

Alcatel-Lucent OpenTouch™ Session Border Controller – R7.4.4

Recommended Security Guidelines Configuration Note

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://myportal.al-enterprise.com/>.

This document is subject to change without notice.

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.

Related Documentation

Document Title - Reference	
Alcatel-Lucent OpenTouch™ Session Border Controller – R7.4.4 Administrator / User manual	8AL90068USAF ed02
Alcatel-Lucent OpenTouch™ Session Border Controller – R7.4.4 Configuration Guide	8AL90065USAI ed03
Alcatel-Lucent OpenTouch™ Session Border Controller - R7.4.4 SNMP Reference Guide	8AL90067USAFed02
Alcatel-Lucent OpenTouch™ Session Border Controller – R7.4.4 Release Note	8AL90062USAH ed02
Alcatel-Lucent OpenTouch™ Session Border Controller - R7.4.4 SIP Message Manipulation Reference Guide	8AL90543USAF ed02
Alcatel-Lucent OpenTouch™ Session Border Controller – R7.4.4 Performance monitoring parameters and alarms	8AL90557USAB ed02
Alcatel-Lucent OpenTouch™ Session Border Controller - R7.4.4 Recommended Security Guidelines Configuration Note	8AL90063USAF ed02
Alcatel-Lucent OpenTouch™ Session Border Controller - R7.4.4 Virtual Edition REST API for Devices	8AL90078USAA ed02
Alcatel-Lucent OpenTouch™ Session Border Controller - R7.4.4 Version 7.2 to 7.4 Upgrade Procedure Configuration note	8AL90079USAA ed02
Alcatel-Lucent OpenTouch™ Session Border Controller - R7.4.4 CLI Reference Guide	8AL90542USAF ed02
Alcatel-Lucent OpenTouch™ Session Border Controller - R7.4.4 Virtual Edition Installation Manual	8AL90061USAF ed02
Alcatel-Lucent OpenTouch™ Session Border Controller - R7.4.4 Upgrade Procedure to Versions using Signed CMP	8AL90170USAA ed01

Table of Contents

1	Introduction	1
	Security Threats	1
	AudioCodes Security Solution	3
2	Separate Network Traffic	5
	Identify Trusted and Un-trusted Networks	5
	Implement Physical Network Separation using Ethernet Port Groups	5
3	Implement Layer 3/4 (Network) Firewall	7
	Block Unused Network Ports	7
	Define VoIP Traffic Firewall Rules	7
4	Secure Management Access	10
	Change Default Management User Login Passwords	10
	User Authentication by Third-Party Server	11
	LDAP-based User Authentication and Authorization	11
	RADIUS-based User Authentication	11
	OAuth 2.0 Authentication using Azure AD	12
	Implement Two-Way Authentication with X.509 Certificates	12
	Secure HTTP Access using HTTPS	14
	Secure Telnet Sessions	14
	Secure CLI Sessions by SSH	14
	Define Web, Telnet, and SSH Authorized Access List	15
	Protect Against DNS Rebinding Attacks	15
	HTTP Host Header Validation	16
	Secure SNMP Interface Access	16
	Prefer SNMPv3 over SNMPv2	16
	Secure SMNPv2 Access	17
	Secure LDAP Communication	17
	Customizing Access Levels per Web Page	18
5	Secure SIP using TLS (SIPS)	19
	Use Strong Authentication Passwords	19
	Use TLS Version 1.2 or 1.3	19
	Block Multiple Client-Initiated TLS Renegotiations	20
	Use TLS for SIP Interfaces and Block TCP/UDP Ports	20
	Use TLS for Routing Rules	21
	Implement X.509 Certificates for SIPS (TLS) Sessions	21
	Use an NTP Server	22
	OAuth 2.0-based Authentication for SIP Requests using Azure AD	23
6	Implement LDAP-based Conditional Call Routing	24
7	Define SIP Message Blocklist/Allowlist	25
8	Monitor and Log Events	26
	Implement Dynamic Blocklisting of Malicious Activity (IDS)	26
	Enable Syslog	27
	Enable Logging of Management-Related Events	28
	Enable Call Detail Records	29
9	GDPR for Protecting Personal Information	31

Masking PII	31
Deleting Locally Stored CDRs and SDRs	32
Deleting Persistent Logs	32
Encrypting the SIP Header Value	33
10 SBC-Specific Security Guidelines	34
General Guidelines	34
Secure Media (RTP) Traffic using SRTP	34
Implement SIP Authentication and Encryption	35
Authenticating Users as an Authentication Server	35
OAuth 2.0 Token-based SIP Authentication	36
Authenticating Users by RADIUS Server	37
Authenticating SIP Servers as an Authentication Server	37
Enforce SIP Client Authentication by SIP Proxy	38
Enforce SIP Digest Authentication by IP PBX	38
Secure Routing Rules	38
Classify by Classification Rules versus Proxy Set	38
Define Strict Classification Rules	39
Validate Source IP Address of Incoming SIP Dialog Requests	41
Block Unclassified Calls	42
Allow Calls Only with Specific SIP User-Agent Header Value	42
Define Strict Routing Rules	43
Define Call Admission Control Rules	43
Define Maximum Call Duration	44
Secure SIP User Agent Registration	44
Configure Identical Registration Intervals	44
Limit SBC Registered Users per IP Group, SIP Interface or SRD	45
Block Calls from Unregistered Users	45
Block Registration from Un-Authenticated New Users	45
Authenticate SIP BYE Messages	46
Use SIP Message Manipulation for Topology Hiding	46
Define Malicious Signatures	47
Secure Media Cluster Management Interface	48
11 Gateway-Specific Security Guidelines	49
Block Calls from Unknown IP Addresses	49
Enable Secure SIP (SIPS)	49
Define Strict Routing Rules	50
Define Call Admission Control	50
Define Maximum Call Duration	50
12 Network Port Assignment	52

1 Introduction

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

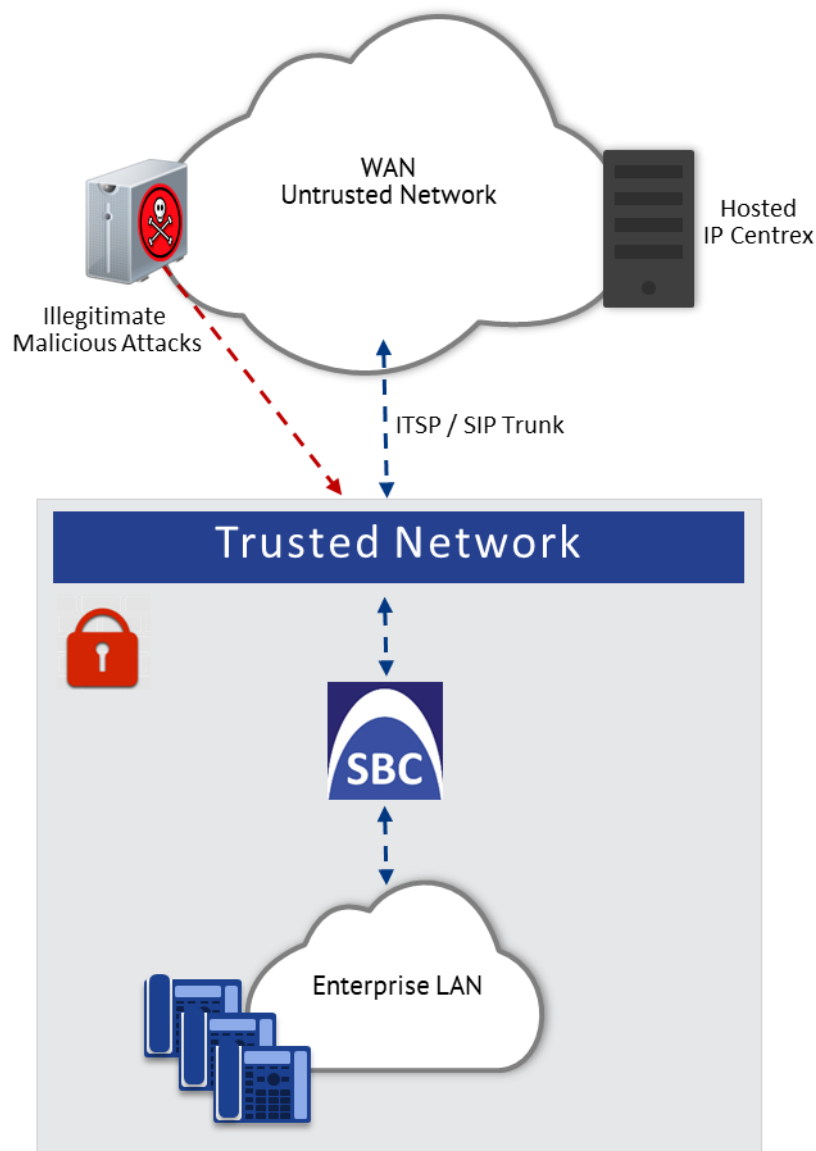


- This document provides **only** recommended security guidelines; your network architecture may require additional and/or different security measures.
- The document includes partial configuration. For detailed configuration, refer to the device's User's Manual.
- The document may refer to AudioCodes products not included in Version 7.4. For a list of supported products, refer to the [Release Notes](#).

Security Threats

AudioCodes devices are commonly located at the demarcation point between safe (trusted) and unsafe (untrusted) 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 following figure illustrates this basic concept of trusted and untrusted networks.

Figure 1-1: Trusted and Untrusted 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).
- **Untrusted access:** Unmanaged Internet for connections to work-at-home agents or inbound callers.

AudioCodes Security Solution

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

- **Securing the Service:** Secures the call services by implementing separation and defense of different network entities (e.g., SIP Trunk, softswitch, and users):
 - Physical separation of networks
 - SRDs per SIP entity (user agent)
 - IP Groups per SIP entity (user agent)
- **Securing the Device:**
 - Ensures that only authorized users can access the device's management interface
 - Protection against attacks on the device from SIP signaling and media (RTP).

For the SBC application, the device provides built-in protection from Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks:

- ◆ Prevention of DoS/DDoS SIP flood attacks
- ◆ Defense against TCP\IP vulnerabilities

- ◆ Defense against ICMP flooding
- ◆ Optimal handling of SIP user registration avalanche
- ◆ Prevents over-the-top traffic from unknown sources

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's AudioCodes security solutions that are designed to help safeguard your trusted network from such threats.

2 Separate Network Traffic

This chapter provides recommendations for separating network traffic.

Identify Trusted and Un-trusted Networks

It's 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.

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.

➤ **To implement physical network separation:**

1. Open the Ethernet Groups table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Groups**), and then assign ports to different Ethernet Group:

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. Open the Ethernet Devices table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Devices**), and then configure VLAN IDs per Ethernet Group:

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. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**), and then assign the Ethernet Devices (VLANs) to the different traffic network 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 therefore, configuring firewall rules is recommended to protect the device from external attacks.

Block Unused Network Ports

It's recommended that you disable network ports that are not needed in your deployment. For example, if you don't need TFTP in your network, then disable this network port application.

Define VoIP Traffic Firewall Rules

For packets whose source IP addresses are known, it's 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's recommended to configure firewall rules for packets from source IP addresses received on the OAMP interface and each SIP Control (SIP) interface (configured in the IP Interfaces table). A less recommended alternative is to define a single rule that applies to all interfaces (by configuring the 'Use Specific Interface' parameter to **Disable**).
- Define bandwidth limitation per rule: For each IP network interface, it's advised to configure 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's 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).



- 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, make



- sure that you also set the 'Prefix Length' field to a value other than "0".
- The device provides built-in firewall rules that allow High Availability (HA) traffic between Active and Redundant devices on the Maintenance network interface.

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

Table 3-1: Configuration Example of Firewall Rules in the Firewall Table

Parameter	Index				
	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

- Index 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.

- Index 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.
- Index 4: Allows traffic from the LAN voice interface and limits bandwidth.
- Index 5: Blocks all other traffic.

4 Secure Management Access

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

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 with username **Admin** and password **Admin**. This user has full read-write access privileges to the device. It's recommended to change this default password to a hard-to-hack string. You can change the username and password in the Local Users table (**Setup** menu > **Administration** tab > **WEB & CLI** folder > **Local Users**):

Figure 4-1: Changing Default Password of Security Administrator User

The screenshot shows the 'Local Users' configuration page. It has two main tabs: 'GENERAL' and 'SECURITY'. Under 'GENERAL', fields include Index (0), Username (Admin), Password (a masked field), User Level (Security Administrator), SSH Public Key, and Status (Valid). Under 'SECURITY', fields include Password Age (0), Web Session Limit (5), CLI Session Limit (-1), Web Session Timeout (180), and Block Duration (60).

- Enforce password complexity, by configuring the [EnforcePasswordComplexity] parameter to 1. If you enable password complexity, you can also configure the minimum length (number of characters) of the password, using the [MinWebPasswordLen] parameter.
- The device is shipped with a default Monitor access-level user account with username **User** and password **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:

Figure 4-2: 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 (e.g., once a month).

User Authentication by Third-Party Server

For securing access to the device, it's recommended to implement a third-party authentication server.

LDAP-based User Authentication and Authorization

You can 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 > **AAA Servers** folder.

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

RADIUS-based User Authentication

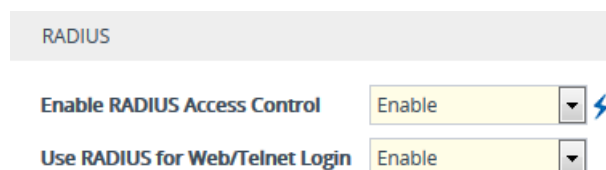
You can implement a third-party, RADIUS server in your network for authenticating Web / Telnet management users and thereby, preventing unauthorized access. RADIUS allows you to define different passwords for different interface users, with centralized management of the password database. When RADIUS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

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

➤ To enable RADIUS-based user authentication:

1. Open the Authentication Server page (**Setup** menu > **Administration** tab > **WEB & CLI** folder > **Authentication Server**), and then configuring the following parameters:
 - 'Enable RADIUS Access Control': **Enable**
 - 'Use RADIUS for Web/Telnet Login': **Enable**

Figure 4-3: Enabling RADIUS for Web User Authentication



The screenshot shows a configuration page titled 'RADIUS'. It contains two settings, each with a label, a dropdown menu, and a lightning bolt icon indicating a required setting. The first setting is 'Enable RADIUS Access Control' with a dropdown menu showing 'Enable'. The second setting is 'Use RADIUS for Web/Telnet Login' with a dropdown menu showing 'Enable'.

RADIUS	
Enable RADIUS Access Control	Enable
Use RADIUS for Web/Telnet Login	Enable

2. Open the RADIUS Servers table (**Setup** menu > **IP Network** tab > **AAA Servers** folder > **RADIUS Servers**), and then configure the RADIUS authentication server for authenticating the device with the RADIUS server:

Figure 4-4: Configuring RADIUS Servers for Management User Authentication

INDEX	IP ADDRESS	AUTHENTICATION PORT	ACCOUNTING PORT	SHARED SECRET	INTERFACE NAME
0	10.6.6.7	1645	1646	*	O+M+C

OAuth 2.0 Authentication using Azure AD

You can implement Microsoft's Azure Active Directory (Azure AD) to authenticate (credentials) and authorize (privilege level) users attempting to log in to the device's management interfaces (Web interface, CLI, and REST API). Authentication is done using the OAuth 2.0 protocol.

OAuth authentication is configured in the OAuth Servers table and Login OAuth Servers table. However, for full configuration details, refer to the User's Manual.

Implement Two-Way Authentication with X.509 Certificates

It's 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, preventing unauthorized access to the Web management tool.



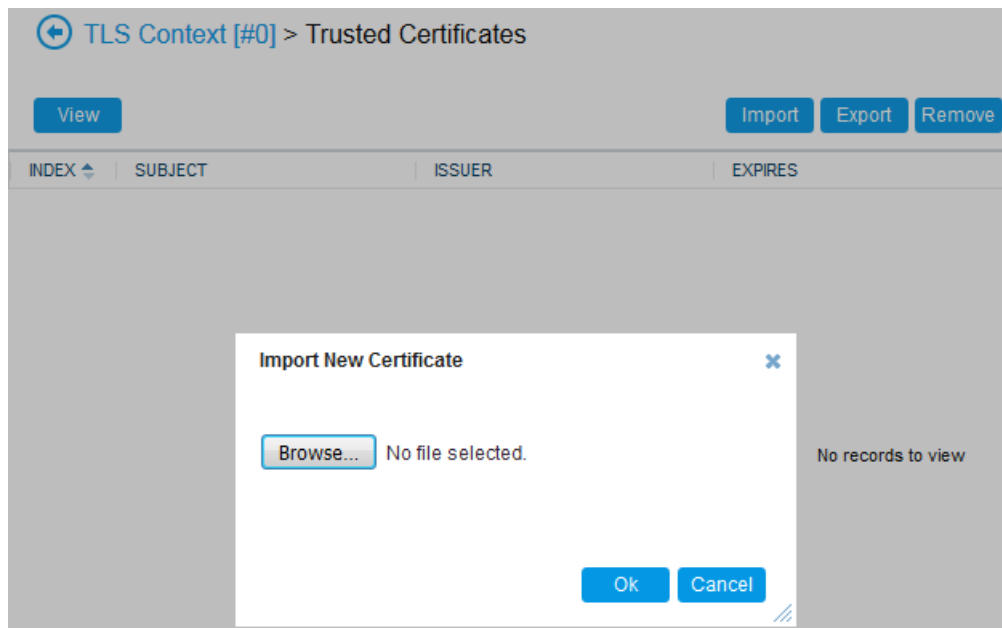
- Implementation of two-way authentication requires a third-party security equipment vendor, CA server, and security administrator personnel. These should create certificates and deploy them to all the computers in the organization.
- The device is supplied with a working TLS configuration consisting 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.

- 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 4-5: Importing CA Certificate to CA Store



- 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.
- Make sure that client certificates for HTTPS connections are required. Open the Web Interfaces table (**Setup** menu > **Administration** tab > **WEB & CLI** folder > **Web Interfaces**), and then from the 'Require Client Certificate' drop-down list of the OAMP Web interface, select **Yes**:

Web Interfaces

GENERAL	
Index	0
Interface Name	#0 [O+M+C] View
HTTP Port	80
HTTPS Port	443
TLS Context Name	#0 [default] View
Require Client Certificate	Yes
HTTPS Only	Use global definition

Secure HTTP Access using HTTPS

It's recommended to allow access to the Web interface through HTTPS only. In addition, it's recommended to block port 80. This is done on, by configuring the 'Secured Web Connection (HTTPS)' parameter to HTTPS Only (reset device for setting to take effect):

➤ **To allow Web access only through HTTPS:**

1. Open the Web Settings page (**Setup** menu > **Administration** tab > **WEB & CLI** folder > **Web Settings**).
2. From the 'Secured Web Connection (HTTPS)' drop-down list, select **HTTPS Only**:

Figure 4-6: Securing Access to Web Interface using HTTPS



Secure Telnet Sessions

It's recommended to disable access through Telnet. However, if you do require Telnet and your management software provides a secure Telnet application, then use a secured Telnet connection (i.e., TLS). TLS protects Telnet traffic from network sniffing.

➤ **To secure Telnet:**

1. Open the CLI Settings page (**Setup** menu > **Administration** tab > **WEB & CLI** folder > **CLI Settings**).
2. From the 'Enable Telnet Server' drop-down list, select **Enable Secured**:

Figure 4-7: Securing Telnet with TLS



Secure CLI Sessions by SSH

It's 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.

➤ **To enable SSH:**

1. Open the SSH Settings page (**Setup** menu > **Administration** tab > **WEB & CLI** folder > **SSH Settings**).
2. Configure the following parameters:
 - 'Enable SSH Server': **Enable**.

- 'Kex Algorithms String': Define the Key Exchange Method (e.g., Diffie-Hellman-Group-Exchange-SHA256).
- 'Ciphers String': Define the cipher string (e.g., AES128-CTR).
- 'MACs String': Define the HMAC (e.g., HMAC-SHA2-256).

Figure 4-8: Securing CLI

SECURE SHELL (SSH)

Enable SSH Server Enable

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.

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.



- 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 [Block Unused Network Ports](#) on page 7).

➤ To configure access list:

1. Open the Access List page (**Setup** menu > **Administration** tab > **WEB & CLI** folder > **Access List**).
2. Add allowed IP addresses:

Figure 4-9: Authorized IP Addresses for Accessing Web, Telnet and SSH Interfaces
Access List

Add an authorized IP address

Add New Entry

DELETE ROW		AUTHORIZED IP ADDRESS
1	<input type="checkbox"/>	10.13.2.3

Protect Against DNS Rebinding Attacks

The device can provide protection against DNS rebinding attacks. DNS rebinding allows attackers to access and attack your device and internal network, by remapping hostname-to-IP

address lookups. This may occur when management users access the device using the device's host name (if configured) instead of its IP address.

➤ **To protect against DNS rebinding attacks:**

1. Open the Web Settings page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Web Settings**).
2. From the 'DNS Rebinding Protection' drop-down list, select **Enable**:

DNS Rebinding Protection

Enable

HTTP Host Header Validation

You can enable the device to validate the Host header in incoming HTTP requests that are used for accessing the Web interface. When enabled, the device checks that the value of the Host header matches the IP address (or hostname, if configured) of the device's management interface. If there is no match, the device rejects the request with an HTTP 403 Forbidden response.

This feature ensures that only direct access to the Web interface is allowed, blocking all access attempts through a proxy or tunnel. This may help protect the device against malicious attacks using Host header manipulation (injection).

➤ **To enable HTTP Host header protection:**

- Enable the ini file parameter [HostHeaderProtection], or CLI command `configure system > web > host-headerprotection`.

Secure SNMP Interface Access

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

Prefer SNMPv3 over SNMPv2

It's 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 (e.g., MD5, SHA-1 or SHA-2) and encryption (e.g., DES, 3DES, AES-128, AES-192, or AES-256) of packets over the network. It's also recommended that you periodically change the SNMPv3 authentication and privacy keys.

➤ **To configure SNMPv3 users:**

1. Open the SNMPv3 Users table (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP V3 Users**).
2. Click **New**, and then configure an SNMPv3 user:

Figure 4-10: Configuring SNMPv3 Users

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

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's also recommended that you periodically change these SNMP community string values.

➤ To secure SNMPv2:

1. Open the SNMP Community Settings page (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP Community Settings**), and then configure the SNMPv2 community strings:

Figure 4-11: Configuring SNMPv2 Community Strings

READ-ONLY COMMUNITY STRINGS		READ-WRITE COMMUNITY STRINGS	
Read-Only 1	<input type="text" value="....."/>	Read-Write 1	<input type="text" value="....."/>
Read-Only 2	<input type="text"/>	Read-Write 2	<input type="text"/>
Read-Only 3	<input type="text"/>	Read-Write 3	<input type="text"/>
Read-Only 4	<input type="text"/>	Read-Write 4	<input type="text"/>
Read-Only 5	<input type="text"/>	Read-Write 5	<input type="text"/>

2. Open the SNMP Trusted Managers table (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP Trusted Managers**), and then configure the SNMPv2 management stations:

Figure 4-12: Configuring SNMPv2 Trusted Managers

DELETE	TRUSTED MANAGERS IP ADDRESS	
<input type="checkbox"/>	SNMP Trusted Manager 1	<input type="text" value="10.3.2.1"/>
<input type="checkbox"/>	SNMP Trusted Manager 2	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>	SNMP Trusted Manager 3	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>	SNMP Trusted Manager 4	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>	SNMP Trusted Manager 5	<input type="text" value="0.0.0.0"/>

Secure LDAP Communication

If you are using LDAP-based login management (username-password) and/or LDAP-based SIP routing in your deployment, it's 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.

➤ **To secure LDAP-based applications:**

1. Open the LDAP Servers table (**Setup** menu > **IP Network** tab > **AAA Servers** folder > **LDAP Servers**).
2. For the relevant LDAP server, configure the following:
 - From the 'Use TLS' drop-down list, select **Yes**.
 - From the 'TLS Context' drop-down list, select the TLS Context from the TLS Contexts table.

Figure 4-13: Configuring Secure LDAP Server Communication

The screenshot shows the 'LDAP Servers' configuration page. The 'GENERAL' tab is active, displaying fields for Index (0), LDAP Network Interface (eth0), Use TLS (Yes), TLS Context (TLSContexts_1), Verify Certificate (Yes), and Verify Certificate Subject Name (No). The 'CONNECTION' tab is also visible, showing LDAP Server IP (10.3.9.93), LDAP Server Port (389), LDAP Server Max Respond Time (3000), LDAP Server Domain Name, and Server's Connection Status. A 'QUERY' section at the bottom shows LDAP Password (masked), LDAP Bind DN (s@test.local), Management Attribute (memberOf), and No Op Timeout (0).

Customizing Access Levels per Web Page

You can overwrite the default access privileges (read-only or read-write) per user level (Monitor, Administrator, or Security Administrator) per Web interface page.

➤ **To customize access levels per Web page:**

1. Open the Customize Access Level table (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Customize Access Level**).
2. Configure customization rules. For example, the configuration below allows only users with Security Administrator level to configure the Logging Filters page, while allowing users with Monitor level to view only.

Figure 4-14: Customizing Access Level to Web Page

The screenshot shows the 'Customize Access Level' configuration page. The 'GENERAL' tab is active, displaying fields for Index (0), Page Name (Logging Filters), Read-Write Access Level (Security Administrator), and Read-Only Access Level (Monitor).

5 Secure SIP using TLS (SIPS)

It's crucial that you implement the TLS-over-TCP protocol to 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.

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.

Use TLS Version 1.2 or 1.3

It's recommended to use the highest TLS version 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's also recommended not to configure the device to use any TLS version (**Any TLS1.x**). However, if some network entities use SSL 3.0 handshakes and some use a higher TLS version (e.g., TLS 1.1), then you need to configure the device to use any version.

➤ To configure the TLS version:

1. Open the TLS Contexts table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. For the relevant TLS Context, from the 'TLS Version' drop-down list, select the required TLS version. The example below assumes that the highest TLS versions supported by the network entities are 1.1 and 1.2.

Figure 5-1: Configuring TLS Version

The screenshot shows the 'TLS Contexts [default]' configuration window. It has two tabs: 'GENERAL' and 'OCSF'. In the 'GENERAL' tab, the 'Index' is 0, 'Name' is 'default', 'TLS Version' is set to 'TLSv1.1 and TLSv1.2', and 'DTLS Version' is set to 'DTLSv1.0 and DTLSv1.2'. In the 'OCSF' tab, 'OCSP Server' is set to 'Disable', 'OCSP Interface' is set to '--', 'Primary OCSP Server' is '0.0.0.0', and 'Secondary OCSP Server' is '0.0.0.0'.

Block Multiple Client-Initiated TLS Renegotiations

The device can block client-initiated TLS renegotiations (handshakes). This is useful for preventing DoS attacks on the device caused by multiple TLS renegotiations per second of the encrypted key initiated by the attacker.

➤ To block multiple client-initiated TLS renegotiations:

1. Open the TLS Contexts table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. For the relevant TLS Context, from the 'TLS Renegotiation' drop-down list, select **Disable**:

Figure 5-2: Blocking TLS Renegotiations

The image shows a close-up of the 'TLS Renegotiation' dropdown menu. The 'Disable' option is selected and highlighted in yellow.

Use TLS for SIP Interfaces and Block TCP/UDP Ports

Each port can be vulnerable to attacks. Therefore, it's 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.

➤ To configure TLS for SIP Interfaces:

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. For the relevant SIP Interface, configure the following:
 - In the 'UDP Port' field, enter 0.
 - In the 'TCP Port' field, enter 0.
 - In the 'TLS Port' field, enter a port number (non-zero).

Figure 5-3: Configuring TLS for SIP Interface

SIP Interfaces [SIPInterface_0]

SRD: #0 [DefaultSRD]

GENERAL	MEDIA
Index: 0	Media Realm: -- View
Name: SIPInterface 0	Direct Media: Disable
Topology Location: Down	
Network Interface: #0 [O+M+C] View	
Application Type: GW	
UDP Port: 0	
TCP Port: 0	
TLS Port: 5061	
	SECURITY
	TLS Context Name: #0 [default] View
	TLS Mutual Authentication: --
	Message Policy: -- View
	User Security Mode: Not Configured

Use TLS for Routing Rules

It's recommended that your routing rules use TLS as the transport type.

➤ To enable TLS for routing rules:

1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. For the relevant IP-to-IP Routing rule, from the 'Destination Transport Type' drop-down list, select **TLS**:

Figure 5-4: Configuring TLS for IP-to-IP Routing Rule

IP-to-IP Routing

Routing Policy: #0 [Default_SBCRoutingPolicy]

GENERAL	ACTION
Index: 1	Destination Type: Dest Address
Name:	Destination IP Group: -- View
Alternative Route Options: Route Row	Destination SIP Interface: -- View
	Destination Address: Internal
	Destination Port: 0
	Destination Transport Type: TLS
MATCH	
Source IP Group: Any View	

Implement X.509 Certificates for SIPS (TLS) Sessions

It's 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's 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.

Use an NTP Server

It's 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's 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.

➤ To implement NTP server:

1. Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date** home icon).
2. From the 'Enable NTP' drop-down list, select **Enable**:

Figure 5-5: Configuring NTP Server

NTP SERVER	
Enable NTP	<input type="button" value="Enable"/>
NTP Interface	<input type="button" value="O+M+C"/>
Primary NTP Server Address (IP or FQDN)	<input type="button" value="15.3.6.70"/>
Secondary NTP Server Address (IP or FQDN)	<input type="text"/>
NTP Update Interval	Hours: <input type="text" value="24"/> Minutes: <input type="text" value="0"/>
NTP Authentication Key Identifier	<input type="text" value="0"/>
NTP Authentication Secret Key	<input type="password" value="....."/>

OAuth 2.0-based Authentication for SIP Requests using Azure AD

You can implement Microsoft Azure Active Directory (Azure AD) to authenticate SIP User Agents (UA) of incoming SIP messages (including WebRTC), based on the OAuth 2.0 protocol.

Azure AD is Microsoft's cloud-based identity and access management service, designed for Internet-based applications. As Azure AD doesn't support OAuth Token Introspection, the device validates the received token using its embedded NGINX server, which simulates an OAuth 2.0 Introspection endpoint.

For configuring OAuth 2.0-based authentication of SIP messages, refer to the User's Manual.

6 Implement LDAP-based Conditional Call Routing

It's 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.

➤ **To configure LDAP-based conditional routing:**

1. For configuring LDAP, use the LDAP Settings page, LDAP Server Groups table, and LDAP Servers table (**Setup** menu > **IP Network** tab > **AAA Servers** folder).
2. 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

The screenshot shows the 'Call Setup Rules' configuration window. It is divided into two main sections: 'GENERAL' and 'ACTION'.

GENERAL Section:

- Index: 0
- Name: (empty field)
- Rules Set ID: 0
- Request Type: LDAP (dropdown menu)
- Request Target: (empty field)
- Request Key: 'telephoneNumber=*Param.Call.Src.User' (with an 'Editor' link)
- Attributes To Get: 'telephoneNumber' (with an 'Editor' link)
- Row Role: Use Current Condition (dropdown menu)
- Condition: 'LDAP Found lexists' (with an 'Editor' link)

ACTION Section:

- Action Subject: (empty field) (with an 'Editor' link)
- Action Type: Exit (dropdown menu)
- Action Value: 'False' (with an 'Editor' link)



Make sure that you implement secure LDAP communication, as discussed in Section [Secure LDAP Communication](#) on page 17.

7 Define SIP Message Blocklist/Allowlist

It's recommended to configure SIP message policy rules for blocking (blocklist) unwanted incoming SIP messages or allowing (allowlist) 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 blocklist or allowlist.

➤ To configure SIP message blocklists and allowlists:

1. Open the Message Policies table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Policies**).
2. Click **New** to configure a rule.

The following displays an example of a configured rule 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: Configuring 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

8 Monitor and Log Events

It's 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.

Implement Dynamic Blocklisting of Malicious Activity (IDS)

It's important to use the device's 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's crucial to be aware of any attacks to ensure that the legitimate call service is always maintained. If any user-defined attacks are identified, the device can do the following:

- Block (blocklist) remote hosts (IP addresses / ports) considered as malicious. The device automatically blocks the malicious source for a user-defined period after which it's removed from the blocklist.
- Send SNMP traps to notify of the malicious activity and/or whether an attacker has been added to or removed from the blocklist.

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).

➤ To configure IDS:

1. Open the IDS General Settings page (**Setup** menu > **Signaling & Media** tab > **Intrusion Detection** folder > **IDS General Settings**), and then from the 'Intrusion Detection System (IDS)' drop-down list, select **Enable**:

Intrusion Detection System (IDS) ● Enable ▼

2. Open the IDS Policies table (**Setup** menu > **Signaling & Media** tab > **Intrusion Detection** folder > **IDS Policies**), and then configure an IDS policy "ITSP DoS", as shown selected below:

Figure 8-1: Configuring 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

3. Open the IDS Rule table by clicking the **IDS Rule** link located below the IDS Policies table, and then configure IDS rules for the "ITSP DoS" IDS policy:

Figure 8-2: Configuring Rules in IDS Rule Table

INDEX	REASON	THRESHOLD SCOPE	THRESHOLD WINDOW	MINOR-ALARM THRESHOLD	MAJOR-ALARM THRESHOLD	CRITICAL-ALARM 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

- Open the IDS Matches table (**Setup** menu > **Signaling & Media** tab > **Intrusion Detection** folder > **IDS Matches**), and then assign the IDS Policy to a specific SIP interface and subnet:

Figure 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

Enable Syslog

The device supports generation and reporting of syslog messages and SNMP traps to external logging servers. It's 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's recommended that you make sure that your syslog server saves all logged events for future analysis and reference.

➤ To enable syslog:

- Open the Logging Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Logging Settings**).
- From the 'Enable Syslog' drop-down list, select **Enable**, and then configure the relevant parameters:

Figure 8-4: Enabling Syslog

Syslog Settings

SYSLOG		ACTIVITY TYPES TO REPORT	
Enable Syslog	• Enable	Parameters Value Change	<input checked="" type="checkbox"/>
Syslog server IP	10.8.7.5	Auxiliary Files Loading	<input checked="" type="checkbox"/>
Syslog Server Port	514	Device Reset	<input checked="" type="checkbox"/>
Syslog CPU Protection	Enabled	Flash Memory Burning	<input checked="" type="checkbox"/>
Syslog Optimization	Disabled	Device Software Update	<input checked="" type="checkbox"/>
Debug Level	• Detailed	Non-Authorized Access	<input checked="" type="checkbox"/>
		Sensitive Parameters Value Change	<input checked="" type="checkbox"/>
		Login and Logout	<input checked="" type="checkbox"/>
		CLI Activity	<input checked="" type="checkbox"/>
		Action Executed	<input checked="" type="checkbox"/>

- Open the Syslog Servers table (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Syslog Servers**), and then configure a syslog server(s):

Figure 8-5: Configuring Syslog Servers

Syslog Servers - x

GENERAL

Index	<input type="text" value="0"/>
Address	<input type="text" value="0.0.0.0"/>
Port	<input type="text" value="514"/>
Transport Protocol	<input type="text" value="UDP"/>
Interface	<input type="text" value="--"/> View
Information Type	<input type="text" value="All"/>
Severity Level	<input type="text" value="Notice"/>
Mode	<input type="text" value="Enable"/>

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)

➤ To log management-related events:

1. Open the Logging Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Logging Settings**).
2. Select the type of events that you want logged:

Figure 8-6: Enabling Logging of Management Events to a Syslog Server

ACTIVITY TYPES TO REPORT	
Select All	<input checked="" type="checkbox"/>
Parameters Value Change	<input checked="" type="checkbox"/>
Auxiliary Files Loading	<input checked="" type="checkbox"/>
Device Restart	<input checked="" type="checkbox"/>
Flash Memory Burning	<input checked="" type="checkbox"/>
Device Software Upgrade	<input checked="" type="checkbox"/>
Non-Authorized Access	<input checked="" type="checkbox"/>
Sensitive Parameters Value Change	<input checked="" type="checkbox"/>
Login and Logout	<input checked="" type="checkbox"/>
CLI Activity	<input checked="" type="checkbox"/>
Action Executed	<input checked="" type="checkbox"/>
Incremental INI	<input checked="" type="checkbox"/>
Incremental INI Activity Logs Max Number	<input type="text" value="1000"/>

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.

➤ To enable CDR generation:

1. Open the Advanced Parameters page (**Troubleshoot** menu > **Troubleshoot** tab > **Call Detail Record** folder > **Call Detail Record Settings**).
2. Configure the relevant parameters:

Figure 8-7: Enabling CDR Generation

SYSLOG CDR REPORTS	
CDR Syslog Server IP Address	<input type="text" value="10.15.8.1"/>
CDR Report Level	<input type="text" value="Start & End & Connect Call"/> ▼
Media CDR Report Level	<input type="text" value="End Media"/> ▼
CDR Syslog Sequence Number	<input type="text" value="Enable"/> ▼



For CDRs, you must enable syslog functionality.

9 GDPR for Protecting Personal Information

To help you comply with the European Union's (EU) General Data Protection Regulation (GDPR) to protect and respect personal data processed by the device, the device offers various means to mask (hide) personally identifiable information (PII).

Masking PII

- **AudioCodes PII Log Scrubber Tool:** This tool is based on a Python script that masks PII from syslog files created by the device. You can run this tool on any computer or server that has Python 3 installed. To download the tool from AudioCodes website, click [here](#).
- **Masking PII in CDRs and SDRs:** You can mask PII in CDRs and SDRs that are displayed in the Web interface and CLI, and mask PII in CDRs that are sent to syslog, REST, RADIUS, Local Storage, or OVOC (depending on configuration). In addition, you can mask digits in syslog and DR.
 - a. Open the SIP Definitions General Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **SIP Definitions General Settings**).
 - b. Use the following parameters:
 - ◆ 'Mask PII in CDRs': Defines where the masking is done – CDRs/SDRs displayed in the Web interface and CLI only, or also in those that are sent to local storage and remote servers (e.g., syslog).
 - ◆ 'Mask PII in QoE CDRs for OVOC': Enables masking in CDRs (QoE) sent to OVOC.
 - ◆ 'Mask URI Host Part in CDRs': Masks the host part of URIs (including IP addresses) in CDRs.
 - ◆ 'Number of Unmasked Characters in PII' and 'Location in PII of Unmasked Characters': Defines the number of characters to not mask, starting from the end or beginning of the PII element (e.g., phone number).
 - ◆ 'Mask Digits': Masks digits (typically, in-band DTMF) sent as events and detected by the device, including SIP messages (INFO and NOTIFY) in syslog and Debug Recording (message body) generated by the device.

Figure 9-1: Configuring PII Masking

PERSONALLY IDENTIFIABLE INFORMATION (PII) MASKING	
Mask PII in CDRs	• Mask PII in Web or CLI
Mask PII in QoE CDRs for OVOC	• Enable
Mask URI Host Part in CDRs	Disable
Number of Unmasked Characters in PII	• 6
Location in PII of Unmasked Characters	Last Characters
Mask Digits	Disable

Deleting Locally Stored CDRs and SDRs

If you have enabled local storage of CDRs or SDRs on the device, you can delete them from storage at any time through CLI:

■ CDRs:

```
# clear storage-history cdr-storage-history
```

■ SDRs:

```
# clear storage-history sdr-storage-history
```

Deleting Persistent Logs

The device automatically stores logged system event messages in its memory, where they persist even if the device undergoes a reset or powers off. To make sure that the device does not store these logged files indefinitely, allowing personal information to always be available, it's recommended that you configure an "age" period for the file rotation process (i.e., creation of new file and deletion of oldest file).

If you configure an "age" period, the device creates a new file when either the configured file size is reached ('Persistent Log Size' parameter) or the "age" is reached ('Persistent Log Period' parameter) -- whichever occurs first. Therefore, even if the configured file size for file rotation is not reached (even empty), when the period expires the device creates a new file, deleting the oldest persistent log file from storage.

➤ To configure persistent log period:

1. Open the Logging Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Logging Settings**).
2. In the 'Persistent Log Size' field, enter the log size for file rotation.
3. In the 'Persistent Log Period' field, enter the age period for file rotation.

Figure 9-2: Configuring Persistent File Rotation with File Age

Persistent Log Size [KB]

Persistent Log Period [min]



Persistent logging is applicable only to Mediant 90xx and Mediant Software SBCs.

Encrypting the SIP Header Value

For enhanced security, you can configure the device to encrypt the value of a specific SIP header. Encryption is done using the AES-256 key algorithm. This feature is typically used between two AudioCodes devices, where one encrypts the SIP header value before sending the SIP message, while the other decrypts the value when it receives the SIP message.



This feature is intended for SIP headers that are **not** used by the device for classification or routing. For example, you may want to encrypt the value of a proprietary SIP header called "P- Access- Network- Info" that may contain sensitive information.

➤ To configure SIP header value encryption:

1. Open the SIP Definitions General Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **SIP Definitions General Settings**), and then in the 'AES-256 Encryption Key' parameter, configure the encryption key.



- The key must be 32 characters.
- Configure both devices with the same key.

2. Open the Message Manipulations table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**), and then configure a Message Manipulation rule to specify the SIP header to encrypt. Use the **Funct.Encrypt** and **Funct.Decrypt** keywords in the 'Action Value' field to encrypt and decrypt the header, respectively. For more information, refer to the device's *User's Manual*.
3. Open the IP Groups table, and then assign the Manipulation Set ID (configured in the previous step) to the relevant IP Group.

10 SBC-Specific Security Guidelines

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



This section is applicable only to the Session Border Controller (SBC) application.

General Guidelines

It's 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).

Secure Media (RTP) Traffic using SRTP

It's 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.

➤ To secure RTP traffic:

- **Globally (all calls):** Media Security page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Security**) - from the 'Media Security' drop-down list, select **Enable**:

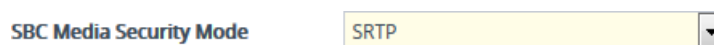
Figure 10-1: Enabling SRTP Globally



- **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 10-2: Enabling SRTP per Specific Calls



Implement SIP Authentication and Encryption

It's 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.

Authenticating Users as an Authentication Server

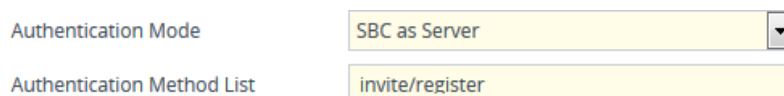
Instead of relying on external, third-party authentication servers, the device can be configured to act as an Authentication server, performing authentication and validation challenges with SIP UAs. The SIP method (INVITE or REGISTER) on which it challenges can be defined. If the message is received 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.

The cryptographic hash algorithm used when the device sends the authentication challenge in the SIP 401 or 407 response can be configured, using the [SIPServerDigestAlgorithm] parameter.

➤ To authenticate users:

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Identities** folder > **IP Groups**).
2. For the IP Group (**User-type**) of the UAs, configure the following:
 - From the 'Authentication Mode' drop-down list, select **SBC as Server**.
 - In the 'Authentication Method List' field, enter the SIP message(s) to authenticate (e.g., "INVITE\REGISTER").

Figure 10-3: Configuring SBC as Authentication Server for User-type IP Group



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

- a. Open the Proxy & Registration page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder>, and then from the 'User-Information Usage' drop-down list, select **Enable** to enable the SBC User Info feature:

Figure 10-4: Enabling User Information Feature

Enable User-Information Usage • ⚡



The 'User-Information Usage' field is available only if your device's License Key includes a license for far-end users ("FEU").

- b. Open the SBC User Information table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC User Information**), and then add users with authentication usernames and passwords:

Figure 10-5: Configured User in SBC User Information Table

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

OAuth 2.0 Token-based SIP Authentication

The device can authenticate any incoming SIP requests (e.g., REGISTER and INVITE) from client applications, based on access tokens with an OAuth 2.0 Authorization Server (internal or external).

When the device receives a SIP request (with an OAuth access token) from a client application (e.g., WebRTC client), the device introspects the token with the OAuth Authorization server (HTTP server). Upon successful introspection, the device allows the client access to the device's resources (e.g., registration and calls) and continues to handle and process the SIP request as usual.

➤ To configure OAuth-based SIP authentication:

1. Open the Remote Web Services table (**Setup** menu > **IP Network** tab > **Web Services** folder > **Remote Web Services**), add then configure a Remote Web Service to represent the OAuth Authentication server.
2. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Identities** folder > **IP Groups**), and then configure the following parameters:
 - 'Authentication Mode': **SBC as Server**
 - 'Authentication Method List': "register/setup-invite"
 - 'SBC Server Authentication Type': **Authenticate with OAuth Server**
 - 'OAuth HTTP Service': Assign the Remote Web Service that you configured in Step 1

Figure 10-6: Configuring OAuth-based SIP Authentication

Authentication Mode	SBC as Server	▼
Authentication Method List	register/setup-invite	
SBC Server Authentication Type	Authenticate with OAuth Server	▼
OAuth HTTP Service	#0 [SIP auth]	▼ View

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 authenticate users by RADIUS server:

1. Open the RADIUS Servers table (**Setup** menu > **IP Network** tab > **AAA Servers** folder > **RADIUS Servers**), and then configure the RADIUS sever (IP address, port and shared secret password):

Figure 10-7: Configuring RADIUS Server for User Authentication

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 an RFC 5090 compliant RADIUS server.

Authenticating SIP Servers as an Authentication Server

It's recommended to enable the device (acting as an authentication server) to authenticate remote SIP servers (e.g., SIP 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 username and password that is shared with the remote server. From such a challenge, the device can check if the server's identity is genuine. The type of SIP message (e.g., INVITE) to authenticate can also be specified.

➤ To configure SIP server authentication:

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Identities** folder > **IP Groups**).
2. For the IP Group of the SIP server, configure the following:
 - From the 'Authentication Mode' drop-down list, select **SBC as Server**.
 - In the 'Authentication Method List' field, enter the SIP message(s) to authenticate.
 - In the 'Username' field, enter the authentication username.
 - In the 'Password' field, enter the authentication password.

Figure 10-8: Configured SIP Server Authentication

Authentication Mode	SBC as Server
Authentication Method List	INVITE
Username	ipbx fool
Password	••••

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's the SIP proxy that handles and enforces SIP client authentication. Therefore, it's imperative that your SIP proxy server be configured to enforce SIP client authentication.

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's 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.).

Secure Routing Rules

This section provides recommended security guidelines regarding routing rules.

Classify by Classification Rules versus Proxy Set

An important security functionality of the device is to make sure that incoming SIP dialog- initiating requests (e.g., INVITE messages) from malicious attackers are not mistakenly identified as belonging to a configured Server-type IP Group entity.

The device provides two optional mechanisms that can be employed to identify incoming dialogs as coming from a specific Server-type IP Group:

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

Recommended usage:

If the IP address of the IP Group entity is known, it's recommended to employ 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 strictness of the classification process.

When Classification rules are used and classify by Proxy Set is disabled (see below), it's recommended to enable the 'Validate Source IP' parameter in the IP Groups table. This

setting verifies that the incoming dialog was sent from one of the IP addresses (including DNS-resolved IP addresses) of the Proxy Set associated with the classified IP Group (see [Validate Source IP Address of Incoming SIP Dialog Requests](#) on page 41). IP address validation is also typically needed when multiple IP Groups are assigned to the same Proxy Set and therefore, Classification rules are necessary to produce the desired mapping (classification) of the incoming SIP dialogs to the different IP Groups.

Figure 10-9: Enabling Source IP Validation in IP Groups Table

Classify By Proxy Set	Disable
Validate Source IP	Enable



The device uses the Classification table for classification only if the following classification stages fail (listed chronologically):

1. The incoming SIP dialog is not from a SIP UA that is registered with the device (i.e., not in user registration database).
2. The Classify by Proxy Set feature is disabled for the IP Group (i.e., source IP address of incoming dialog is matched with a Proxy Set associated with the IP Group but Classify by Proxy Set is disabled for the IP Group).

- **Classification by Proxy Set:** Identifies incoming dialogs based on source IP address (Layer 3) only. The Proxy Set defines the address of the IP Group. For this method, the device searches for a Proxy Set that has the same source IP address as the incoming dialog, and then classifies it to the IP Group that is assigned to this Proxy Set. Classification by Proxy Set is enabled in the IP Groups table, using the 'Classify By Proxy Set' parameter:

Figure 10-10: Enabling Classification by Proxy Set in the IP Groups Table

Classify By Proxy Set	Enable
-----------------------	--------

Recommended usage:

If the IP address is unknown, in other words, the Proxy Set associated with the IP Group is configured with an FQDN, it's 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.

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.



If the IP address is unknown (i.e., the Proxy Set associated with the IP Group is configured with an FQDN), it's recommended to employ SIP dialog classification based on Proxy Set (see [Classify by Classification Rules versus Proxy Set](#) on page 38).

- It's recommended to enable the 'Validate Source IP' parameter in the IP Groups table. This setting verifies that the incoming dialog was sent from one of the IP addresses (including DNS-resolved IP addresses) of the Proxy Set associated with the classified IP Group (see [Validate Source IP Address of Incoming SIP Dialog Requests](#) on the next page). IP address validation is also typically needed when multiple IP Groups are assigned to the same Proxy Set and therefore, Classification rules are necessary to produce the desired mapping (classification) of the incoming SIP dialogs to the different IP Groups.
- For Server-type IP Groups whose IP addresses are known, it's recommended to also configure VoIP firewall rules (see [Block Unused Network Ports](#) on page 7).
- 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.
- Make sure that you configure the device to block unclassified calls, as described in Section [Validate Source IP Address of Incoming SIP Dialog Requests](#) on the next page.
- 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:

- a. Configure a Message Condition rule in the Message Conditions table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Conditions**). The

following figure shows a Message Condition rule example for P-Asserted-Identity headers that contain "abc":

Figure 10-11: 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'

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

Figure 10-12: Assigned Message Condition Rule in Classification Table

Message Condition #0 [P-Asserted-Identity he

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

Figure 10-13: 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	DefaultSRC	Any	[2-4]	domain.com	[1-7]	*	Allow	ITSP
1	Deny	DefaultSRC	Any	*	*	*	*	Deny	--

- 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).

Validate Source IP Address of Incoming SIP Dialog Requests

When classification is according to Classification rules and you need to classify SIP dialogs originating from the same Proxy Set into multiple IP Groups, and where Classification rules are necessary to produce the desired mapping (classification) to the different IP Groups, it's recommended that you configure the device to validate the source IP address of incoming SIP dialog-initiating requests (e.g., INVITE).

The device checks that it matches an IP address (or DNS-resolved IP address) of the Proxy Set that is associated with the IP Group to which it's classified.

➤ **To validate source IP addresses:**

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. From the 'Validate Source IP' drop-down list, select **Enable**:

Figure 10-14: Configuring Source IP Address Validation

Validate Source IP Enable ▼



Validation is done for the IP address only (not port, transport, or SIP Interface).

Block Unclassified Calls

It's recommended that you block incoming calls that can't 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.

➤ **To block unclassified calls:**

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).
2. From the 'Unclassified Calls' drop-down list, select **Reject**:

Figure 10-15: Blocking Unclassified Incoming Calls

Unclassified Calls Reject ▼

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's recommended to configure the device so that it accepts only calls with a specific User-Agent header value.

➤ **To configure security based on SIP User-Agent header:**

1. Open the Message Conditions table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Conditions**), and then add a rule that specifies a value for the User-Agent header.

The following figure shows a rule where the SIP User-Agent header value is "abc.com":

Figure 10-16: Message Condition Rule for SIP User-Agent Header

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

2. Open the Classification table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Classification**), and then assign the Message Condition rule to the relevant Classification rule.

Define Strict Routing Rules

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

- Make sure that your routing rules are accurate and correctly defined. Inaccurate or weak routing rules can easily result in Service Theft.
- Make sure 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.

Define Call Admission Control Rules

It's recommended to configure 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's crucial that your CAC rules include call limitations per user. This ensures that a user doesn't make unlimited, simultaneous calls.
- Define rules as specific as possible. For example, instead of defining one rule for all SIP request types, create rules per request type.



If call routing to a specific IP Group is blocked due to a CAC rule, the device searches for an alternative route (if configured) in the SBC IP- to- IP Routing table. If this alternative route doesn't exceed the CAC rule limitation, the device uses it to route the call.

➤ To configure CAC rules:

1. Open the Call Admission Control Profile table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Call Admission Control Profile**).
2. Click **New** to add a new CAC rule.

The following displays an example of a CAC rule that defines a maximum of 100 concurrent SIP INVITE requests. SIP requests received above this threshold are rejected:

Figure 10-17: Configuring CAC Rules in Call Admission Control Profile Table

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

Define Maximum Call Duration

It's recommended to configure the 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.

➤ **To configure maximum SBC call duration:**

1. Open the Gateway Advanced Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).
2. In the 'Max Call Duration' field, enter the maximum call duration:

Figure 10-18: Configuring Maximum Call Duration

Max Call Duration [min]

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.

Configure Identical Registration Intervals

Scenarios in which the device doesn't forward user registrations to a server (e.g., a PBX) and the device receives a new SIP 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, make sure that you configure the user and proxy registration times with identical values.

➤ **To configure identical registration intervals for user and proxy:**

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Proxy & Registration**).
2. In the 'User Registration Time' field, configure the duration of the periodic registrations between the user and the device.

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

Figure 10-19: Configuring User Registration Times

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

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

It's 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.

➤ To limit number of SBC registered users:

1. Open either the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Identities** folder > **IP Groups**), SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Identities** folder > **SIP Interfaces**), or SRDs table (**Setup** menu > **Signaling & Media** tab > **Core Identities** folder > **SRDs**).
2. For the relevant IP Group, SIP Interface or SRD, in the 'Max. Number of Registered Users' field, enter the maximum number of registered users:

Figure 10-20: Configuring Maximum Number of Allowed Registered Users

Max. Number of Registered Users	120
---------------------------------	-----

Block Calls from Unregistered Users

Make sure that calls from unregistered users are blocked (rejected) and that calls from only registered users are allowed.

➤ To block calls from unregistered users:

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Identities** folder > **SIP Interfaces**) or SRDs table (**Setup** menu > **Signaling & Media** tab > **Core Identities** folder > **SRDs**).
2. For the relevant SIP Interface or SRD, from the 'User Security Mode' drop-down list, select **Accept Registered Users**:

Figure 10-21: Blocking Unregistered Users

User Security Mode	Accept Registered Users ▼
--------------------	---------------------------

Block Registration from Un-Authenticated New Users

Typically, when a SIP proxy (registrar) server is available, the device forwards SIP REGISTER requests from new users to the proxy and if authenticated by the proxy (i.e., device receives a

success response), the device 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 can't be authenticated. For these scenarios, make sure that the device is configured to reject such unauthenticated request messages from new users.

➤ **To block registration of un-authenticated users:**

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Identities** folder > **SIP Interfaces**) or SRDs table (**Setup** menu > **Signaling & Media** tab > **Core Identities** folder > **SRDs**).
2. For the relevant SIP Interface or SRD, from the 'Enable Un-Authenticated Registrations' drop-down list, select **Disable**:

Figure 10-22: Blocking Local Registration of Un-Authenticated Users

Enable Un-Authenticated Registrations **Disable**



The device accepts registration refreshes from users already in its database.

Authenticate SIP BYE Messages

It's 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 device receives a BYE request from a third-party imposter assuming the identity of a participant in the call and therefore, the call is inappropriately disconnected.

When the device 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.

➤ **To authenticate SIP BYE messages:**

1. Open the Proxy & Registration page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Proxy & Registration**).
2. From the 'BYE Authentication' drop-down list, select **Enable**:

Figure 10-23: Enabling SIP BYE Authentication

BYE Authentication **Enable**

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).

Define Malicious Signatures

To protect the device from malicious attacks on SBC calls, it's 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").

➤ To configure malicious signatures:

1. Open the Malicious Signature table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Malicious Signature**), and then configure malicious signatures. The device provides preconfigured malicious signatures.

Figure 10-24: Configuring 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'

2. Open the Message Policies table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Policies**), and then configure a Message Policy and enable it to use the malicious signatures, by configuring 'Malicious Signature Database' to **Enable**:

Figure 10-25: Enabling Malicious Signatures for Message Policy

Malicious Signature Database ▼

3. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
4. For the SIP Interface of the calls that you want to apply the malicious signatures policy, from the 'Message Policy' drop-down list, select the Message Policy that you configured in Step 1:

Figure 10-26: Assigning Message Policy to SIP Interface



Secure Media Cluster Management Interface

By default, connectivity between the Signaling Component and Media Components for management of the Media Components is secured using TLS. Configuration is done using the [TpncpEncryptionEnable] parameter.

11 Gateway-Specific Security Guidelines

This section describes recommended security guidelines for the Gateway application (IP-to-Tel and Tel-to-IP call routing).

Block Calls from Unknown IP Addresses

Make sure that the device accepts incoming calls only from source IP addresses that appear in the Proxy Sets or Tel-to-IP Routing tables. In addition, if an FQDN appears in these tables, the call is accepted only if the resolved DNS IP address of the call appears in any one of these tables. The device rejects calls whose source IP addresses don't appear in these tables. This is useful in preventing unwanted SIP calls, SIP messages, or VoIP spam.

➤ **To block calls from unknown IP addresses:**

1. Open the Gateway Advanced Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway Advanced Settings**).
2. From the 'IP Security' drop-down list, select **Secure All calls**:

Figure 11-1: Allowing Calls only from Configured IP Addresses



Enable Secure SIP (SIPS)

Make sure 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's 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 enable SIPS:**

1. Open the Transport Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Transport Settings**).
2. From the 'SIPS' drop-down list, select **Enable**:

Figure 11-2: Enabling SIPS





It's 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).

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

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's crucial that you adhere to the following security guidelines:

- Make sure 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.

Define Call Admission Control

Make sure that you configure the maximum number of concurrent calls per routing rule or IP Group.

➤ To configure maximum concurrent calls:

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. For the relevant IP Profile, in the 'Number of Calls Limit' field, enter the maximum number of concurrent calls:

Figure 11-3: Configuring Maximum Concurrent Calls for IP Profile

Number of Calls Limit

120

3. Assign the IP Profile in the IP-to-Tel Routing table, Tel-to-IP Routing table, or IP Groups table.



The maximum number of concurrent calls considers incoming and outgoing calls (i.e., summation of all calls).

Define Maximum Call Duration

It's recommended to configure 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.

➤ **To configure maximum Gateway call duration:**

1. Open the Gateway Advanced Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway Advanced Settings**).
2. In the 'Max Call Duration' field, enter the maximum call duration:

Figure 11-4: Configuring Maximum Call Duration

Max Call Duration [min]

45

12 Network Port Assignment

The following table 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's highly recommended that you disable them for security reasons.



For increased security against attacks, it's highly recommended to change the default port numbers (especially for the SIP application).

Table 12-1: Network Port Assignments

Interface Type	Port	Protocol	Application	Default	Port Configuration
OAMP	22	TCP	SSH server	Enabled	<ul style="list-style-type: none"> ■ 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	Disabled	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ Enable / Disable: Secured Web Connection (HTTPSOnly) – when set to HTTPS Only ■ Port Definition:

Interface Type	Port	Protocol	Application	Default	Port Configuration
					HTTPPort <ul style="list-style-type: none"> ■ Access Control: Layer 3/4 Firewall and Access List table (WebAccessList_x)
	443	TCP	Web server (HTTPS)	Enabled	<ul style="list-style-type: none"> ■ 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)	Disabled - Mediant 90xx / Software Enabled - other products	<ul style="list-style-type: none"> ■ Enable / Disable: Disable SNMP (DisableSNMP) ■ Port Definition: <ul style="list-style-type: none"> ✓ 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	<ul style="list-style-type: none"> ■ Enable / Disable: DHCP Server table ■ Interface Definition: Interface Name (DHCPServer_InterfaceName) ■ Port Definition: Fixed ■ Access Control: Layer



Interface Type	Port	Protocol	Application	Default	Port Configuration
					3/4 Firewall
Control	5060	UDP / TCP	SIP traffic	Enabled	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ Applicable to: <ul style="list-style-type: none"> ✓ Standalone SBC ✓ Signaling

Interface Type	Port	Protocol	Application	Default	Port Configuration
					<p>Component in Mediant CE</p> <ul style="list-style-type: none"> ✓ Signaling <p>Component in Media Transcoding Cluster</p> <ul style="list-style-type: none"> ■ Enable / Disable: HA Remote Address (HARemoteAddress) ■ Port Definition: N/A
	680	UDP	HA keep-alive	Disabled	<ul style="list-style-type: none"> ■ Applicable to: <ul style="list-style-type: none"> ✓ Standalone SBC ✓ Signaling ✓ 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	<ul style="list-style-type: none"> ■ Applicable to: <ul style="list-style-type: none"> ✓ Standalone SBC ✓ Signaling ✓ Signaling Component in Mediant CE ✓ Signaling Component in Media Transcoding Cluster ■ Enable / Disable: HA Remote Address (HARemoteAddress)



Interface Type	Port	Protocol	Application	Default	Port Configuration
					■ Port Definition: N/A
	2442	TCP	HA data sync	Disabled	■ Applicable to: <ul style="list-style-type: none"> ✓ 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: <ul style="list-style-type: none"> ✓ 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: <ul style="list-style-type: none"> ✓ Signaling

Interface Type	Port	Protocol	Application	Default	Port Configuration
					<p>Component in Mediant CE</p> <ul style="list-style-type: none"> ✓ 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