Zoom Phone and Generic SIP Trunk using AudioCodes Mediant™ SBC

Version 7.2
Table of Contents

1 Introduction ............................................................................................................. 7
  1.1 Intended Audience ............................................................................................ 7
  1.2 About the Zoom Phone System ......................................................................... 7
  1.3 About AudioCodes SBC Product Series ........................................................... 7

2 Component Information ....................................................................................... 9
  2.1 AudioCodes SBC Version ................................................................................. 9
  2.2 Generic SIP Trunking Version .......................................................................... 9
  2.3 Zoom Phone System Version .......................................................................... 9
  2.4 Interoperability Test Topology ....................................................................... 10
    2.4.1 Environment Setup .................................................................................... 11
    2.4.2 Known Limitations .................................................................................... 11

3 Setting Up Zoom Phone System .......................................................................... 13

4 Configuring AudioCodes SBC ........................................................................... 15
  4.1 IP Network Interfaces Configuration ............................................................... 16
    4.1.1 Configure VLANs ..................................................................................... 17
    4.1.2 Configure Network Interfaces ................................................................. 17
  4.2 SIP TLS Connection Configuration ................................................................. 19
    4.2.1 Configure the NTP Server Address ............................................................ 19
    4.2.2 Create a TLS Context for Zoom Phone System .......................................... 20
    4.2.3 Configure a Certificate ............................................................................. 21
  4.3 Configure Media Realms .................................................................................. 25
  4.4 Configure SIP Signaling Interfaces ................................................................. 26
  4.5 Configure Proxy Sets and Proxy Address ....................................................... 27
    4.5.1 Configure a Proxy Address ....................................................................... 28
  4.6 Configure Coders ............................................................................................ 30
  4.7 Configure IP Profiles ...................................................................................... 34
  4.8 Configure IP Groups ....................................................................................... 36
  4.9 Configure SRTP .............................................................................................. 37
  4.10 Configure IP-to-IP Call Routing Rules ............................................................ 38
  4.11 Configure Number Manipulation Rules .......................................................... 39
  4.12 Configure Message Manipulation Rules ......................................................... 40
  4.13 Configure Registration Accounts (Optional) .................................................. 42
  4.14 Miscellaneous Configuration ........................................................................ 43
    4.14.1 Optimizing CPU Cores Usage for a Specific Service (relevant for Mediant 9000 and Software SBC only) ........................................................................ 43

A AudioCodes INI File ............................................................................................ 45
This page is intentionally left blank.
Notice

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

This document is subject to change without notice.

Date Published: January-23-2020

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.

Document Revision Record

<table>
<thead>
<tr>
<th>LTRT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29330</td>
<td>Initial document release for Version 7.2.</td>
</tr>
</tbody>
</table>

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 http://online.audiocodes.com/doc-feedback.
This page is intentionally left blank.
1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (hereafter, referred to as SBC) for interworking between Generic SIP Trunk and the Zoom Phone 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 Intended Audience

This document is intended for engineers, or AudioCodes and Generic partners who are responsible for installing and configuring Generic SIP Trunk and Zoom Phone Service for enabling VoIP calls using AudioCodes SBC.

1.2 About the Zoom Phone System

The Zoom Phone system is a modern cloud platform for video, voice, chat, and collaboration. With Zoom's Bring Your Own Carrier (BYOC) capabilities, enterprise customers can keep their current PSTN service provider to power the Zoom Phone cloud PBX service. Zoom Phone supports traditional business phone system features delivered with a streamlined user experience to modernize employee and customer interactions. Zoom Phone quickly provisions and manages users and intelligently monitors business interactions with an easy-to-use centralized administration portal. The globally distributed Zoom cloud platform delivers secure HD Voice with enterprise-class reliability and quality of service to ensure every call is perfect.

1.3 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.
2 Component Information

2.1 AudioCodes SBC Version

Table 2-1: AudioCodes SBC Version

<table>
<thead>
<tr>
<th>SBC Vendor</th>
<th>AudioCodes</th>
</tr>
</thead>
</table>
| Models     | • Mediant 500 Gateway & E-SBC  
• Mediant 500L Gateway & E-SBC  
• Mediant 800B Gateway & E-SBC  
• Mediant 800C Gateway & E-SBC  
• Mediant 1000B Gateway & E-SBC  
• Mediant 2600 E-SBC  
• Mediant 4000 SBC  
• Mediant 4000B SBC  
• Mediant 9000 SBC  
• Mediant 9030 SBC  
• Mediant 9080 SBC  
• Mediant Software SBC (VE/SE/CE) |
| Software Version | 7.20A.254.565 or later |
| Protocol | • SIP/UDP (to the Generic SIP Trunk)  
• SIP/UDP (to the Zoom Phone system) |
| Additional Notes | None |

2.2 Generic SIP Trunking Version

Table 2-2: Generic Version

<table>
<thead>
<tr>
<th>Vendor/Service Provider</th>
<th>Generic</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSW Model/Service</td>
<td></td>
</tr>
<tr>
<td>Software Version</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>SIP</td>
</tr>
<tr>
<td>Additional Notes</td>
<td>None</td>
</tr>
</tbody>
</table>

2.3 Zoom Phone System Version

Table 2-3: Zoom Phone System Version

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Zoom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>Phone system</td>
</tr>
<tr>
<td>Software Version</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>SIP</td>
</tr>
<tr>
<td>Additional Notes</td>
<td>None</td>
</tr>
</tbody>
</table>
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes SBC and Generic 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 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 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 Generic'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 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

<table>
<thead>
<tr>
<th>Area</th>
<th>Setup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>▪ Both, Zoom Phone system and Generic SIP Trunk environments are located on the WAN</td>
</tr>
<tr>
<td>Signaling</td>
<td>▪ Zoom Phone system operates with SIP-over-UDP transport type</td>
</tr>
<tr>
<td>Transcoding</td>
<td>▪ Generic SIP Trunk operates with SIP-over-UDP transport type</td>
</tr>
<tr>
<td>Codecs Transcoding</td>
<td>▪ Zoom Phone system supports G.711A-law, G.711U-law, G.722, and OPUS coders</td>
</tr>
<tr>
<td></td>
<td>▪ Generic SIP Trunk supports G.711A-law, G.711U-law, and G.729 coders</td>
</tr>
<tr>
<td>Media Transcoding</td>
<td>▪ Zoom Phone system operates with RTP media type</td>
</tr>
<tr>
<td></td>
<td>▪ Generic SIP Trunk operates with RTP media type</td>
</tr>
</tbody>
</table>

2.4.2 Known Limitations

The following limitation was observed in the interoperability tests performed for the AudioCodes SBC interworking between the Zoom Phone system and Generic's SIP Trunk:

- When working in secure mode (TLS connectivity method), Zoom works in a non-standard way. According to the RFC, it is required to declare “transport=tls” in the contact header, when using TLS for signaling. In all implementations, the lack of transport is defined to indicate UDP. The Zoom side is responding to our INVITE in TLS, but the contact headers do not declare TLS. Due to this, the ACK that the AudioCodes SBC sends to the 200 OK, is in UDP and not TLS. This means that the call does not connect, because Zoom doesn't see the ACK. As a result, it times out and sends a BYE.

To resolve this, a message manipulation rule is used to add “transport=tls” to all incoming from Zoom messages (see Section 4.12 on page 40).
This page is intentionally left blank.
3 Setting Up Zoom Phone System

For instructions on setting up the Zoom Phone system, contact Zoom Sales at https://zoom.us/contactsales.
This page is intentionally marked blank.
4 Configuring AudioCodes SBC

This section provides step-by-step procedures on how to configure AudioCodes SBC for interworking between the Zoom Phone system and the Generic SIP Trunk. 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 – 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).

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]
  - DSP Channels [If media transcoding is needed]
  - Transcoding sessions [If media transcoding is needed]
  For more information about the License Key, contact your AudioCodes sales representative.
- The scope of this document does not cover all security aspects for configuring this topology. Comprehensive security measures should be implemented per your organization’s security policies. For security recommendations on AudioCodes’ products, refer to the Recommended Security Guidelines document, which can be found at AudioCodes’ web site.
4.1 IP Network Interfaces Configuration

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 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 4-1: Network Interfaces in Interoperability Test Topology
4.1.1 Configure VLANs

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

- LAN VoIP (assigned the name “LAN_IF”)
- WAN VoIP (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).
2. There will be one existing row for VLAN ID 1 and underlying interface GROUP_1.
3. Add another VLAN ID 2 for the WAN side.

4.1.2 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>
<thead>
<tr>
<th>Index</th>
<th>Application Types</th>
<th>Interface Mode</th>
<th>IP Address</th>
<th>Prefix Length</th>
<th>Gateway</th>
<th>DNS</th>
<th>I/F Name</th>
<th>Ethernet Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>OAMP+ Media + Control</td>
<td>IPv4 Manual</td>
<td>10.15.77.77</td>
<td>16</td>
<td>10.15.0.1</td>
<td>10.15.27.1</td>
<td>LAN_IF</td>
<td>vlan 1</td>
</tr>
<tr>
<td>1</td>
<td>Media + Control (as this interface points to the internet, enabling OAMP is not recommended)</td>
<td>IPv4 Manual</td>
<td>195.189.192.157 (DMZ IP address of SBC)</td>
<td>25</td>
<td>195.189.192.129 (router's IP address)</td>
<td>According to your Internet provider's instructions</td>
<td>WAN_IF</td>
<td>vlan 2</td>
</tr>
</tbody>
</table>
The configured IP network interfaces are shown below:

**Figure 4-3: Configured Network Interfaces in IP Interfaces Table**
4.2 SIP TLS Connection Configuration

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.

This certificate module is based on the GoDaddy Certificate Chain. For more certificate structure options, refer to Zoom Phone System documentation.

Note: The following configuration steps are required only if the connection to the Zoom Phone System is made using TLS.

4.2.1 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 will be located on the OAMP IP Interface (LAN_IF in our case) or 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).

Figure 4-4: Configuring NTP Server Address

3. Click Apply.
4.2.2 Create a TLS Context for Zoom Phone System

This section describes how to configure TLS Context in the SBC. AudioCodes recommends implementing only TLS to avoid flaws in SSL.

➢ To configure the TLS version:
1. Open the TLS Contexts table (Setup menu > IP Network tab > Security folder > TLS Contexts).
2. Create a new TLS Context by clicking New at the top of the interface, and then configure the parameters using the table below as a reference:

   Table 4-2: New TLS Context
   
<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>TLS Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Zoom (arbitrary descriptive name)</td>
<td>TLSv1.2</td>
</tr>
</tbody>
</table>

   All other parameters can be left unchanged with their default values.

   Figure 4-5: Configuring TLS Context for Zoom Phone System

3. Click Apply.
4.2.3 Configure a Certificate

This section describes how to request a certificate for the SBC and to configure it based on the example of 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:


b. Requesting Device Certificate from CA.

c. Obtaining Trusted Root/Intermediate Certificate from CA.

d. Deploying Device and Trusted Root/Intermediate Certificates on SBC.

➢ To configure a certificate:

1. Open the TLS Contexts page (Setup menu > IP Network tab > Security folder > TLS Contexts).

2. 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.

3. Under the Certificate Signing Request group, do the following:

   a. In the 'Subject 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 the example above, sbc.audiocodes.com).

   c. Change the 'Private Key Size' based on the requirements of your Certification Authority (CA). Many CAs do not support private key size of 1024. In this case, you must change the key size to 2048.

   d. To change the key size on TLS Context:
      ♦ Navigate to Generate New Private Key and Self-Signed Certificate
      ♦ Change the 'Private Key Size' field to 2048
      ♦ Click Generate Private-Key

   e. To use 1024 as a Private Key Size value, click Generate Private-Key without changing the default key size value.

   f. Fill in the remaining fields according to your security provider's instructions.

   g. 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-----" 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 the certreq.txt file to the Certified Authority Administrator for signing.
6. After obtaining an SBC signed and Trusted Root/Intermediate Certificate from the CA, 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.

   **Figure 4-7: Uploading the Certificate Obtained from the Certification Authority**

   ![Certificate Upload Interface](image)

   **Note:** Replacing the private key is not recommended but if it’s done, it should be over a physically-secure network link.

7. Confirm 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.

8. In the SBC’s Web interface, do the following:
   a. Return to the **TLS Contexts** page
   b. Select the required TLS Context index row
   c. Click the **Certificate Information** link, located at the bottom of the TLS
   d. Validate the **Key size**, **Certificate Status** and **Subject Name**
9. 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 to load.
10. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store:

    **Figure 4-9: Example of Configured Trusted Root Certificates**

    | INDEX | SUBJECT | ISSUER | EXPIRES |
    |-------|---------|--------|---------|
    | 0     | Go Daddy Secure Certificate Auth | Go Daddy Root Certificate Auth | 5/03/2031 |
    | 1     | Go Daddy Root Certificate Auth | The Go Daddy Group, Inc. | 5/30/2031 |
    | 2     | The Go Daddy Group, Inc. | The Go Daddy Group, Inc. | 6/29/2034 |
4.3 Configure Media Realms

This section describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for the SIP Trunk traffic and one for the Zoom traffic. During interoperability testing, only one Media Realm was used, because both SIP trunk and the Zoom Phone system are on the WAN interface and use the same signaling and media resources.

➢ 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

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>IPv4 Interface Name</th>
<th>Port Range Start</th>
<th>Number of Media Session Legs</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>MR-WAN</td>
<td>WAN_IF</td>
<td>6000</td>
<td>100 (media sessions assigned with port range)</td>
</tr>
</tbody>
</table>

   All other parameters can be left unchanged at their default values.

The configured Media Realm are shown in the figure below:

Figure 4-10: Configured Media Realm in Media Realm Table
4.4 Configure SIP Signaling Interfaces

This section describes how to configure SIP Interfaces. The simplest configuration is to create two SIP Interfaces - one for the SIP Trunk and one for the Zoom Phone system. But, for the interoperability test topology, only one SIP Interface was configured.

➢ To configure SIP Interfaces:

1. Open the SIP Interfaces table (Setup menu > Signaling & Media tab > Core Entities folder > SIP Interfaces).

2. Configure SIP Interface. 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 Interface in SIP Interface Table

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Network Interface</th>
<th>Application Type</th>
<th>UDP Port</th>
<th>TCP Port</th>
<th>TLS Port</th>
<th>Media Realm</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SIPInterface_WAN</td>
<td>WAN_IF</td>
<td>SBC</td>
<td>5060 (according to requirement)</td>
<td>0</td>
<td>5061 (according to requirement)</td>
<td>MR-WAN</td>
</tr>
</tbody>
</table>

All other parameters can be left unchanged at their default values.

The configured SIP Interface is shown in the figure below:

Figure 4-11: Configured SIP Interface in SIP Interface Table
4.5 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, two Proxy Sets need to be configured for the following IP entities:

- Generic SIP Trunk
- Zoom Phone system

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>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>SBC IPv4 SIP Interface</th>
<th>TLS Context Name</th>
<th>Proxy Keep-Alive</th>
<th>Redundancy Mode</th>
<th>Proxy Hot Swap</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Zoom</td>
<td>SIPInterface_WAN</td>
<td>Zoom</td>
<td>Using Options</td>
<td>Homing</td>
<td>Enable</td>
</tr>
<tr>
<td>2</td>
<td>SIPTrunk</td>
<td>SIPInterface_WAN</td>
<td>Default</td>
<td>Using Options</td>
<td>According to SIP Trunk requirement</td>
<td>According to SIP Trunk requirement</td>
</tr>
</tbody>
</table>

The configured Proxy Sets are shown in the figure below:

**Figure 4-12: Configured Proxy Sets in Proxy Sets Table**
4.5.1 Configure a Proxy Address

This section shows how to configure a Proxy Address.

➢ To configure a Proxy Address for the Zoom Phone system:

1. Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets) and then click the Proxy Set Zoom, and then click the Proxy Address link located below the table; the Proxy Address table opens.

2. Click +New; the following dialog box appears:

Figure 4-13: Configuring Proxy Address for Zoom Phone System Interface

3. Configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-6: Configuration Proxy Address for UDP connection to Zoom Phone System

<table>
<thead>
<tr>
<th>Index</th>
<th>Proxy Address</th>
<th>Transport Type</th>
<th>Proxy Priority</th>
<th>Proxy Random Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>162.12.233.58:5060</td>
<td>UDP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>162.12.232.58:5060</td>
<td>UDP</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

4. Click Apply.

Note: The connection to the Zoom Phone system may change according to your specific deployment topology (UDP or TLS). Refer to Zoom support website for specific IP addresses.

➢ 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; the following dialog box appears:
3. 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**

<table>
<thead>
<tr>
<th>Index</th>
<th>Proxy Address</th>
<th>Transport Type</th>
<th>Proxy Priority</th>
<th>Proxy Random Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SIPTrunk.com:5060 (SIP Trunk IP / FQDN and port)</td>
<td>UDP</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

4. Click **Apply**.
4.6 Configure Coders

This section describes how to configure coders (termed Coder Group). As the Zoom Phone system supports the G.722 and OPUS 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. Configure a Coder Group for the Zoom Phone system:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coder Group Name</td>
<td>AudioCodersGroups_1</td>
</tr>
<tr>
<td>Coder Name</td>
<td>▪ G.722 ▪ Opus</td>
</tr>
</tbody>
</table>

Figure 4-15: Configuring Coder Group for Zoom Phone System

3. Click Apply.
4. Configure a Coder Group for SIP Trunk:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coder Group Name</td>
<td>AudioCodersGroups_2</td>
</tr>
<tr>
<td>Coder Name</td>
<td>▪ G.729</td>
</tr>
</tbody>
</table>

Figure 4-16: Configuring Coder Group for SIP Trunk

5. Click Apply.
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.

   **Figure 4-17: Configuring Allowed Coders Group for Generic SIP Trunk**

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:

<table>
<thead>
<tr>
<th>Index</th>
<th>Coder</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>G.729</td>
</tr>
<tr>
<td>1</td>
<td>G.711 U-law</td>
</tr>
<tr>
<td>2</td>
<td>G.711 A-law</td>
</tr>
</tbody>
</table>

   **Figure 4-18: Configuring Allowed Coders for Generic SIP Trunk**
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.

![Figure 4-19: Configuring Allowed Coders Group for the Zoom Phone](image)

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:

<table>
<thead>
<tr>
<th>Index</th>
<th>Coder</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Opus</td>
</tr>
<tr>
<td>1</td>
<td>G.722</td>
</tr>
<tr>
<td>2</td>
<td>G.711 U-law</td>
</tr>
<tr>
<td>3</td>
<td>G.711 A-law</td>
</tr>
</tbody>
</table>

![Figure 4-20: Configuring Allowed Coders for Zoom Phone](image)
6. Open the Media Settings page (Setup menu > Signaling & Media tab > Media folder > Media Settings).

![Figure 4-21: SBC Preferences Mode](image)

7. From the 'Preferences Mode' drop-down list, select Include Extensions.
8. Click Apply.
4.7 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 then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>1</td>
</tr>
<tr>
<td>Name</td>
<td>Zoom (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Media Security</td>
<td></td>
</tr>
<tr>
<td>SBC Media Security Mode</td>
<td>Not Secured or Secured (according to connectivity)</td>
</tr>
<tr>
<td>SBC Media</td>
<td></td>
</tr>
<tr>
<td>Extension Coders Group</td>
<td>AudioCodersGroups_1</td>
</tr>
<tr>
<td>Allowed Audio Coders</td>
<td>Zoom Allowed Coders</td>
</tr>
<tr>
<td>Allowed Coders Mode</td>
<td>Restriction and Preference (reorder coders according to Allowed Coders including extension coders)</td>
</tr>
<tr>
<td>RFC 2833 Mode</td>
<td>Extend</td>
</tr>
<tr>
<td>SBC Signaling</td>
<td></td>
</tr>
<tr>
<td>Session Expires Mode</td>
<td>Supported</td>
</tr>
</tbody>
</table>

![Figure 4-22: Configuring IP Profile for Zoom Phone System](image)

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, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>2</td>
</tr>
<tr>
<td>Name</td>
<td>SIPTrunk</td>
</tr>
<tr>
<td><strong>Media Security</strong></td>
<td></td>
</tr>
<tr>
<td>SBC Media Security Mode</td>
<td>Not Secured</td>
</tr>
<tr>
<td><strong>SBC Media</strong></td>
<td></td>
</tr>
<tr>
<td>Extension Coders Group</td>
<td>AudioCodersGroups_2</td>
</tr>
<tr>
<td>Allowed Audio Coders</td>
<td>SIPTrunk Allowed Coders</td>
</tr>
<tr>
<td>Allowed Coders Mode</td>
<td>Restriction and Preference (reorder coders according to Allowed Coders including extension coders)</td>
</tr>
<tr>
<td><strong>SBC Signaling</strong></td>
<td></td>
</tr>
<tr>
<td>P-Asserted-Identity Header Mode</td>
<td>Add (required for anonymous calls)</td>
</tr>
</tbody>
</table>

3. Click Apply.
4.8 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 system
- Generic 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>2</td>
</tr>
<tr>
<td>Name</td>
<td>Zoom</td>
</tr>
<tr>
<td>Type</td>
<td>Server</td>
</tr>
<tr>
<td>Proxy Set</td>
<td>Zoom</td>
</tr>
<tr>
<td>IP Profile</td>
<td>Zoom</td>
</tr>
<tr>
<td>Media Realm</td>
<td>MR-Wan</td>
</tr>
<tr>
<td>SIP Group Name</td>
<td>(according to ITSP requirement)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>1</td>
</tr>
<tr>
<td>Name</td>
<td>SIPTrunk</td>
</tr>
<tr>
<td>Type</td>
<td>Server</td>
</tr>
<tr>
<td>Proxy Set</td>
<td>SIPTrunk</td>
</tr>
<tr>
<td>IP Profile</td>
<td>SIPTrunk</td>
</tr>
<tr>
<td>Media Realm</td>
<td>MR-Wan</td>
</tr>
<tr>
<td>SIP Group Name</td>
<td>(according to ITSP requirement)</td>
</tr>
</tbody>
</table>
4.9 Configure SRTP

This section describes how to configure media security. Zoom Phone System can be configured to use of SRTP, so you need to configure the SBC to operate in the same manner.

➢ 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.
4.10 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 Zoom Phone system to Generic SIP Trunk
- Calls from Generic 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>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Source IP Group</th>
<th>Request Type</th>
<th>Dest Type</th>
<th>Dest IP Group</th>
<th>Dest Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Terminate OPTIONS</td>
<td>Any</td>
<td>OPTION S</td>
<td>Dest Address</td>
<td></td>
<td>internal</td>
</tr>
<tr>
<td>1</td>
<td>Zoom to ITSP (arbitrary name)</td>
<td>Zoom</td>
<td>IP Group</td>
<td>SIPTrunk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ITSP to Zoom (arbitrary name)</td>
<td>SIPTrunk</td>
<td>IP Group</td>
<td>Zoom</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The configured routing rules are shown in the figure below:

Note: The routing configuration may change according to your specific deployment topology.
4.11 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 4.8 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 "+1" (plus sign) to the destination number (if it not exists) for calls from the Generic 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 figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between the Zoom Phone system IP Group and Generic SIP Trunk IP Group:

Figure 4-27: Example of Configured IP-to-IP Outbound Manipulation Rules

<table>
<thead>
<tr>
<th>Rule Index</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Calls from SIP Trunk IP Group to Zoom IP Group with the prefix destination number &quot;+1&quot;, do nothing.</td>
</tr>
<tr>
<td>1</td>
<td>Calls from SIP Trunk IP Group to Zoom IP Group with any destination number between 2 to 9, add &quot;+1&quot; to the prefix of the destination number.</td>
</tr>
</tbody>
</table>
4.12 Configure 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:

1. Open the Message Manipulations page (Setup menu > Signaling & Media tab > Message Manipulation folder > Message Manipulations).
2. Configure a new manipulation rule (Manipulation Set 0) for the Zoom Phone system. This rule applies to messages received from the Zoom IP Group. This adds 'transporttype=tls' to the SIP Contact Header.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>0</td>
</tr>
<tr>
<td>Name</td>
<td>Add TLS to Contact from Zoom</td>
</tr>
<tr>
<td>Manipulation Set ID</td>
<td>0</td>
</tr>
<tr>
<td>Message Type</td>
<td>Any.Response</td>
</tr>
<tr>
<td>Condition</td>
<td>Header.Contact.URL.Host.Port=='5061'</td>
</tr>
<tr>
<td>Action Subject</td>
<td>Header.Contact.URL.TransportType</td>
</tr>
<tr>
<td>Action Type</td>
<td>Modify</td>
</tr>
<tr>
<td>Action Value</td>
<td>'2'</td>
</tr>
</tbody>
</table>

Figure 4-28: Configuring SIP Message Manipulation Rule 0 (for the Zoom Phone)
3. Assign Manipulation Set ID 0 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 0.

   Figure 4-29: Assigning Manipulation Set to the Zoom IP Group

   d. Click Apply.

   **Note:** Configure additional Message Manipulation Rules if this is required by the SIP Trunk. For a detailed description please refer to the Configuration Notes document for the particular SIP Trunk.
4.13 Configure Registration Accounts (Optional)

This section describes how to configure SIP registration accounts. This is required so that the SBC can register with the Generic SIP Trunk on behalf of the Zoom Phone system. The Generic 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 Generic SIP Trunk IP Group.

**Note:** 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 from , for example:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Served IP Group</td>
<td>Zoom</td>
</tr>
<tr>
<td>Application Type</td>
<td>SBC</td>
</tr>
<tr>
<td>Serving IP Group</td>
<td>SIPTrunk</td>
</tr>
<tr>
<td>Host Name</td>
<td>As provided by the SIP Trunk provider</td>
</tr>
<tr>
<td>Register</td>
<td>Regular</td>
</tr>
<tr>
<td>Contact User</td>
<td>8325624857 (trunk main line)</td>
</tr>
<tr>
<td>Username</td>
<td>As provided by the SIP Trunk provider</td>
</tr>
<tr>
<td>Password</td>
<td>As provided by the SIP Trunk provider</td>
</tr>
</tbody>
</table>

![Figure 4-30: Configuring a SIP Registration Account](image)

4. Click Apply.
4.14 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

4.14.1 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:

   ![SBC Performance Profile](image)

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.
A AudioCodes INI File

The ini configuration file of the SBC, corresponding to the Web-based configuration as described in Section 4 on page 15, is shown below:

**Note:** To load or save an ini file, use the Configuration File page (Setup menu > Administration tab > Maintenance folder > Configuration File).

```ini
;**************
;** Ini File **
;**************

[SYSTEM Params]
SyslogServerIP = 10.10.10.10
EnableSyslog = 1
NTPServerUTCOffset = 7200
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '10.15.28.1'
SBCWizardFilename = 'templates4.zip'

[BSP Params]
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]

[ControlProtocols Params]

[Voice Engine Params]
ENABLEMEDIASECURITY = 1
PLThresholdLevelsPerMille_0 = 5
PLThresholdLevelsPerMille_1 = 10
PLThresholdLevelsPerMille_2 = 20
PLThresholdLevelsPerMille_3 = 50
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]
UseProductName = 1
Languages = 'en-US', '', '', '', '', '', '', '', ''

[SIP Params]
GWDEBUGLEVEL = 5
```
**Configuration Note 46**

**Document #: LTRT-29330**

**Zoom Phone & Generic SIP Trunk**

```
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCCPREFERENCESMODE = 1
MEDIACDRREPORTLEVEL = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144

[SNMP Params]

[ DeviceTable ]

FORMAT Index = VlanID, UnderlyingInterface, DeviceName, Tagging, MTU;
DeviceTable 0 = 1, "GROUP_1", "vlan 1", 0, 1500;
DeviceTable 1 = 2, "GROUP_2", "vlan 2", 0, 1500;

[ InterfaceTable ]

FORMAT Index = ApplicationTypes, InterfaceMode, IPAddress, PrefixLength, Gateway, InterfaceName, PrimaryDNSServerIPAddress, SecondaryDNSServerIPAddress, UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.77.55, 16, 10.15.0.1, "LAN_IF", 10.15.27.1, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.153, 24, 195.189.192.129, "WAN_IF", 80.179.52.100, 80.179.55.100, "vlan 2";

[ TLSContexts ]

FORMAT Index = Name, TLSVersion, DTLSVersion, ServerCipherString, ClientCipherString, RequireStrictCert, TlsRenegotiation, OcspEnable, OcspServerPrimary, OcspServerSecondary, OcspServerPort, OcspDefaultResponse, DHKeySize;
TLSContexts 0 = "default", 7, 0, "RC4:EXP", "ALL:!ADH", 0, 1, 0, 0.0.0.0, 0.0.0.0, 2560, 0, 1024;
TLSContexts 1 = "Zoom", 4, 0, "DEFAULT", "DEFAULT", 0, 1, 0, 0.0.0.0, 0.0.0.0, 2560, 0, 1024;

[ AudioCodersGroups ]

FORMAT Index = Name;
AudioCodersGroups 0 = "AudioCodersGroups_0";
AudioCodersGroups 1 = "AudioCodersGroups_1";
AudioCodersGroups 2 = "AudioCodersGroups_2";

[ AllowedAudioCodersGroups ]

FORMAT Index = Name;
```
Configuration Note

A. AudioCodes INI File

Version 7.2 47 AudioCodes Mediant SBC

AllowedAudioCodersGroups 0 = "SIPTrunk Allowed Coders";
AllowedAudioCodersGroups 1 = "Zoom Allowed Coders";

[ \AllowedAudioCodersGroups ]

[ IpProfile ]

FORMAT Index = ProfileName, IpPreference, CodersGroupName, IsFaxUsed,
JitterBufMinDelay, JitterBufOptFactor, IPDiffServ, SigIPDiffServ,
RTPRedundancyDepth, NGXMode, VxVTransportType, NSEMode, IsDTMFused,
EnableEchoCanceller, CopyDest2RedirectNumber, MediaSecurityBehaviour,
CallLimit, DisconnectOnBrokenConnection, FirstTxDtmfOption,
SecondTxDtmfOption, RxDTMFOption, EnableHold, InputGain, VoiceVolume,
AddIEInSetup, SBCExtensionCodersGroupName, MediaIPv4VersionPreference,
TranscodingMode, SBCAllowedMediaTypes, SBCAllowedAudioCodersGroupName,
SBCAllowedVideoCodersGroupName, SBCAllowedCodersMode,
SBCMediaSecurityBehaviour, SBCRFC2833Behavior, SBCAlternativeDTMFMethod,
SBSendMultipleDTMFMethods, SBCAssertIdentity,
AMDSensitivityParameterSuit, AMDSensitivityLevel,
SBCMaxPostSilenceGreetingTime, SBCMaxGreetingTime,
SBCMaxGreetingTime, SBCMaxSilenceGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
SBCMaxSillyGreetingTime, SBCMaxGreetingTime,
[ CpMediaRealm ]

FORMAT Index = MediaRealmName, IPv4IF, IPv6IF, RemoteIPv4IF, RemoteIPv6IF, PortRangeStart, MediaSessionLeg, PortRangeEnd, TCPPortRangeStart, TCPPortRangeEnd, IsDefault, QoeProfile, BWProfile, TopologyLocation;
CpMediaRealm 0 = "MR-WAN", "WAN_IF", ",", ",", ",", 6000, 100, 6999, 0, 0, ",", ",", 0;

[ \CpMediaRealm ]

[ SBCRoutingPolicy ]

FORMAT Index = Name, LCREnable, LCRAverageCallLength, LCRDefaultCost, LdapServerGroupName;
SBCRoutingPolicy 0 = "Default_SBCRoutingPolicy", 0, 1, 0, "";

[ \SBCRoutingPolicy ]

[ SRD ]

FORMAT Index = Name, BlockUnRegUsers, MaxNumOfRegUsers, EnableUnAuthenticatedRegistrations, SharingPolicy, UsedByRoutingServer, SBCOperationMode, SBCRoutingPolicyName, SBCDialPlanName, AdmissionProfile;
SRD 0 = "DefaultSRD", 0, -1, 1, 0, 0, "Default_SBCRoutingPolicy", ",", "";

[ \SRD ]

[ MessagePolicy ]

FORMAT Index = Name, MaxMessageLength, MaxHeaderLength, MaxBodyLength, MaxNumHeaders, MaxNumBodies, SendRejection, MethodList, MethodListType, BodyList, BodyListType, UseMaliciousSignatureDB;
MessagePolicy 0 = "Malicious Signature DB Protection", -1, -1, -1, -1, -1, -1, ",", 0, ",", 0, 1;

[ \MessagePolicy ]

[ SIPInterface ]

FORMAT Index = InterfaceName, NetworkInterface, SCTPSecondaryNetworkInterface, ApplicationType, UDPPort, TCPPort, TLSPort, SCTPPort, AdditionalUDPPorts, AdditionalUDPPortsMode, SRDName, MessagePolicyName, TLSContext, TLSMutualAuthentication, TCPKeepaliveEnable, ClassificationFailureResponseType, PreClassificationManSet, EncapsulatingProtocol, MediaRealm, SBCDirectMedia, BlockUnRegUsers, MaxNumOfRegUsers, EnableUnAuthenticatedRegistrations, UsedByRoutingServer, TopologyLocation, PreParsingManSetsetName, AdmissionProfile, CallSetupRulesSetId;
SIPInterface 0 = "SIPInterface_WAN", "WAN IP", "", 2, 5060, 5060, 5061, 0, "", 0, "DefaultSRD", "", "Zoom", -1, 0, 500, -1, 0, "MR-WAN", 0, -1, -1, 0, 0, "", "", -1;

[ \SIPInterface ]

[ ProxySet ]

FORMAT Index = ProxyName, EnableProxyKeepAlive, ProxyKeepAliveTime, ProxyLoadBalancingMethod, IsProxyHotSwap, SRDName, ClassificationInput, TLSContextName, ProxyRedundancyMode, DNSResolveMethod, KeepAliveFailureResp, GWIPv4SIPInterfaceName, SBCIPv4SIPInterfaceName, GWIPv6SIPInterfaceName, SBCIPv6SIPInterfaceName, MinActiveServersLB, SuccessDetectionRetries, SuccessDetectionInterval, FailureDetectionRetransmissions;
ProxySet 0 = "ProxySet_0", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "SIPInterface_WAN", "", "", 1, 1, 10, -1;
ProxySet 1 = "Zoom", 1, 60, 0, 1, "DefaultSRD", 0, "Zoom", 1, -1, "", "SIPInterface_WAN", "", "", 1, 1, 10, -1;
ProxySet 2 = "SIPTrunk", 1, 60, 0, 1, "DefaultSRD", 0, "default", 1, 1, "", "SIPInterface_WAN", "", "", 1, 1, 10, -1;

[ \ProxySet ]

[ SBCAltRoutingReasonsSet ]

FORMAT Index = Name, Description;
SBCAltRoutingReasonsSet 0 = "SBCAltRoutingReasonsSet_0", "";

[ \SBCAltRoutingReasonsSet ]

[ IPGroup ]

FORMAT Index = Type, Name, ProxySetName, SIPGroupName, ContactUser, SIPReRoutingReasonsSet, AlwaysUseRouteTable, SRDName, MediaRealm, InternalMediaRealm, ClassifyByProxySet, ProfileName, MaxNumOfRegUsers, InboundManSet, OutboundManSet, RegistrationMode, AuthenticationMode, MethodList, SBCServerAuthType, OAuthHTTPService, EnableSBCClientForking, SourceUriInput, DestUriInput, ContactName, Username, Password, UIFormat, QOEProfile, BWProfile, AlwaysUseSourceAddr, MsgManUserDef1, MsgManUserDef2, SIPConnect, SBCPSAPMode, DTLSContext, CreatedByRoutingServer, UsedByRoutingServer, SBCOperationMode, SBCRouteUsingRequestURIOr, SBCKeepOriginalCallID, TopologyLocation, SBCDialPlanName, CallSetupRulesSetID, Tags, SBCUserStickiness, UserUDPPortAssignment, AdmissionProfile, ProxyKeepAliveUsingIPG, SBCAltRouteReasonsSetName, TeamsMediaOptimization;
IPGroup 0 = 0, "Default_IPG", "ProxySet_0", "", -1, 0, "DefaultSRD", "", "", 0, 0, "", -1, -1, 0, 0, "", -1, "", 0, -1, -1, "", "SIPInterface_WAN", "", "", 0, 0, "", "", 0, 0, "", "SBCAltRoutingReasonsSet_0", 0;
IPGroup 1 = 0, "Zoom", "Zoom", "", -1, 0, "DefaultSRD", "MR-WAN", "", 1, "Zoom", -1, 0, -1, 0, 0, "", -1, "", 0, -1, -1, "", "Admin", "$1$gQ==", 0, "", "", 0, 0, "", 0, -1, 0, 0, 0, "", -1, "", 0, 0, "", 0, 0, "", "SBCAltRoutingReasonsSet_0", 0;
IPGroup 2 = 0, "SIPTrunk", "SIPTrunk", "", -1, 0, "DefaultSRD", "MR-WAN", "", 1, "SIPTrunk", -1, -1, 0, 0, 0, "", -1, -1, "", "Admin", "$1$aCkNBwIC", 0, "", "", 0, 0, "", 0, 0, "", 0, -1, 0, 0, 0, "", -1, "", 0, 0, "", 0, 0, "", "SBCAltRoutingReasonsSet_0", 0;
### Configuration Note

#### ProxyIp

<table>
<thead>
<tr>
<th>ProxySetId</th>
<th>ProxyIndex</th>
<th>IpAddress</th>
<th>TransportType</th>
<th>Priority</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>&quot;162.12.233.58:5060&quot;</td>
<td>0, 0, 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>&quot;162.12.232.58:5060&quot;</td>
<td>0, 0, 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>&quot;SIPTrunk.com:5060&quot;</td>
<td>0, 0, 0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Account

<table>
<thead>
<tr>
<th>AccountName</th>
<th>ServedTrunkGroup</th>
<th>ServedIPGroupName</th>
<th>ServingIPGroupName</th>
<th>Username</th>
<th>Password</th>
<th>HostName</th>
<th>ContactUser</th>
<th>Register</th>
<th>RegistrarStickiness</th>
<th>RegistrarSearchMode</th>
<th>RegEventPackageSubscription</th>
<th>ApplicationType</th>
<th>RegByServedIPG</th>
<th>UDPPortAssignment</th>
<th>ReRegisterOnInviteFailure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-1</td>
<td>&quot;Zoom&quot;</td>
<td>&quot;SIPTrunk&quot;</td>
<td>&quot;1234567890&quot;</td>
<td>&quot;password&quot;</td>
<td>&quot;SIPTrunk.com&quot;</td>
<td>&quot;1234567890&quot;</td>
<td>1, 0, 0, 2, 0, 0, 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### IP2IPRouting

| RouteName                              | RoutingPolicyName | SrcIPGroupName | SrcUsernamePrefix | DestIPGroupName | DestUsernamePrefix | DestHost | RequestType | MessageConditionName | ReRouteIPGroupName | Trigger | CallSetupRulesSetId | DestType | DestIPGroupName | DestSIPInterfaceName | DestAddress | DestPort | DestTransportType | AltRouteOptions | GroupPolicy | DestTags | IPGroupSetName | RoutingTagName | InternalAction |
|----------------------------------------|-------------------|----------------|------------------|-----------------|-------------------|---------|-------------|--------------------|-------------------|---------|-------------------|---------|-----------------|-------------------|-------------|---------|----------------|----------------|-------------|---------|---------------|--------------|--------------|---------|
| "Terminate OPTIONS"                    | "Default_SBCRoutingPolicy" | "Any", "*", "*", "*", "*", "*", "Any", 0, -1, 1, "*", "*", "internal", 0, -1, 0, 0, "*", "*", "*", "*", "default", "*"; |
| "Zoom to ITSP"                         | "Default_SBCRoutingPolicy" | "Zoom", "*", "*", "*", "*", "Any", 0, -1, 0, "SIPTrunk", "*", "*", 0, -1, 0, 0, "*", "*", "*", "*", "default", "*"; |
| "ITSP to Zoom"                         | "Default_SBCRoutingPolicy" | "ITSP", "*", "*", "*", "*", "Any", 0, -1, 0, "Zoom", "*", "*", 0, -1, 0, 0, "*", "*", "*", "*", "default", "*"; |

#### IPOutboundManipulation

<table>
<thead>
<tr>
<th>ManipulationName</th>
<th>RoutingPolicyName</th>
<th>IsAdditionalManipulation</th>
<th>SrcIPGroupName</th>
<th>DestIPGroupName</th>
<th>SrcUsernamePrefix</th>
<th>DestUsernamePrefix</th>
<th>CallingNamePrefix</th>
<th>MessageConditionName</th>
<th>RequestType</th>
<th>ReRouteIPGroupName</th>
<th>Trigger</th>
<th>ManipulatedURI</th>
<th>RemoveFromLeft</th>
<th>RemoveFromRight</th>
<th>LeaveFromRight</th>
<th>Prefix2Add</th>
<th>Suffix2Add</th>
<th>PrivacyRestrictionMode</th>
<th>DestTags</th>
<th>SrcTags</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Do Nothing&quot;</td>
<td>&quot;Default_SBCRoutingPolicy&quot;</td>
<td>0</td>
<td>&quot;SIPTrunk&quot;, &quot;<em>&quot;, &quot;</em>&quot;, &quot;<em>&quot;, &quot;</em>&quot;, &quot;<em>&quot;, &quot;Any&quot;, 0, 1, 0, 0, 255, &quot;</em>&quot;, &quot;<em>&quot;, 0, &quot;</em>&quot;, &quot;*&quot;;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IPOutboundManipulation 1 = "Add +1", "Default SBCRoutingPolicy", 0, "SIPTrunk", "Zoom", "*", "*", "[2-9]", "*", "*", "*", 0, "Any", 0, 1, 0, 0, 255, "+1", "", 0, "", "";

[ 
IPOutboundManipulation ]

[ MessageManipulations ]

FORMAT Index = ManipulationName, ManSetID, MessageType, Condition, ActionSubject, ActionType, ActionValue, RowRole;
MessageManipulations 0 = "Add TLS to Contact from Zoom", 0, "Any.Response", "Header.Contact.URL.Host.Port=='5061'";
MessageManipulations 0 = "Add TLS to Contact from Zoom", 0, "Any.Response", "Header.Contact.URL.TransportType=='2'";

[ 
MessageManipulations ]

[ GwRoutingPolicy ]

FORMAT Index = Name, LCREnable, LCRAverageCallLength, LCRDefaultCost, LdapServerGroupName;
GwRoutingPolicy 0 = "GwRoutingPolicy", 0, 1, 0, "";

[ 
GwRoutingPolicy ]

[ ResourcePriorityNetworkDomains ]

FORMAT Index = Name, Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 1;
ResourcePriorityNetworkDomains 2 = "dod", 1;
ResourcePriorityNetworkDomains 3 = "drsn", 1;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 1;

[ 
ResourcePriorityNetworkDomains ]

[ MaliciousSignatureDB ]

FORMAT Index = Name, Pattern;
MaliciousSignatureDB 0 = "SIPVicious", "Header.User-Agent.content prefix 'friendly-scanner'";
MaliciousSignatureDB 1 = "SIPScan", "Header.User-Agent.content prefix 'sip-scan'";
MaliciousSignatureDB 2 = "Smap", "Header.User-Agent.content prefix 'smap'";
MaliciousSignatureDB 3 = "Sipsak", "Header.User-Agent.content prefix 'sipsak'";
MaliciousSignatureDB 4 = "Sipcli", "Header.User-Agent.content prefix 'sipcli'";
MaliciousSignatureDB 5 = "Sivus", "Header.User-Agent.content prefix 'SIVuS'";
MaliciousSignatureDB 6 = "Gulp", "Header.User-Agent.content prefix 'Gulp'";
MaliciousSignatureDB 7 = "Sipv", "Header.User-Agent.content prefix 'sipv'";
MaliciousSignatureDB 8 = "Sundayddr Worm", "Header.User-Agent.content prefix 'sundayddr';
MaliciousSignatureDB 9 = "VaxIPUserAgent", "Header.User-Agent.content prefix 'VaxIPUserAgent';
MaliciousSignatureDB 10 = "VaxSIPUserAgent", "Header.User-Agent.content prefix 'VaxSIPUserAgent';
MaliciousSignatureDB 11 = "SipArmyKnife", "Header.User-Agent.content prefix 'siparmyknife';"

[ MaliciousSignatureDB ]

[ AllowedAudioCoders ]

FORMAT Index = AllowedAudioCodersGroupName, AllowedAudioCodersIndex, CoderID, UserDefineCoder;
AllowedAudioCoders 0 = "SIPTrunk Allowed Coders", 0, 3, "";
AllowedAudioCoders 1 = "SIPTrunk Allowed Coders", 1, 1, "";
AllowedAudioCoders 2 = "SIPTrunk Allowed Coders", 2, 2, "";
AllowedAudioCoders 3 = "Zoom Allowed Coders", 0, 40, "";
AllowedAudioCoders 4 = "Zoom Allowed Coders", 1, 20, "";
AllowedAudioCoders 5 = "Zoom Allowed Coders", 2, 2, "";
AllowedAudioCoders 6 = "Zoom Allowed Coders", 3, 1, "";

[ 
AllowedAudioCoders ]

[ AudioCoders ]

FORMAT Index = AudioCodersGroupId, AudioCodersIndex, Name, pTime, rate, PayloadType, Sce, CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 0, 2, 2, 90, -1, 1, "";
AudioCoders 1 = "AudioCodersGroups_0", 1, 1, 2, 90, -1, 1, "";
AudioCoders 2 = "AudioCodersGroups_1", 0, 20, 1, 90, -1, 0, "";
AudioCoders 3 = "AudioCodersGroups_1", 1, 40, 2, 255, 102, 0, "";
AudioCoders 4 = "AudioCodersGroups_2", 0, 3, 2, 19, -1, 0, "";

[ 
AudioCoders ]

[ SBCAltRoutingReasonsList ]

FORMAT Index = SBCAltRoutingReasonsSet, SBCAltRouteIndex, ReleaseCauseCode;
SBCAltRoutingReasonsList 0 = "SBCAltRoutingReasonsSet_0", 0, 503;

[ 
SBCAltRoutingReasonsList ]
This page is intentionally left blank.
International Headquarters
1 Hayarden Street,
Airport City
Lod 701900, 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

©2020 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What’s Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocalNom, AudioCodes One Voice, AudioCodes Meeting Insights, AudioCodes Room Experience and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-29330