Configuration Note

AudioCodes Professional Services – Interoperability Lab

AudioCodes SBC as Zoom Phone Local Proxy

zoomphone

audiocodes

Table of Contents

This page is intentionally left blank.

Notice

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

This document is subject to change without notice.

Date Published: June-23

-2022

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes

Abbreviations and Terminology

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

Related Documentation

Document Name
Mediant 500 Gateway & E-SBC User's Manual
Mediant 500L Gateway & E-SBC User's Manual
Mediant 800 Gateway & E-SBC User's Manual
Mediant 1000B Gateway & E-SBC User's Manual
Mediant 2600 E-SBC User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
Gateway and SBC CLI Reference Guide
SIP Message Manipulation Reference Guide
AudioCodes Configuration Notes

Document Revision Record

LTRT	Description
29350	Initial document release.
29353	Update Zoom Proxy Set and IP Group configuration for trigger switch to another DC upon receiving 503 error from primary DC.
29357	Update for Version 7.40A.250 and removed screenshots.

Documentation Feedback

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

1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (*SBC*) as a Zoom Phone Local Proxy.

You can also use the AudioCodes' SBC Wizard tool to automatically configure the SBC based on this interoperability setup. However, it is recommended to read through this document to better understand the various configuration options. For more information on AudioCodes' SBC Wizard including the download option, visit the AudioCodes Website at https://www.audiocodes.com/partners/sbc-interoperability-list.

1.1 About the Zoom Phone System and Local Proxy

Zoom Phone is a fully featured cloud PBX designed with security, reliability, scalability and centralized management in mind. Zoom Phone was built from the ground up to seamlessly integrate with the Zoom Collaboration platform to deliver a feature-rich UCaaS user experience. Zoom Phone offers various deployment options providing organizations with the flexibility to migrate and deploy the platform in a manner that best suits their requirements. Zoom Phone leverages global carrier relationships to deliver PSTN connectivity in many regions of the world offering phone number portability to Zoom in most regions thereby simplifying the telephony environment with one partner for your PBX and PSTN connectivity needs.

Native Zoom Phone meets the requirements of most organizations, it’s understood that some customers have environment restrictions, especially security conscious customers. Some customer security teams limit Zoom clients from routing UDP traffic for SRTP directly to the internet and prefers to use a device in the DMZ to relay UDP traffic from clients to internet. For these purposes Zoom introduced Zoom Phone Local Proxy where the traffic is proxied through a Session Border Controller.

1.2 About AudioCodes SBC Product Series

AudioCodes' family of SBC devices enables reliable connectivity and security between the Enterprise's and the service provider's VoIP networks.

The SBC provides perimeter defense as a way of protecting Enterprises from malicious VoIP attacks; mediation for allowing the connection of any PBX and/or IP-PBX to any service provider; and Service Assurance for service quality and manageability.

Designed as a cost-effective appliance, the SBC is based on field-proven VoIP and network services with a native host processor, allowing the creation of purpose-built multiservice appliances, providing smooth connectivity to cloud services, with integrated quality of service, SLA monitoring, security and manageability. The native implementation of SBC provides a host of additional capabilities that are not possible with standalone SBC appliances such as VoIP mediation, PSTN access survivability, and third-party value-added services applications. This enables Enterprises to utilize the advantages of converged networks and eliminate the need for standalone appliances.

AudioCodes SBC is available as an integrated solution running on top of its field-proven Mediant Media Gateway and Multi-Service Business Router platforms, or as a software-only solution for deployment with third-party hardware. The SBC can be offered as a Virtualized SBC, supporting the following platforms: Hyper-V, AWS, AZURE, AWP, KVM and VMWare.

This page is intentionally left blank.

2 Environment Information

This section describes interoperability test environment.

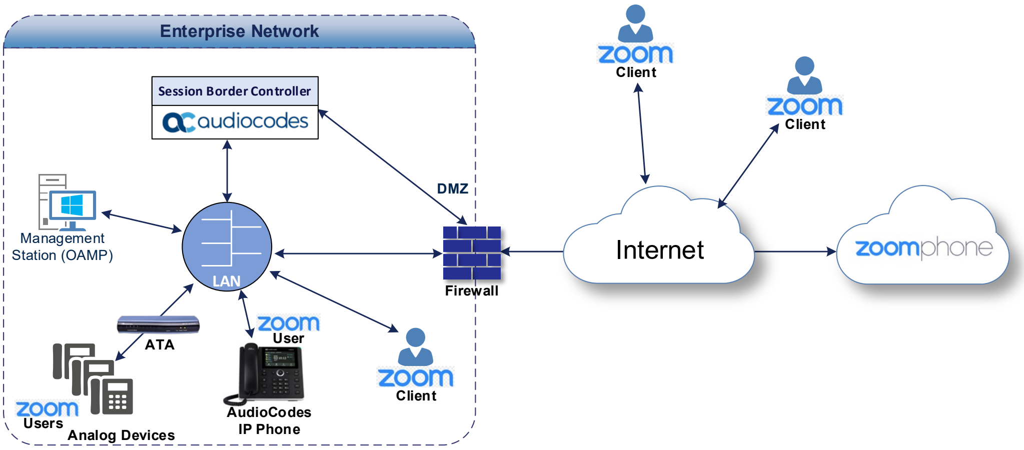
2.1 Tested Topology

The interoperability testing between AudioCodes SBC as a Zoom Phone Local Proxy, Zoom Desktop Clients, AudioCodes IP Phones, and AudioCodes MediaPack ATA devices in the branch was performed using the following topology setup:

- Enterprise deployed with Zoom Desktop Clients, AudioCodes IP Phones and AudioCodes MediaPack ATA devices and the administrator's management station, located on the LAN.
- Enterprise deployed with the Zoom Phone system located on the WAN for enhanced communication within the Enterprise.
- AudioCodes SBC is implemented as Local Proxy to interconnect between the Zoom Desktop Clients, AudioCodes IP Phones, AudioCodes MediaPack ATA devices and the Zoom Phone system.
    - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
    - **Border:** IP-to-IP network border - Zoom Desktop Clients, AudioCodes IP Phones, and AudioCodes MediaPack ATA devices are located in the Enterprise LAN, the Zoom Phone system is located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Layout of an Interoperability Test Environment



2.1.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-1: Environment Setup

Area	Setup
Network	▪ Zoom Desktop Clients, AudioCodes IP Phones, and AudioCodes MediaPack ATA devices are located on the LAN ▪ The Zoom Phone system environment is located on the WAN
Signaling Transcoding	▪ All entities operate with SIP-over-TLS transport type
Codecs Transcoding	▪ Zoom Phone system, Zoom Desktop Clients, and IP Phones support OPUS, G.711A-law, G.711U-law and G.722 coders ▪ AudioCodes MediaPack ATA devices support G.711A-law and G.711U-law coders
Media Transcoding	▪ All entities operate with SRTP media type

3 Configuring Zoom Phone System

For configuring the Zoom Phone System, refer to Zoom Help Center at https://support.zoom.us/hc/en-us/articles/360001297663-Getting-started-with-Zoom-Phone-admin-.

Notes:

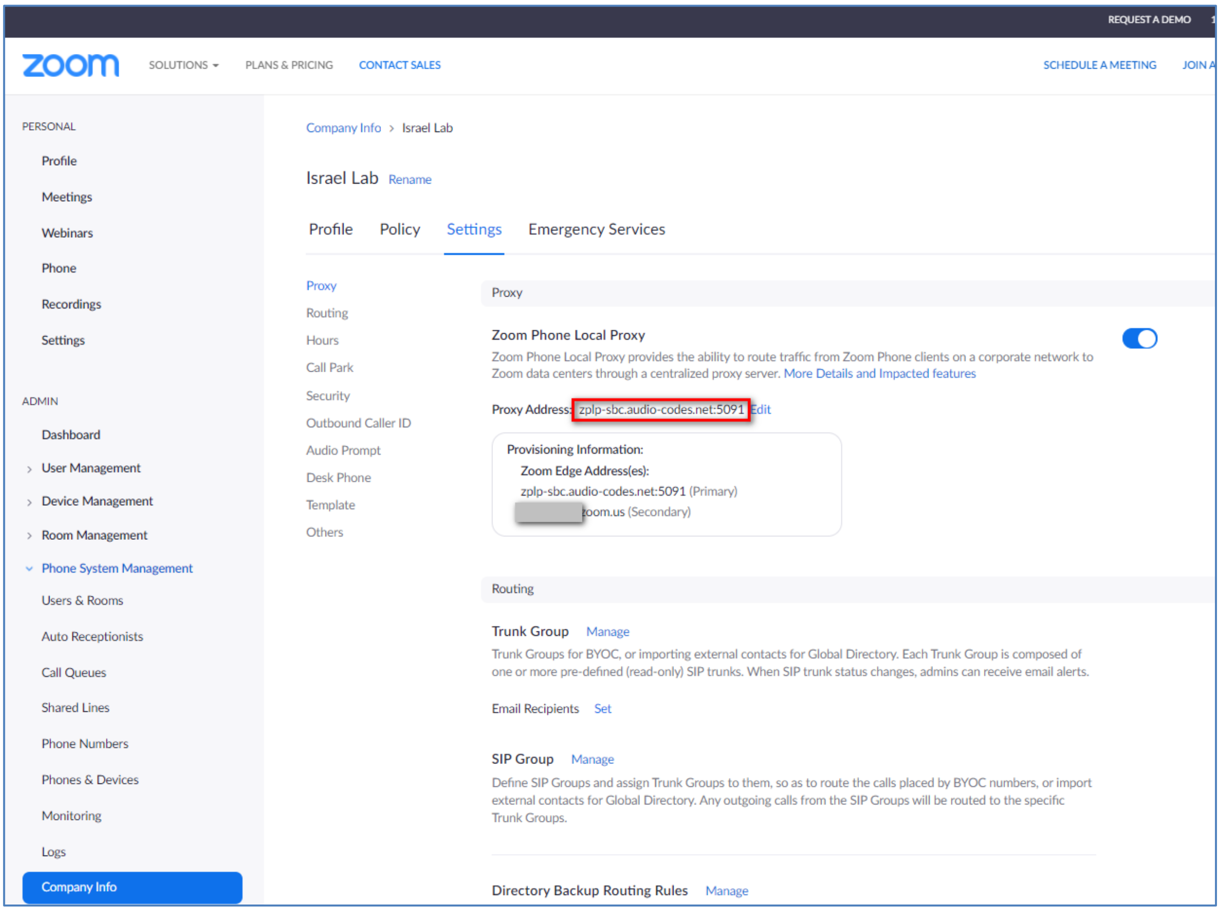
Before you begin configuration:

- Contact your Zoom Representative to enable Zoom Phone Local Proxy for your Zoom Phone account.
- Make sure you have Zoom Portal admin credentials. Be aware that each customer needs to have a Zoom Phone admin account and all Zoom Phone related configuration will be done by the customer and not by the Zoom engineer.

3.1 Enabling Zoom Phone Local Proxy

After configuring appropriated site in the Zoom Phone administration portal, enable Local Proxy on a site level under **Phone System Management** > **Company Info** > **<site name>** > **Settings** > **Zoom Phone Local Proxy**:

Figure 3-1: Enable Zoom Phone Local Proxy



Proxy

Zoom Phone Local Proxy

Zoom Phone Local Proxy provides the ability to route traffic from Zoom Phone clients on a corporate network to Zoom data centers through a centralized proxy server. More Details and Impacted features

Proxy Address: zplp-sbc.audio-codes.net:5091 Edit

Provisioning Information:
Zoom Edge Address(es):
zplp-sbc.audio-codes.net:5091 (Primary)
[redacted]zoom.us (Secondary)

Routing

Trunk Group Manage

Trunk Groups for BYOC, or importing external contacts for Global Directory. Each Trunk Group is composed of one or more pre-defined (read-only) SIP trunks. When SIP trunk status changes, admins can receive email alerts.

Email Recipients Set

SIP Group Manage

Define SIP Groups and assign Trunk Groups to them, so as to route the calls placed by BYOC numbers, or import external contacts for Global Directory. Any outgoing calls from the SIP Groups will be routed to the specific Trunk Groups.

Directory Backup Routing Rules Manage

Notes:

- SBC must have a certificate that is signed by one of Zoom’s approved CA vendors.
- Certificate must have the FQDN or domain name that is configured on the Zoom admin portal in the CN/SAN.
- FQDN or SRV must be resolvable within the internal corporate DNS servers. These entries should not be resolvable on external DNS servers and let traffic route directly to Zoom servers.

4 Configuring AudioCodes SBC

This section shows how to configure AudioCodes SBC as a Zoom Phone Local Proxy. These configuration procedures are based on the interoperability test topology described in Section 2.1 on page 9, and includes the following main areas:

- SBC LAN interface – Zoom Desktop Clients, AudioCodes IP Phones, AudioCodes MediaPack ATA devices and Management Station
- SBC WAN interface – Zoom Phone system environment

This configuration is done using the SBC's embedded Web server (hereafter, referred to as *Web interface*).

4.1 Validate AudioCodes SBC License and Version

Zoom has successfully conducted validation tests with AudioCodes' Mediant SBC Ver. 7.40A.250. The previous certified firmware version is 7.20A.258.

Notes:

- For implementing the Zoom Phone system and Generic SIP Trunk based on the configuration described in this section, AudioCodes SBC must be installed with a License Key that includes the following software features:
  - √ **Number of SBC sessions** [Based on requirements]
  - √ **FEU (Far-End User)** [For registration of the IP Phones]
  - √ **DSP Channels** [Based on requirements]
  - √ **Transcoding sessions** [Based on requirements]
  - √ **Coders** [Based on requirements]

  For more information about the License Key, contact your AudioCodes sales representative.
- If your SBC is deployed in a virtual environment and transcoding is required, your virtual machine must have a minimum of two vCPUs. For more information, please refer to the appropriate *Installation Manual,* which can be found on AudioCodes website.
- The scope of this document does **not** cover all security aspects for configuring this topology. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document, which can be found at AudioCodes web site

4.2 Prerequisites

Before you begin configuration, make sure you have obtained the following for each SBC you wish to pair with Zoom Phone System:

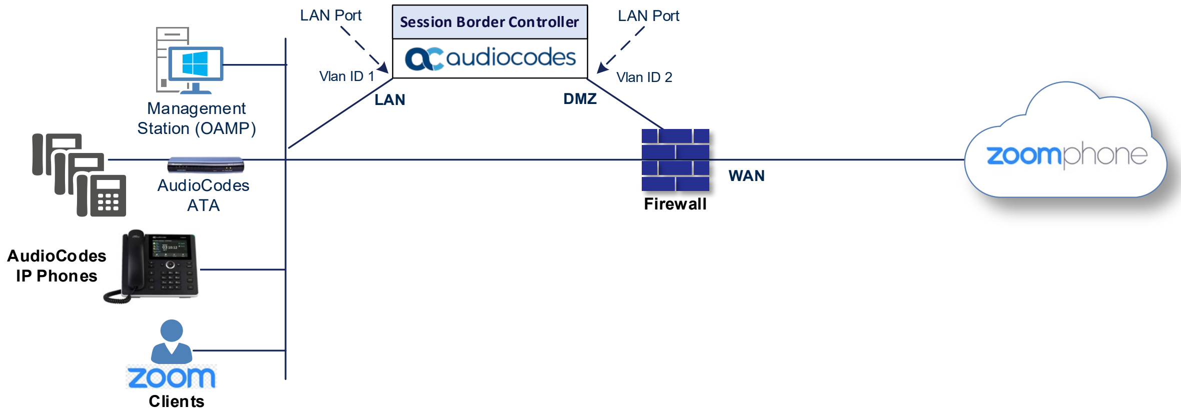
- Public IP address
- Public certificate that is issued by one of the Zoom supported CAs

4.3 Configure IP Network Interfaces

This section describes how to configure the SBC's IP network interfaces. There are several ways to deploy the SBC; however, this interoperability test topology employs the following deployment method:

- SBC interfaces with the following IP entities:
  - Zoom Desktop Clients, AudioCodes IP Phones, AudioCodes MediaPack ATA devices and Management Servers located on the LAN
  - Zoom Phone system located on the WAN
- SBC connects to the WAN through a DMZ network
- Physical connection: The type of physical connection depends on the method used to connect to the Enterprise's network. In the interoperability test topology, SBC connects to the LAN and DMZ using dedicated Ethernet ports (i.e., two ports and two network cables are used).
- SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - DMZ (VLAN ID 2)

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.3.1 Configure LAN and WAN VLANs

This section describes how to configure VLANs for each of the following interfaces:

- LAN (assigned the name "LAN_IF")
- WAN (assigned the name "WAN_IF")

➢ **To configure the VLANs:**

1. Open the Ethernet Device table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet** Devices). There will be one existing row for VLAN ID 1 and underlying interface GROUP_1.
2. Add another VLAN ID 2 for the WAN side.

4.3.2 Configure Network Interfaces

This section describes how to configure the IP network interfaces for each of the following interfaces:

- LAN Interface (assigned the name "LAN_IF")
- WAN Interface (assigned the name "WAN_IF")

➢ **To configure the IP network interfaces:**

1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Configure the IP interfaces as follows (your network parameters might be different):

Table 4-1: Configuration Example of the Network Interface Table

Index	Application Types	Interface Mode	IP Address	Prefix Length	Gateway	DNS	I/F Name	Ethernet Device
0	OAMP+ Media + Control	IPv4 Manual	10.15.77.10	16	10.15.0.1	10.15.27.1	LAN_IF	vlan 1
1	Media + Control (as this interface points to the internet, enabling OAMP is not recommended)	IPv4 Manual	195.189.192.152 (DMZ IP address of SBC)	25	195.189.192.129 (router's IP address)	According to your Internet provider's instructions	WAN_IF	vlan 2

4.4 Configure TLS Context for Zoom

This section describes how to configure the SBC for using a TLS connection with the Zoom Phone System. This configuration is essential for a secure SIP TLS connection.

The example described in this section is based on the DigiCert Certificate Chain as Certificate Authority (CA).

4.4.1 Configure the NTP Server Address

This section describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (local NTP server or another global NTP server) to ensure that the SBC receives the current date and time. This is necessary for validating certificates of remote parties. It is important, that the NTP Server is located on the OAMP IP Interface (LAN_IF in our case) or will be accessible through it.

➢ **To configure the NTP server address:**

1. Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**).
2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., **10.15.28.1**).
3. Click **Apply**.

4.4.2 Create a TLS Context for Zoom Phone System

The section below describes how to request a certificate for the SBC WAN interface and configure it, based on the example of the DigiCert Global Root CA. The certificate is used by the SBC to authenticate the connection with the Zoom Phone System.

The procedure involves the following main steps:

- Create a TLS Context for Zoom Phone System
- Generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority
- Deploy the SBC and Root certificates on the SBC

➢ **To create a TLS Context for Zoom Phone System:**

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. Create a new TLS Context by clicking **+New**, and then configure the parameters using the table below as reference.

Table 4-2: New TLS Context

Index	Name	TLS Version
1	Zoom (arbitrary descriptive name)	TLSv1.2 and TLSv1.3
All other parameters can be left unchanged with their default values.		

3. Click **Apply**; you should see the new TLS Context and option to manage the certificates at the bottom of 'TLS Context' table.

4.4.3 Generate a CSR and Obtain the Certificate from a Supported CA

This section shows how to generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority (DigiCert in our example).

➢ **To generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority:**

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the **Zoom TLS Context** index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
3. Under the Certificate Signing Request group, do the following:
   a. In the 'Common Name [CN]' field, enter the SBC FQDN name (for example, **zplp-sbc.audio-codes.net**).

> **Note:** SBC FQDN (**zplp-sbc.audio-codes.net** in our example) must be resolvable within the internal corporate DNS servers only. This entry should not be resolvable on external DNS servers and let traffic route directly to Zoom Phone Servers.

   b. In the '1st Subject Alternative Name [SAN]' field, change the type to 'DNS' and enter the SBC FQDN name (based on example above, **zplp-sbc.audio-codes.net**).
   c. Change the 'Private Key Size' based on the requirements of your Certification Authority. Many CAs do not support private key of size 1024.
   d. To change the key size on TLS Context, go to: **Generate New Private Key and Self-Signed Certificate**, change the 'Private Key Size' and then click **Generate Private-Key**. To use 2048 as a Private Key Size value, you can click **Generate Private-Key** without changing the default key size value.
   e. Fill in the rest of the request fields according to your security provider's instructions.
   f. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button.
4. Copy the CSR from the line "----BEGIN CERTIFICATE REQUEST" to "END CERTIFICATE REQUEST----" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, for example certreq.txt.
5. Send certreq.txt file to the Certified Authority Administrator for signing.

4.4.4 Deploy the SBC Signed and Trusted by Zoom Root Certificates

After obtaining the SBC signed and Trusted Root/Intermediate Certificate from the CA, download the trusted by Zoom Public Root Certificates and install the following:

- SBC certificate signed by the public CA authority that was authorized by Zoom (refer to Appendix A on page 31)
- Trusted by Zoom Public Root certificates

Currently, Zoom Data Centers (DC) used DigiCert public CA certificates. So, in order to be able to establish a TLS connection with Zoom Phone infrastructure, download and install as trusted root following public CA certificates:

- https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem
- https://cacerts.digicert.com/DigiCertGlobalRootG2.crt.pem
- https://cacerts.digicert.com/DigiCertGlobalRootG3.crt.pem

➢ To install the SBC certificate:

1. In the SBC's Web interface, return to the TLS Contexts page and do the following:
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
   b. Scroll down to the Upload certificates files from your computer group, click the **Choose File** button corresponding to the 'Send Device Certificate...' field, navigate to the certificate file obtained from the CA, and then click **Load File** to upload the certificate to the SBC.
2. Validate that the certificate was uploaded correctly. A message indicating that the certificate was uploaded successfully is displayed in blue in the lower part of the page.
3. In the SBC's Web interface, return to the TLS Contexts page, select the required TLS Context index row, and then click the **Certificate Information** link, located at the bottom of the TLS. Then validate the Key size, certificate status and Subject Name.
4. In the SBC's Web interface, return to the TLS Contexts page.
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the Trusted Root **Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
   b. Click the **Import** button, and then select all Root/Intermediate Certificates obtained from your Certification Authority and trusted by Zoom public CA certificates (obtained from the link at the beginning of this section) to load.
5. Click **OK**.
6. Repeat the same procedure for loading AudioCodes Root Certificates for working with IP Phones and MediaPack ATA devices and click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.

Note: The above method creates a signed certificate for an explicit device, on which a Certificate Sign Request was generated (and signed with private key).

4.5 Configure Media Realms

This section describes how to configure Media Realms. Media Realms allows the dividing of the UDP port ranges for use on different interfaces. In the example below, two Media Realms are configured:

- One for the IP interface towards all users (Zoom Desktop Clients, AudioCodes IP Phones, and AudioCodes MediaPack ATA devices), with the UDP port range starting at 7000 and the number of media session legs is 100.
- One for the IP interface towards the Zoom Phone System, with the UDP port starting at 10000 and the number of media session legs is 100 (you need to calculate number of media session legs based on your usage).

➢ **To configure Media Realms:**

1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Configure Media Realm as follows (you can use the default Media Realm (Index 0), but modify it):

Table 4-3: Configuration Example Media Realms in Media Realm Table

Index	Name	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
0	MR-Users (arbitrary name)	LAN_IF	7000	100 (media sessions assigned with port range)
1	MR-Zoom (arbitrary name)	WAN_IF	10000	100 (media sessions assigned with port range)
All other parameters can be left unchanged at their default values.				

4.6 Configure SIP Signaling Interfaces

This section shows how to configure a SIP Signaling Interfaces. A SIP Interface defines a listening port and type (UDP, TCP, or TLS) for SIP signaling traffic on a specific logical IP network interface (configured in the Interface Table above) and Media Realm.

AudioCodes also offers a comprehensive suite of documents covering the interconnection between different trunks and equipment.

➢ **To configure SIP Interfaces:**

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Configure SIP Interfaces. You can use the default SIP Interface (Index 0), but modify it as shown in the table below. The table below shows an example of the configuration. You can change some parameters according to your requirements.

Table 4-4: Configured SIP Interfaces in SIP Interface Table

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Media Realm	TLS Context Name
0	**SI-Users** (arbitrary name)	LAN_IF	SBC	0	0	5091	MR-Users	Zoom
1	**SI-Zoom** (arbitrary name)	WAN_IF	SBC	0	0	5091	MR-Zoom	default
All other parameters can be left unchanged at their default values.								

Note: For enhanced security, AudioCodes recommends implementing a Mutual TLS connection with the Zoom Phone System. For required configuration, see Section 4.16.1 on page 29.

4.7 Configure Proxy Sets and Proxy Address

This section describes how to configure Proxy Sets. The Proxy Set defines the destination address (IP address or FQDN) of the IP entity server. Proxy Sets can also be used to configure load balancing between multiple servers.

For the interoperability test topology, Proxy Sets for Zoom PBX need to be configured.

The Proxy Sets will later be applied to the VoIP network by assigning it to an IP Group.

➢ **To configure Proxy Sets:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Configure Proxy Sets as shown in the table below:

Table 4-5: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Keep-Alive Failure Responses	Redundancy Mode	Proxy Hot Swap
1	**Zoom PBX** (arbitrary name)	SI-Zoom	Zoom[1]	Using Options	503	Homing	Enable

Note: On Hybrid SBCs (with Onboard PSTN interfaces) it's recommended to leave Proxy Set 0 unconfigured for possible future use for PSTN Fallback.

4.7.1 Configure a Proxy Address

This section shows how to configure a Proxy Address.

➢ **To configure a Proxy Address for Zoom PBX:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) click the Proxy Set **Zoom PBX**, and then click the Proxy Address link located below the table; the Proxy Address table opens.
2. Click **+New,** and then configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-6: Configuration Proxy Address for Zoom PBX

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	<Zoom PBX FQDN>:5091 (according to configuration on Zoom Phone System Management Dashboard)	TLS	0	0

3. Click **Apply**.

[1] Configured in Section 4.4.

4.8 Configure IP Profiles

This section describes how to configure IP Profiles. The IP Profile defines a set of call capabilities relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder and transcoding method).

➢ **To configure IP Profile for the Zoom Users:**

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **+New** and add the IP Profile for Zoom Users interface. Configure the parameters using the table below as reference.

Table 4-7: Configuration Example: Zoom Users IP Profile

Parameter	Value
General	
Index	**1**
Name	**Users** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Secured**
SBC Remove Unknown Crypto	**Yes**
All other parameters can be left unchanged with their default values.	

3. Click **Apply**.

➢ **To configure IP Profile for the Zoom Phone system:**

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **+New** and add the IP Profile for Zoom PBX interface. Configure the parameters using the table below as reference.

Table 4-8: Configuration Example: Zoom PBX IP Profile

Parameter	Value
General	
Index	**2**
Name	**Zoom** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Secured**
SBC Signaling	
Session Expires Mode	**Supported**
All other parameters can be left unchanged with their default values.	

3. Click **Apply**.

4.9 Configure SIP Response Codes for Alternative Routing Reasons

This section describes how to configure the SBC's handling of SIP 503 responses received for outgoing SIP dialog-initiating methods, e.g., INVITE, OPTIONS, and SUBSCRIBE messages. In this case, the SBC attempts to locate an alternative route for the call. This feature works together with the Proxy Hot Swap feature, which is configured in the Proxy Sets table. Alternative routing based on SIP responses is configured using two tables with 'parent-child' relationships:

- Alternative Reasons Set table ('parent'): Defines the name of the Alternative Reasons Set.
- Alternative Reasons Rules table ('child'): Defines SIP response codes per Alternative Reasons Set.

To apply your configured alternative routing reason rules, you need to assign the Alternative Reasons Set for which you configured the rules, to the Bell Canada SIP Trunk IP Group in the IP Groups table, using the 'SBC Alternative Routing Reasons Set' parameter.

➢ **To configure SIP reason codes for alternative IP routing:**

1. Open the Alternative Routing Reasons table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **Alternative Reasons Set**).
2. Click **New** and configure a name for the Alternative Routing Reasons Set (e.g., *503*).
3. Click **Apply**.
4. Select the index row of the Alternative Reasons Set that you added, and then click the Alternative Reasons Rules link located at the bottom of the page; the Alternative Reasons Rules table opens.
5. Click **New** and select **503 Service Unavailable** from the 'Release Cause Code' drop-down list.
6. Click **Apply**.

4.10 Configure IP Groups

This section describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the SBC communicates. This can be a server (e.g., IP PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

In this interoperability test topology, IP Groups must be configured for the following IP entities:

- Zoom Users (Zoom Desktop Clients, AudioCodes IP Phones, and AudioCodes MediaPack ATA devices)
- Zoom Phone PBX

➢ **To configure IP Groups:**

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Configure an IP Group for the Zoom Users:

Parameter	Value
Index	**1**
Name	**Users** (arbitrary descriptive name)
Type	**User**
Proxy Set	**-**
IP Profile	**Users**
Media Realm	**MR-Users**
Classify By Proxy Set	**Disable**
All other parameters can be left unchanged with their default values.	

3. Configure an IP Group for the Zoom Phone PBX:

Parameter	Value
Index	**2**
Name	**Zoom PBX** (arbitrary descriptive name)
Type	**Server**
Proxy Set	**Zoom PBX**
IP Profile	**Zoom**
Media Realm	**MR-Zoom**
SBC Alternative Routing Reason Set	**503** (created in Section 4.9 on page 23)
Proxy Keep-Alive using IP Group settings	**Enable**
All other parameters can be left unchanged with their default values.	

4.11 Configure SRTP

This section describes how to configure media security. The Zoom Phone System Interface needs to use of SRTP only, so you need to configure the SBC to operate in the same manner. By default, SRTP is disabled.

➢ To configure media security:

1. Open the Media Security page (**Setup menu > Signaling & Media tab > Media folder > Media Security**).
2. From the '**Media Security**' drop-down list, select **Enable** to enable SRTP.
3. Click **Apply**.

4.12 Configure Message Condition Rules

This section describes how to configure the Message Condition Rules. A Message Condition defines special conditions (requisites) for incoming SIP messages. These rules can be used as additional matching criteria for the classification incoming messages in the Classification Table.

Note: The following condition verifies that the User-Agent header contains a string, which defines AudioCodes IP Phone, Zoom Desktop Client, or AudioCodes MediaPack ATA device. If your environment contains IP Phones from other vendors (e.g., Polycom or Yealink), just add an additional condition with the appropriated string.

➢ To configure a Message Condition rule:

1. Open the Message Conditions table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Conditions**).
2. Click **New**, and then configure condition rule:

Parameter	Value
Index	**0**
Name	**Users** (arbitrary descriptive name)
Condition	**Header.User-Agent contains 'AUDC-IPPhone' OR Header.User-Agent contains 'ZoomPbxPhone' OR Header.User-Agent contains 'MP-1'**

3. Click **Apply**.

4.13 Configure Classification Rules

This section describes how to configure Classification rules. A Classification rule classifies incoming SIP dialog-initiating requests (e.g., INVITE messages) to a "source" IP Group. The source IP Group is the SIP entity that sends the SIP dialog request. Once classified, the device uses the IP Group to process the call (manipulation and routing).

You can also use the Classification table for employing SIP-level access control for successfully classified calls, by configuring Classification rules with whitelist and blacklist settings. If a Classification rule is configured as a whitelist ("Allow"), the device accepts the SIP dialog and processes the call. If the Classification rule is configured as a blacklist ("Deny"), the device rejects the SIP dialog.

➢ **To configure a Classification rule for IP Phones:**

1. Open the Classification table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Classification Table**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	**0**
Name	**Users**
Source SIP Interface	**SI-Users**
Source Transport Type	**TLS**
Message Condition	**Users** (rule, created in the previous section)
Action Type	**Allow**
Source IP Group	**Users**

3. Click **Apply**.

4.14 Configure IP-to-IP Call Routing Rules

This section describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Zoom Phone system (Zoom PBX) and local users:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity.
- Calls from Users to Zoom Phone PBX.
- Calls from Zoom Phone PBX to the Users.

➢ **To configure IP-to-IP routing rules:**

1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure routing rules as shown in the table below:

Table 4-9: Configuration IP-to-IP Routing Rules

Index	Name	Source IP Group	Request Type	Dest Type	Dest IP Group	Internal Action
0	Terminate OPTIONS	Any	OPTIONS	Dest Address		Reply (Response='200')
1	Users to Zoom PBX	Users	All	IP Group	Zoom PBX	
4	Zoom PBX to Users	Zoom PBX	All	IP Group	Users	

Note: The routing configuration may change according to your specific deployment topology.

4.15 Configure Message Manipulation Rules

This section describes how to configure SIP message manipulation rules. SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Manipulation rules are grouped into Manipulation Sets, enabling you to apply multiple rules to the same SIP message (IP entity).

Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

➢ **To configure SIP message manipulation rule for Zoom PBX:**

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 2) for Zoom PBX IP Group. This rule applies to OPTIONS messages sent to the Zoom PBX IP Group. This replaces the host part of the SIP Request-URI Header with the destination (Zoom Phone System Server) IP address in all OPTIONS messages sent from SBC towards Zoom PBX.

Parameter	Value
Index	**0**
Name	**Zoom-Options** (arbitrary name)
Manipulation Set ID	**2**
Message Type	**Options.Request**
Action Subject	**Header.Request-URI.URL.Host**
Action Type	**Modify**
Action Value	**Param.Message.Address.Dst.IP**

3. Configure another manipulation rule (Manipulation Set 2) for Zoom PBX IP Group. This rule applies to messages sent to the Zoom PBX IP Group. This replaces the host part of the SIP To Header with the value from SIP From Header.

Parameter	Value
Index	**1**
Name	**Normalize To Header Host**
Manipulation Set ID	**2**
Message Type	**Any.Request**
Action Subject	**Header.To.URL.Host**
Action Type	**Modify**
Action Value	**Header.From.URL.Host**

4. Assign Manipulation Set ID 2 to the Zoom PBX IP Group:
   a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
   b. Select the row of the Zoom PBX IP Group, and then click **Edit**.
   c. Set the 'Outbound Message Manipulation Set' field to **2**.
   d. Click **Apply**.

Note: In your implementation, additional message manipulation rules may be required. Refer to the appropriate Implementation Guide or contact an AudioCodes representative to order Professional Services from AudioCodes, and our Professional Services team will help you with your configuration.

4.16 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

4.16.1 Configuring SBC to Keep Original User in Register

This section describes how to configure the SBC to Keep Original User in Register.

➢ **To configure SBC to Keep Original User in Register:**

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).
2. From the '**Keep original user in Register**' drop-down list, select '**Keep user without unique identifier**' value.
3. Click **Apply**.

4.16.2 Configuring Mutual TLS Authentication for SIP

This section describes how to configure SBC to work in mutual (two-way) TLS authentication mode.

Note: This section is required only if implementation of MTLS connection with the Zoom Phone System is required and depends on enabling MTLS on the Zoom side.

➢ **To configure Mutual TLS authentication for SIP messaging with Zoom:**

1. Enable two-way authentication on the Zoom SIP Interface:
2. In the SIP Interface table, assign Zoom TLS context to the Zoom SIP Interface and configure the '**TLS Mutual Authentication**' parameter to **Enable**.
3. Make sure that the TLS certificate is signed by a Zoom Trusted Public Certificate Authority (refer to list in Appendix A on page 31).
4. Make sure that CA root certificates are imported into the Trusted Root Certificates table.

In order to further enhance security, it is possible to configure the SBC to verify the server certificates, when it acts as a client for the TLS connection.

➢ **To configure SBC to verify Server certificate:**

1. Open the SBC Security Settings page (**Setup** menu > **IP Network** tab > **Security** folder > **Security Settings**).
2. From the '**TLS Client Verify Server Certificate**' drop-down list, select **Enable**.
3. Click **Apply**.

4.16.3 Optimizing CPU Cores Usage for a Specific Service (Relevant for Mediant 9000 and Software SBC Only)

This section describes how to optimize the SBC's CPU cores usage for a specified profile to achieve maximum capacity for that profile. The supported profiles include:

- **SIP profile**: Improves SIP signaling performance, for example, SIP calls per second (CPS)
- **SRTP profile**: Improves maximum number of SRTP sessions
- **Transcoding profile**: Enables all DSP-required features, for example, transcoding and voice in-band detectors

➢ **To optimize core allocation for a profile:**

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).
2. From the 'SBC Performance Profile' drop-down list, select the required profile (e.g., *Optimized for transcoding*).
3. Click **Apply**, and then reset the device with a burn-to-flash for your settings to take effect.

A Zoom Public Trusted Certificate List

The following table lists the Zoom Public Trusted Certificates.

Table A-1: Zoom Public Trusted Certificate List

Certificate Issuer Organization	Common Name or Certificate Name
Buypass AS-983163327	Buypass Class 2 Root CA
Buypass AS-983163327	Buypass Class 3 Root CA
Baltimore	Baltimore CyberTrust Root
Cybertrust, Inc	Cybertrust Global Root
DigiCert Inc	DigiCert Assured ID Root CA
DigiCert Inc	DigiCert Assured ID Root G2
DigiCert Inc	DigiCert Assured ID Root G3
DigiCert Inc	DigiCert Global Root CA
DigiCert Inc	DigiCert Global Root G2
DigiCert Inc	DigiCert Global Root G3
DigiCert Inc	DigiCert High Assurance EV Root CA
DigiCert Inc	DigiCert Trusted Root G4
GeoTrust Inc.	GeoTrust Global CA
GeoTrust Inc.	GeoTrust Primary Certification Authority
GeoTrust Inc.	GeoTrust Primary Certification Authority - G2
GeoTrust Inc.	GeoTrust Primary Certification Authority - G3
GeoTrust Inc.	GeoTrust Universal CA
GeoTrust Inc.	GeoTrust Universal CA 2
DigiCert Inc	DigiCert Global Root G3
Symantec Corporation	Symantec Class 1 Public Primary Certification Authority - G4
Symantec Corporation	Symantec Class 1 Public Primary Certification Authority - G6
Symantec Corporation	Symantec Class 2 Public Primary Certification Authority - G4
Symantec Corporation	Symantec Class 2 Public Primary Certification Authority - G6
Thawte, Inc.	Thawte Primary Root CA
Thawte, Inc.	Thawte Primary Root CA - G2
Thawte, Inc.	Thawte Primary Root CA - G3
VeriSign, Inc.	VeriSign Class 1 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 2 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G4
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign, Inc.	VeriSign Universal Root Certification Authority
AffirmTrust	AffirmTrust Commercial
AffirmTrust	AffirmTrust Networking
AffirmTrust	AffirmTrust Premium

Certificate Issuer Organization	Common Name or Certificate Name
AffirmTrust	AffirmTrust Premium ECC
Entrust, Inc.	Entrust Root Certification Authority
Entrust, Inc.	Entrust Root Certification Authority - EC1
Entrust, Inc.	Entrust Root Certification Authority - G2
Entrust, Inc.	Entrust Root Certification Authority - G4
Entrust.net	Entrust.net Certification Authority (2048)
GlobalSign	GlobalSign
GlobalSign	GlobalSign
GlobalSign	GlobalSign
GlobalSign nv-sa	GlobalSign Root CA
The GoDaddy Group, Inc.	Go Daddy Class 2 CA
GoDaddy.com, Inc.	Go Daddy Root Certificate Authority - G2
Starfield Technologies, Inc.	Starfield Class 2 CA
Starfield Technologies, Inc.	Starfield Root Certificate Authority - G2
QuoVadis Limited	QuoVadis Root CA 1 G3
QuoVadis Limited	QuoVadis Root CA 2
QuoVadis Limited	QuoVadis Root CA 2 G3
QuoVadis Limited	QuoVadis Root CA 3
QuoVadis Limited	QuoVadis Root CA 3 G3
QuoVadis Limited	QuoVadis Root Certification Authority
Comodo CA Limited	AAA Certificate Services
AddTrust AB	AddTrust Class 1 CA Root
AddTrust AB	AddTrust External CA Root
COMODO CA Limited	COMODO Certification Authority
COMODO CA Limited	COMODO ECC Certification Authority
COMODO CA Limited	COMODO RSA Certification Authority
The USERTRUST Network	USERTrust ECC Certification Authority
The USERTRUST Network	USERTrust RSA Certification Authority
T-Systems Enterprise Services GmbH	T-TeleSec GlobalRoot Class 2
T-Systems Enterprise Services GmbH	T-TeleSec GlobalRoot Class 3

This page is intentionally left blank.

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

AudioCodes Inc.
200 Cottontail Lane
Suite A101E
Somerset NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

Document #: LTRT-29356