBC as Authentication Server for User-type IP Group

Authentication Mode	SBC as Server
Authentication Method List	invite/register

- 'Authentication Mode': select **SBC as Server**.
- 'Authentication Method List': enter "INVITE\REGISTER".

2. Configure the authentication usernames and passwords of the users:

   a. Enable the SBC User Info feature, by configuring the 'User-Information Usage' parameter to **Enable** on the Proxy & Registration page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Proxy & Registration**):

Figure 8: Enabling User Info File

User-Information Usage	Enable

⚠️ **Note:** Make sure that your device's License Key provides far-end users support ("FEU"); otherwise, this parameter will not be displayed.

   b. Add users with authentication usernames and passwords in the SBC User Info table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **User Information**):

Figure 9: Configured User in SBC User Info Table

INDEX ⇕	LOCAL USER	USERNAME	PASSWORD	IP GROUP	STATUS
0	John Dee	johnd	*	ITSP	Not Registered

9.3.2 Authenticating Users by RADIUS Server

Instead of authenticating calls locally by the device, digest authentication of SIP users can be done by a RADIUS server (according to RFC 5090). In this way, the device offloads the MD5 calculation (validation) to a RADIUS server, where the device is classed as a RADIUS client.

To implement this, the following configuration is required:

1. Configure the RADIUS sever (IP address, port and shared secret password) in the RADIUS Servers table (**Setup** menu > **IP Network** tab > **RADIUS & LDAP** folder > **RADIUS Servers**):

Figure 10: Configured RADIUS Server for User Authentication in RADIUS Servers Table

INDEX ⇕	IP ADDRESS	AUTHENTICATION PORT	ACCOUNTING PORT	SHARED SECRET
0	202.100.0.2	1645	1645	*

2. Configure the SBCServerAuthMode parameter to 1 to enable authentication by a RFC 5090 compliant RADIUS server.

9.3.3 Authenticating SIP Servers as an Authentication Server

It is recommended to enable the device to authenticate remote SIP servers (for example, Proxy servers). This provides protection from rogue SIP servers, preventing unauthorized usage of the device's resources and functionality. The device authenticates remote servers by challenging them with a user-defined username and password that is shared with the remote server. From such a challenge, the device can confirm the server's identity as being genuine. The type of SIP message (e.g., INVITE) to authenticate must also be defined.

SIP server authentication is configured per IP Group in the IP Groups table, enabling unique authentication handling per specific server:

Figure 11: Configured SIP Server Authentication by SBC in IP Groups Table

Authentication Mode	SBC as Server ▼
Authentication Method List	INVITE
Username	ipbx_foo
Password	••••

9.3.4 Enforce SIP Client Authentication by SIP Proxy

When the device is located between a SIP client and a third-party SIP proxy server and SIP Digest Authentication is used, the device relays authentication messages between these entities. Although the device gathers and maintains some information in its registration database (Address of Record / AOR) it does not actively participate in the authentication process. Instead, it is the SIP proxy that handles and enforces SIP client authentication. Therefore, it is imperative that your SIP proxy server be configured to enforce SIP client authentication.

9.3.5   Enforce SIP Digest Authentication by IP PBX

If TLS cannot be configured (for whatever reason) and if you are using an on-premises IP PBX, it is crucial that your IP PBX implements SIP Digest Authentication for remote users. In addition, authentication should be applied to as many SIP methods as possible (i.e., not only on REGISTER messages, but also INVITEs, re-INVITEs, etc.).

9.4   Secure Routing Rules

This section provides recommended security guidelines regarding routing rules.

9.4.1   Classify by Classification Rules versus Proxy Set

An important security functionality of the SBC is to make sure that it does not mistakenly identify incoming SIP dialog-initiating requests (e.g., INVITE messages) from malicious attackers as belonging to a configured server-type IP Group entity. The SBC provides two optional mechanisms that can be employed to identify incoming dialogs as coming from a specific server-type IP Group:

■ **Classification rules in the Classification table:** Identifies incoming dialogs based on the characteristics of the SIP message such as host name in the INVITE message (Layer 4-7), and/or based on the source IP address (Layer-3).

■ **Proxy Set:** Identifies incoming dialogs based on source IP address (Layer-3) only. The Proxy Set defines the address of the IP Group.

Regarding which classification method to employ:

■ If the IP address of the IP Group entity is known, it is recommended to employ SIP dialog classification based on a Classification rule, where the rule is configured with not only the IP address, but also with SIP message characteristics to increase the strictness of the classification process. For more information on configuring Classification rules, see Section 9.4.2.

■ If the IP address is unknown, in other words, the Proxy Set associated with the IP Group is configured with an FQDN, it is recommended to employ SIP dialog classification based on Proxy Set. This allows the SBC to classify the incoming dialog based on the DNS-resolved IP address. The reason for classifying by Proxy Set is that IP address forgery (commonly known as IP spoofing) is more difficult than malicious SIP message tampering and therefore, using a Classification rule without an IP address offers a weaker form of security. When classification is based on Proxy Set, the Classification table is ignored.

Classification by Proxy Set is enabled in the IP Groups table, using the 'Classify By Proxy Set' parameter:

Figure 12: Enabling Classification based on Proxy Set in the IP Groups Table
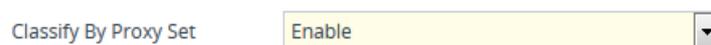
9.4.2   Define Strict Classification Rules

Classification rules are used to identify incoming SIP dialog-initiating requests (e.g., INVITE messages) and bond them to IP Groups. In other words, these rules identify the source of the call. Once the source IP Group is identified, the traffic can then be routed to its destination according to IP-to-IP routing rules.

When defining Classification rules, adhere to the following recommendations:

■   For Server-type IP Groups, use Classification rules **only** if the IP address of the IP Group is known. If known, include the IP address in the Classification rule ('Source IP Address' parameter). In addition, to increase classification strictness, configure SIP message characteristics in the rule as well.

> **Note:**   If the IP address is unknown (i.e., the Proxy Set associated with the IP Group is configured with an FQDN), it is recommended to employ SIP dialog classification based on Proxy Set (see Section 9.4.1). In such a scenario, the Classification table is ignored and must not be configured for the specific IP Group.

■   For Server-type IP Groups whose IP addresses are known, it is recommended to also configure VoIP firewall rules (see Section 3.1).

■   Use strict Classification rules over vague ones so that all other potentially malicious SIP traffic is rejected. In other words, configure the rule with as much information as possible that accurately characterizes the incoming SIP dialog (e.g. source and destination host name).

■   Define a range for the source and destination prefix numbers.

■   Define a combination of Classification rules to guarantee correct and accurate identity of sender of call.

■   Use Message Condition rules to increase the strictness of the Classification process. Message Condition rules enhance the process of classifying incoming SIP dialogs to an IP Group. When a Classification rule is associated with a Message Condition rule, the Classification rule is used only if its' associated Message Condition rule are matched. Message Condition rules are SIP message conditions based on the same syntax used in the Message Manipulations table. You can define complex rules using the "AND" or "OR" Boolean operands. You can also use regular expressions (regex) as Message Condition rules, for example:

•   "body.sdp regex pcmu" can be used to enable routing based on the offered codec (G.711 Mu) in the incoming SDP message

•   "body.sdp regex (AVP[0-9||\s]*\s8[\s||\n])" can be used to enable routing based on payload type 8 in the incoming SDP message

To implement message conditions:

1.   Configure a Message Condition rule in the Message Conditions table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Conditions**). The figure below shows a Message Condition rule example for P-Asserted-Identity headers that contain "abc":

Figure 13: Configured Message Condition Rule in Message Conditions Table

INDEX ⬍	NAME	CONDITION
0	P-Asserted-Identity header with "sbc"	header.p-asserted-identity.url.user contains 'abc'

2. Assign the Message Condition rule to the Classification rule in the Classification table, using the 'Message Condition' parameter:

Figure 14: Assigned Message Condition Rule in Classification Table

Message Condition   #0 [P-Asserted-Identity he ▼]
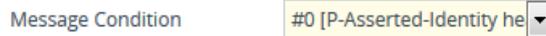
■ Make sure that you configure the device to block all unclassified calls, as described in Section 9.4.3.

Classification rules are configured in the Classification table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Classification**). The figure below shows an example of two Classification rules:

■ **Index 0 "ITSP":** Classifies received calls to Server-type IP Group "ITSP" if they have the following incoming matching characteristics:

  • 'Source IP Address': 10.15.7.96

  • 'Source Username Prefix': 2 through 4

  • 'Source Host': domain.com

  • 'Destination Username Prefix': 1 through 7

  • 'Message Condition': SIP message with P-Asserted-Identity header containing "abc" (Message Condition rule described previously in this section)

■ **Index 2 "Deny":** Denies calls that cannot be classified (unknown calls).

Figure 15: Configured Classification Rules in Classification Table

INDEX	NAME	SRD	SOURCE SIP INTERFACE	SOURCE USERNAME PREFIX	SOURCE HOST	DESTINATION USERNAME PREFIX	DESTINATION HOST	ACTION TYPE	SOURCE IP GROUP
0	ITSP	■ DefaultSRD	Any	[2-4]	domain.com	[1-7]	*	Allow	ITSP
1	Deny	■ DefaultSRD	Any	*	*	*	*	Deny	--

9.4.3 Block Unclassified Calls

It is recommended that you block incoming calls that cannot be classified to an IP Group, based on the rules in the Classification table (discussed in the previous section). If unclassified calls are not blocked, they are sent to the default SRD / IP Group and therefore, illegitimate calls can be established.

This is done on the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**), by configuring the 'Unclassified Calls' parameter to **Reject**:

Figure 16: Blocking Unclassified Incoming Calls

Unclassified Calls   Reject   ▼

9.4.4 Allow Calls Only with Specific SIP User-Agent Header Value

The SIP User-Agent header contains information about the User Agent Client (UAC) initiating the SIP dialog request. This information is unique to the Enterprise and therefore, it is recommended to configure your device so that it accepts only calls that have a specified User-Agent header value. This is configured by adding a Message Condition rule (in the

Message Conditions table) for this SIP header type and then assigning it to a Classification rule (in the Classification table).

The figure below shows a Message Condition rule in the Message Conditions table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Conditions**) whose condition is for the SIP User-Agent header to have the value "abc.com":

Figure 17: Message Condition Rule for SIP User-Agent Header in Message Condition Table

INDEX ⇕	NAME	CONDITION
0	Only sbc.com calls	header.user-agent='abc.com'

9.4.5   Define Strict Routing Rules

It is crucial that you adhere to the following guidelines when configuring IP-to-IP Routing rules:

■ Ensure that your routing rules are accurate and correctly defined. Inaccurate or weak routing rules can easily result in Service Theft.

■ Ensure that your routing rules from **source IP Group** to **destination IP Group** are accurately defined for the desired call routing outcome.

■ If possible, avoid using the asterisk (*) symbol to indicate "any" for a specific parameter in your routing rule. This constitutes weak routing rules that can be vulnerable to attackers. For strong routing rules, enter specific alphanumerical values instead of the asterisk.

9.5   Define Call Admission Control Rules

It is recommended to define call admission control (CAC) rules for regulating VoIP traffic volume. CAC rules can assist in limiting the rate of call requests, preventing excessive signaling requests originating from malicious and legitimate sources from overwhelming your network resources.

CAC rules can limit the number of concurrent calls (SIP dialogs) per IP Group, SIP Interface or SRD. The call limitation can be defined per SIP-dialog initiating request type (e.g., INVITE or REGISTER messages), request direction (inbound, outbound, or both), and user. Requests that exceed the user-defined limits are rejected (with SIP 480 "Temporarily Unavailable" responses). You can also limit the incoming packet rate based on the "token bucket" mechanism.

Adhere to the following CAC recommendations:

■ It is crucial that your CAC rules include call limitations per user. This ensures that a user does not make unlimited, simultaneous calls.

■ Define rules as specific as possible. For example, instead of defining one rule for all SIP request types, create rules for each SIP request type.

Note that if call routing to a specific IP Group is blocked due to a CAC rule, the device searches for an alternative route (if defined) in the SBC IP-to-IP Routing table. If this alternative route does not exceed the CAC rule limitation, the device uses it to route the call.

CAC rules are configured in the Call Admission Control Profile table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Call Admission Control Profile**). The figure below displays a CAC rule that defines a maximum of 100 concurrent SIP INVITE requests. SIP requests received above this threshold are rejected:

Figure 18: Configured CAC Rule in Call Admission Control Rule Table

INDEX ⇕	REQUEST TYPE	REQUEST DIRECTION	LIMIT	LIMIT PER USER
0	INVITE	Both	100	-1

9.6 Define Maximum Call Duration

It is recommended to define maximum call duration (in minutes) to prevent SBC calls from utilizing valuable device resources that could otherwise be used for additional new calls. If a call exceeds this duration, the device terminates the call.

This is done on the Gateway Advanced Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**), by configuring the 'Max Call Duration' parameter:

Figure 19: Configured Maximum Call Duration

Max Call Duration [min]	45

9.7 Secure SIP User Agent Registration

Service theft can result from a lack of security in the SIP user registration process. This section provides recommended guidelines regarding user registration.

9.7.1 Configure Identical Registration Intervals

Scenarios in which the device does not forward user registrations to a server (e.g., a PBX) and the device receives a new REGISTER request from the same number (i.e., same AOR) but without an Authentication header, the device still sends a SIP 200 OK response to the user. This is because the AOR already exists in the device's registration database. Therefore, if an illegitimate user attempts to connect with a legitimate IP address and phone number (without authentication), the malicious user can connect and steal calls.

To overcome this issue and prevent stealing of calls, ensure that you set the user and proxy registration times with **identical** values. On the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Proxy & Registration**), do the following:

■ Define the duration of the periodic registrations between the user and the device in the 'User Registration Time' field.

■ Define the time interval (in seconds) that the device must register to the server (e.g., PBX) in the 'Proxy Registration Time' field.

Figure 20: Configured User Registration Times

User Registration Time [sec]	100
Proxy Registration Time [sec]	100

9.7.2   Limit SBC Registered Users per IP Group, SIP Interface or SRD

It is recommended that you define a maximum number of allowed registered users per IP Group (User-type IP Group), SIP Interface, or SRD. This ensures that illegitimate users are blocked from registering with the IP Group. This can be configured in the IP Groups table, SIP Interfaces table, or SRDs table, by using the 'Max. Number of Registered Users' parameter:

Figure 21: Configured Maximum Number of Allowed Registered Users

Max. Number of Registered Users   120

9.7.3   Block Calls from Unregistered Users

Ensure that calls from unregistered users are blocked (rejected) and that calls from only registered users are allowed. This can be configured per SRD or SIP Interface, by configuring the 'User Security Mode' parameter to **Accept Registered Users**:

Figure 22: Blocking Unregistered Users

User Security Mode   Accept Registered Users   ▼

9.7.4   Block Registration from Un-Authenticated New Users

In normal operation scenarios in which a SIP proxy (registrar) server is available, the SBC forwards REGISTER requests from new users to the proxy, and if authenticated by the proxy (i.e., SBC receives a success response) the SBC adds the user to its registration database. However, if the proxy becomes unavailable at any time (e.g., due to network connectivity loss), the REGISTER requests cannot therefore be authenticated. In such scenarios, make sure that the SBC is configured to reject such unauthenticated REQUEST messages from new users. Note that the SBC does accept registration refreshes from users already in its database.

Blocking registration of un-authenticated users can be done per SRD or SIP Interface, by configuring the 'Enable Un-Authenticated Registrations' parameter to **Disable**:

Figure 23: Blocking Local Registration of Un-Authenticated Users

Enable Un-Authenticated Registrations   Disable   ▼

9.8   Authenticate SIP BYE Messages

It is recommended to enable the device to authenticate incoming SIP BYE requests before it releases the call. This prevents, for example, a scenario in which the SBC SIP client receives a BYE request from a third-party imposer assuming the identity of a participant in the call and therefore, the call between the legitimate first and second parties is inappropriately disconnected.

When the SBC is configured to authenticate BYE messages, it sends a SIP authentication response to the sender of the BYE request and waits for the sender (user) to authenticate it. The call is disconnected only if the authenticating server responds with a 200 OK.

This is done on the Proxy & Registration page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Proxy & Registration**), by configuring the 'BYE Authentication' to **Enable**:

Figure 9-24: Enabling SIP BYE Authentication

BYE Authentication	Enable ▾
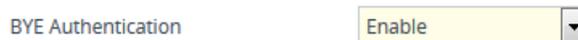
9.9   Use SIP Message Manipulation for Topology Hiding

The device intrinsically employs topology hiding, limiting the amount of topology information displayed to external parties (i.e., un-trusted networks). This anonymous information minimizes the chances of directed attacks on your network.

The device employs topology hiding by implementing back-to-back user agent (B2BUA) leg routing:

- Strips all incoming SIP Via header fields and creates a new Via value for the outgoing message

- Each leg has its own Route/Record Route set

- Generates a new SIP Call-ID header value (different between legs)

- Changes the SIP Contact header to the device's address

- Performs Layer-3 topology hiding by modifying the source IP address in the SIP IP header (for example, IP addresses of ITSPs equipment such as proxies, gateways, and application servers can be hidden from outside parties)

In addition, to enhance topology hiding, you can modify the SIP To header, From header, and/or Request-URI host name. This can be done using the Message Manipulation table or the IP Group (for SIP URI host part manipulations). The Message Manipulation table also supports Regular Expressions (Regex).

9.10   Define Malicious Signatures

To protect the device from malicious attacks on SBC calls, it is recommended to employ the device's Malicious Signature feature, which defines malicious signature patterns. The Malicious Signature feature identifies and protects against SIP (Layer 5) threats by examining new inbound SIP dialog messages. Once the device identifies an attack based on the configured malicious signature patterns, it marks the SIP message as invalid and discards it (or alternatively, rejects it with a SIP response). Malicious signatures are typically based on the SIP User-Agent header, which attackers often use as their identification string (e.g., "User-Agent: VaxSIPUserAgent").

Malicious signatures are configured in the Malicious Signature table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Malicious Signature**). (The device provides preconfigured malicious signatures.)

Figure 9-25: Configured Malicious Signatures

INDEX ⇕	NAME	PATTERN
0	SIPVicious	Header.User-Agent.content prefix 'friendly-scanner'
1	SIPScan	Header.User-Agent.content prefix 'sip-scan'
2	Smap	Header.User-Agent.content prefix 'smap'
3	Sipsak	Header.User-Agent.content prefix 'sipsak'

To apply the malicious signatures:

1.   In the Message Policies table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Policies**), configure a Message Policy and enable it to use the malicious signatures:

Figure 9-26: Enabling Malicious Signatures for Message Policy

Malicious Signature Database | Enable |

2.   Assign the Message Policy to the SIP Interface of the calls that you want to apply the malicious signatures:

Figure 9-27: Assigning Message Policy (with Malicious Signatures) to SIP Interface

Message Policy   #0 [Malicious Sign| **View**

This page is intentionally left blank.

10   Gateway-Specific Security Guidelines

This section describes recommended security guidelines for the device's supporting the Gateway application. These guidelines are important for preventing malicious attacks such as DoS.

10.1   Block Calls from Unknown IP Addresses

Ensure that the device accepts incoming calls only from source IP addresses that are defined in the Proxy Sets table or Tel-to-IP Routing table. In addition, if an FQDN is defined in these tables, the call is accepted only if the resolved DNS IP address of the call is defined in any one of these tables. All other calls whose source IP address is not defined in these tables are rejected. This is useful in preventing unwanted SIP calls, SIP messages, and VoIP spam.

This is configured on the Gateway Advanced Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway Advanced Settings**), by configuring the 'IP Security' parameter to **Secure All calls**:

Figure 28: Allowing Calls only from Defined IP Addresses

IP Security	Secure All calls ▾

10.2   Enable Secure SIP (SIPS)

Ensure that you enable Secure SIP (SIPS) so that the device initiates TLS all the way to the destination, i.e., over multiple hops. SIPS runs SIP-over-TLS on a hop-by-hop basis. This is important as using TLS as a transport by itself guarantees only encryption over a single hop. Since it is very common for a SIP call to traverse multiple proxy servers from one end to the other, there is a need to guarantee end-to-end security for SIP traffic. A call to a SIPS URI is guaranteed to be encrypted from end to end. All SIP traffic within this call is secured using TLS from the sender to the domain of the final recipient.

To implement SIPS:

1. Enable secure SIP (SIPS): On the Transport Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Transport Settings**), configure the 'SIPS' to **Enable**:

Figure 29: Enabling SIPS

Enable SIPS	Enable ▾

> **Note:** It is recommended to use the 'SIPS' parameter and not the 'SIP Transport Type' parameter to define TLS. The 'SIP Transport Type' parameter provides only a TLS connection to the next network hop, whereas the 'SIPS' parameter provides TLS to the final destination (over multiple hops).

2. Configure the local SIP TLS port for the SIP Interface in the SIP Interfaces table.

10.3   Define Strict Routing Rules

When defining IP-to-Tel (IP-to-Trunk Group Routing table) and Tel-to-IP (Tel-to-IP Routing table) routing rules, it is crucial that you adhere to the following security guidelines:

■ Ensure that your routing rules are accurate and correctly defined for the desired routing outcome. Inaccurate or "loose" routing rules can easily result in service theft.

■ Avoid, if possible, using the asterisk "*" symbol and **Any** option to indicate any for a specific parameter in your routing rules. This constitutes weak routing rules that can be vulnerable to attackers. For strong routing rules, enter specific alphanumerical values instead of the asterisk.

10.4   Define Call Admission Control

Ensure that you set the maximum, allowed concurrent calls per routing rule or IP Group. This is done by defining a call limit for an IP Profile and then assigning the IP Profile to IP-to-Tel and/or Tel-to-IP routing rules, or IP Groups. Note that the maximum number of calls considers incoming and outgoing calls (i.e., summation of all calls to which the IP Profile is assigned).

This is done in the IP Profile table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**), by configuring the 'Number of Calls Limit' parameter:

Figure 30: Configured Maximum Concurrent Calls for IP Profile

Number of Calls Limit   120

10.5   Define Maximum Call Duration

It is recommended to define maximum call duration (in minutes) to prevent Gateway calls from utilizing valuable device resources that could otherwise be used for additional new calls. If a call exceeds this duration, the device terminates the call.

This is done on the Gateway Advanced Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway Advanced Settings**), by configuring the 'Max Call Duration' parameter:

Figure 31: Configured Maximum Call Duration

Max Call Duration [min]   45

11   Network Port Assignment

The table below lists the device's network port assignments. This table also shows whether these ports are enabled or disabled by default and how to configure them. For ports that you do not need in your deployment but that are enabled by default, it is highly recommended that you disable them for security reasons.

> **Note:** For increased security against attacks, it is highly recommended to change the default port numbers (especially for the SIP application).

Table 11-1: Network Port Assignments

Interface Type	Port	Protocol	Application	Default	Port Configuration
OAMP	22	TCP	SSH server	Enabled	▪ Enable / Disable: Enable SSH Server (SSHServerEnable) ▪ Port Definition: Server Port (SSHServerPort) ▪ Access Control: Layer 3/4 Firewall and Access List table (WebAccessList_x)
	23	TCP	Telnet server	Enabled	▪ Enable / Disable: Embedded Telnet Server (TelnetServerEnable) ▪ Port Definition: Telnet Server TCP Port (TelnetServerPort) ▪ Access Control: Layer 3/4 Firewall and Access List table (WebAccessList_x)
	80	TCP	Web server (HTTP)	Enabled	▪ Enable / Disable: Secured Web Connection (HTTPSOnly) – when set to HTTPS Only ▪ Port Definition: HTTPPort ▪ Access Control: Layer 3/4 Firewall and Access List table (WebAccessList_x)
	443	TCP	Web server (HTTPS)	Enabled	▪ Port Definition: HTTPSPort ▪ Access Control: Layer 3/4 Firewall and Access List table (WebAccessList_x)

	161	UDP	SNMP server (GET / SET) and client (Trap sender)	Enabled	▪ Enable / Disable: Disable SNMP (DisableSNMP)
					▪ Port Definition:
					  ✓ SNMPPort – GET / SET
					  ✓ SNMP Trap Destinations table (SNMPManagerIsUsed_x) – Trap sender
					▪ Access Control: Layer 3/4 Firewall and SNMP Trusted Managers table (SNMPTrustedMgr_x)

Any	67	UDP	DHCP server	Disabled	▪ Enable / Disable: DHCP Server table ▪ Interface Definition: Interface Name (DHCPServer_InterfaceName) ▪ Port Definition: Fixed ▪ Access Control: Layer 3/4 Firewall

Interface Type	Port	Protocol	Application	Default	Port Configuration
Control	5060	UDP / TCP	SIP traffic	Enabled	▪ Enable / Disable: SIP Interfaces table – UDP Port / TCP Port (SIPInterface) ▪ Port Definition: SIP Interfaces table – UDP Port / TCP Port (SIPInterface) ▪ Access Control: Layer 3/4 Firewall
	5061	TCP	SIPS traffic	Enabled	▪ Enable / Disable: SIP Interfaces table – TLS Port (SIPInterface) ▪ Port Definition: SIP Interfaces table – TLS Port (SIPInterface) ▪ Access Control: Layer 3/4 Firewall
Media	6000-65535	UDP	Media traffic (RTP, RTCP, T.38)	Enabled	▪ Enable / Disable: Enabled during SIP session establishment ▪ Port Definition: Media Realms table – Port Range Start (CpMediaRealm_PortRangeStart) and Number Of Media Session Legs (CpMediaRealm_MediaSessionLeg) ▪ Access Control: N/A
Maintenance (HA)	669	UDP	HA status	Disabled	▪ Applicable to: ✓ Standalone SBC ✓ Signaling Component in Mediant CE ✓ Signaling Component in Media Transcoding Cluster ▪ Enable / Disable: HA Remote Address (HARemoteAddress) ▪ Port Definition: N/A
	680	UDP	HA keep-alive	Disabled	▪ Applicable to: ✓ Standalone SBC ✓ Signaling Component in Mediant CE ✓ Signaling Component in Media Transcoding Cluster ▪ Enable / Disable: HA Remote Address (HARemoteAddress) ▪ Port Definition: N/A
	80	TCP	HA file sync	Disabled	▪ Applicable to: ✓ Standalone SBC ✓ Signaling Component in Mediant CE ✓ Signaling Component in Media Transcoding Cluster ▪ Enable / Disable: HA Remote Address (HARemoteAddress) ▪ Port Definition: N/A

Interface Type	Port	Protocol	Application	Default	Port Configuration

	2442	TCP	HA data sync	Disabled	▪ Applicable to:
					  ✓ Standalone SBC
					  ✓ Signaling Component in Mediant CE
					  ✓ Signaling Component in Media Transcoding Cluster
					▪ Enable / Disable: HA Remote Address (HARemoteAddress)
					▪ Port Definition: N/A

Cluster	2424	TCP	Cluster control	Disabled	▪ Applicable to:
					  ✓ Signaling Component in Mediant CE
					  ✓ Media Component in Mediant CE
					  ✓ Signaling Component in Media Transcoding Cluster
					  ✓ Media Component in Media Transcoding Cluster
					▪ Enable / Disable: Cluster Mode (ClusterMode)
					▪ Port Definition: N/A

	3900	UDP	Cluster keep-alive	Disabled	▪ Applicable to:
					  ✓ Signaling Component in Mediant CE
					  ✓ Media Component in Mediant CE
					  ✓ Signaling Component in Media Transcoding Cluster
					  ✓ Media Component in Media Transcoding Cluster
					▪ Enable / Disable: Cluster Mode (ClusterMode)
					▪ Port Definition: N/A

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/

Document #: LTRT-30218