AudioCodes Mediant™ SBC for Sunrise SIP Trunk with Microsoft® Skype for Business Server 2015

Version 7.0
Table of Contents

1 Introduction ......................................................................................................... 7
  1.1 Intended Audience ................................................................................................. 7
  1.2 About AudioCodes SBC Product Series ................................................................. 7

2 Component Information ...................................................................................... 9
  2.1 AudioCodes SBC Version ....................................................................................... 9
  2.2 Sunrise SIP Trunking Version ................................................................................ 9
  2.3 Microsoft Skype for Business Server 2015 Version ................................................ 9
  2.4 Interoperability Test Topology .............................................................................. 10
    2.4.1 Environment Setup ................................................................................................ 11
    2.4.2 Known Limitations ............................................................................................... 11

3 Configuring Skype for Business Server 2015 ................................................. 13
  3.1 Configuring the SBC as an IP / PSTN Gateway .................................................... 13
  3.2 Configuring the "Route" on Skype for Business Server 2015 ................................ 21

4 Configuring AudioCodes SBC ......................................................................... 33
  4.1 Step 1: IP Network Interfaces Configuration ......................................................... 34
    4.1.1 Step 1a: Configure VLANs ....................................................................................... 35
    4.1.2 Step 1b: Configure Network Interfaces .................................................................... 35
    4.1.3 Step 1c: Adding Static Routes to Sunrise SBC ....................................................... 37
  4.2 Step 2: Enable the SBC Application ..................................................................... 39
  4.3 Step 3: Configure Media Realms .......................................................................... 40
  4.4 Step 4: Configure SIP Signaling Interfaces ........................................................... 42
  4.5 Step 5: Configure Proxy Sets ............................................................................... 43
  4.6 Step 6: Configure IP Profiles ................................................................................ 48
  4.7 Step 7: Configure IP Groups ................................................................................. 56
  4.8 Step 8: Configure Coders ..................................................................................... 58
  4.9 Step 9: SIP TLS Connection Configuration ........................................................... 60
    4.9.1 Step 9a: Configure the NTP Server Address ........................................................... 60
    4.9.2 Step 9b: Configure the TLS version ........................................................................ 61
    4.9.3 Step 9c: Configure a Certificate ............................................................................... 61
  4.10 Step 10: Configure SRTP ..................................................................................... 64
  4.11 Step 11: Configure Maximum IP Media Channels ................................................ 65
  4.12 Step 12: Configure IP-to-IP Call Routing Rules .................................................... 65
  4.13 Step 13: Configure Message Manipulation Rules ................................................. 76
  4.14 Step 14: Miscellaneous Configuration ................................................................. 81
    4.14.1 SBC General Settings .............................................................................................. 81
    4.14.2 Configure SBC Alternative Routing Reasons .......................................................... 81
  4.15 Step 15: Reset the SBC ....................................................................................... 82

A AudioCodes INI File .......................................................................................... 83

B Configuring Analog Devices (ATAs) for Fax Support .................................... 93
  B.1 Step 1: Configure the Endpoint Phone Number Table ........................................... 93
  B.2 Step 2: Configure Tel to IP Routing Table ............................................................. 93
  B.3 Step 3: Configure Coders Table .............................................................................. 94
  B.4 Step 4: Configure SIP UDP Transport Type and Fax Signaling Method ............... 95
This page is intentionally left blank.
Notice

This document describes how to connect the Microsoft Skype for Business Server 2015 and Sunrise SIP Trunk using AudioCodes Mediant SBC product series.

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 and other documents as well as software files can be viewed by registered customers at http://www.audiocodes.com/downloads.

© Copyright 2016 AudioCodes Ltd. All rights reserved.
This document is subject to change without notice.

Date Published: March-31-2016

Trademarks

AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, VMAS, VolPerfect, VolPerfectHD, Your Gateway To VoIP, 3GX, VocaNOM and CloudBond 365 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.

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 Web site at www.audiocodes.com/support.

Document Revision Record

<table>
<thead>
<tr>
<th>LTRT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12620</td>
<td>Initial document release for Version 7.0.</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://www.audiocodes.com/downloads.
This page is intentionally left blank.
1 Introduction

This Configuration Note describes how to set up AudioCodes Enterprise Session Border Controller (hereafter, referred to as SBC) for interworking between Sunrise's SIP Trunk and Microsoft's Skype for Business Server 2015 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 in order to better understand the various configuration options. For more information on AudioCodes' SBC Wizard including download option, visit AudioCodes Web site at http://www.audiocodes.com/sbc-wizard (login required).

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and Sunrise Partners who are responsible for installing and configuring Sunrise's SIP Trunk and Microsoft's Skype for Business Server 2015 for enabling VoIP calls using AudioCodes SBC.

1.2 About AudioCodes SBC Product Series

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

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

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

AudioCodes SBC is available as an integrated solution running on top of its field-proven Mediant Media Gateway and Multi-Service Business Router platforms, or as a software-only solution for deployment with third-party hardware.
This page is intentionally left blank.
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>
<tbody>
<tr>
<td>Models</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mediant 500 E-SBC</td>
</tr>
<tr>
<td></td>
<td>• Mediant 800 Gateway &amp; E-SBC</td>
</tr>
<tr>
<td></td>
<td>• Mediant 1000B Gateway &amp; E-SBC</td>
</tr>
<tr>
<td></td>
<td>• Mediant 3000 Gateway &amp; SBC</td>
</tr>
<tr>
<td></td>
<td>• Mediant 2600 E-SBC</td>
</tr>
<tr>
<td></td>
<td>• Mediant 4000 SBC</td>
</tr>
<tr>
<td>Software Version</td>
<td>SIP_7.00A.058.002</td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SIP/UDP (to the Sunrise SIP Trunk)</td>
</tr>
<tr>
<td></td>
<td>• SIP/TCP or TLS (to the S4B FE Server)</td>
</tr>
<tr>
<td>Additional Notes</td>
<td>None</td>
</tr>
</tbody>
</table>

2.2 Sunrise SIP Trunking Version

Table 2-2: Sunrise Version

<table>
<thead>
<tr>
<th>Vendor/Service Provider</th>
<th>Sunrise</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSW Model/Service</td>
<td>IMS SIP Trunk</td>
</tr>
</tbody>
</table>
| Software Version        | IMS 10.2  
CSCF - V100R010C20SPC100,  
patch CSCF_V100R010C20SPH101  
SBC - V300R001C20SPC100,  
patch SE2900_V300R001C20SPH109  |
| Protocol                | SIP |
| Additional Notes        | None |

2.3 Microsoft Skype for Business Server 2015 Version

Table 2-3: Microsoft Skype for Business Server 2015 Version

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Microsoft</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>Skype for Business</td>
</tr>
<tr>
<td>Software Version</td>
<td>Release 2015 6.0.9319.0, CU December 2015 or higher</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 Sunrise SIP Trunk with Skype for Business 2015 was done using the following topology setup:

- Enterprise deployed with Microsoft Skype for Business Server 2015 in its private network 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 Sunrise’s SIP Trunking service.
- AudioCodes SBC is implemented to interconnect between the Enterprise LAN and the SIP Trunk.
  - **Session**: Real-time voice session using the IP-based Session Initiation Protocol (SIP).
  - **Border**: IP-to-IP network border between Skype for Business Server 2015 network in the Enterprise LAN and Sunrise’s SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

**Figure 2-1: Interoperability Test Topology between SBC and Microsoft Skype for Business with Sunrise SIP Trunk**
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>
</table>
| **Network**           | ▪ Microsoft Skype for Business Server 2015 environment is located on the Enterprise's LAN  
                        | ▪ Sunrise SIP Trunk is located on the WAN                           |
| **Signaling Transcoding** | ▪ Microsoft Skype for Business Server 2015 operates with SIP-over-TLS transport type  
                            | ▪ Sunrise SIP Trunk operates with SIP-over-UDP transport type       |
| **Codecs Transcoding** | ▪ Microsoft Skype for Business Server 2015 supports G.711A-law and G.711U-law coders  
                            | ▪ Microsoft Skype for Business Clients (Media Bypass) supports G.722, G.711A-law and G.711U-law coders  
                            | ▪ Sunrise SIP Trunk supports G.722, G729, G.711A-law and G.711U-law coders |
| **Media Transcoding**  | ▪ Microsoft Skype for Business Server 2015 operates with SRTP media type  
                            | ▪ Sunrise SIP Trunk operates with RTP media type                    |

2.4.2 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes SBC interworking between Microsoft Skype for Business Server 2015 and Sunrise’s SIP Trunk.
This page is intentionally left blank.
3 Configuring Skype for Business Server 2015

This chapter describes how to configure Microsoft Skype for Business Server 2015 to operate with AudioCodes SBC.

Note: Dial plans, voice policies, and PSTN usages are also necessary for Enterprise voice deployment; however, they are beyond the scope of this document.

3.1 Configuring the SBC as an IP / PSTN Gateway

The procedure below describes how to configure the SBC as an IP / PSTN Gateway.

➢ To configure SBC as IP/PSTN Gateway and associate it with Mediation Server:

1. On the server where the Topology Builder is installed, start the Skype for Business Server 2015 Topology Builder (Windows Start menu > search for Skype for Business Server Topology Builder), as shown below:

   Figure 3-1: Starting the Skype for Business Server Topology Builder

   ![Skype for Business Server Topology Builder](image)
The following is displayed:

**Figure 3-2: Topology Builder Dialog Box**

![Topology Builder Dialog Box]

2. Select the **Download Topology from existing deployment** option, and then click **OK**; you are prompted to save the downloaded Topology:

**Figure 3-3: Save Topology Dialog Box**

![Save Topology Dialog Box]

3. Enter a name for the Topology file, and then click **Save**. This step enables you to roll back from any changes you make during the installation.
4. The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology

5. Under the Shared Components node, right-click the PSTN gateways node, and then from the shortcut menu, choose New IP/PSTN Gateway, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway
6. The following is displayed:

   **Figure 3-6: Define the PSTN Gateway FQDN**

   ![Figure 3-6: Define the PSTN Gateway FQDN](image)

7. Enter the Fully Qualified Domain Name (FQDN) of the SBC (e.g., **ITSP.S4B.interop**). This FQDN should be equivalent to the configured Subject Name (CN) in the TLS Certificate Context (see Section 4.9.3 on page 61).

8. Click **Next**; the following is displayed:

   **Figure 3-7: Define the IP Address**

   ![Figure 3-7: Define the IP Address](image)

9. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click **Next**.

10. Define a **root trunk** for the PSTN gateway. A trunk is a logical connection between the Mediation Server and a gateway uniquely identified by the following combination: Mediation Server FQDN, Mediation Server listening port (TLS or TCP), gateway IP
and FQDN, and gateway listening port.

**Notes:**
- When defining a PSTN gateway in Topology Builder, you must define a root trunk to successfully add the PSTN gateway to your topology.
- The root trunk cannot be removed until the associated PSTN gateway is removed.

![Figure 3-8: Define the Root Trunk](image)

a. In the 'Listening Port for IP/PSTN Gateway' field, enter the listening port that the SBC will use for SIP messages from the Mediation Server that will be associated with the root trunk of the PSTN gateway (e.g., **5067**). This parameter is later configured in the SIP Interface table (see Section 0 on page 42).

b. In the 'SIP Transport Protocol' field, select the transport type (e.g., **TLS**) that the trunk uses. This parameter is later configured in the SIP Interface table (see Section 0 on page 42).

c. In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN gateway.

d. In the 'Associated Mediation Server Port' field, enter the listening port that the Mediation Server will use for SIP messages from the SBC (e.g., **5067**).

e. Click **Finish**.

The SBC is added as a PSTN gateway, and a trunk is created as shown below:
11. Publish the Topology: In the main tree, select the root node **Skype for Business Server**, and then from the Action menu, choose **Publish Topology**, as shown below:

**Figure 3-10: Choosing Publish Topology**
The following is displayed:

**Figure 3-11: Publish the Topology**

![Publish Topology](image1.png)

12. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

**Figure 3-12: Publishing in Progress**

![Publishing in progress](image2.png)
13. Wait until the publishing topology process completes successfully, as shown below:

**Figure 3-13: Publishing Wizard Complete**

14. Click **Finish**.
3.2 Configuring the "Route" on Skype for Business Server 2015

The procedure below describes how to configure a "Route" on the Skype for Business Server 2015 and to associate it with the SBC PSTN gateway.

➢ To configure the "route" on Skype for Business Server 2015:

1. Start the Microsoft Skype for Business Server 2015 Control Panel (Start > search for Microsoft Skype for Business Server Control Panel), as shown below:

   Figure 3-14: Opening the Skype for Business Server Control Panel

2. You are prompted to enter your login credentials:
3. Enter your domain username and password, and then click OK; the Microsoft Skype for Business Server 2015 Control Panel is displayed:

Figure 3-16: Microsoft Skype for Business Server 2015 Control Panel

4. To enable Media bypass, select **Network Configuration** in the left navigation pane.
5. Select **Global** and click to **Edit**. The **Edit Global Settings** page appears:

![Figure 3-18: Global Settings Page](image)

6. Activate **Enable Media bypass** and click to **Commit**.

7. In the left navigation pane, select **Voice Routing**.

8. In the left navigation pane, select **Voice Routing**.
9. In the Voice Routing page, select the **Route** tab.

**Figure 3-20: Route Tab**
10. Click **New**; the New Voice Route page appears:

![Figure 3-21: Adding New Voice Route](image)

11. In the 'Name' field, enter a name for this route (e.g., **ITSP**).
12. In the ‘Starting digits for numbers that you want to allow’ field, enter the starting digits you want this route to handle (e.g., * to match all numbers), and then click **Add**.
13. Associate the route with the SBC Trunk that you created:
   a. Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

![Figure 3-22: List of Deployed Trunks](image)
b. Select the SBC Trunk you created, and then click OK; the trunk is added to the ‘Associated Trunks’ group list:

Figure 3-23: Selected SBC Trunk

14. Associate a PSTN Usage to this route:
   a. Under the ‘Associated PSTN Usages’ group, click Select and then add the associated PSTN Usage.

Figure 3-24: Associating PSTN Usage to Route
15. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

**Figure 3-25: Confirmation of New Voice Route**

16. From the **Commit** drop-down list, choose **Commit all**, as shown below:

**Figure 3-26: Committing Voice Routes**
The Uncommitted Voice Configuration Settings page appears:

**Figure 3-27: Uncommitted Voice Configuration Settings**

<table>
<thead>
<tr>
<th>Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
</tr>
<tr>
<td>Route to Sunrise IMS</td>
</tr>
</tbody>
</table>

17. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

**Figure 3-28: Confirmation of Successful Voice Routing Configuration**
18. Click Close; the new committed Route is displayed in the Voice Routing page, as shown below:

**Figure 3-29: Voice Routing Screen Displaying Committed Routes**

19. For ITSPs that implement a call identifier, continue with the following steps:

**Note:** The SIP History-Info header provides a method to verify the identity (ID) of the call forwarder (i.e., the Skype for Business user number). This ID is required by Sunrise SIP Trunk in the SIP diversion header. The device adds this ID to the diversion header in the sent INVITE message using the IP Profile (see Section 4.6 on page 48).

   a. In the Voice Routing page, select the **Trunk Configuration** tab. Note that you can add and modify trunk configuration by site or by pool.

   **Figure 3-30: Voice Routing Screen – Trunk Configuration Tab**

   b. Click **Edit**; the Edit Trunk Configuration page appears:
c. Select the **Enable forward call history** check box, and then click **OK**.

d. Repeat Steps 11 through 13 to commit your settings.

e. Verify de-activation of RTCP, activation of Session timers and Media Bypass and deactivation of Refer support. Since some of these parameters are not visible on the graphical interface, the Skype for Business server Management Shell must be used. Use the following command on the Skype for Business server Management Shell:

   ```powershell
   Set-CsTrunkConfiguration -Identity Global -EnableBypass $true -EnableReferSupport $false -RTCPActiveCalls $false -RTCPCallsOnHold $false -EnableSessionTimer $true
   ```

   
f. To verify the configuration, use the following cmdlet:

   ```powershell
   Get-CsTrunkConfiguration
   ```

   ```powershell
   Identity : Global
   OutboundTranslationRulesList : ()
   SipResponseCodeTranslationRulesList : ()
   OutboundCallingNumberTranslationRulesList : ()
   PstnUsages : ()
   Description : 
   ConcentratedTopology : True
   EnableBypass : True
   EnableMobileTrunkSupport : False
   EnableReferSupport : False
   EnableSessionTimer : True
   EnableSignalBoost : False
   MaxEarlyDialogs : 20
   ```
<table>
<thead>
<tr>
<th>Configuration Note</th>
<th>3. Configuring Skype for Business Server 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>RemovePlusFromUri</td>
<td>False</td>
</tr>
<tr>
<td>RTCPActiveCalls</td>
<td>False</td>
</tr>
<tr>
<td>RTCPCallsOnHold</td>
<td>False</td>
</tr>
<tr>
<td>SRTFMode</td>
<td>Required</td>
</tr>
<tr>
<td>EnablePIDFLOSupport</td>
<td>False</td>
</tr>
<tr>
<td>EnableRTPLatching</td>
<td>False</td>
</tr>
<tr>
<td>EnableOnlineVoice</td>
<td>False</td>
</tr>
<tr>
<td>ForwardCallHistory</td>
<td>True</td>
</tr>
<tr>
<td>Enable3pccRefer</td>
<td>False</td>
</tr>
<tr>
<td>ForwardPAI</td>
<td>False</td>
</tr>
<tr>
<td>EnableFastFailoverTimer</td>
<td>True</td>
</tr>
<tr>
<td>EnableLocationRestriction</td>
<td>False</td>
</tr>
<tr>
<td>NetworkSiteID</td>
<td>:</td>
</tr>
</tbody>
</table>
This page is intentionally left blank.
4 Configuring AudioCodes SBC

This chapter provides step-by-step procedures on how to configure AudioCodes SBC for interworking between Microsoft Skype for Business Server 2015 and the Sunrise 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 WAN interface - Sunrise SIP Trunking environment
- SBC LAN interface - Skype for Business Server 2015 environment

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

**Notes:**

- For implementing Microsoft Skype for Business and Sunrise SIP Trunk based on the configuration described in this section, AudioCodes SBC must be installed with a Software License Key that includes the following software features:
  - Microsoft
  - SBC
  - Security
  - DSP
  - RTP
  - SIP

For more information about the Software License Key, contact your AudioCodes sales representative.

- The scope of this interoperability test and document does not cover all security aspects for connecting the SIP Trunk to the Microsoft Skype for Business environment. 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.

- Before you begin configuring the SBC, ensure that the SBC's Web interface Navigation tree is in Advanced-menu display mode. To do this, select the Advanced option, as shown below:

![Advanced menu display](image)

Note that when the SBC is reset, the Navigation tree reverts to Basic-menu display.
4.1 **Step 1: IP Network Interfaces Configuration**

This step 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:
  - Skype for Business servers, located on the LAN
  - Sunrise SIP Trunk, located on the WAN
- SBC connects to the WAN through a DMZ network
- Physical connection: The type of physical connection to the LAN depends on the method used to connect to the Enterprise's network. In the interoperability test topology, SBC connects to the LAN and WAN using dedicated LAN ports (i.e., two ports and two network cables are used).
- SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - WAN (VLAN ID 2)

*Figure 4-1: Network Interfaces in Interoperability Test Topology*
4.1.1 Step 1a: Configure VLANs

➢ To configure the VLANs:

1. Open the Ethernet Device Table page (Configuration tab > VoIP menu > Network > Ethernet Device Table).
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 as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>1</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>2</td>
</tr>
<tr>
<td>Underlying Interface</td>
<td>GROUP_2 (Ethernet port group)</td>
</tr>
<tr>
<td>Name</td>
<td>vlan 2</td>
</tr>
<tr>
<td>Tagging</td>
<td>Untagged</td>
</tr>
</tbody>
</table>

Figure 4-2: Configured VLAN IDs in Ethernet Device Table

4.1.2 Step 1b: Configure Network Interfaces

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

- LAN VoIP (assigned the name "SfB")
- WAN VoIP (assigned the name "Sunrise")

➢ To configure the IP network interfaces:

1. Open the IP Interfaces Table page (Configuration tab > VoIP menu > Network > IP Interfaces Table).
2. Modify the existing LAN network interface:
   a. Select the line with 'Index' 0 of the OAMP + Media + Control table row, and then click Edit.
   b. Configure the interface as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>10.145.205.12 (IP address of SBC)</td>
</tr>
</tbody>
</table>
### Configuration Note 36

**Microsoft Skype for Business 2015 & Sunrise SIP Trunk**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix Length</td>
<td>24 (subnet mask in bits for 255.255.0.0)</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>10.145.205.1</td>
</tr>
<tr>
<td>Interface Name</td>
<td>SfB (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Primary DNS Server IP Address</td>
<td>10.145.205.51</td>
</tr>
<tr>
<td>Secondary DNS Server IP Address</td>
<td>10.145.205.52</td>
</tr>
<tr>
<td>Underlying Device</td>
<td>vlan 1</td>
</tr>
</tbody>
</table>

**a.** Click **Save**.

**3.** Add a network interface for the WAN side:

**b.** Click **Add**.

**c.** Configure the interface as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Type</td>
<td>Media + Control</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.201.30 (WAN IP address)</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>24 (for 255.255.255.128)</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Interface Name</td>
<td>Sunrise</td>
</tr>
<tr>
<td>Primary DNS Server IP Address</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Secondary DNS Server IP Address</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Underlying Device</td>
<td>vlan 2</td>
</tr>
</tbody>
</table>

**a.** Click **Add**.

The configured IP network interfaces are shown below:

**Figure 4-3: Configured Network Interfaces in IP Interfaces Table**

![Image](image-url)
4.1.3 Step 1c: Adding Static Routes to Sunrise SBC

This step describes how to configure the following static IP routes to sunrise SBCs:

- 192.168.200.0/24 IMS Next Hop
- 10.17.220.0/28 IMS Zürich SIP
- 10.17.220.16/28 IMS Zürich Media
- 10.24.220.0/28 IMS Bern SIP
- 10.24.220.16/28 IMS Bern Media

To configure the IP network interfaces:

1. Open the Static Route Table page (Configuration tab > VoIP menu > Network > Static Route Table).
   a. Click Add.
   b. Configure the static route as follows:
      
      | Parameter    | Value                          |
      |--------------|-------------------------------|
      | Index        | 0                             |
      | Device Name  | vlan 2                         |
      | Destination  | 192.168.200.0                 |
      | Prefix length| 24                            |
      | Gateway      | 192.168.201.20 (Firewall internal IP address) |
      | Description  | IMS Next Hop                  |
   c. Click to Add.

2. Add the static route to IMS Zürich for SIP.
   a. Click Add.
   b. Configure the static route as follows:
      
      | Parameter    | Value                          |
      |--------------|-------------------------------|
      | Index        | 1                             |
      | Device Name  | vlan 2                         |
      | Destination  | 10.17.220.0                  |
      | Prefix length| 28                            |
      | Gateway      | 192.168.201.20 (Firewall internal IP address) |
      | Description  | IMS ZUR SIP                  |
   c. Click to Add.
3. Add the static route to IMS Zürich for Media.
   a. Click **Add**.
   b. Configure the static route as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>2</td>
</tr>
<tr>
<td>Device Name</td>
<td>vlan 2</td>
</tr>
<tr>
<td>Destination</td>
<td>10.17.220.16</td>
</tr>
<tr>
<td>Prefix length</td>
<td>28</td>
</tr>
<tr>
<td>Gateway</td>
<td>192.168.201.20 (Firewall internal IP address)</td>
</tr>
<tr>
<td>Description</td>
<td>IMS ZUR Media</td>
</tr>
</tbody>
</table>
   c. Click to **Add**.

4. Add the static route to IMS Bern for SIP.
   a. Click **Add**.
   b. Configure the static route as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>3</td>
</tr>
<tr>
<td>Device Name</td>
<td>vlan 2</td>
</tr>
<tr>
<td>Destination</td>
<td>10.24.220.0</td>
</tr>
<tr>
<td>Prefix length</td>
<td>28</td>
</tr>
<tr>
<td>Gateway</td>
<td>192.168.201.20 (Firewall internal IP address)</td>
</tr>
<tr>
<td>Description</td>
<td>IMS BER SIP</td>
</tr>
</tbody>
</table>
   c. Click to **Add**.

5. Add the static route to IMS Bern for Media.
   a. Click **Add**.
   b. Configure the static route as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>4</td>
</tr>
<tr>
<td>Device Name</td>
<td>vlan 2</td>
</tr>
<tr>
<td>Destination</td>
<td>10.24.220.0</td>
</tr>
<tr>
<td>Prefix length</td>
<td>28</td>
</tr>
<tr>
<td>Gateway</td>
<td>192.168.201.20 (Firewall internal IP address)</td>
</tr>
<tr>
<td>Description</td>
<td>IMS BER Media</td>
</tr>
</tbody>
</table>
   c. Click to **Add**.
The configured static IP routes are shown below:

Figure 4-4: Configured Network Interfaces in IP Interfaces Table

### 4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

- **To enable the SBC application:**
  1. Open the Applications Enabling page (Configuration tab > VoIP menu > Applications Enabling > Applications Enabling).
  2. From the 'SBC Application' drop-down list, select **Enable**.
  3. Click **Submit**.
  4. Reset the SBC with a burn to flash for this setting to take effect (see Section 4.15 on page 82).
4.3 Step 3: Configure Media Realms

This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

- **To configure Media Realms:**
  1. Open the Media Realm Table page (Configuration tab > VoIP menu > VoIP Network > Media Realm Table).
  2. Add a Media Realm for the LAN interface. You can use the default Media Realm (Index 0), but modify it as shown below:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>0</td>
</tr>
<tr>
<td>Media Realm Name</td>
<td>MR SfB (descriptive name)</td>
</tr>
<tr>
<td>IPv4 Interface Name</td>
<td>Voice</td>
</tr>
<tr>
<td>Port Range Start</td>
<td>6000 (represents lowest UDP port number used for media on LAN)</td>
</tr>
<tr>
<td>Number of Media Session Legs</td>
<td>100 (media sessions assigned with port range)</td>
</tr>
</tbody>
</table>

![Figure 4-6: Configuring Media Realm for LAN](image)

3. Configure a Media Realm for WAN traffic:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>1</td>
</tr>
<tr>
<td>Media Realm Name</td>
<td>MR Sunrise (arbitrary name)</td>
</tr>
<tr>
<td>IPv4 Interface Name</td>
<td>Sunrise</td>
</tr>
<tr>
<td>Port Range Start</td>
<td>7000 (represents lowest UDP port number used for media on WAN)</td>
</tr>
<tr>
<td>Number of Media Session Legs</td>
<td>100 (media sessions assigned with port range)</td>
</tr>
</tbody>
</table>
The configured Media Realms are shown in the figure below:

**Figure 4-8: Configured Media Realms in Media Realm Table**
4.4 Step 4: Configure SIP Signaling Interfaces

This step describes how to configure SIP Interfaces. For the interoperability test topology, an internal and external SIP Interface must be configured for the SBC.

To configure SIP Interfaces:

1. Open the SIP Interface Table page (Configuration tab > VoIP menu > VoIP Network > SIP Interface Table).
2. Add a SIP Interface for the LAN interface. You can use the default SIP Interface (Index 0), but modify it as shown below:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>0</td>
</tr>
<tr>
<td>Interface Name</td>
<td>SfB (see note at the end of this section)</td>
</tr>
<tr>
<td>Network Interface</td>
<td>SfB</td>
</tr>
<tr>
<td>Application Type</td>
<td>SBC</td>
</tr>
<tr>
<td>UDP Port (for supporting Fax ATA device)</td>
<td>5068 (if required)</td>
</tr>
<tr>
<td>TCP Port</td>
<td>5068 (if required)</td>
</tr>
<tr>
<td>TLS Port</td>
<td>5067 (see note below)</td>
</tr>
<tr>
<td>Media Realm</td>
<td>MR SfB</td>
</tr>
</tbody>
</table>

Note: The TLS port parameter must be identically configured in the Skype for Business Topology Builder (see Section 3.1 on page 13).

3. Configure a SIP Interface for the WAN:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>1</td>
</tr>
<tr>
<td>Interface Name</td>
<td>Sunrise</td>
</tr>
<tr>
<td>Network Interface</td>
<td>Sunrise</td>
</tr>
<tr>
<td>Application Type</td>
<td>SBC</td>
</tr>
<tr>
<td>UDP Port</td>
<td>5061</td>
</tr>
<tr>
<td>TCP Port</td>
<td>0</td>
</tr>
<tr>
<td>TLS Port</td>
<td>5061 (only for TLS connection option)</td>
</tr>
<tr>
<td>Media Realm</td>
<td>MR Sunrise</td>
</tr>
</tbody>
</table>
4. Configuring AudioCodes SBC

The configured SIP Interfaces are shown in the figure below:

Figure 4-9: Configured SIP Interfaces in SIP Interface Table

![SIP Interface Table](image)

Note: Unlike in previous software releases where configuration entities (e.g., SIP Interface, Proxy Sets, and IP Groups) were associated with each other using table row indices, Version 7.0 uses the string names of the configuration entities. Therefore, it is recommended to configure each configuration entity with meaningful names for easy identification.

4.5 Step 5: Configure Proxy Sets

This step 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:

- Microsoft Skype for Business Server 2015
- Sunrise SIP Trunk
- Fax supporting ATA device (optional)

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

➢ To configure Proxy Sets:

1. Open the Proxy Sets Table page (Configuration tab > VoIP menu > VoIP Network > Proxy Sets Table).
2. Add a Proxy Set for the Skype for Business Server 2015. You can use the default Proxy Set (Index 0), but modify it as shown below:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Set ID</td>
<td>0</td>
</tr>
<tr>
<td>Proxy Name</td>
<td>SfB</td>
</tr>
<tr>
<td>SBC IPv4 SIP Interface</td>
<td>SfB</td>
</tr>
<tr>
<td>Proxy Keep Alive</td>
<td>Using Options</td>
</tr>
<tr>
<td>Load Balancing Method</td>
<td>Round Robin</td>
</tr>
</tbody>
</table>
3. Configure a Proxy Address Table for Proxy Set for Skype for Business Server 2015:
   a. Go to Configuration tab > VoIP menu > VoIP Network > Proxy Sets Table > Proxy Address Table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>0</td>
</tr>
<tr>
<td>Proxy Address</td>
<td>FEPool01.sunlab.ch:5067</td>
</tr>
<tr>
<td></td>
<td>(Skype for Business Server 2015 FQDN and destination port)</td>
</tr>
<tr>
<td>Transport Type</td>
<td>TLS</td>
</tr>
</tbody>
</table>
### 4. Configuring AudioCodes SBC

#### Figure 4-11: Configuring Proxy Address for Microsoft Skype for Business Server 2015

![Figure 4-11: Configuring Proxy Address for Microsoft Skype for Business Server 2015](image)

#### Figure 4-12: Configuring Proxy Set for Sunrise SIP Trunk

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Set ID</td>
<td>1</td>
</tr>
<tr>
<td>Proxy Name</td>
<td>Sunrise</td>
</tr>
<tr>
<td>SBC IPv4 SIP Interface</td>
<td>Sunrise</td>
</tr>
<tr>
<td>Proxy Keep Alive</td>
<td>Using Options</td>
</tr>
<tr>
<td>Proxy Hot Swap</td>
<td>Disable</td>
</tr>
</tbody>
</table>

![Figure 4-12: Configuring Proxy Set for Sunrise SIP Trunk](image)
a. Configure a Proxy Address Table for Proxy Set 1:

b. Go to Configuration tab > VoIP menu > VoIP Network > Proxy Sets Table > Proxy Address Table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>0</td>
</tr>
<tr>
<td>Proxy Address</td>
<td>10.17.220.5:5060 (IP address / FQDN and destination port)</td>
</tr>
<tr>
<td>Transport Type</td>
<td>UDP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>1</td>
</tr>
<tr>
<td>Proxy Address</td>
<td>10.24.220.5:5060 (IP address / FQDN and destination port)</td>
</tr>
<tr>
<td>Transport Type</td>
<td>UDP</td>
</tr>
</tbody>
</table>

Figure 4-13: Configuring Proxy Address for Sunrise SIP Trunk

5. Configure a Proxy Set for Fax supporting ATA device (if required):

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Set ID</td>
<td>2</td>
</tr>
<tr>
<td>Proxy Name</td>
<td>Fax</td>
</tr>
<tr>
<td>SBC IPv4 SIP Interface</td>
<td>SfB</td>
</tr>
</tbody>
</table>
4. Configuring AudioCodes SBC

Version 7.0 47 AudioCodes Mediant SBC

Figure 4-14: Configuring Proxy Set for Fax ATA device

a. Configure a Proxy Address Table for Proxy Set 2:

b. Go to Configuration tab > VoIP menu > VoIP Network > Proxy Sets Table > Proxy Address Table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>0</td>
</tr>
<tr>
<td>Proxy Address</td>
<td>10.145.205.99:5060 (IP address / FQDN and destination port)</td>
</tr>
<tr>
<td>Transport Type</td>
<td>UDP</td>
</tr>
</tbody>
</table>

Figure 4-15: Configuring Proxy Address for Fax ATA device
Step 6: Configure IP Profiles

This step 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).

In this interoperability test topology, IP Profiles need to be configured for the following IP entities:

- Microsoft Skype for Business Server 2015 - to operate in secure mode using SRTP and TLS
- Sunrise SIP trunk - to operate in non-secure mode using RTP and UDP (optional SRTP and TLS available)

To configure IP Profile for the Skype for Business Server 2015:

1. Open the IP Profile Settings page (Configuration tab > VoIP > Coders and Profiles > IP Profile Settings).
2. Click Add.
3. Click the Common tab, and then configure the parameters as follows:

<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>SfB</td>
</tr>
<tr>
<td>Signaling DiffServ</td>
<td>24</td>
</tr>
<tr>
<td>Symmetric MKI</td>
<td>Enable</td>
</tr>
<tr>
<td>MKI Size</td>
<td>1</td>
</tr>
<tr>
<td>Reset SRTP State Upon Re-key</td>
<td>Enable</td>
</tr>
<tr>
<td>Generate SRTP keys mode:</td>
<td>Always</td>
</tr>
</tbody>
</table>
4. Click the **SBC Signaling** tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-Asserted-Identity Header Mode</td>
<td>Remove</td>
</tr>
<tr>
<td>Session Expires Mode</td>
<td>Supported</td>
</tr>
<tr>
<td>Remote Update Support</td>
<td>Supported Only After Connect</td>
</tr>
<tr>
<td>Remote re-INVITE Support</td>
<td>Supported Only With SDP</td>
</tr>
<tr>
<td>Remote Delayed Offer Support</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Remote REFER Mode</td>
<td>Handle Locally (required, as Skype for Business Server 2015 does not support receipt of SIP REFER)</td>
</tr>
<tr>
<td>Remote 3xx Mode</td>
<td>Handle Locally (required, as Skype for Business Server 2015 does not support receipt of SIP 3xx responses)</td>
</tr>
<tr>
<td>Remote Early Media RTP Detection Behavior</td>
<td>By Media (required, as Skype for Business Server 2015 does not send RTP immediately to remote side when it sends a SIP 18x response)</td>
</tr>
<tr>
<td>Reliable Held Tone Source</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Configuration Note 50

**Microsoft Skype for Business 2015 & Sunrise SIP Trunk**

#### Figure 4-18: Configuring IP Profile for Skype for Business Server 2015 – SBC Signaling Tab

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Play Held Tone</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote Hold Format</td>
<td>Inactive</td>
</tr>
</tbody>
</table>

5. Click the **SBC Media** tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extension Coders Group ID</td>
<td>Coders Group 1</td>
</tr>
<tr>
<td>Allowed Audio Coders Group ID</td>
<td>Coders Group 1</td>
</tr>
<tr>
<td>Allowed Coders Mode</td>
<td>Restriction and Preference</td>
</tr>
<tr>
<td>SBC Media Security Mode</td>
<td>SRTP</td>
</tr>
<tr>
<td>Enforce MKI Size</td>
<td>Enforce</td>
</tr>
<tr>
<td>Use Silence Suppression</td>
<td>Add</td>
</tr>
</tbody>
</table>
To configure an IP Profile for the Sunrise SIP Trunk:

1. Click **Add**.
2. Click the **Common** tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>2</td>
</tr>
<tr>
<td>Profile Name</td>
<td>Sunrise</td>
</tr>
<tr>
<td>Signaling DiffServ</td>
<td>24</td>
</tr>
</tbody>
</table>
3. Click the **SBC Signaling** tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-Asserted-Identity Header Mode</td>
<td>As Is</td>
</tr>
<tr>
<td>Diversion Header Mode</td>
<td>Add (required for anonymous calls)</td>
</tr>
<tr>
<td>Session Expires Mode</td>
<td>Supported</td>
</tr>
<tr>
<td>Remote Update Support</td>
<td>Not Supported (to make sure, UPDATE is converted to re-INVITE)</td>
</tr>
<tr>
<td>Remote REFER Behavior</td>
<td>Handle Locally (SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)</td>
</tr>
<tr>
<td>Remote Early Media RTP Detection Mode</td>
<td>By Media</td>
</tr>
<tr>
<td>Play Held Tone</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote Hold Format</td>
<td>Not Supported (To make sure MoH from Skype for Business or SBC is played and not Sunrise default MoH)</td>
</tr>
</tbody>
</table>
4. Click the SBC Media tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extension Coders Group ID</td>
<td>Coders Group 2</td>
</tr>
<tr>
<td>Allowed Audio Coders Group ID</td>
<td>Coders Group 2</td>
</tr>
<tr>
<td>Allowed Coders Mode</td>
<td>Restriction and Preference</td>
</tr>
<tr>
<td>Media Security Behavior</td>
<td>RTP</td>
</tr>
</tbody>
</table>
To configure an IP Profile for the FAX supporting ATA (if required):

1. Click Add.
2. Click the Common tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>3</td>
</tr>
<tr>
<td>Profile Name</td>
<td>Fax</td>
</tr>
<tr>
<td>Signaling DiffServ</td>
<td>24</td>
</tr>
</tbody>
</table>
3. Click the **SBC Signaling** tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Parameters</td>
<td>Leave as Default</td>
</tr>
</tbody>
</table>

4. Click the **SBC Media** tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Parameters</td>
<td>Leave as default</td>
</tr>
</tbody>
</table>
4.7  **Step 7: Configure IP Groups**

This step 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:

- Skype for Business Server 2015 (Mediation Server) located on LAN
- Sunrise SIP Trunk located on WAN
- Fax supporting ATA device located on LAN (if required)

**To configure IP Groups:**

1. Open the IP Group Table page (Configuration tab > VoIP menu > VoIP Network > IP Group Table).
2. Add an IP Group for the Skype for Business Server 2015. You can use the default IP Group (Index 0), but modify it as shown below:

<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>SfB</td>
</tr>
<tr>
<td>Type</td>
<td>Server</td>
</tr>
<tr>
<td>Proxy Set</td>
<td>SfB</td>
</tr>
<tr>
<td>IP Profile</td>
<td>SfB</td>
</tr>
<tr>
<td>Media Realm</td>
<td>MR SfB</td>
</tr>
<tr>
<td>Classify By Proxy Set</td>
<td>Enable</td>
</tr>
<tr>
<td>Inbound Message Manipulation Set</td>
<td>1</td>
</tr>
<tr>
<td>Outbound Message Manipulation Set</td>
<td>1</td>
</tr>
</tbody>
</table>

3. Configure an IP Group for the Sunrise 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>Sunrise</td>
</tr>
<tr>
<td>Type</td>
<td>Server</td>
</tr>
<tr>
<td>Proxy Set</td>
<td>Sunrise</td>
</tr>
<tr>
<td>IP Profile</td>
<td>Sunrise</td>
</tr>
<tr>
<td>Media Realm</td>
<td>MR Sunrise</td>
</tr>
<tr>
<td>Inbound Message Manipulation Set</td>
<td>2</td>
</tr>
<tr>
<td>Outbound Message Manipulation Set</td>
<td>2</td>
</tr>
</tbody>
</table>
4. Configure an IP Group for the Fax supporting ATA device:

<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>Fax</td>
</tr>
<tr>
<td>Type</td>
<td>Server</td>
</tr>
<tr>
<td>Proxy Set</td>
<td>Fax</td>
</tr>
<tr>
<td>IP Profile</td>
<td>Fax</td>
</tr>
<tr>
<td>Media Realm</td>
<td>MR SfB</td>
</tr>
</tbody>
</table>

The configured IP Groups are shown in the figure below:

Figure 4-24: Configured IP Groups in IP Group Table
4.8 Step 8: Configure Coders

This step describes how to configure coders (termed Coder Group). As Skype for Business Server 2015 supports the G.711 coder and with media bypass a long list of other coders while the network connection to Sunrise SIP Trunk restrict operation to G.722, G.729, and G.711, you need to add a Coder Group with the G.722 and G.729 coder for the Sunrise SIP Trunk.

Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 4.6 on page 48).

➢ To configure coders:
1. Open the Coder Group Settings (Configuration tab > VoIP menu > Coders and Profiles > Coders Group Settings).
2. Configure a Coder Group for Skype for Business Server 2015:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coder Group ID</td>
<td>1</td>
</tr>
<tr>
<td>Coder Name</td>
<td>▪ G.711 U-law</td>
</tr>
<tr>
<td></td>
<td>▪ G.711 A-law</td>
</tr>
<tr>
<td>Silence Suppression</td>
<td>Enable (for both coders)</td>
</tr>
</tbody>
</table>

Figure 4-25: Configuring Coder Group for Skype for Business Server 2015

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Skype for Business Server 2015 the G.722 coder whenever possible (only for media bypass) and remove unsupported coders. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the Skype for Business Server Trunk (see Section 4.6 on page 48).

➢ To set a preferred coder for the Sunrise SIP Trunk:
1. Open the Allowed Coders Group page (Configuration tab > VoIP menu > SBC > Allowed Audio Coders Group).
2. Configure an Allowed Coder as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed Audio Coders Group ID</td>
<td>1</td>
</tr>
<tr>
<td>Coder Name</td>
<td>G.722</td>
</tr>
<tr>
<td></td>
<td>G.711 A-law</td>
</tr>
<tr>
<td></td>
<td>G.711 U-law</td>
</tr>
</tbody>
</table>
3. Configure a Coder Group for Sunrise SIP Trunk:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coder Group ID</td>
<td>2</td>
</tr>
</tbody>
</table>
| Coder Name         | G.729
|                    | G.711 A-Law
|                    | G.711 U-Law |

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Sunrise SIP Trunk uses the G.722 coder whenever possible. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the Sunrise SIP Trunk (see Section 4.6 on page 48).

➢ To set a preferred coder for the Sunrise SIP Trunk:

1. Open the Allowed Coders Group page (Configuration tab > VoIP menu > SBC > Allowed Audio Coders Group).

2. Configure an Allowed Coder as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed Audio Coders Group ID</td>
<td>2</td>
</tr>
</tbody>
</table>
| Coder Name         | G.722
|                    | G.729
|                    | G.711 A-Law
|                    | G.711 U-Law |
4.9 Step 9: SIP TLS Connection Configuration

This section describes how to configure the SBC for using a TLS connection with the Skype for Business Server 2015 Mediation Server. This is essential for a secure SIP TLS connection.

4.9.1 Step 9a: Configure the NTP Server Address

This step describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or a third-party server) to ensure that the SBC receives the accurate and current date and time. This is necessary for validating certificates of remote parties.

➢ To configure the NTP server address:

1. Open the Application Settings page (Configuration tab > System > Time And Date).
2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., 10.145.205.51).
3. Configure Time Zone settings as required.

4. Click Submit.
4.9.2 **Step 9b: Configure the TLS version**

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

➢ **To configure the TLS version:**
1. Open the TLS Contexts page *(Configuration tab > System menu > TLS Contexts).*
2. In the TLS Contexts table, select the required TLS Context index row (usually default index 0 will be used), and then click ‘Edit’.
3. From the ‘TLS Version’ drop-down list, select ‘TLSv1.0 TLSv1.1 and TLSv1.2’

![Figure 4-30: Configuring TLS version](image)

4. Click **Submit**.

4.9.3 **Step 9c: Configure a Certificate**

This step describes how to exchange a certificate with Microsoft Certificate Authority (CA). The certificate is used by the SBC to authenticate the connection with Skype for Business Server 2015.

The procedure involves the following main steps:

b. Requesting Device Certificate from CA.
c. Obtaining Trusted Root Certificate from CA.
d. Deploying Device and Trusted Root Certificates on SBC.

**Note:** The Subject Name (CN) field parameter should be identically configured in the DNS Active Directory and Topology Builder (see Section 3.1 on page 13).
Configuration Note 62

Document #: LTRT-12620

Microsoft Skype for Business 2015 & Sunrise SIP Trunk

Configure a certificate:

1. Open the TLS Contexts page (Configuration tab > System menu > TLS Contexts).
2. In the TLS Contexts table, select the required TLS Context index row (usually default index 0 will be used), and then click the TLS Context Certificates button, located at the bottom of the TLS Contexts page; the Context Certificates page appears.
3. Change Private Key Size to 2048.
4. Click the Generate Private-Key button and accept the warning message box with Ok.
5. Under the Certificate Signing Request, do the following:
   a. In the 'Subject Name [CN]' field, enter the SBC FQDN name (e.g., NE0002.intra.sunlab.ch).
   b. Fill in the rest of the request fields according to your security provider's instructions.
6. Click the Create CSR button; a textual certificate signing request is displayed in the area below the button:

   **Figure 4-31: Certificate Signing Request – Creating CSR**

   ```
   -----BEGIN CERTIFICATE REQUEST-----
   MIICCsTCAZrCAxQAumoDEhNHA0GUA1UEEAkWNiMBAAYmYaJJLeguL1Bn2a5mB1m4bO
   1BLkBGcR36YXvZkJ1MwMTEyMDQwMTY0MDE0NTg0MDAgBg==
   NE0002.intra.sunlab.ch
   NE0002.intra.sunlab.ch
   IT
   Sunnac
   CH
   Zurich
   2H
   CH
   
   After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.
   
   -----BEGIN CERTIFICATE REQUEST-----

   Copy the CSR from the line "-----BEGIN CERTIFICATE REQUEST-----" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, certreq.txt.

8. Open a command prompt on your Windows PC or Server: Press Windows-Key + R, enter cmd.exe and press Enter key.

9. Enter the following command (one line, you can modify the CertificateTemplate Attribute as requested, make sure, to enter the correct path to certreq.txt):

certreq.exe -submit -attrib "CertificateTemplate:WebServer" certreq.txt newcert.cer
10. A window appears. Choose your issuing CA:

**Figure 4-32: Microsoft Certificate Services Web Page**

![Certificate Authority List](image)

11. The certificate will be stored in the defined file. For confirmation, you get the following response in command prompt:

```
Active Directory Enrollment Policy
{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}
ldap:
RequestId: 29
RequestId: "29"
Certificate retrieved(Issued) Issued
```

12. Request the public root certificate of your CA as Base64 file from your CA Administrator.

13. In the SBC's Web interface, return to the **TLS Contexts** page and do the following:
   a. In the TLS Contexts table, select the required TLS Context index row (typically, the default TLS Context at Index 0 is used), and then click the **TLS Context Certificates** button, located at the bottom of the TLS Contexts page; the Context Certificates page appears.
   b. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the `gateway.cer` certificate file that you saved on your computer in Step 11, and then click **Send File** to upload the certificate to the SBC.

**Figure 4-33: Upload Device Certificate Files from your Computer Group**

![Upload Device Certificate Files](image)

c. In the SBC's Web interface, return to the **TLS Contexts** page.
d. In the TLS Contexts table, select the required TLS Context index row, and then click the **TLS Context Trusted-Roots Certificates** button, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.

e. Click the **Import** button, and then select the root certificate file to load.

Figure 4-34: Importing Root Certificate into Trusted Certificates Store

14. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.

15. Reset the SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 82).

### 4.10 Step 10: Configure SRTP

This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the SBC to operate in the same manner. Note that SRTP was enabled for Skype for Business Server 2015 when you configured an IP Profile for Skype for Business Server 2015 (see Section 4.6 on page 48).

➢ **To configure media security:**

1. Open the Media Security page (*Configuration* tab > *VoIP* menu > *Media* menu > *Media Security*).

2. Configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Security</td>
<td>Enable</td>
</tr>
</tbody>
</table>

Figure 4-35: Configuring SRTP

3. Click **Submit**.

4. Reset the SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 82).
4.11 Step 11: Configure Maximum IP Media Channels

This step describes how to configure the maximum number of required IP media channels. The number of media channels represents the number of DSP channels that the SBC allocates to call sessions.

**Note:** This step is required only if transcoding is required.

To configure the maximum number of IP media channels:

1. Open the IP Media Settings page (Configuration tab > VoIP menu > SIP Definitions > Advanced Parameters).

   ![Figure 4-36: Configuring Number of Media Channels](image)

2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., 30).
3. Click Submit.
4. Reset the SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 82).

4.12 Step 12: Configure IP-to-IP Call Routing Rules

This step 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. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 0 on page 55, IP Group 1 represents Skype for Business Server 2015, and IP Group 2 represents Sunrise SIP Trunk.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Skype for Business Server 2015 (LAN) and Sunrise SIP Trunk (WAN):

- Terminate SIP OPTIONS messages on the SBC that are received from the LAN
- Calls from Skype for Business Server 2015 to Sunrise SIP Trunk
- Calls from Sunrise SIP Trunk to Fax supporting ATA device (if required)
- Calls from Sunrise SIP Trunk to Skype for Business Server 2015
- Calls from Fax supporting ATA device to Sunrise SIP Trunk (if required)

To configure IP-to-IP routing rules:

1. Open the IP-to-IP Routing Table page (Configuration tab > VoIP menu > SBC > Routing SBC > IP-to-IP Routing Table).
2. Configure a rule to terminate SIP OPTIONS messages received from the LAN:
   a. Click Add.
   b. Click the Rule tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Destination Type</td>
<td>Dest Address</td>
</tr>
<tr>
<td>Destination Address</td>
<td>internal</td>
</tr>
</tbody>
</table>

**Figure 4-37: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab**

\[\text{Click the Action tab, and then configure the parameters as follows:} \]

Index | 0  
Name | OPTIONS termination (arbitrary descriptive name)  
Source IP Group | Any  
Request Type | OPTIONS  

**Table:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Type</td>
<td>Dest Address</td>
</tr>
<tr>
<td>Destination Address</td>
<td>internal</td>
</tr>
</tbody>
</table>
Figure 4-38: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab

3. To configure rule to route calls from Sunrise SIP Trunk to Fax supporting ATA device:
   a. Click **Add**.
   b. Click the **Rule** tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>1</td>
</tr>
<tr>
<td>Route Name</td>
<td>ITSP to Fax (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Source IP Group</td>
<td>Sunrise</td>
</tr>
</tbody>
</table>
c. Click the **Action** tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Type</td>
<td>IP Group</td>
</tr>
<tr>
<td>Destination IP Group</td>
<td>Fax</td>
</tr>
<tr>
<td>Destination SIP Interface</td>
<td>SfB</td>
</tr>
</tbody>
</table>
4. Configure a rule to route calls from Skype for Business Server 2015 to Sunrise SIP Trunk:
   
   a. Click Add.
   
   b. Click the Rule tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>2</td>
</tr>
<tr>
<td>Route Name</td>
<td>SfB to ITSP (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Source IP Group</td>
<td>SfB</td>
</tr>
</tbody>
</table>
c. Click the **Action** tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Type</td>
<td>IP Group</td>
</tr>
<tr>
<td>Destination IP Group</td>
<td>Sunrise</td>
</tr>
<tr>
<td>Destination SIP Interface</td>
<td>Sunrise</td>
</tr>
</tbody>
</table>
5. To configure rule to route calls from Sunrise SIP Trunk to Skype for Business Server 2015:
   a. Click **Add**.
   b. Click the **Rule** tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>3</td>
</tr>
<tr>
<td>Route Name</td>
<td>ITSP to SfB (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Source IP Group</td>
<td>Sunrise</td>
</tr>
</tbody>
</table>
c. Click the **Action** tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Type</td>
<td>IP Group</td>
</tr>
<tr>
<td>Destination IP Group</td>
<td>SfB</td>
</tr>
<tr>
<td>Destination SIP Interface</td>
<td>SfB</td>
</tr>
</tbody>
</table>
6. Configure a rule to route calls from Fax supporting ATA device to Sunrise SIP Trunk:
   a. Click Add.
   b. Click the Rule tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>4</td>
</tr>
<tr>
<td>Route Name</td>
<td>Fax to ITSP (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Source IP Group</td>
<td>Fax</td>
</tr>
</tbody>
</table>
c. Click the Action tab, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Type</td>
<td>IP Group</td>
</tr>
<tr>
<td>Destination IP Group</td>
<td>Sunrise</td>
</tr>
<tr>
<td>Destination SIP Interface</td>
<td>Sunrise</td>
</tr>
</tbody>
</table>
The configured routing rules are shown in the figure below:

**Figure 4-47: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table**

**Note:** The routing configuration may change according to your specific deployment topology.
4.13 Step 13: Configure Message Manipulation Rules

This step 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:

1. Open the Message Manipulations page (Configuration tab > VoIP menu > SIP Definitions > Msg Policy & Manipulation > Message Manipulations).
2. Configure a new manipulation rule (Manipulation Set 1) for Skype For Business Server. This rule applies to response messages sent to the Skype For Business Server IP Group to make sure Session Timer Updates will be sent.

<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 Allow UPDATE</td>
</tr>
<tr>
<td>Manipulation Set ID</td>
<td>1</td>
</tr>
<tr>
<td>Message Type</td>
<td>invite.response</td>
</tr>
<tr>
<td>Condition</td>
<td>header.allow !contains 'UPDATE'</td>
</tr>
<tr>
<td>Action Subject</td>
<td>header.allow</td>
</tr>
<tr>
<td>Action Type</td>
<td>Modify</td>
</tr>
<tr>
<td>Action Value</td>
<td>'CANCEL,BYE,INVITE,PRACK,UPDATE'</td>
</tr>
</tbody>
</table>

Figure 4-48: Configuring SIP Message Manipulation Rule 0 (for Skype For Business Servers)
3. Configure another two manipulation rules (Manipulation Set 2) for Sunrise SIP Trunk. This rule is applied to request messages sent to the Sunrise SIP Trunk IP Group for transferred calls on Skype for Business Server 2015. This rule generates changes the Referred-by header from Skype For Business to a diversion header.

<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>Change Referred-by</td>
</tr>
<tr>
<td>Manipulation Set ID</td>
<td>2</td>
</tr>
<tr>
<td>Message Type</td>
<td>invite.request</td>
</tr>
<tr>
<td>Condition</td>
<td>header.referred-by exists</td>
</tr>
<tr>
<td>Action Subject</td>
<td>header.Diversion</td>
</tr>
<tr>
<td>Action Type</td>
<td>Add</td>
</tr>
<tr>
<td>Action Value</td>
<td>'&lt;+header.referred-by.URL+&gt;'</td>
</tr>
</tbody>
</table>

Figure 4-49: Configuring SIP Message Manipulation Rule 1 (for Sunrise SIP Trunk)

<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>Remove Referred-by</td>
</tr>
<tr>
<td>Manipulation Set ID</td>
<td>2</td>
</tr>
<tr>
<td>Action Subject</td>
<td>header.referred-by</td>
</tr>
<tr>
<td>Action Type</td>
<td>Remove</td>
</tr>
<tr>
<td>Row Role</td>
<td>Use Previous Condition</td>
</tr>
</tbody>
</table>
4. Assign Manipulation Set IDs 1 to the Skype for Business 2015 IP Group:
   a. Open the IP Group Table page (Configuration tab > VoIP menu > VoIP Network > IP Group Table).
   b. Select the row of the Skype for Business 2015 IP Group, and then click Edit.
   c. Click the SBC tab.
   d. Set the 'Inbound Message Manipulation Set' field to 1.
4. Configuring AudioCodes SBC

**Figure 4-52: Assigning Manipulation Set to the Skype for Business 2015 IP Group**

![Edit Row](image)

**e.** Click **Submit**.

5. Assign Manipulation Set ID 2 to the Sunrise SIP trunk IP Group:
   a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
   b. Select the row of the Sunrise SIP trunk IP Group, and then click **Edit**.
   c. Click the **SBC** tab.
   d. Set the 'Outbound Message Manipulation Set' field to 2.
Figure 4-53: Assigning Manipulation Set 2 to the Sunrise SIP Trunk IP Group

![Edit Row window](image)

**e.** Click Submit.
4.14 **Step 14: Miscellaneous Configuration**

This section describes miscellaneous SBC configuration.

**4.14.1 SBC General Settings**

- **To configure call forking:**
  1. Open the General Settings page (
     Configuration tab > VoIP menu > SBC > General Settings).
  2. From the ‘SBC Forking Handling Mode’ drop-down list, select **Sequential**.
     For the interoperability test topology, if a SIP 18x response with SDP is received, the
     SBC opens a voice stream according to the received SDP. The SBC re-opens the
     stream according to subsequently received 18x responses with SDP or plays a
     ringback tone if a 180 response without SDP is received. It is mandatory to set this
     field for the Skype for Business Server 2015 environment.
  3. Set the value of ‘Session-Expires [sec]’ to 1800.
  4. Set the value of ‘Max Forwards Limit’ to 70.

![Figure 4-54: Configuring SBC General Settings](image)

  5. Click **Submit**.

**4.14.2 Configure SBC Alternative Routing Reasons**

This step 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 SBC attempts to locate an alternative route for the call.

- **To configure SIP reason codes for alternative IP routing:**
  1. Open the SBC Alternative Routing Reasons page (Configuration tab > VoIP menu >
2. Click **Add**; the following dialog box appears:

**Figure 4-55: SBC Alternative Routing Reasons Table - Add Record**

![Add Row dialog box](image)

3. Click **Add**.

### 4.15 Step 15: Reset the SBC

After you have completed the configuration of the SBC described in this chapter, save ("burn") the configuration to the SBC’s flash memory with a reset for the settings to take effect.

➢ **To save the configuration to flash memory:**

1. Open the Maintenance Actions page (**Maintenance** tab > **Maintenance** menu > **Maintenance Actions**).

**Figure 4-56: Resetting the SBC**

![Resetting the SBC](image)

2. Ensure that the 'Burn to FLASH' field is set to **Yes** (default).

3. Click the **Reset** button.
# AudioCodes INI File

The ini configuration file of the SBC, corresponding to the Web-based configuration as described in Section 4 on page 33, is shown below:

Note: To load and save an ini file, use the Configuration File page (Maintenance tab > Software Update menu > Configuration File).

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

;Board: Mediant 1000
;HW Board Type: 47 FK Board Type: 71
;Serial Number: 9032540
;Slot Number: 1
;Software Version: 7.00A.058.002
;DSP Software Version: 624AE3=> 660.14
;Second DSP Software Version: 2041M3=> 660.14
;Board IP Address: 10.145.205.12
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 10.145.205.1
;Ram size: 496M Flash size: 64M
;Num of DSP Cores: 15 Num DSP Channels: 84
;Num of physical LAN ports: 7
;Profile: NONE

;;Key features:;Board Type: Mediant 1000 ;Security: IPSEC
MediaEncryption StrongEncryption EncryptControlProtocol ;Channel Type:
RTP DspCh=240 IPMediaDspCh=240 ;Coders: G723 G729 NETCODER GSM-FR G727
ILBC G722 ;BSTM Protocols: ISDN IUA=4 CAS ;DSP Voice features:
Ipmdetector ;IP Media: Conf VXML VoicePromptAnnounc(H248.9) ;E1Trunks=8
;T1Trunks=8 ;Control Protocols: MGCP MEGACO Sip SBC=10 MSFT ;Default
features; ;Coders: G711 G726;

---------  HW components ---------

; Slot #: Module type : # of ports : # of DSPs
;-----------------------------------------------
; 1 : FALC56 : 2 : 3
; 2 : BRI : 4 : 2
; 3 : FXS : 4 : 1
; 4 : Empty
; 5 : Empty
; 6 : Empty
;-----------------------------------------------

[System Params]

SyslogServerIP = 10.145.205.57
EnableSyslog = 0
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = 3600
;VpFileLastUpdateTime is hidden but has non-default value
```
DayLightSavingTimeStart = '03:SUN/05:02:00'
DayLightSavingTimeEnd = '10:SUN/05:03:00'
DayLightSavingTimeEnable = 1
TLSPkeySize = 2048
TLSPkeyPassphrase = '
NTPServerIP = '10.145.205.51'
NTPSecondaryServerIP = '10.145.205.52'
;LastConfigChangeTime is hidden but has non-default value
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value

[BSP Params]
PCMLawSelect = 3
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]

[ControlProtocols Params]

[MGCP Params]

[MEGACO Params]

[EP_Num_Params]
EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0

[PSTN Params]

[SS7 Params]

[Voice Engine Params]
PrerecordedTonesFileName = 'Sunrise_MoH_SfB_8kHz_8Bit_aLaw.dat'
ENABLEMEDIASECURITY = 1

[WEB Params]
LogoWidth = '145'

[SIP Params]
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
MEDIASECURITYBEHAVIOUR = 3
A. AudioCodes INI File

- ENABLESBCAPPLICATION = 1
- MSLDAPPRIIMARYKEY = 'telephoneNumber'
- SBCMAXFORWARDSLIMIT = 70
- SBCFORKINGHANDLINGMODE = 1
- SBCSESSIONEXPIRES = 1800
- ENERGYDETECTORCMD = 587202560
- ANSWERDETECTORCMD = 10485760

;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[SCTP Params]

[VXML Params]

[IPsec Params]

[Audio Staging Params]

[SNMP Params]

[PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable.SpeedDuplex,
PhysicalPortsTable.PortDescription, PhysicalPortsTable.GroupMember,
PhysicalPortsTable.GroupStatus;

PhysicalPortsTable 0 = "GE_0_1", 1, 4, "User Port #0", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_0_2", 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_7_1", 1, 4, "User Port #2", "GROUP_2",
"Active";
PhysicalPortsTable 3 = "GE_7_2", 1, 4, "User Port #3", "GROUP_2",
"Redundant";
PhysicalPortsTable 4 = "GE_7_3", 1, 4, "User Port #4", "GROUP_3",
"Active";
PhysicalPortsTable 5 = "GE_7_4", 1, 4, "User Port #5", "GROUP_3",
"Redundant";

[EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable.Member1, EtherGroupTable.Member2;

EtherGroupTable 0 = "GROUP_1", 2, "GE_0_1", "GE_0_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_7_1", "GE_7_2";
EtherGroupTable 2 = "GROUP_3", 2, "GE_7_3", "GE_7_4";
EtherGroupTable 3 = "GROUP_4", 0, "", "";
EtherGroupTable 4 = "GROUP_5", 0, "", "";
EtherGroupTable 5 = "GROUP_6", 0, "", "";

[ \EtherGroupTable ]
DeviceTable

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName,
DeviceTable_Tagging;
DeviceTable 0 = 1, "GROUP_1", "vlan 1", 0;
DeviceTable 1 = 2, "GROUP_2", "vlan 2", 0;
DeviceTable 2 = 3, "GROUP_3", "vlan 3", 0;

InterfaceTable

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryD NSServerIPAddress,
InterfaceTable_SecondaryDNServerIPAddress,
InterfaceTable_Tagging;
InterfaceTable 0 = 0, 5, 10.145.205.1, 0, 10.145.205.1, "Sunrise",
10.145.205.51, 10.145.205.52, "vlan 1";
InterfaceTable 1 = 0, 5, 192.168.201.30, 0, 0.0.0.0, "SfB",
0.0.0.0, 0.0.0.0, "vlan 2";

WebUsers

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_SessionTimeout, WebUsers_BlockTime, WebUsers_UserLevel,
WebUsers_PwNonce;
WebUsers 0 = "Admin",
"$1$7qh8qD1ra2n8av8+Pj+qqym1MXHwZXDn8ORmpPJn26dytODhtCCh4TUjYydjY/Y34n18
6byoqH3pviirr2u/s="", 1, 0, 2, 15, 60, 200,
"6a2b760a8f2b9909545740b788f0d4a6";
WebUsers 1 = "User",
"$1$Z6q19s/e3u008v2Tpfbxxo/0s+qn/Kv/eiy5uHntOGivke/guvt77nw1tPX19yE0ndjNjffj
1t/cwJoxjJkRwJHOz8s="", 3, 0, 2, 15, 60, 50,
"8f2c00dsbee5308693007fe1d0e981e4";
[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion, TLSContexts_ServerCipherString, TLSContexts_ClientCipherString, TLSContexts_OscspEnable, TLSContexts_OscspServerPrimary, TLSContexts_OscspServerSecondary, TLSContexts_OscspServerPort, TLSContexts_OscspDefaultResponse;
TLSContexts 0 = "default", 7, "RC4:AES128", "ALL:!aNULL", 0, 0, 0, 0, 0;

[ \TLSContexts ]

[ IpProfile ]

IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders, 
IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader, 
IpProfile_SBCRemoteMultipleEarlyDialogs, 
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag, 
IpProfile_SBCAdaptRFC2833BWtoVoiceCoderBW;

IpProfile 1 = "SfB", 1, 0, 0, 10, 10, 46, 24, 1, 0, 0, 2, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", 1, 0, 0, "", 1, -1, 2, 1, 0, 
0, 2, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 3, 1, 1, 0, 3, 2, 1, 0, 1, 
0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 3, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 250, -1, -1, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, 0, "";
0;IpProfile 2 = "Sunrise", 1, 0, 0, 10, 10, 46, 24, 0, 0, 0, 2, 0, 0, 
0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 0, 0, "", 2, 0, 0, "", 2, -1, 2, 
2, 0, 0, 0, 0, 0, 0, 0, 8, 300, 400, 1, 0, 0, -1, 0, 0, 1, 3, 3, 0, 2, 1, 3, 0, 1, 
0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 5, 0, 0, 0, 0, 0, 0, 
0, 0, 0, 250, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, 0, "";
0;IpProfile 3 = "Fax", 1, 0, 0, 10, 10, 46, 24, 0, 0, 0, 2, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", -1, -1, 0, 0, 
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1, 
0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 
0, 250, -1, -1, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, 0, "";
0;

[ \IpProfile ]

[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;

CpMediaRealm 0 = "MR SfB", "SfB", 
"", 6000, 100, 6999, 1, 
"", 
"";

CpMediaRealm 1 = "MR Sunrise", "Sunrise", 
"", 7000, 100, 7999, 0, 
"", 
"";

[ \CpMediaRealm ]

[ SBCRoutingPolicy ]

FORMAT SBCRoutingPolicy_Index = SBCRoutingPolicy_Name,
SBCRoutingPolicy_LCREnable, SBCRoutingPolicy_LCRAverageCallLength,
SBCRoutingPolicy_LCRDefaultCost, SBCRoutingPolicy_LdapServerGroupName;
SBCRoutingPolicy 0 = "Default_SBC RoutingPolicy", 0, 1, 0, 
"";

[ \SBCRoutingPolicy ]

[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations, SRD_SharingPolicy,
SRD_UsedByRoutingServer, SRD_SBCOperationMode, SRD_SBCRoutingPolicyName,
SRD_SBCDialPlanName;
SRD 0 = "DefaultSRD", 0, -1, 1, 0, 0, 
0, "Default_SBCRoutingPolicy", 
"";

[ \SRD ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName, 
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
A. AudioCodes INI File

SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_SRDNName, SIPInterface_MessagePolicyName,
SIPInterface_TLSContext, SIPInterface_TLSMutualAuthentication,
SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer;
SIPInterface = "SfB", "SfB", 2, 0, 5068, 5067, "DefaultSRD", "",
"default", -1, 0, 500, -1, -1, -1, 0;
SIPInterface = "Sunrise", "Sunrise", 2, 5061, 0, 5061, "DefaultSRD", 
"", "default", -1, 0, 500, -1, -1, -1, 0;

[ \SIPInterface ]

[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap,
ProxySet_SRDNName, ProxySet_ClassificationInput, ProxySet_TLSContextName,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName,
ProxySet_SBCIPv4SIPInterfaceName, ProxySet_SASIPv4SIPInterfaceName,
ProxySet_DNSResolveMethod, ProxySet_KeepAliveFailureResp,
ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv6SIPInterfaceName,
ProxySet_SASIPv6SIPInterfaceName;
ProxySet 0 = "SfB", 1, 60, 1, 1, "DefaultSRD", 0, "",
"SfB", "", "", "", "SfB", 0, 0, -1, -1, -1, -1, 0;
ProxySet 1 = "Sunrise", 1, 60, 0, 0, "DefaultSRD", 0, "",
"Sunrise", "", "", "", "Sunrise", 0, 0, -1, -1, -1, -1, 0;
ProxySet 2 = "Fax", 0, 60, 0, 0, "DefaultSRD", 0, "",
"Fax", "", "", "", "Fax", 0, 0, -1, -1, -1, -1, 0;

[ \ProxySet ]

[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SRDNName, IPGroup_MediaRealm, IPGroup_ProfileName,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UIUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AudioCodeProfile, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAMode,
IPGroup_DTLSContext, IPGroup_ExcellentRoutingServer,
IPGroup_SBCOperationMode, IPGroup_SBCRouteUsingRequestURIPort,
IPGroup_SBCKeepOriginalCallID,
IPGroup_SBCDirectPlanName;
IPGroup 0 = 0, "SfB", "SfB", "", "", -1, 0, "DefaultSRD", "MR SfB", 1,
"SfB", -1, 1, 0, 0, "", 0, -1, -1, "", "", "$s$gQ==", 0, ",", ",", ",
0, ",", ",", 0, 0, -1, 0, 0, "";
IPGroup 1 = 0, "Sunrise", "Sunrise", "", 0, -1, 0, "DefaultSRD", "MR
Sunrise", 1, "Sunrise", -1, 2, 2, 0, 0, "", 0, -1, -1, "", "", "$s$gQ==", 
0, ",", ",", 0, 0, 0, 0, 0, 0, 0, ";
IPGroup 2 = 0, "Fax", "Fax", ",", ",", -1, 0, "DefaultSRD", "MR SfB", 1, "Fax", -1, -1, -1, 0, ",", 0, -1, -1, ",", ",", ",", ",", ",", ",", 0, 0, "", 0, 0, -1, 0, "", "";

[ \IPGroup ]

[ SBCAlternativeRoutingReasons ]

FORMAT SBCAlternativeRoutingReasons_Index = SBCAlternativeRoutingReasons_ReleaseCause;
SBCAlternativeRoutingReasons 0 = 503;

[ \SBCAlternativeRoutingReasons ]

[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex, ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 0 = "0", 0, "FEPool01.intra.sunlab.ch:5067", 2;
ProxyIp 1 = "0", 1, "FEPool02.intra.sunlab.ch:5067", 2;
ProxyIp 2 = "1", 0, "10.17.220.5:5060", 0;
ProxyIp 3 = "1", 1, "10.24.220.5:5060", 0;
ProxyIp 4 = "2", 0, "10.145.205.99:5060", 0;

[ \ProxyIp ]

[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName, IP2IPRouting_RoutingPolicyName, IP2IPRouting_SrcIPGroupName, IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost, IP2IPRouting_RequestType, IP2IPRouting_MessageConditionName, IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger, IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType, IP2IPRouting_DestIPGroupName, IP2IPRouting_DestSIPInterfaceName, IP2IPRouting_DestAddress, IP2IPRouting_DestPort, IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions, IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup, IP2IPRouting_DestTags, IP2IPRouting_SrcTags;
IP2IPRouting 0 = "OPTIONS termination", "Default_SBCRoutingPolicy", "Any", ",", ",", ",", ",", 6, ",", "Any", 0, -1, 1, ",", ",", "internal", 0, -1, 0, 0, ",", ",", ",";
IP2IPRouting 1 = "ITSP to Fax", "Default_SBCRoutingPolicy", "Sunrise", ",", ",", ",", ",", ",", +41991234567, ",", 0, ",", "Any", 0, -1, 0, "Fax", "SfB", ",", 0, -1, 0, 0, ",", ",", ",";
IP2IPRouting 2 = "SfB to ITSP", "Default_SBCRoutingPolicy", "SfB", ",", ",", ",", ",", 0, ",", "Any", 0, -1, 0, "Sunrise", "Sunrise", ",", 0, -1, 0, 0, ",", ",", ",";
IP2IPRouting 3 = "ITSB to SfB", "Default_SBCRoutingPolicy", "Sunrise", ",", ",", ",", ",", 0, ",", "Any", 0, -1, 0, "SfB", "SfB", ",", 0, -1, 0, 0, ",", ",", ",";
IP2IPRouting 4 = "Fax to ITSP", "Default_SBCRoutingPolicy", "Fax", ",", ",", ",", 0, ",", "Any", 0, -1, 0, "Sunrise", "Sunrise", ",", 0, -1, 0, 0, ",", ",", ",";

[ \IP2IPRouting ]
[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime, CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce, CodersGroup0_CoderSpecific;
CodersGroup0 0 = "g711Alaw64k", 20, 255, -1, 0, "";

[ CodersGroup0 ]

[ CodersGroup1 ]

FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime, CodersGroup1_rate, CodersGroup1_PayloadType, CodersGroup1_Sce, CodersGroup1_CoderSpecific;
CodersGroup1 0 = "g711Alaw64k", 20, 0, -1, 1, "";
CodersGroup1 1 = "g711Ulaw64k", 20, 0, -1, 1, "";

[ CodersGroup1 ]

[ CodersGroup2 ]

FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime, CodersGroup2_rate, CodersGroup2_PayloadType, CodersGroup2_Sce, CodersGroup2_CoderSpecific;
CodersGroup2 0 = "g729", 20, 0, -1, 1, "";
CodersGroup2 1 = "g711Alaw64k", 20, 0, -1, 1, "";
CodersGroup2 2 = "g711Ulaw64k", 20, 0, -1, 1, "";

[ CodersGroup2 ]

[ AllowedCodersGroup1 ]

FORMAT AllowedCodersGroup1_Index = AllowedCodersGroup1_Name;
AllowedCodersGroup1 0 = "g722";
AllowedCodersGroup1 1 = "g711Alaw64k";
AllowedCodersGroup1 2 = "g711Ulaw64k";

[ AllowedCodersGroup1 ]

[ AllowedCodersGroup2 ]

FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g722";
AllowedCodersGroup2 1 = "g729";
AllowedCodersGroup2 2 = "g711Alaw64k";
AllowedCodersGroup2 3 = "g711Ulaw64k";

[ AllowedCodersGroup2 ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index = MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations MessageType, MessageManipulations_CommandName, MessageManipulations_ActionName, MessageManipulations_ValueName, MessageManipulations_RowRole; MessageManipulations 0 = "Add Allow UPDATE", 1, "invite.response", "header.allow !contains 'UPDATE'", "header.allow", 2, "'CANCEL,BYE,INVITE,PRACK,UPDATE'", 0;
MessageManipulations 1 = "Change Referred-by", 2, "invite.request", "header.referred-by exists", "header.Diversion", 0, "'<'+header.referred-by.URL+'>'", 0;
MessageManipulations 2 = "Remove Referred-by", 2, "", "", "header.referred-by", 1, "", 1;

[ MessageManipulations ]

[ GwRoutingPolicy ]

FORMAT GwRoutingPolicy_Index = GwRoutingPolicy_Name, GwRoutingPolicy_LCREnable, GwRoutingPolicy_LCRAverageCallLength, GwRoutingPolicy_LCRDefaultCost, GwRoutingPolicy_LdapServerGroupName;
GwRoutingPolicy 0 = "GwRoutingPolicy", 0, 1, 0, ""

[ GwRoutingPolicy ]

[ ResourcePriorityNetworkDomains ]

FORMAT ResourcePriorityNetworkDomains_Index = ResourcePriorityNetworkDomains_Name, ResourcePriorityNetworkDomains_Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 1;
ResourcePriorityNetworkDomains 2 = "dod", 1;
ResourcePriorityNetworkDomains 3 = "drsn", 1;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 1;

[ ResourcePriorityNetworkDomains ]

[ StaticRouteTable ]

FORMAT StaticRouteTable_Index = StaticRouteTable_DeviceName, StaticRouteTable_Destination, StaticRouteTable_PrefixLength, StaticRouteTable_Gateway, StaticRouteTable_Description;
StaticRouteTable 0 = "vlan 2", 192.168.200.0, 24, 192.168.201.20, "IMS Next Hop"
StaticRouteTable 1 = "vlan 2", 10.17.220.0, 28, 192.168.201.20, "IMS ZUR SIP"
StaticRouteTable 2 = "vlan 2", 10.17.220.16, 28, 192.168.201.20, "IMS ZUR Media"
StaticRouteTable 3 = "vlan 2", 10.24.220.0, 28, 192.168.201.20, "IMS BER SIP"
StaticRouteTable 4 = "vlan 2", 10.24.220.16, 28, 192.168.201.20, "IMS BER Media"

[ StaticRouteTable ]
B Configuring Analog Devices (ATAs) for Fax Support

This section describes how to configure the analog device entity to route its calls to the AudioCodes Media Gateway for supporting faxes. The analog device entity must be configured to send all calls to the AudioCodes SBC.

**Note:** The configuration described in this section is for ATA devices configured for AudioCodes MP-11x series.

### B.1 Step 1: Configure the Endpoint Phone Number Table

The 'Endpoint Phone Number Table' page allows you to activate the MP-11x ports (endpoints) by defining telephone numbers. The configuration below uses the example of ATA destination phone number "5872330307" (IP address 10.15.17.12) with all routing directed to the SBC device (10.15.17.55).

➢ To configure the Endpoint Phone Number table:

1. Open the Endpoint Phone Number Table page (Configuration tab > VoIP menu > GW and IP to IP submenu > Hunt Group sub-menu > Endpoint Phone Number).

![Figure B-1: Endpoint Phone Number Table Page](image)

### B.2 Step 2: Configure Tel to IP Routing Table

This step describes how to configure the Tel-to-IP routing rules to ensure that the MP-11x device sends all calls to the AudioCodes central SBC device.

➢ To configure the Tel to IP Routing table:

1. Open the Tel to IP Routing page (Configuration tab > VoIP menu > GW and IP to IP sub-menu > Routing sub-menu > Tel to IP Routing).

![Figure B-2: Tel to IP Routing Page](image)
B.3  **Step 3: Configure Coders Table**

This step describes how to configure the coders for the MP-11x device.

➢ **To configure MP-11x coders:**

1. Open the Coders page (Configuration tab > VoIP menu > Coders And Profiles sub-menu > Coders).

![Figure B-3: Coders Table Page](image)
B.4 Step 4: Configure SIP UDP Transport Type and Fax Signaling Method

This step describes how to configure the fax signaling method for the MP-11x device.

➢ **To configure the fax signaling method:**

1. Open the SIP General Parameters page (Configuration tab > VoIP menu > SIP Definitions submenu > General Parameters).

   ![Figure B-4: SIP General Parameters Page](image)

2. From the ‘FAX Signaling Method’ drop-down list, select **G.711 Transport** for G.711 fax support and select **T.38 Relay** for T.38 fax support.

3. From the ‘SIP Transport Type’ drop-down list, select **UDP**.

4. In the ‘SIP UDP Local Port’ field, enter **5060** (corresponding to the Central Gateway UDP transmitting port configuration).

5. In the ‘SIP Destination Port’, enter **5060** (corresponding to the Central Gateway UDP listening port configuration).
International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
27 World’s Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: www.audiocodes.com/info
Website: www.audiocodes.com

Document #: LTRT-12620