Configuration Note

AudioCodes Professional Services – Interoperability Lab

Resiliency with SIP Trunking

For Branch Sites in Zoom Phone Environments

zoomphone

audiocodes

Table of Contents

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-26-2022

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
29345	Initial document release.
29346	Updated Tested Topology.
29347	Updated Configuring AudioCodes SBC.
29348	Updates related to new Zoom trusted public certificates.
29349	Disclaimer added to the Introduction section.
29351	Update related to certificates, used for connection to Zoom Data Centers and fix IP to IP routing rule for OPTIONS.
29352	Software version updated to the latest 7.4. Updated concept. Added AudioCodes ATA devices.
29354	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 removing 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

Disclaimer: The resiliency concept described in this document is currently in preview status and not defined for General Availability (GA). However, in the meantime you can test and analyze this concept. AudioCodes will announce once this concept has been approved and defined as GA.

AudioCodes' Resiliency feature provides call survivability (branch-site resiliency) for AudioCodes IP Phone and ATA devices users at the branch site upon connectivity failure with the datacenter in a Zoom Phone environment. This solution is offered per branch site containing an AudioCodes Mediant SBC co-located with AudioCodes Zoom-compatible IP Phones and AudioCodes ATA devices.

For the Mediant 500, Mediant 800B, Mediant 800C and Mediant 1000B devices, in addition to branch-site resiliency, the Resiliency solution can also provide optional Gateway (Enhanced Gateway) and SBC functionalities, servicing all users in the Zoom Phone environment in normal operation. If ordered with PSTN interfaces, the device can provide connectivity to the PSTN network, enabling users to make and receive PSTN calls during normal operation. In survivability mode, the device maintains PSTN services to the branch site users. The device can also provide direct connectivity to a SIP Trunking service, enabling branch site users to make and receive calls during survivability mode.

This Configuration Note describes how to set up the AudioCodes Session Border Controller (hereafter, referred to as *SBC*) for implementing enterprise site resiliency in the Zoom Phone environment.

Note: For configuring AudioCodes SBC for interworking between SIP Trunk and the Zoom Phone Premise Peering (BYOC), refer to the dedicated document on AudioCodes website at *AudioCodes SBC with Zoom Phone Premise Peering Configuration Note*.

1.1 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.

1.2 About the Zoom Phone System

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. While native Zoom Phone meets the requirements of most organizations, it's understood that some organizations have environments that may need additional functionality for global support or migration strategies. For organizations with such diverse requirements of their telephony environments, Zoom's Premise Peering solution is offered.

Zoom Phone Premise Peering provides organizations with flexibility and seamless options to migrate their voice workloads to the cloud. This is accomplished by providing two connection types; Premise Peering PSTN (formally referred to as Bring Your Own Carrier - BYOC) and/or Premise Peering PBX (formally referred to as Bring Your Own PBX - BYOP). Zoom Phone Premise Peering PSTN enables organizations to leverage their existing telephony carrier PSTN environment for Zoom Phone connectivity. Using this functionality organizations can connect Zoom Phone with virtually any telephony carrier.

2 Component Information

2.1 AudioCodes SBC Version

Table 2-1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500/L Gateway & E-SBC ▪ Mediant 800B/C Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000/B SBC ▪ Mediant 9000/9030/9080 SBC ▪ Mediant Software SBC (VE/SE/CE)
Software Version	7.40A.250.262 or later
Protocol	▪ SIP/UDP or SIP/TCP or SIP/TLS (to the Generic SIP Trunk) ▪ SIP/TLS (to the Zoom Phone system) ▪ SIP/TLS (to the AudioCodes IP Phones and ATA devices)
Additional Notes	None

2.2 AudioCodes IP Phones Models and Version

Table 2-2: AudioCodes IP Phones Models and Version

Vendor/Service Provider	AudioCodes
IP Phone Models	405/405HD/420HD/440HD/445HD/450HD/C450HD
Software Version	UC_2.2.16.487 for 405/405HD/420HD and 440HD models UC_3.4.5.18 for 445HD/450HD and C450HD models
Additional Notes	None

2.3 AudioCodes ATA Devices Models and Version

Table 2-3: AudioCodes ATA Devices Models and Version

Vendor	AudioCodes
Models	MP-112/114/118/124
Software Version	6.60A.364 or later
Additional Notes	None

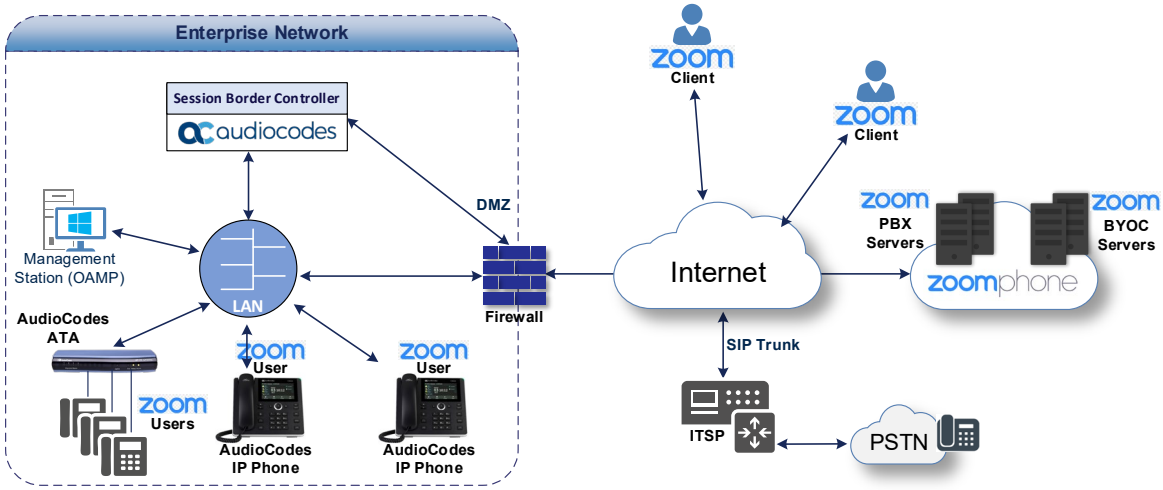
2.4 Tested Topology

Interoperability testing between AudioCodes SBC, AudioCodes IP Phones and ATA devices in the branch and Generic SIP Trunk with the Zoom Phone system was performed using the following topology setup:

- Enterprise deployed with AudioCodes IP Phones and 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.
- Zoom Phone System represented by two entities – Zoom BYOC, responsible for connectivity with Enterprise SIP Trunk and Zoom PBX, which is responsible for IP Phones and ATA devices call process.
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using Generic's SIP Trunking service.
- AudioCodes SBC is implemented to interconnect between the AudioCodes IP Phones and ATA devices, the Zoom Phone system and SIP Trunk.
  - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
  - **Border:** IP-to-IP network border - AudioCodes IP Phones and ATA devices located in the Enterprise LAN, the Generic's SIP Trunk and the Zoom Phone systems are located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Layout of an Interoperability Test Environment



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	▪ AudioCodes IP Phones and ATA devices are located on the LAN ▪ Both, Zoom Phone system and Generic SIP Trunk environments are located on the WAN
Signaling Transcoding	▪ Zoom Phone system, IP Phones and ATA devices operate with SIP-over-TLS transport type ▪ Generic SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Zoom Phone system and IP Phones supports OPUS, G.711A-law, G.711U-law and G.722 coders ▪ AudioCodes ATA devices support G.711A-law and G.711U-law coders ▪ Generic SIP Trunk supports G.711A-law, G.711U-law, and G.729 coders
Media Transcoding	▪ Zoom Phone and IP Phones system operates with SRTP media type ▪ Generic SIP Trunk operates with RTP media type

This page is intentionally left blank.

3 Overview

This section provides a description of the SBC operation in normal and survivability modes.

3.1 Normal Mode

In normal mode of operation, the SBC acts as an outbound proxy server for the IP Phone and ATA devices users, by seamlessly and transparently forwarding calls between the IP Phone and ATA devices users at the branch site and the Zoom Phone PBX at datacenter, which handles the call routing process.

During normal mode, the SBC stores information of the IP Phone and ATA devices users (e.g., real phone number). Thus, in effect, not only are the IP Phone and ATA devices users registered with the Zoom Phone PBX at the datacenter, but also with the SBC. The SBC uses the information for classifying incoming calls from IP Phone and ATA devices users as well as for routing calls between IP Phone and ATA devices users during Call Survivability when connectivity with the Zoom datacenter is down.

The figures below illustrate Call flow example scenarios in the SBC solution when operating in normal mode:

Figure 3-1: Normal Mode - Calls between Branch Users

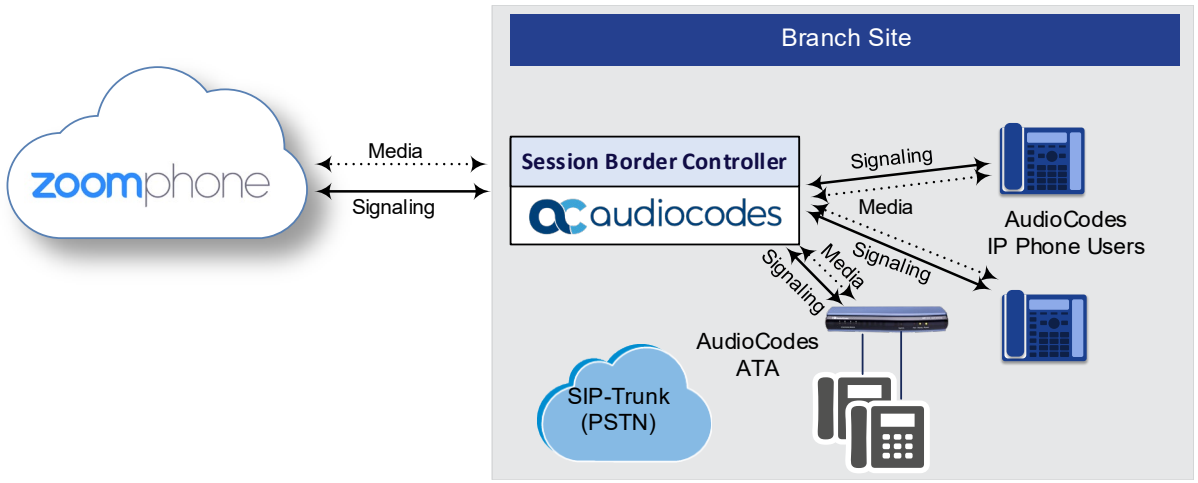
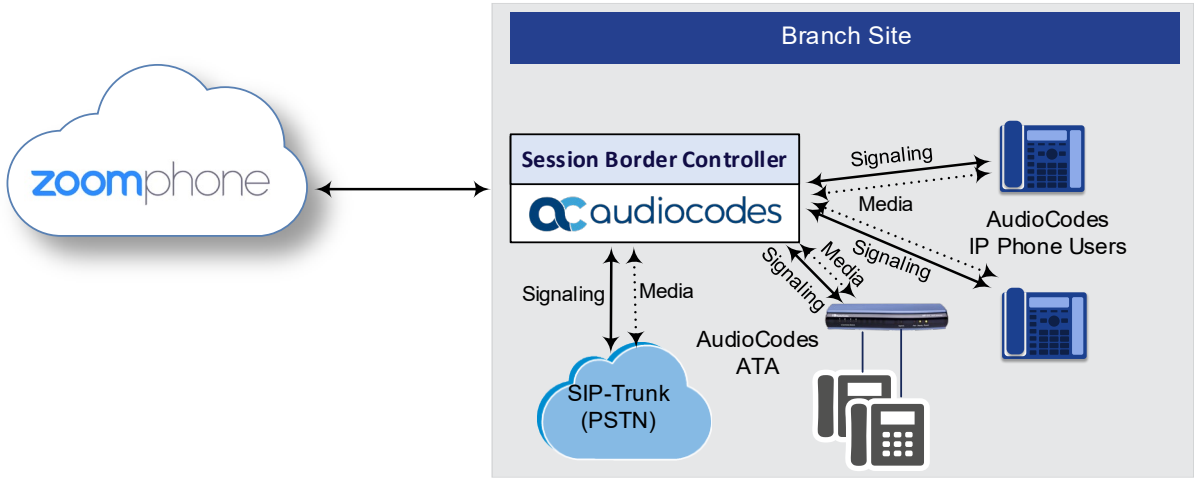


Figure 3-2: Normal Mode - Calls between Branch Users and PSTN (SIP Trunk)



3.2 Survivability Mode

The SBC enters *Survivability* mode of operation upon detection of connectivity loss with the Zoom Phone PBX datacenter. In Survivability mode, the SBC provides voice connectivity at branch level and takes over the handling of call routing for the IP Phone and ATA devices users at the branch site. It enables call routing between the IP Phone and ATA devices users themselves, and between the IP Phone and ATA devices users and other optionally deployed entities such as a SIP Trunk and/or a PSTN network, where users can make and receive calls through the SIP Trunk and/or PSTN respectively.

In survivability mode, the SBC maintains the connection and provides services only to users who have been authorized (registered). However, the SBC also provides services to IP Phone and ATA devices users who are no longer registered due to maintenance reasons (e.g., IP Phone reset or upgrade). In this case, the SBC acts as a Registrar for these users.

The SBC handles call routing based on IP Phone and ATA devices user information that it accumulated during normal operation. It identifies (classifies) incoming calls as received from IP Phone and ATA devices users based on the caller's IP address and routes the call to the destination based on the called telephone number (DID). Only registered IP Phone and ATA devices users are processed; calls from unregistered users are rejected. If the called telephone number is a branch site IP Phone or ATA device user that is registered with the SBC, the call is routed to the IP Phone or ATA device user. If the called telephone number is not listed in the SBC registration database, the call is routed to the PSTN if the setup includes PSTN (SIP Trunk) connectivity; otherwise, the call is rejected.

When the SBC detects that connectivity with the Zoom datacenter has been restored, it exits survivability mode and begins normal operation mode, forwarding calls transparently between the IP Phones and the Zoom datacenter.

Example Call flow scenarios in the SBC solution when in Survivability mode are shown below:

Figure 3-3: Survivability Mode - Calls between Branch Users

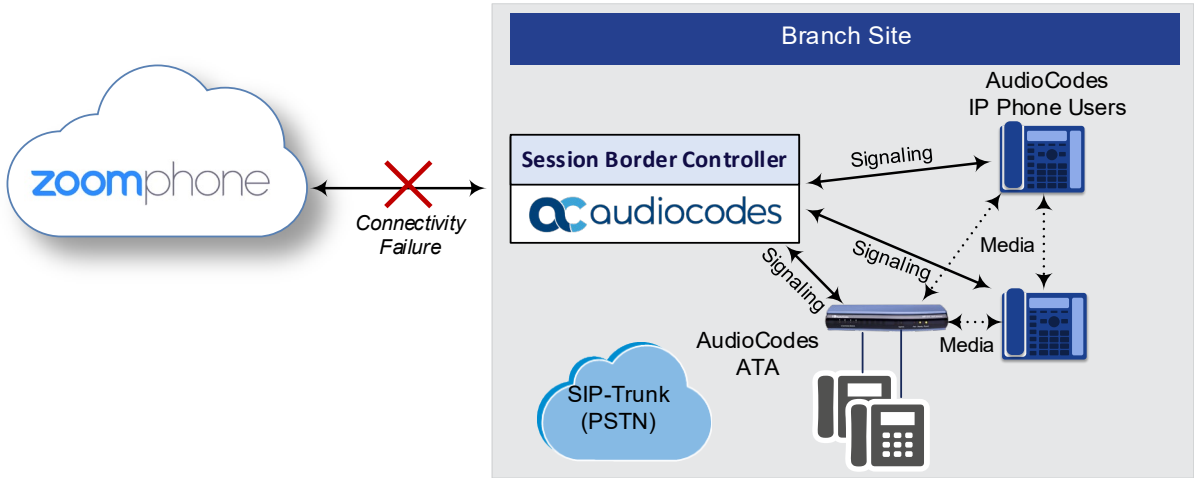
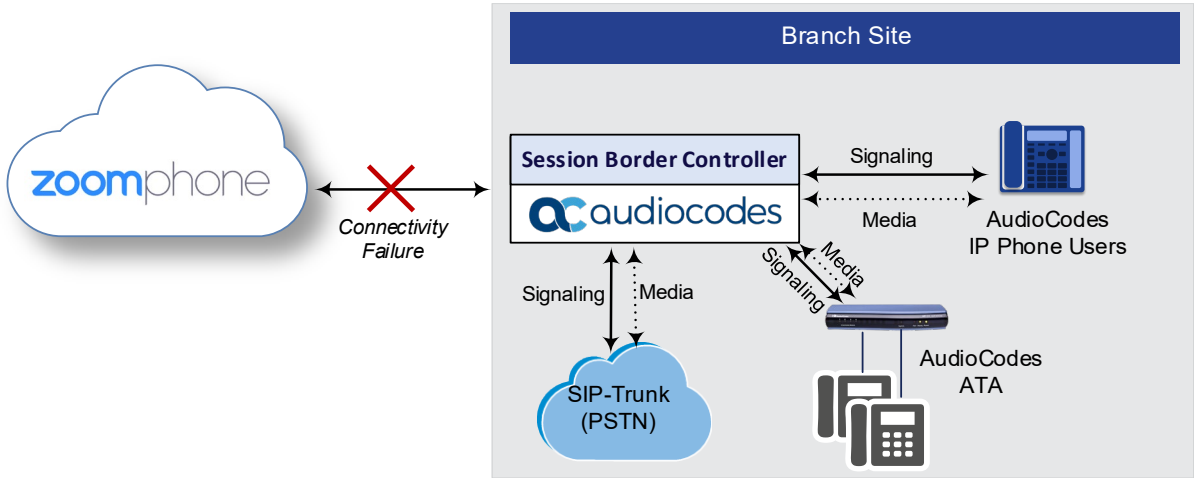


Figure 3-4: Survivability Mode - Calls between Branch Users and PSTN



This page is intentionally left blank.

4 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 SIP groups and set up SIP trunks that are directed toward your SBC 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 carrier.

This page is intentionally marked blank.

5 Configuring AudioCodes SBC

This section shows how to configure AudioCodes SBC for interworking between the Zoom Phone system, the IP Phones and ATA devices users (and Generic SIP Trunk, if required). These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

- SBC LAN interface – AudioCodes IP Phones, ATA devices and Management Station
- SBC WAN interface – Generic SIP Trunking and the Zoom Phone system environment

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

5.1 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 and ATA devices users]
  - √ **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

5.2 Prerequisites

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

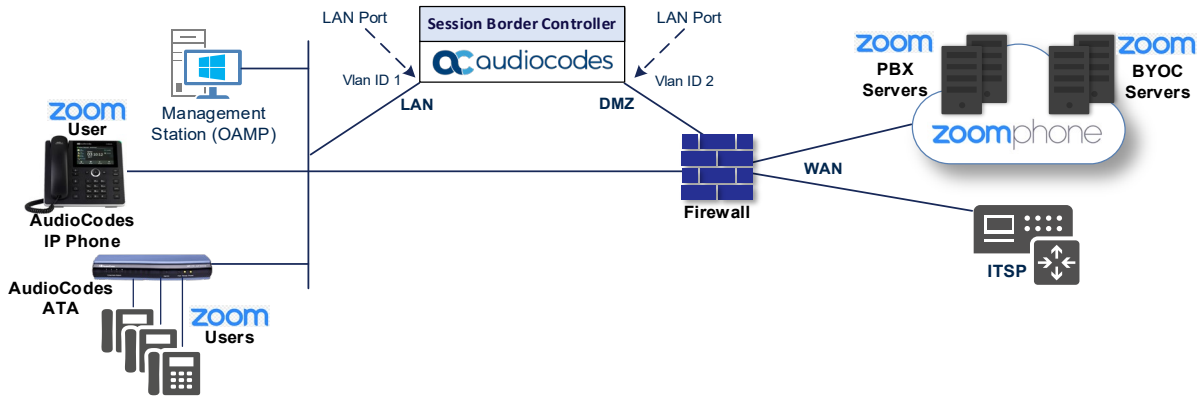
- Public IP address
- Public certificate that is issued by one of the Zoom supported CAs

5.3 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:
  - AudioCodes IP Phones, ATA devices and Management Servers located on the LAN
  - Zoom Phone system and Generic SIP Trunk, 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 5-1: Network Interfaces in Interoperability Test Topology



5.3.1 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.

5.3.2 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	10.15.77.77	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	195.189.192.154 (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

5.4 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 GoDaddy Certificate Chain as Certificate Authority (CA).

5.4.1 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**.

5.4.2 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 GoDaddy 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 5-2: 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.

5.4.3 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 (GoDaddy 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, **sbc.audiocodes.com**).
   b. In the '1st Subject Alternative Name [SAN]' field, change the type to 'DNS' and enter the SBC FQDN name (based on example above, **sbc.audiocodes.com**).
   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.

5.4.4 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 B on page 57)
- Trusted by Zoom Public Root certificates

Currently, Zoom Data Centers (DC) uses DigiCert public CA certificates. Therefore, 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**; 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).

5.5 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, three Media Realms are configured:

- One for the IP interface towards the Zoom Phone System, with the UDP port starting at 10000 and the number of media session legs 100 (you need to calculate number of media session legs based on your usage).
- One for the IP interface towards Generic SIP Trunk, with the UDP port range starting at 6000 and the number of media session legs 100.
- One for the IP interface towards AudioCodes IP Phones and ATA devices, with the UDP port range starting at 7000 and the number of media session legs 100.

➢ **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-Zoom (arbitrary name)	WAN_IF	10000	100 (media sessions assigned with port range)
1	MR-SIPTrunk (arbitrary name)	WAN_IF	6000	100 (media sessions assigned with port range)
2	MR-Zoom-Users (arbitrary name)	LAN_IF	7000	100 (media sessions assigned with port range)
All other parameters can be left unchanged at their default values.				

5.6 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.

Note that the configuration of a SIP interface for the Generic SIP Trunk shows an example and your configuration might be different. For specific configuration of interfaces pointing to SIP trunks and/or a third-party PSTN environment connected to the SBC, see the trunk / environment vendor documentation.

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	Call Setup Rules Set ID	Media Realm	Direct Media
0	**SI-Zoom** (arbitrary name)	**WAN_IF**	**SBC**	**0**	**0**	**5061**	**-**	**MR-Zoom**	**-**
1	**SI-SIPTrunk** (arbitrary name)	**WAN_IF**	**SBC**	**5060** (according to requirement)	**0**	**0**	**-**	**MR-SIPTrunk**	**-**
2	**SI-Zoom-Users** (arbitrary name)	**LAN_IF**	**SBC**	**0**	**0**	**5091**	**0**	**MR-Zoom-Users**	**Enable**
All other parameters can be left unchanged at their default values.									

Notes:

- Make sure that the default TLS Context (certificate) is signed by AudioCodes.
- For enhanced security, AudioCodes recommends implementing a Mutual TLS connection with the Zoom Phone System. For the required configuration, see Section 5.20.3 on page 44.

5.7 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, three Proxy Sets need to be configured for the following IP entities:

- Zoom Phone system
- Generic SIP Trunk
- Zoom PBX

The Proxy Sets will later be applied to the VoIP network by assigning them to IP Groups.

➢ **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 BYOC** (arbitrary name)	SI-Zoom	Zoom[1]	Using Options	503	Homing	Enable
2	**SIPTrunk** (arbitrary name)	SI-SIPTrunk	Default	Using Options	According to SIP Trunk requirement	According to SIP Trunk requirement	According to SIP Trunk requirement
3	**Zoom PBX** (arbitrary name)	SI-Zoom	Zoom[2]	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.

[1] Configured in Section 5.4.
[2] Configured in Section 5.4.

5.7.1 Configure a Proxy Address

This section shows how to configure a Proxy Address.

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

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) click the Proxy Set **Zoom BYOC**, 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 5-6: Configuration Proxy Address for Zoom Phone System

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	us01peer01.am.zoom.us:5061	TLS	0	0
1	us01peer01.fr.zoom.us:5061	TLS	0	0

3. Click **Apply**.

Note: The current example is based on configuration Zoom Europe Data Center's IP address (FQDN). In your implementation, the IP address may be different according to your region. Refer to Appendix A on page 55 for a list of FQDNs / IP addresses of other Zoom Regional Data Centers.

➢ **To configure a Proxy Address for SIP Trunk:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **SIPTrunk**, 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 4-7: Configuration Proxy Address for SIP Trunk

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	SIPTrunk.com:5060 (SIP Trunk IP / FQDN and port)	UDP	0	0

3. Click **Apply**.

➢ **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 5-8: Configuration Proxy Address for Zoom PBX

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	us01sip0g.am.zoom.us:5091 (according to configuration on Zoom Phone System Management Dashboard)	TLS	0	0

3. Click **Apply**.

5.8 Configure Coders

This section describes how to configure coders (termed *Coder Group*). As the Zoom Phone system supports the OPUS and G.722 coders while the network connection to Generic SIP Trunk may restrict operation with other dedicated coders list, you need to add a Coder Group with the supported coders for each leg, the Zoom Phone system and the Generic SIP Trunk.

Note that the Coder Group ID for this entity will be assigned to its corresponding IP Profile in the next step.

➢ **To configure coders:**

1. Open the Coder Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Coder Groups**).
2. From the 'Coder Group Name' dropdown, select **1:Does Not Exist** and add the required codecs as follows:

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
Opus	20	N/A	102	N/A
G.722	20	64	9	Disabled

3. Click **Apply** and confirm the configuration change in the prompt that pops up.

Note: Repeat the same procedure for each Generic SIP Trunk if it's required.

The procedure below describes how to configure Allowed Coders Groups to ensure that voice sent to the Generic SIP Trunk and Zoom Phone system, uses the dedicated coders list whenever possible. Note that the Allowed Coders Group IDs will be assigned to the IP Profiles belonging to the Generic SIP Trunk and Zoom Phone system, in the next step.

➢ **To set a preferred coder for the Generic SIP Trunk:**

1. Open the Allowed Audio Coders Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Audio Coders Groups**).
2. Click **New** and configure a name for the Allowed Audio Coders Group for Generic SIP Trunk (e.g., *SIPTrunk Allowed Coders*).
3. Click **Apply**.
4. Select the new row that you configured, and then click the **Allowed Audio Coders** link located below the table; the Allowed Audio Coders table opens.
5. Click **New** and configure an Allowed Coders as follows:

Index	Coder
0	G.729
1	G.711 U-law
2	G.711 A-law

➢ **To set a preferred coder for the Zoom Phone system:**

1. Open the Allowed Audio Coders Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Audio Coders Groups**).
2. Click **New** and configure a name for the Allowed Audio Coders Group for Generic SIP Trunk (e.g., *Zoom Allowed Coders*).
3. Click **Apply**.
4. Select the new row that you configured, and then click the **Allowed Audio Coders** link located below the table; the Allowed Audio Coders table opens.
5. Click **New** and configure an Allowed Coders as follows:

Index	Coder
0	Opus
1	G.722
2	G.711 U-law
3	G.711 A-law
4	G.729

6. Open the Media Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Settings**).
7. From the '**Extended Coders Behavior**' drop-down list, select **Include Extensions**.
8. Click **Apply**.

5.9 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 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 BYOC interface. Configure the parameters using the table below as reference.

Table 5-9: Configuration Example: Zoom BYOC IP Profile

Parameter	Value
General	
Index	**1**
Name	**Zoom** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Secured**
SBC Media	
Extension Coders Group	**AudioCodersGroups_1**
Allowed Audio Coders	**Zoom Allowed Coders**
Allowed Coders Mode	**Restriction and Preference** (reorder coders according to Allowed Coders including extension coders)
RFC 2833 Mode	**Extend**
SBC Signaling	
Session Expires Mode	**Supported**
SBC Forward and Transfer	
Remote 3xx Mode	**Handle Locally**
All other parameters can be left unchanged with their default values.	

3. Click **Apply**.

➢ **To configure an IP Profile for the Generic SIP Trunk:**

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

Table 5-10: Configuration Example: Generic SIP Trunk IP Profile

Parameter	Value
General	
Index	**2**
Name	**SIPTrunk**
Media Security	
SBC Media Security Mode	**Not Secured**
SBC Media	
Extension Coders Group	**AudioCodersGroups_0**
Allowed Audio Coders	**SIPTrunk Allowed Coders**
Allowed Coders Mode	**Restriction and Preference** (reorder coders according to Allowed Coders including extension coders)
SBC Signaling	
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally**
Remote 3xx Mode	**Handle Locally**
All other parameters can be left unchanged with their default values or configured according to SIP Trunk requirements.	

3. Click **Apply**.

➢ **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 5-11: Configuration Example: Zoom Users IP Profile

Parameter	Value
General	
Index	**3**
Name	**Users** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Secured**
Generate SRTP Keys Mode	**Always**
All other parameters can be left unchanged with their default values.	

3. Click **Apply**.

5.10 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**.

5.11 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 Phone BYOC system
- Generic SIP Trunk
- AudioCodes IP Phones and ATA devices users
- 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 Phone BYOC system:

Parameter	Value
Index	**1**
Name	**Zoom BYOC** (arbitrary descriptive name)
Type	**Server**
Proxy Set	**Zoom BYOC**
IP Profile	**Zoom**
Media Realm	**MR-Zoom**
SIP Group Name	(according to ITSP requirement)
SBC Alternative Routing Reason Set	**503** (created in section 5.10 on page 34)
Proxy Keep-Alive using IP Group settings	**Enable**
All other parameters can be left unchanged with their default values.	

3. Configure an IP Group for the Generic SIP Trunk:

Parameter	Value
Index	**2**
Name	**SIPTrunk** (arbitrary descriptive name)
Type	**Server**
Proxy Set	**SIPTrunk**
IP Profile	**SIPTrunk**
Media Realm	**MR-SIPTrunk**
SIP Group Name	(according to ITSP requirement)
All other parameters can be left unchanged with their default values.	

4. Configure an IP Group for the AudioCodes IP Phones and ATA devices users:

Parameter	Value
Index	**3**
Name	**Users** (arbitrary descriptive name)
Type	**User**
Proxy Set	**-**
IP Profile	**Users**
Media Realm	**MR-Zoom-Users**
Classify By Proxy Set	**Disable**
SIP Group Name	(according to requirement)
All other parameters can be left unchanged with their default values.	

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

Parameter	Value
Index	**4**
Name	**Zoom PBX** (arbitrary descriptive name)
Type	**Server**
Proxy Set	**Zoom PBX**
IP Profile	**Zoom**
Media Realm	**MR-Zoom**
SIP Group Name	(according to ITSP requirement)
All other parameters can be left unchanged with their default values.	

5.12 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**.

5.13 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 IP-to-IP routing rules in the IP-to-IP Routing table.

The following condition verifies that the User-Agent header contains string, which define AudioCodes IP Phone or ATA device.

➢ **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 the parameters as follows:

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

3. Click **Apply**.

5.14 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	**Zoom Users**
Source SIP Interface	**SI-Zoom-Users**
Message Condition	**AUDC-Users**
Action Type	**Allow**
Source IP Group	**Users**

3. Click **Apply**.

5.15 Configure the Dial Plan Table (Users DIDs)

For proper work in survivability mode (as described in Section 3.2 on page 14) SBC need to know the real DID numbers of the IP Phones and ATA devices users, because during users registration on the Zoom portal, IP Phone and ATA device users receive some unique Zoom ID, but not DID number. When IP Phones and ATA devices work in normal mode, Zoom PBX responsible for routing (converting this unique number to DID and vice versa). But in the survivability mode, SBC responsible for that. That's why it's required to know the real DIDs.

Note: Information about unique Zoom IDs and real DIDs of the users need to be obtain from the Zoom for proper implementation. Currently this should be done manually, but AudioCodes working on solution to automate this process.

The Dial Plan (e.g., DIDs) will be configured with a real DID as tag per Zoom unique ID of each user as a prefix.

➢ **To configure Dial Plans:**

1. Open the Dial Plan table (**Setup** menu > **Signaling & Media** tab **> SIP Definitions** folder > **Dial Plan**).
2. Click **New** and then configure a Dial Plan name (e.g., DIDs) according to the parameters described in the table below.
3. Click **Apply**.
4. In the Dial Plan table, select the row for which you want to configure dial plan rules and then click the **Dial Plan Rule** link located below the table; the Dial Plan Rule table appears.
5. Click **New,** and then configure a dial plan rule according to the parameters described in the table below.

Table 5-12: Example of the Dial Plan – Real DIDs per Zoom unique IDs

Index	Name	Prefix	Tag
0	User 1 Name (arbitrary name)	79732789373099396442	97234561000 (real DID)
1	User 2 Name (arbitrary name)	57952615652163521256	97234562000 (real DID)
2	User 3 Name (arbitrary name)	82709763648869671978	97234565000 (real DID)

6. Click **Apply,** and then save your settings to flash memory.

5.16 Configure Call Setup Rules

This section describes how to configure Call Setup Rules based on real DIDs and Zoom unique IDs (Dial Plan). Call Setup rules define various sequences that are run upon receipt of an incoming call (dialog) at call setup before the device routes the call to its destination.

Configured Call Setup Rules need be assigned to a Zoom Users SIP Interface to operate before message entered to classification process.

➢ **To configure a Call Setup Rules based on customer DID range (Dial Plan):**

1. Open the Call Setup Rules table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Call Setup Rules**).
2. Click **New** and configure Call Setup rules according to the parameters described in the table below.

Table 5-13: Call Setup Rules Table

Index	Name	Rules Set ID	Request Type	Request Target	Request Key	Condition	Action Subject	Action Type	Action Value
0	Get Zoom ID	0					Var.Session.ZoomID	Modify	Header.From .URL.User
1	Change AOR User to DID	0	Dial Plan	DIDs	Var.Session. ZoomID	DialPlan.Found exists	Header.To.URL.User	Modify	'+'+DialPlan. Result

3. Click **Apply** and then save your settings to flash memory.

Rule Index	Description
0	For messages, received from the IP Phones or ATA devices, the value of the user part of the SIP From Header is assigned to the 'ZoomID' session variable, which will be used for query Dial Plan.
1	For messages, received from the IP Phones or ATA devices, the Dial Plan is queried according to the 'ZoomID' session variable. The Tag value from the matched row (that is real DID) will be assigned as user part of the SIP To header and will be added as **Address Of Record** to the SBC internal database.

5.17 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 and Generic SIP Trunk:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity.
- Calls from Branch Users to Zoom Phone PBX.
- Alternative Route from Branch Users back to Branch Users for inter-branch calls in Survivability mode.
- Alternative Route from Branch Users to SIP Trunk for calls outside branch in Survivability mode.
- Calls from Zoom Phone PBX to Branch Users.
- Calls from Generic SIP Trunk to Zoom Phone BYOC system.
- Alternative Route from Generic SIP Trunk to Branch Users for inter-branch calls in Survivability mode.
- Calls from Zoom Phone BYOC system to Generic SIP Trunk.

➢ **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 4-14: Configuration IP-to-IP Routing Rules

Index	Name	Alternative Route Options	Source IP Group	Request Type	Dest Type	Dest Username Pattern	Dest IP Group	Internal Action
0	Terminate OPTIONS		Any	OPTIONS	Internal			Reply(Response='200')
1	From Users		Users	All	IP Group		Zoom PBX	
2	Alternative Route Options	Alternative Route Ignore Inputs	Users	All		+9723456	All Users	
3	Resiliency to SIP Trunk	Alternative Route Ignore Inputs	Users	All	IP Group		SIPTrunk	
4	To Users		Zoom PBX	All	IP Group		Users	
5	SIPTrunk to Zoom		SIPTrunk	All	IP Group		Zoom BYOC	
6	Resiliency to Users	Alternative Route Ignore Inputs	SIPTrunk	All	IP Group	+9723456	Users	
7	Zoom to SIPTrunk		Zoom BYOC	All	IP Group		SIPTrunk	

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

5.18 Configure Number Manipulation Rules

This section describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 5.11 on page 29) to denote the source and destination of the call.

Note: Adapt the manipulation table according to your environment dial plan.

For example, for this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number (if it not exists) for calls to the Generic SIP Trunk IP Group for any destination username pattern.

➢ **To configure a number manipulation rule:**

1. Open the Outbound Manipulations table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Outbound Manipulations**).
2. Configure the rules according to your setup.

The table below shows an example of configured IP-to-IP outbound manipulation rules for calls between to the Generic SIP Trunk IP Group:

Rule Index	Description
0	Calls to the SIP Trunk IP Group with any destination number between 1 to 9, add "+" to the prefix of the destination number.

5.19 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 BYOC:**

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 BYOC IP Group. This rule applies to OPTIONS messages sent to the Zoom BYOC IP Group. This replaces the host part of the SIP Request-URI Header with the destination (Zoom BYOC Phone System Server) IP address.

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 1) for Zoom BYOC IP Group. This rule applies to messages received from the Zoom BYOC IP Group. This rule performs normalization of the messages received from Zoom BYOC Phone System.

Parameter	Value
Index	**1**
Name	**Normalization**
Manipulation Set ID	**1**
Message Type	**Any.Request**
Action Subject	**Message**
Action Type	**Normalize**

4. Configure another manipulation rule (Manipulation Set 4) for Zoom PBX IP Group. This rule applies to Register request messages sent to the Zoom PBX IP Group. This replaces the user part of the SIP To Header with the value from SIP From Header. This required for correct registration of the Branch Users in normal mode.

Parameter	Value
Index	**2**
Name	**Change To Header Back**
Manipulation Set ID	**4**
Message Type	**Register.Request**
Action Subject	**Header.To.URL.User**
Action Type	**Modify**
Action Value	**Header.From.URL.User**

5. Assign Manipulation Set IDs 1 and 2 to the Zoom BYOC 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 BYOC IP Group, and then click **Edit**.
   c. Set the 'Inbound Message Manipulation Set' field to **1**.
   d. Set the 'Outbound Message Manipulation Set' field to **2**.
   e. Click **Apply**.
6. Assign Manipulation Set ID 4 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 **4**.
   d. Click **Apply**.

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

5.20 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

5.20.1 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 the **Keep user without unique identifier** option.
3. Click **Apply**.

5.20.2 Configuring the SBC to Reuse the Same TLS Connection

This section describes how to configure the SBC to reuse the same TLS connection for a session with the same user (IP phone or ATA device).

➢ **To configure the SBC to reuse the same TLS connection:**

1. Open the SBC Transport Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Transport Settings**).
2. From the '**Fake TCP alias**' drop-down list, select **Enable**.
3. Click **Apply**.

5.20.3 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 CA.
4. Make sure that CA certificates are imported into the Trusted Root Certificates table.

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**.

5.20.4 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.

This page is intentionally left blank.

6 Configuring AudioCodes IP Phones

This section describes how to configure IP Phones to work with SBC as Outbound Proxy. The table below describes the parameters that must be configured on the IP Phone. Parameters enclosed with square brackets […] denote the parameters of the Configuration file; Parameters not enclosed denote the corresponding Web interface parameters.

Table 6-1: Parameter Settings of IP Phones for work with SBC

Parameter	Settings
Use SIP Outbound Proxy [voip/signalling/sip/sip_outbound_proxy/enabled]	Enables the use of an outbound proxy server (i.e., the SBC) for sending SIP messages. Set the parameter to **[1]** Enable.
Outbound Proxy IP Address or Host Name [voip/signalling/sip/sip_outbound_proxy/addr]	Defines the IP address of the outbound proxy (i.e., SBC). All outgoing SIP messages are sent to this proxy. Set the parameter to the LAN IP address of the SBC.
Registration Expires [voip/signalling/sip/proxy_timeout]	The SIP proxy server registration timeout (in seconds). Set the parameter to **[60]** for decreasing re-registration.

6.1.1 Enable Web Interface on IP Phones

For configuring IP Phones through their web interface, it should be enabled, because default Zoom provisioning disables using the web interface of IP Phones. To do this, a new provisioning template must be created and assigned to all IP Phones.

➢ **To configure the phone provisioning template for enabling Web interface:**

1. Sign-in to the Zoom web portal.
2. In the navigation panel, click **Phone System Management** then **Company Info**.
3. Click **Account Settings**.
4. In the Desk Phone section, click **Manage** under **Provision Template**.
5. Click **Add**.
6. Enter the following:
   - **Name**: Enter a display name to identify the template. (e.g., **EnableWeb**)
   - **Description** (optional): Enter a description to help you identify the template.
   - **Template**: Enter following configuration rows:

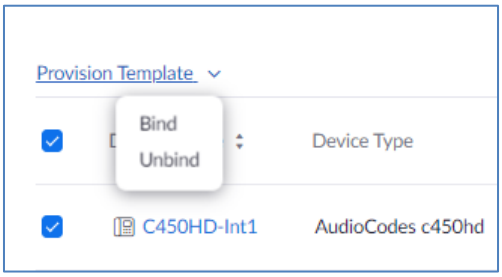
```
system/password=$1$FZ6rOGS1$54ZXSmjh7nod.kXFRyLx70
system/web/enabled=1
```

After creating provisioning template, assigned it to all IP Phones.

➢ **To assign provisioning template to the phones located in the same site:**

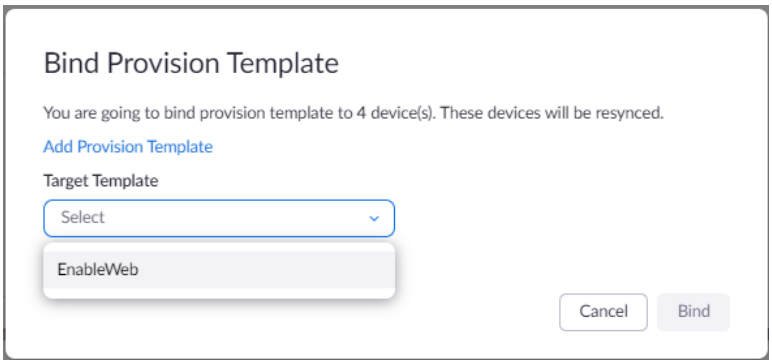
1. Sign in to the Zoom web portal.
2. In the navigation panel, click **Phone System Management** then **Phones & Devices**.
3. In the **Site** drop-down menu located at the top-right area, select a site to view associated desk phones.
4. Click the check box in the first column of the header row to select all desk phones listed.
5. In the **Provision Template** drop-down menu, select **Bind**.

Figure 6-1: Provision Template Bind



6. In the **Target Template** drop-down menu, select the template, created in the previous step, then click **Bind**.

Figure 6-2: Add Provision Template



7. Re-sync the desk phones to finish assigning the provision template.

Note: For a detailed explanation about the provisioning template please refer to Zoom Help Center at *Configuring desk phone provision templates*.

6.1.2 Configuring IP Phones through Web Interface

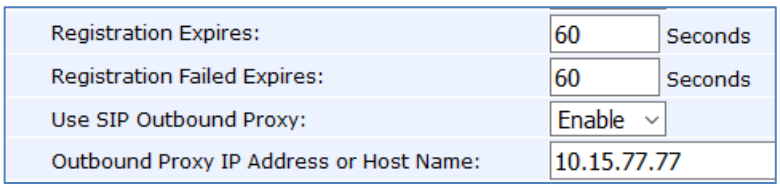
For configuring IP Phones with SBC as Outbound Proxy you need to perform the following procedure on **each** IP Phone.

Note: Perform this configuration **only after** the IP Phone user has signed in to (registered with) Zoom.

➢ **To configure the IP Phone through Web interface:**

1. Open the Signaling Protocol page (**Configuration** tab > **Voice Over IP** menu > **Signaling Protocols**), and then scroll down to the SIP Proxy and Registrar group:

Figure 6-3: Configuring SBC on the IP Phone through Web Interface



2. Configure the parameters according to the instructions above (decrease re-registration timeout, enable use SBC as Outbound Proxy and enter SBC LAN IP address as Outbound Proxy IP address).
3. Click **Submit** to apply your settings.

You can also configure the IP Phone by manually loading a Configuration file (.cfg) through the Web interface:

1. Create a Configuration file that contains the following parameter settings:

```
voip/signalling/sip/proxy_timeout=60
voip/signalling/sip/sip_outbound_proxy/enabled=1
voip/signalling/sip/sip_outbound_proxy/addr=10.15.77.77
```

2. Open the Configuration File page (**Management** tab > **Manual Update** menu > **Configuration File**).
3. Load the Configuration file, by clicking **Loading New Configuration File**.

This page is intentionally left blank.

7 Configuring MP-1xx ATA Devices

This section describes how to configure AudioCodes' MediaPack ATA devices to interoperate with an SBC as Outbound Proxy. To do this, the ATA device must be configured to send all calls to the AudioCodes SBC.

The MP-1xx (MediaPack) ATA device must be configured in the Zoom web portal. Proceed according to the following setup guide: https://assets.zoom.us/docs/zoom-phone/Setting-an-AudioCodes-MediaPack-Series-ATAs.pdf

For more information on MP-1xx Assisted Provisioning, see:

https://support.zoom.us/hc/en-us/articles/360055113731-Setting-up-an-AudioCodes-MediaPack-MP-11x-124-1288-series-ATA

7.1 Configuring SBC as Proxy Server via Zoom Portal

A new provisioning template must be created and assigned to the MP-1xx ATA device. The configuration below uses the example of an ATA device registered to the SBC device (10.15.77.77)

➢ **To create the provisioning template for ATA devices in resiliency mode:**

1. Sign-in to the Zoom web portal.
2. In the navigation panel, click **Phone System Management** then **Company Info**.
3. Click **Account Settings**.
4. In the Desk Phone section, click **Manage** under **Provision Template**.
5. Click **Add**.
6. Enter the following:
   - **Name**: Enter a display name to identify the template. (e.g., **MP-in-Resiliency**)
   - **Description** (optional): Enter a description to help you identify the template.
   - **Template**: Enter following configuration rows:

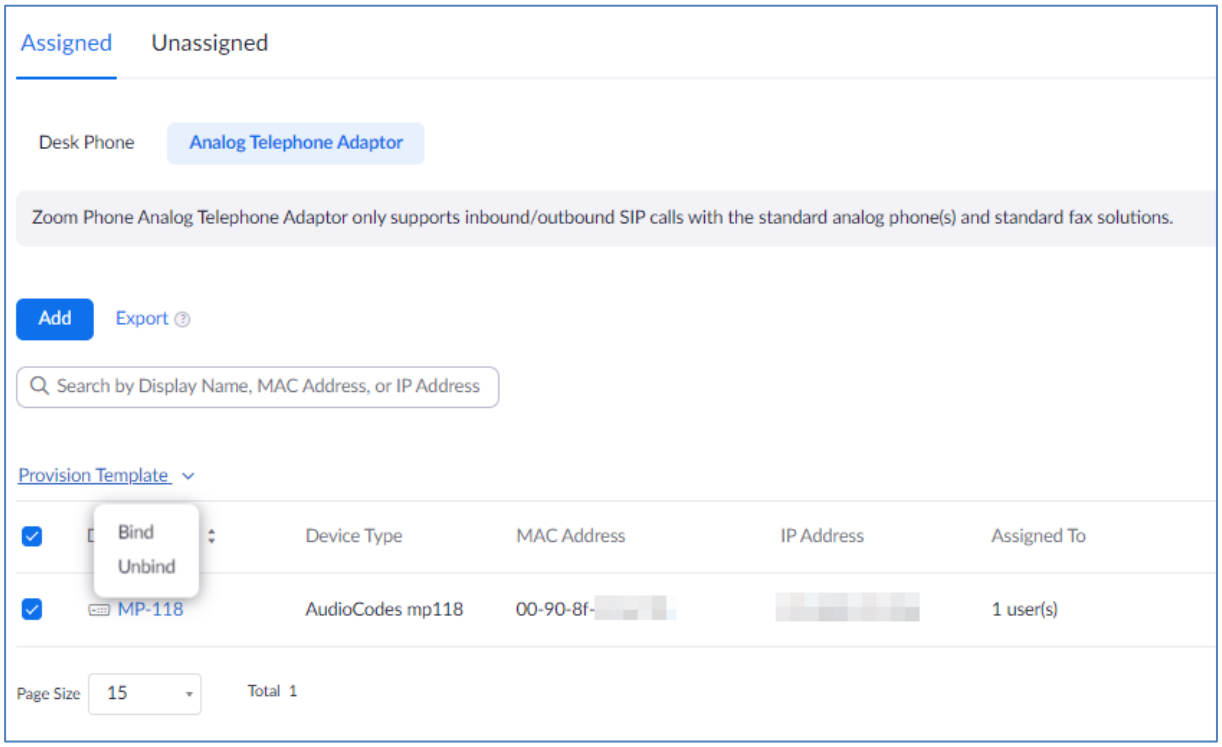
```
[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress,
ProxyIp_TransportType, ProxyIp_ProxySetId;
ProxyIp 0 = "10.15.77.77:5091", 2, 0;

[ \ProxyIp ]
```

After creating provisioning template, assign it to the ATA device.

➢ **To assign a provision template to the ATA devices:**

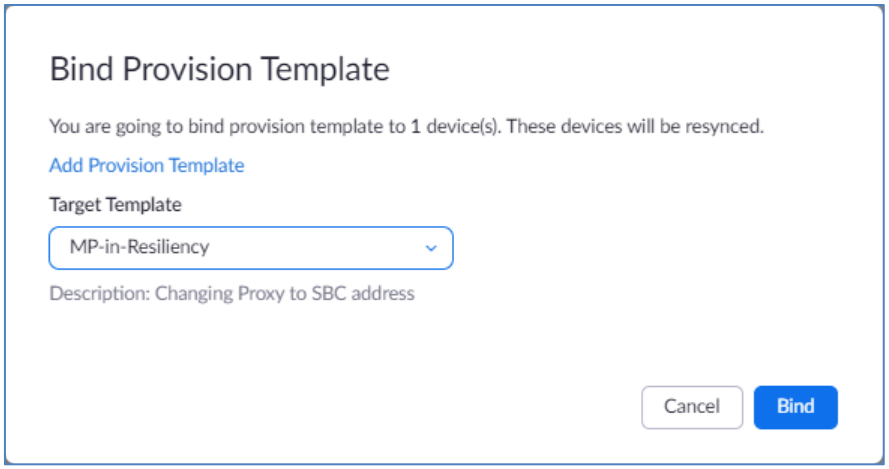
1. Sign-in to the Zoom web portal.
2. In the navigation panel, click **Phone System Management** and then **Phones & Devices**.
3. Choose **Analog Telephone Adaptor** and in the **Site** drop-down menu located at the top-right area, select a site to view associated ATA devices.
4. Click the check box in the first column of the header row to select all ATA devices listed.
5. In the **Provision Template** drop-down menu, select **Bind**.

Figure 7-1: Provision Template Bind



6. In the **Target Template** drop-down menu, select the template, created in the previous step, then click **Bind**.

Figure 7-2: Add Provision Template



7. Re-sync the ATA device to finish assigning the provision template.

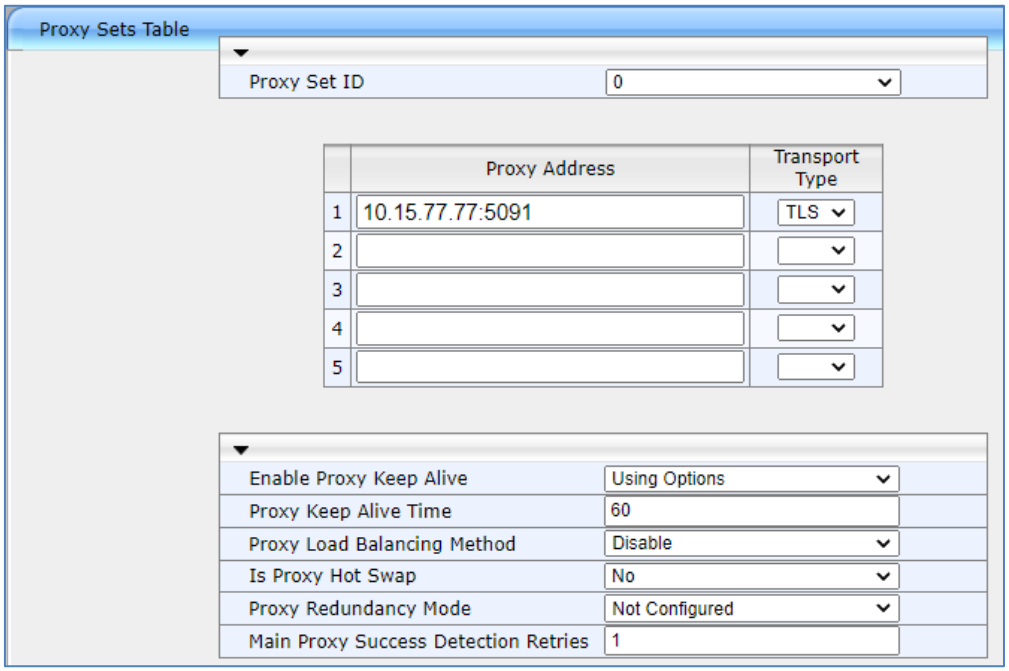
7.2 Configuring an SBC as Proxy Server via MP-1xx Web Interface

This section describes how to configure an SBC as the proxy server of the MP-1xx ATA device via MediaPack's embedded Web interface. The configuration below uses the example of an ATA device registered to the SBC device (10.15.77.77).

➢ **To configure Proxy Server:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **Proxy Sets Table**).

Figure 7-3: Proxy Sets Table



2. In the 'Proxy Address' field, enter the SBC IP address (10.15.77.77 in our example) instead of the address of the Zoom server.
3. Click the **Submit** button.

Note: For detailed information about the configuration of the MediaPack MP-1xx Series, refer to the device's *User's Manual*: https://www.audiocodes.com/library/technical-documents?query=MP-11x

This page is intentionally left blank.

A Zoom Data Centers

Connectivity to the Zoom Phone System signaling via Fully Qualified Domain Names (FQDN) depends on the geographical location of the customer SBC(s) and the corresponding Zoom Data Center that the customer would like to send and receive traffic. Zoom Phone System options are currently available in four separate regions across the globe: North America, Europe, APAC, and Australia.

Table A-1: Regional instances resolve to the following IP addresses

Region	Traffic Type	Protocol	Ports	A Record	IP Address
North America	Signaling	TCP/TLS	5061	us01peer01.sc.zoom.us	162.12.233.59
	Signaling	TCP/TLS	5061	us01peer01.ny.zoom.us	162.12.232.59
	Signaling	TCP/TLS	5061	us01peer01.dv.zoom.us	162.12.235.85
EMEA	Signaling	TCP/TLS	5061	us01peer01.am.zoom.us	213.19.144.198
	Signaling	TCP/TLS	5061	us01peer01.fr.zoom.us	213.244.140.198
Australia	Signaling	TCP/TLS	5061	us01peer01.sy.zoom.us	103.122.166.248
	Signaling	TCP/TLS	5061	us01peer01.me.zoom.us	103.122.167.248
APAC	Signaling	TCP/TLS	5061	us01peer01.hk.zoom.us	209.9.211.198
	Signaling	TCP/TLS	5061	us01peer01.ty.zoom.us	207.226.132.198
South America	Signaling	TCP/TLS	5061	us01peer01.sp.zoom.us	64.211.144.247

Table A-2: Regional Media Traffic and Ports

Region	Traffic Type	Protocol	Ports	Destination
North America	Media	UDP/SRTP	20000-64000	162.12.232.0/22
EMEA	Media	UDP/SRTP	20000-64000	213.19.144.0/24
	Media	UDP/SRTP	20000-64000	213.244.140.0/24
Australia	Media	UDP/SRTP	20000-64000	103.122.166.0/23
APAC	Media	UDP/SRTP	20000-64000	209.9.211.0/24
	Media	UDP/SRTP	20000-64000	207.226.132.0/24

This page is intentionally left blank.

B Zoom Public Trusted Certificate List

The following table lists the Zoom Public Trusted Certificates.

Table B-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-29357