Configuration Note

AudioCodes Professional Services – Interoperability Lab

Connecting Zoom Phone Premise Peering with AudioCodes SBC

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: November-23-2023

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
29330	Initial document release for Version 7.2.
29331	Updates for the latest security recommendations from Zoom.
29332	Updated Configuring AudioCodes SBC; Optimizing CPU Cores Usage for a Specific Service.
29333	Updates related to new Zoom trusted public certificates.
29334	Update related to certificates, used for connection to Zoom Data Centers and fix IP to IP routing rule for OPTIONS.
29336	Update Zoom Proxy Set and IP Group configuration for trigger switch to another DC upon receiving 503 error from primary DC.
29337	Update for Version 7.40A.250 and removed screenshots.
29338	Fixing typos and re-formatting.
29339	TLS Private Key size of 1024 was removed.
29402	Updates related to new Zoom trusted public certificates.

Documentation Feedback

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

1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (hereafter, referred to as *SBC*) for interworking between Audiocodes SIP Trunk and the Zoom Phone Premise Peering (formally referred to as Bring Your Own Carrier - BYOC) environment.

You can also use 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 AudioCodes Web site at https://www.audiocodes.com/partners/sbc-interoperability-list.

1.1 About the Zoom Phone System

Zoom Phone is a fully featured cloud PBX designed with security, reliability, scalability and centralized management. Zoom Phone was built from the ground up to seamlessly integrate with the Zoom Collaboration platform to deliver a feature-rich Unified communications as a service (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 require additional functionality for global support or migration strategies. For organizations with such diverse requirements for 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 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.

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. It allows for the creation of purpose-built multiservice appliances, provides 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.

2 Environment Information

This section describes the interoperability test environment.

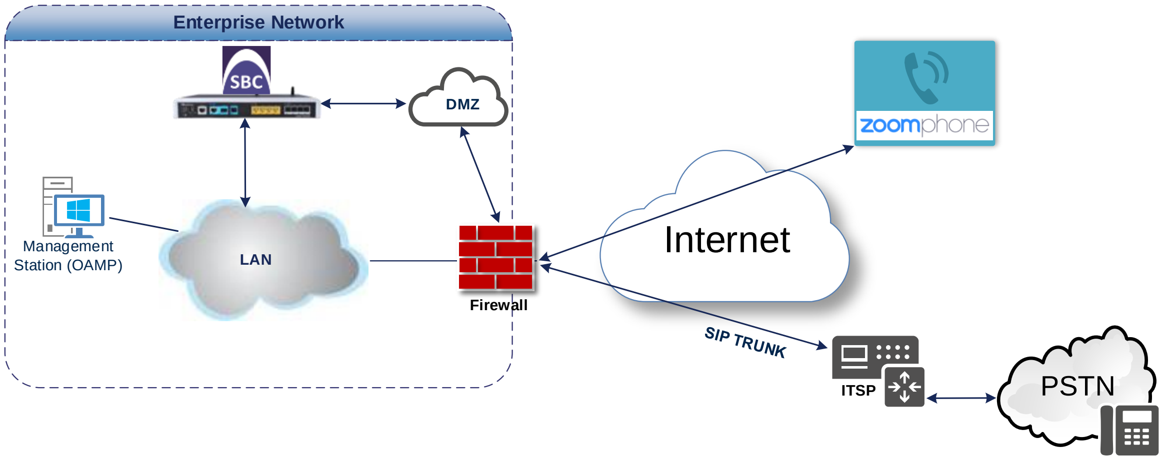
2.1 Interoperability Test Topology

The interoperability testing between AudioCodes SBC and Audiocodes SIP Trunk with the Zoom Phone system was done using the following topology setup:

- Enterprise deployed with third-party 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.
- Enterprise offers its employees enterprise-voice capabilities and the ability to connect the Enterprise to the PSTN network using Audiocodes's SIP Trunking service.
- AudioCodes SBC is implemented to interconnect between the SIP Trunk and the Zoom Phone system.
  - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
  - **Border:** IP-to-IP network border - The Audiocodes's SIP Trunk is located in the Enterprise WAN and the Zoom Phone system is located in the public network.

The figure below illustrates this interoperability test topology:

Figure 1: Layout of an Interoperability Test Environment



2.1.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 1: Environment Setup

Area	Setup
Network	■ Both, Zoom Phone system and Audiocodes SIP Trunk environments are located on the WAN.
Signaling Transcoding	■ Zoom Phone system operates with SIP-over-TLS transport type. ■ Audiocodes SIP Trunk operates with SIP-over-UDP transport type.
Codecs Transcoding	■ Zoom Phone system supports OPUS, G.711A-law, G.711U-law and G.722 coders. ■ Audiocodes SIP Trunk supports G.711A-law, G.711U-law, and G.729 coders.
Media Transcoding	■ Zoom Phone system operates with SRTP media type. ■ Audiocodes SIP Trunk operates with RTP media type.

2.1.2 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes SBC interworking between the Zoom Phone system and Audiocodes's SIP Trunk.

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-.

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 is done by the customer and not by the carrier.

4 Configuring AudioCodes SBC

This section describes how to configure AudioCodes SBC for interworking between the Zoom Phone system and the Audiocodes SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.1 on page 2, and includes the following main areas:

- SBC LAN interface - Management Station
- SBC WAN interface - Audiocodes SIP Trunking and the Zoom Phone system environment

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

4.1 Validating 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.

- For implementing the Zoom Phone system and Audiocodes 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]
  - **DSP Channels** [If media transcoding is needed]
  - **Transcoding sessions** [If media transcoding is needed]
  - **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 the 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 on the AudioCodes website.

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:

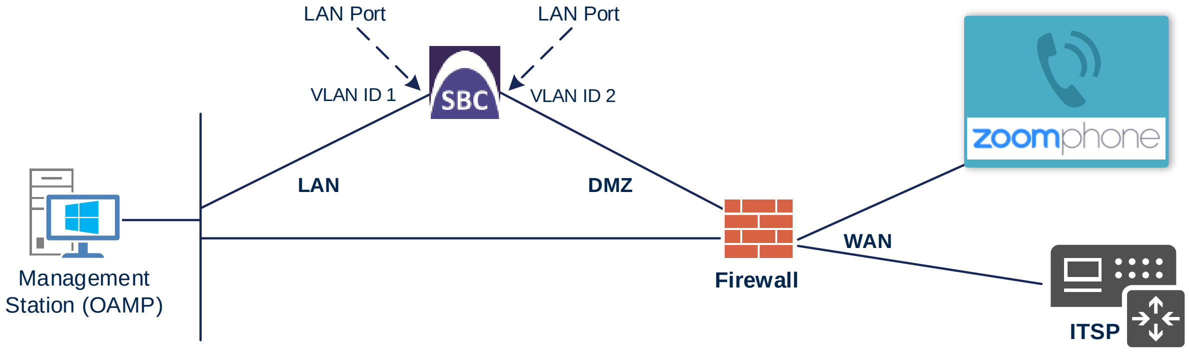
- Public IP address
- Public certificate that is issued by one of the Zoom supported CAs

4.3 Configuring 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:
  - Management Servers located on the LAN
  - Zoom Phone system and Audiocodes 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 2: Network Interfaces in Interoperability Test Topology



4.3.1 Configuring 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 is 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 Configuring 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 2: 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	195.189.192.157 (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 Configuring 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 procedure involves the following main steps:

- Configuring the NTP Server Address.
- Creating a TLS Context for Zoom Phone System.
- Generating a CSR and Obtaining the Certificate from a Supported CA.
- Deploying the SBC Signed and Trusted by Zoom Root Certificates.

4.4.1 Configuring 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 is 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 Creating a TLS Context for Zoom Phone System

The section describes how to request a certificate for the SBC WAN interface and configure it is 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.

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 3: 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 Generating a CSR and Obtaining the Certificate from a Supported CA

This section describes how to generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority.

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. Fill in the rest of the request fields according to your security provider's instructions.
   d. 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 Deploying the SBC Signed and Trusted by Zoom Root Certificates

After obtaining the SBC signed certificate from the CA, download 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 27)
- Trusted by Zoom Public Root certificates

Currently, Zoom Data Centers (DC) uses DigiCert public CA certificates. Zoom is currently in the process of transitioning root certificate to **DigiCert Global Root G2** and **DigiCert TLS RSA4096 Root G5** certificate, which begins after December 1st, 2023. Therefore, to establish a TLS connection with Zoom Phone infrastructure, download and install as trusted root following public CA certificates:

- https://cacerts.digicert.com/DigiCertGlobalRootG2.crt.pem
- https://cacerts.digicert.com/DigiCertTLSRSA4096RootG5.crt.pem
- https://cacerts.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-1.crt.pem
- https://cacerts.digicert.com/DigiCertG5TLSRSA4096SHA3842021CA1-1.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 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.

> 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 Configuring 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 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 Audiocodes SIP Trunk, with the UDP port range starting at 6000 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: 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)
All other parameters can be left unchanged at their default values.				

4.6 Configuring SIP Signaling Interfaces

This section describes 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 this configuration of a SIP interface for the Generic SIP Trunk is a configuration 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 is a configuration example. You can change some parameters according to your requirements.

Table 5: Configured SIP Interfaces in SIP Interface Table

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Media Realm
0	**SIPInterface_Zoom** (arbitrary name)	**WAN_IF**	**SBC**	**0**	**0**	**5061** (according to requirement)	**MR-Zoom**
1	**SIPInterface_SIPTrunk** (arbitrary name)	**WAN_IF**	**SBC**	**5060** (according to requirement)	**0**	**0**	**MR-SIPTrunk**
All other parameters can be left unchanged at their default values.							

For enhanced security, AudioCodes recommends implementing a Mutual TLS connection with the Zoom Phone System. For required configuration, see section 4.18.1 on page 25.

4.7 Configuring 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, two Proxy Sets need to be configured for the following IP entities:

- Zoom Phone system
- Audiocodes SIP Trunk

The Proxy Sets is later 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 6: 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)	SIPInterface_Zoom	Zoom[1]	Using Options	503	Homing	Enable
2	**SIPTrunk** (arbitrary name)	SIPInterface_SIPTrunk	Default	Using Options	According to SIP Trunk requirement	According to SIP Trunk requirement	According to SIP Trunk requirement

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 4.4.

4.7.1 Configuring a Proxy Address

This section describes how to configure a Proxy Address.

To configure a Proxy Address for Zoom:

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 7: 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**.

> This 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 26 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 8: 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**.

4.8 Configuring Coders

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

Note that the Coder Group ID for this entity is 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.

> 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 Audiocodes SIP Trunk and Zoom Phone system, uses the dedicated coders list whenever possible. Note that the Allowed Coders Group IDs are assigned to the IP Profiles belonging to the Audiocodes SIP Trunk and Zoom Phone system, in the next step.

To set a preferred coder for the Audiocodes 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 then configure a name for the Allowed Audio Coders Group for Audiocodes 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 then configure a name for the Allowed Audio Coders Group for Zoom Phone system (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**.

4.9 Configuring 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 Phone System interface. Configure the parameters using the table below as reference.

Table 9: Configuration Example: Zoom 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**
All other parameters can be left unchanged with their default values.	

3. Click **Apply**.

To configure an IP Profile for the Audiocodes 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 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_2**
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)

3. Click **Apply**.

4.10 Configuring 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 Zoom 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**.

4.11 Configuring 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 system
- Audiocodes SIP Trunk

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 system:

Parameter	Value
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 4.10 on page 18)
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 Audiocodes SIP Trunk:

Parameter	Value
Index	**1**
Name	**SIPTrunk** (arbitrary descriptive name)
Type	**Server**
Proxy Set	**SIPTrunk**
IP Profile	**SIPTrunk**
Media Realm	**MR-SIPTrunk**
SIP Group Name	(according to ITSP requirement)

4.12 Configuring SRTP

This section describes how to configure media security. The Zoom Phone System Interface requires the SRTP, 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**.

4.13 Configuring 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 Audiocodes SIP Trunk:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity
- Calls from Zoom Phone system to Audiocodes SIP Trunk
- Calls from Audiocodes SIP Trunk to Zoom Phone system

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 11: 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	Internal		Reply(Response='200')
1	Zoom to ITSP (arbitrary name)	Zoom BYOC		IP Group	SIPTrunk	
2	ITSP to Zoom (arbitrary name)	SIPTrunk		IP Group	Zoom BYOC	

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

4.14 Configuring 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 4.11 on page 19) to denote the source and destination of the call.

Adapt the manipulation table according to your environment dial plan.

For example, for this interoperability test topology, a manipulation is configured to add the "+1" (plus sign) to the destination number (if it does not exists) for calls from the Audiocodes SIP Trunk IP Group to the Zoom Phone system 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 the Zoom Phone system IP Group and Audiocodes SIP Trunk IP Group:

Rule Index	Description
0	Calls from SIP Trunk IP Group to Zoom IP Group with the prefix destination number "+1", do nothing.
1	Calls from SIP Trunk IP Group to Zoom IP Group with any destination number between 2 to 9, add "+1" to the prefix of the destination number.

4.15 Configuring 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:

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 IP Group. This rule applies to OPTIONS messages sent to the Zoom IP Group. This replaces the host part of the SIP Request-URI Header with the destination (Zoom 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 IP Group. This rule applies to messages received from the Zoom IP Group. This rule performs normalization of the messages received from Zoom Phone System.

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

4. Assign Manipulation Set IDs 1 and 2 to the Zoom 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 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**.

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.

4.16 Configuring Registration Accounts (Optional)

This section describes how to configure SIP registration accounts. This is required so that the SBC can register with the Audiocodes SIP Trunk on behalf of the Zoom Phone system. The Audiocodes SIP Trunk requires registration and authentication to provide service.

In the interoperability test topology, the Served IP Group is Zoom Phone system IP Group and the Serving IP Group is Audiocodes SIP Trunk IP Group.

Configure Registration Account only if this is required by SIP Trunk.

To configure a registration account:

1. Open the Accounts table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**).
2. Click **New**.
3. Configure the account according to the provided information, for example:

Parameter	Value
Served IP Group	**Zoom**
Application Type	**SBC**
Serving IP Group	**SIPTrunk**
Host Name	As provided by the SIP Trunk provider
Register	**Regular**
Contact User	Trunk main line as provided by the SIP Trunk provider
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

4. Click **Apply**.

4.17 Configuring Firewall Settings (Optional)

As an additional security measure, there is an option to configure traffic filtering rules (access list) for incoming traffic on AudioCodes SBC. For each packet received on the configured network interface, the SBC searches the table from top to bottom until the first matching rule is found. The matched rule can permit (allow) or deny (block) the packet. Once a rule in the table is located, subsequent rules further down the table are ignored. If the end of the table is reached without a match, the packet is accepted. Please note that the firewall is stateless. The blocking rules apply to all incoming packets, including UDP or TCP responses.

To configure a firewall rule:

1. Open the Firewall table (**Setup** menu > **IP Network** tab > **Security** folder> **Firewall**).
2. Configure the following Access list rules for WAN IP Interface, based on the list of Zoom Phone System Servers:

Table 12: Firewall Table Rules

Index	Source IP	Subnet Prefix	Start Port	End Port	Protocol	Use Specific Interface	Interface ID	Allow Type
0	<Public DNS Server IP> (e.g. 8.8.8.8)	32	0	65535	Any	Enable	WAN_IF	Allow
1	162.12.233.59	32	0	65535	TCP	Enable	WAN_IF	Allow
2	162.12.232.59	32	0	65535	TCP	Enable	WAN_IF	Allow
3	162.12.235.85	32	0	65535	TCP	Enable	WAN_IF	Allow
4	213.19.144.198	32	0	65535	TCP	Enable	WAN_IF	Allow
5	213.244.140.198	32	0	65535	TCP	Enable	WAN_IF	Allow
6	103.122.166.248	32	0	65535	TCP	Enable	WAN_IF	Allow
7	103.122.167.248	32	0	65535	TCP	Enable	WAN_IF	Allow
8	209.9.211.198	32	0	65535	TCP	Enable	WAN_IF	Allow
9	207.226.132.198	32	0	65535	TCP	Enable	WAN_IF	Allow
10	64.211.144.247	32	0	65535	TCP	Enable	WAN_IF	Allow
11	<SIP Trunk IP address>	32	0	65535	TCP	Enable	WAN_IF	Allow
49	0.0.0.0	0	0	65535	Any	Enable	WAN_IF	Block

Be aware, that if in your configuration, connectivity to SIP Trunk (or other entities) is performed through the same IP Interface as Zoom (WAN_IF in our example), you must add rules to allow traffic from these entities. See an example in the table row with index 11.

4.18 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

4.18.1 Configuring Mutual TLS Authentication for SIP

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

> 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.

   In the SIP Interface table, assign Zoom TLS context to the Zoom SIP Interface and configure the '**TLS Mutual Authentication**' parameter to **Enable**.
2. Ensure that the TLS certificate is signed by a CA.
3. Ensure 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**.

4.18.2 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, e.g., SIP calls per second (CPS)
- SRTP profile – improves maximum number of SRTP sessions
- Transcoding profile – enables all DSP-required features, e.g., 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.

> 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 the AudioCodes website.

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 the separate regions across the globe: North America, South 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

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

Certificate Issuer Organization	Common Name or Certificate Name
AffirmTrust	AffirmTrust Networking
AffirmTrust	AffirmTrust Premium
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

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

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
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-29402