Microsoft® Skype for Business Server 2015 and QSC AG SIP Trunk using AudioCodes Mediant™ E-SBC

Version 7.2
# Table of Contents

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

2 Component Information ...................................................................................... 9  
   2.1 AudioCodes E-SBC Version ................................................................................... 9  
   2.2 QSC AG IP 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 E-SBC as an IP / PSTN Gateway ................................................ 13  
   3.2 Configuring the "Route" on Skype for Business Server 2015 ................................ 21  

4 Configuring AudioCodes E-SBC ...................................................................... 31  
   4.1 Step 1: IP Network Interfaces Configuration ......................................................... 32  
      4.1.1 Step 1a: Configure VLANs ............................................................................... 33  
      4.1.2 Step 1b: Configure Network Interfaces .............................................................. 34  
   4.2 Step 2: Enable the SBC Application .................................................................. 36  
   4.3 Step 3: Configure Media Realms ........................................................................ 37  
   4.4 Step 4: Configure SIP Signaling Interfaces ......................................................... 40  
   4.5 Step 5: Configure Proxy Sets ............................................................................ 42  
   4.6 Step 6: Configure Coders ................................................................................. 47  
   4.7 Step 7: Configure IP Profiles ........................................................................... 50  
   4.8 Step 8: Configure IP Groups ............................................................................ 54  
   4.9 Step 9: SIP TLS Connection Configuration ...................................................... 56  
      4.9.1 Step 9a: Configure the NTP Server Address ...................................................... 56  
      4.9.2 Step 9b: Configure the TLS version .................................................................. 57  
      4.9.3 Step 9c: Configure a Certificate for Operation with Microsoft Skype for Business  
                      Server 2015 .............................................................................................. 58  
      4.9.4 Step 9d: Configure a Certificate for work with QSC AG SIP Trunk ................. 64  
   4.10 Step 10: Configure SRTP .............................................................................. 65  
   4.11 Step 11: Configure Maximum IP Media Channels ............................................ 66  
   4.12 Step 12: Configure IP-to-IP Call Routing Rules .............................................. 67  
   4.13 Step 13: Configure Message Manipulation Rules .......................................... 72  
   4.14 Step 14: Configure Registration Accounts ..................................................... 80  
   4.15 Step 15: Miscellaneous Configuration ............................................................ 82  
      4.15.1 Step 15a: Configure Call Forking Mode ......................................................... 82  
      4.15.2 Step 15b: Configure SBC Alternative Routing Reasons ............................... 83  
   4.16 Step 16: Reset the E-SBC ............................................................................ 84  

A AudioCodes INI File .......................................................................................... 85
This page is intentionally left blank.
Notice

This document describes how to connect the Microsoft Skype for Business Server 2015 and QSC AG SIP Trunk using AudioCodes Mediant E-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: November-16-2016

Trademarks

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

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>33403</td>
<td>Initial document release for Version 7.2.</td>
</tr>
</tbody>
</table>

Documentation Feedback

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

This Configuration Note describes how to set up AudioCodes Enterprise Session Border Controller (hereafter, referred to as E-SBC) for interworking between QSC AG’s SIP Trunk, called “IPfonie extended connect” with and without the TLS/SRTP encryption option, and the Microsoft’s Skype for Business Server 2015 environment.

You can also use AudioCodes’ SBC Wizard tool to automatically configure the E-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 QSC AG Partners who are responsible for installing and configuring QSC AG’s SIP Trunk and Microsoft’s Skype for Business Server 2015 for enabling VoIP calls using AudioCodes E-SBC.

1.2 About AudioCodes E-SBC Product Series

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

The E-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 E-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 E-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.
2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

<table>
<thead>
<tr>
<th>SBC Vendor</th>
<th>AudioCodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Models</td>
<td></td>
</tr>
<tr>
<td>▪ Mediant 500 E-SBC</td>
<td></td>
</tr>
<tr>
<td>▪ Mediant 500L Gateway &amp; E-SBC</td>
<td></td>
</tr>
<tr>
<td>▪ Mediant 800B Gateway &amp; E-SBC</td>
<td></td>
</tr>
<tr>
<td>▪ Mediant 1000B Gateway &amp; E-SBC</td>
<td></td>
</tr>
<tr>
<td>▪ Mediant 2600 E-SBC</td>
<td></td>
</tr>
<tr>
<td>▪ Mediant 4000 SBC</td>
<td></td>
</tr>
<tr>
<td>▪ Mediant 4000B SBC</td>
<td></td>
</tr>
<tr>
<td>▪ Mediant 9000 SBC</td>
<td></td>
</tr>
<tr>
<td>▪ Mediant Software SBC (SE and VE)</td>
<td></td>
</tr>
<tr>
<td>Software Version</td>
<td>SIP_7.20A.002</td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
</tr>
<tr>
<td>▪ SIP/UDP or SIP/TLS (to the QSC AG SIP Trunk)</td>
<td></td>
</tr>
<tr>
<td>▪ SIP/TCP or SIP/TLS (to the S4B FE Server)</td>
<td></td>
</tr>
<tr>
<td>Additional Notes</td>
<td>None</td>
</tr>
</tbody>
</table>

2.2 QSC AG IP Trunking Version

Table 2-2: QSC AG Version

<table>
<thead>
<tr>
<th>Vendor/Service Provider</th>
<th>QSC AG</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSW Model/Service</td>
<td>SIP Trunk Model: IPfonie extended connect with registration mode</td>
</tr>
<tr>
<td>Software Version</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>SIP - according to SIPconnect 1.1</td>
</tr>
<tr>
<td>Additional Notes</td>
<td>None</td>
</tr>
</tbody>
</table>

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</td>
</tr>
<tr>
<td>Protocol</td>
<td>Microsoft SIP</td>
</tr>
<tr>
<td>Additional Notes</td>
<td>None</td>
</tr>
</tbody>
</table>
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and QSC AG 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 QSC AG’s SIP Trunking service.
- AudioCodes E-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 QSC AG’s SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

**Figure 2-1: Interoperability Test Topology between E-SBC and Microsoft Skype for Business with QSC AG 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>
<tbody>
<tr>
<td>Network</td>
<td>• Microsoft Skype for Business Server 2015 environment is located on the Enterprise's LAN</td>
</tr>
<tr>
<td></td>
<td>• QSC AG SIP Trunk is located on the WAN</td>
</tr>
<tr>
<td>Signaling</td>
<td>• Microsoft Skype for Business Server 2015 operates with SIP-over-TLS transport type</td>
</tr>
<tr>
<td>Transcoding</td>
<td>• QSC AG SIP Trunk operates with SIP-over-UDP or SIP-over-TLS transport types</td>
</tr>
<tr>
<td>Codecs Transcoding</td>
<td>• Microsoft Skype for Business Server 2015 supports G.711A-law and G.711U-law coders</td>
</tr>
<tr>
<td></td>
<td>• QSC AG SIP Trunk supports G.711A-law, G.711U-law, and G.729 coder</td>
</tr>
<tr>
<td>Media Transcoding</td>
<td>• Microsoft Skype for Business Server 2015 operates with SRTP media type</td>
</tr>
<tr>
<td></td>
<td>• QSC AG SIP Trunk operates with RTP or SRTP media types</td>
</tr>
</tbody>
</table>

2.4.2 Known Limitations

The following limitations were observed during interoperability tests performed for the AudioCodes E-SBC interworking between Microsoft Skype for Business Server 2015 and QSC AG ‘s SIP Trunk:

- Early Media is not supported by the QSC AG SIP Trunk.
- If the Microsoft Skype for Business Server 2015 sends one of the following error responses:
  - 603 Decline
  - 503 Service Unavailable
  - 488 Not Acceptable Here
  QSC AG SIP Trunk still sends re-INVITEs and does not disconnect the call.
To disconnect the call, a message manipulation rule is used to replace the above error response with the ‘486 Busy Here’ response (see Section 4.13 on page 72).
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 E-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 E-SBC as an IP / PSTN Gateway

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

➢ To configure E-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
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.
The Topology Builder screen with the downloaded Topology is displayed:

**Figure 3-4: Downloaded Topology**

4. 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**
5. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., \texttt{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 58).

6. Click Next; the following is displayed:

   \textbf{Figure 3-7: Define the IP Address}

7. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click Next.
8. 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**

```plaintext
Figure 3-8: Define the Root Trunk
```

a. In the 'Listening Port for IP/PSTN Gateway' field, enter the listening port that the E-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 4.3 on page 37).

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 4.3 on page 37).

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 E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

**Figure 3-9: E-SBC added as IP/PSTN Gateway and Trunk Created**

9. 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**

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

**Figure 3-12: Publishing in Progress**
11. Wait until the publishing topology process completes successfully, as shown below:

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

![Publishing Wizard Complete](image)

12. 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 E-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:

   **Figure 3-15: Skype for Business Server 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. In the left navigation pane, select **Voice Routing**.

**Figure 3-17: Voice Routing Page**

5. In the Voice Routing page, select the **Route** tab.

**Figure 3-18: Route Tab**
6. Click **New**; the New Voice Route page appears:

**Figure 3-19: Adding New Voice Route**

7. In the 'Name' field, enter a name for this route (e.g., **ITSP**).
8. 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**.
9. Associate the route with the E-SBC Trunk that you created:
   a. Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

**Figure 3-20: List of Deployed Trunks**
b. Select the E-SBC Trunk you created, and then click OK; the trunk is added to the 'Associated Trunks' group list:

Figure 3-21: Selected E-SBC Trunk

10. Associate a PSTN Usage to this route:
   - Under the 'Associated PSTN Usages' group, click Select and then add the associated PSTN Usage.

Figure 3-22: Associating PSTN Usage to Route
11. Click OK (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

![Figure 3-23: Confirmation of New Voice Route](image)

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

![Figure 3-24: Committing Voice Routes](image)
The Uncommitted Voice Configuration Settings page appears:

**Figure 3-25: Uncommitted Voice Configuration Settings**

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

**Figure 3-26: Confirmation of Successful Voice Routing Configuration**
14. Click Close; the new committed Route is displayed in the Voice Routing page, as shown below:

Figure 3-27: Voice Routing Screen Displaying Committed Routes

15. 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 QSC AG SIP Trunk in the P-Asserted-Identity header. The device adds this ID to the P-Asserted-Identity header in the sent INVITE message using the IP Profile (see Section 4.6 on page 47).

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 3-28: 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.

16. Use the following command on the Skype for Business Server Management Shell after reconfiguration to verify correct values:

   ```
   Get-CsTrunkConfiguration
   ```

   ```plaintext
   Identity : Service:PstnGateway:ITSP.S4B.interop
   OutboundTranslationRulesList : {}
   SipResponseCodeTranslationRulesList : {}
   OutboundCallingNumberTranslationRulesList : {}
   PstnUsages : {}
   Description : ConcentratedTopology : True
   EnableBypass : True
   EnableMobileTrunkSupport : False
   EnableReferSupport : True
   EnableSessionTimer : True
   EnableSignalBoost : False
   MaxEarlyDialogs : 20
   RemovePlusFromUri : False
   RTCPActiveCalls : True
   RTCPCallsOnHold : True
   SRTPMode : Required
   EnablePIDFLOSupport : False
   EnableRTPLatching : False
   EnableOnlineVoice : False
   ForwardCallHistory : True
   ```
<table>
<thead>
<tr>
<th>Configuration</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<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>
4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Skype for Business Server 2015 and the QSC AG 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:

- E-SBC WAN interface - QSC AG SIP Trunking environment
- E-SBC LAN interface - Skype for Business Server 2015 environment

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

**Notes:**

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

  For more information about the 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.
4.1 Step 1: IP Network Interfaces Configuration

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

- E-SBC interfaces with the following IP entities:
  - Skype for Business servers, located on the LAN
  - QSC AG SIP Trunk, located on the WAN
- E-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, E-SBC connects to the LAN and DMZ using dedicated LAN ports (i.e., two ports and two network cables are used).
- E-SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - DMZ (VLAN ID 2)

Figure 4-1: Network Interfaces in Interoperability Test Topology
4. Configuring AudioCodes E-SBC

4.1.1 Step 1a: Configure VLANs

This step describes how to define VLANs for each of the following interfaces:

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

To configure the VLANs:

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

➢ To configure the IP network interfaces:

1. Open the IP Interfaces table (Setup menu > IP Network tab > Core Entities folder > IP Interfaces).

2. Modify the existing LAN network interface:
   a. Select the 'Index' radio button 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>Name</td>
<td>LAN_IF (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Ethernet Device</td>
<td>vlan 1</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.15.17.77 (LAN IP address of E-SBC)</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>16 (subnet mask in bits for 255.255.0.0)</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>10.15.0.1</td>
</tr>
<tr>
<td>Primary DNS</td>
<td>10.15.27.1</td>
</tr>
</tbody>
</table>

3. Add a network interface for the WAN side:
   a. Click New.
   b. Configure the interface as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>WAN_IF</td>
</tr>
<tr>
<td>Application Type</td>
<td>Media + Control</td>
</tr>
<tr>
<td>Ethernet Device</td>
<td>vlan 2</td>
</tr>
<tr>
<td>IP Address</td>
<td>195.189.192.157 (DMZ IP address of E-SBC)</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>25 (subnet mask in bits for 255.255.128)</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>195.189.192.129 (router's IP address)</td>
</tr>
<tr>
<td>Primary DNS</td>
<td>80.179.52.100</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td>80.179.55.100</td>
</tr>
</tbody>
</table>

4. Click Apply.
The configured IP network interfaces are shown below:

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

<table>
<thead>
<tr>
<th>INDEX</th>
<th>NAME</th>
<th>APPLICATION TYPE</th>
<th>INTERFACE MODE</th>
<th>IP ADDRESS</th>
<th>PREFIX LENGTH</th>
<th>DEFAULT GATEWAY</th>
<th>PRIMARY DNS</th>
<th>SECONDARY DNS</th>
<th>ETHERNET DEVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>LAN IF</td>
<td>DAI/Media + IPv4 Manual</td>
<td>10.15.17.77</td>
<td>16</td>
<td>10.15.0.1</td>
<td>10.15.27.1</td>
<td>0.0.0.0</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>WAN IF</td>
<td>Media + Control</td>
<td>IPv4 Manual</td>
<td>108.169.102.187</td>
<td>28</td>
<td>195.162.192.120</td>
<td>80.170.59.100</td>
<td>80.170.58.100</td>
<td>vlan 2</td>
</tr>
</tbody>
</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 (Setup menu > Signaling & Media tab > Core Entities folder > Applications Enabling).

   ![Figure 4-4: Enabling SBC Application](image)

2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Apply**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.16 on page 84).
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 Realms table (Setup menu > Signaling & Media tab > Core Entities folder > Media Realms).
  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>Name</td>
<td>MRLan (descriptive name)</td>
</tr>
<tr>
<td>IPv4 Interface Name</td>
<td>LAN_IF</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 4-5: Configuring Media Realm for LAN
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>Name</td>
<td>MRWan (arbitrary name)</td>
</tr>
<tr>
<td>Topology Location</td>
<td>Up</td>
</tr>
<tr>
<td>IPv4 Interface Name</td>
<td>WAN_IF</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>

Figure 4-6: Configuring Media Realm for WAN
The configured Media Realms are shown in the figure below:

Figure 4-7: 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 E-SBC.

➢ To configure SIP Interfaces:

1. Open the SIP Interfaces table (Setup menu > Signaling & Media tab > Core Entities folder > SIP Interfaces).
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>Name</td>
<td>S4B (see note at the end of this section)</td>
</tr>
<tr>
<td>Network Interface</td>
<td>LAN_IF</td>
</tr>
<tr>
<td>Application Type</td>
<td>SBC</td>
</tr>
<tr>
<td>UDP</td>
<td>0</td>
</tr>
<tr>
<td>TCP</td>
<td>0</td>
</tr>
<tr>
<td>TLS Port</td>
<td>5067 (see note below)</td>
</tr>
<tr>
<td>Media Realm</td>
<td>MRLan</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>Name</td>
<td>QSC</td>
</tr>
<tr>
<td>Network Interface</td>
<td>WAN_IF</td>
</tr>
<tr>
<td>Application Type</td>
<td>SBC</td>
</tr>
<tr>
<td>UDP Port</td>
<td>5060 (for non-secure connection)</td>
</tr>
<tr>
<td>TCP</td>
<td>0</td>
</tr>
<tr>
<td>TLS</td>
<td>5061 (for secure connection)</td>
</tr>
<tr>
<td>Media Realm</td>
<td>MRWan</td>
</tr>
</tbody>
</table>
The configured SIP Interfaces are shown in the figure below:

**Figure 4-8: Configured SIP Interfaces in SIP Interface Table**

![SIP Interfaces Table]

**Note:** Current software releases uses the string *names* of the configuration entities (e.g., SIP Interface, Proxy Sets, and IP Groups). 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
- QSC AG SIP Trunk

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

**To configure Proxy Sets:**

1. Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets).
2. Add a Proxy Set for the Skype for Business Server 2015 as shown below:

<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>S4B</td>
</tr>
<tr>
<td>SBC IPv4 SIP Interface</td>
<td>S4B</td>
</tr>
<tr>
<td>Proxy Keep-Alive</td>
<td>Using Options</td>
</tr>
<tr>
<td>Redundancy Mode</td>
<td>Homing</td>
</tr>
<tr>
<td>Proxy Hot Swap</td>
<td>Enable</td>
</tr>
<tr>
<td>Proxy Load Balancing Method</td>
<td>Round Robin</td>
</tr>
<tr>
<td>TLS Context Name</td>
<td>default</td>
</tr>
</tbody>
</table>
a. Select the index row of the Proxy Set that you added, and then click the Proxy Address link located below the table; the Proxy Address table opens.

b. Click New; the following dialog box appears:

Figure 4-10: Configuring Proxy Address for Microsoft Skype for Business Server 2015

C. Configure the address of the Proxy Set according to the parameters described in the table below.
d. Click **Apply**.

<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>FE.S4B.interop:5067</td>
</tr>
<tr>
<td></td>
<td>(Skype for Business Server 2015 IP address / FQDN and destination port)</td>
</tr>
<tr>
<td>Transport Type</td>
<td>TLS</td>
</tr>
</tbody>
</table>

### 3. Configure a Proxy Set for the QSC AG 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>QSC</td>
</tr>
<tr>
<td>SBC IPv4 SIP Interface</td>
<td>QSC</td>
</tr>
<tr>
<td>Proxy Keep-Alive</td>
<td>Using Options</td>
</tr>
<tr>
<td>DNS Resolve Method</td>
<td>SRV</td>
</tr>
<tr>
<td>TLS Context Name</td>
<td>QSC (for secure connection only)</td>
</tr>
</tbody>
</table>

**Figure 4-11: Configuring Proxy Set for QSC AG SIP Trunk**

a. Select the index row of the Proxy Set that you added, and then click the `Proxy Address` link located below the table; the Proxy Address table opens.
b. Click New; the dialog box appears.
   - **For non-secure connection** configure the address of the Proxy Set according to the parameters described in the table below:

<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>sipconnect.qsc.de</td>
</tr>
<tr>
<td>Transport Type</td>
<td>UDP</td>
</tr>
</tbody>
</table>

   Figure 4-12: Proxy Address for non-secure QSC AG SIP Trunk

   c. Click Apply.

   - **For secure connection** configure the address of the Proxy Set according to the parameters described in the table below:

<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>secure-sipconnect.qsc.de</td>
</tr>
<tr>
<td>Transport Type</td>
<td>TLS</td>
</tr>
</tbody>
</table>

   d. Click Apply.

   Figure 4-13: Proxy Address for Secure QSC AG SIP Trunk
e. Click Apply.

The configured Proxy Sets are shown in the figure below:

Figure 4-14: Configured Proxy Sets in Proxy Sets Table
4.6 Step 6: Configure Coders

This step describes how to configure coders (termed Coder Group). As Skype for Business Server 2015 supports the G.711 coder while the network connection to QSC AG SIP Trunk may restrict operation with a lower bandwidth coder such as G.729, you need to add a Coder Group with the G.729 coder for the QSC AG SIP Trunk. Note that the Coder Group ID for this entity will be assign to its corresponding IP Profile in the next step.

➢ To configure coders:
1. Open the Coder Groups table (Setup menu > Signaling & Media tab > Coders & Profiles folder > Coder Groups).
2. Configure a Coder Group for Skype for Business Server 2015:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coder Group Name</td>
<td>AudioCodersGroups_1</td>
</tr>
<tr>
<td>Coder Name</td>
<td>G.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 4-15: Configuring Coder Group for Skype for Business Server 2015

3. Configure a Coder Group for QSC AG SIP Trunk:

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

Figure 4-16: Configuring Coder Group for QSC AG SIP Trunk
The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the QSC AG SIP Trunk uses the G.729 coder whenever there are bandwidth limitations. Note that this Allowed Coders Group ID will be assign to the IP Profile belonging to the QSC AG SIP Trunk in the next step.

➢ To set a preferred coder for the QSC AG SIP Trunk:
1. Open the Allowed Audio Coders Groups table (Setup menu > Signaling & Media tab > Coders & Profiles folder > Allowed Audio Coders Groups).
2. Click New and configure a name for the Allowed Audio Coders Group for QSC AG SIP Trunk.

Figure 4-17: Configuring Allowed Coders Group for QSC AG SIP Trunk

<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>G.711U-law</td>
</tr>
<tr>
<td>Index</td>
<td>1</td>
</tr>
<tr>
<td>Name</td>
<td>G.711A-law</td>
</tr>
<tr>
<td>Index</td>
<td>2</td>
</tr>
<tr>
<td>Name</td>
<td>G.729</td>
</tr>
<tr>
<td>Index</td>
<td>3</td>
</tr>
<tr>
<td>Name</td>
<td>G.722</td>
</tr>
</tbody>
</table>
6. Open the Media Settings page (Setup menu > Signaling & Media tab > Media folder > Media Settings).

7. From the 'Preferences Mode' drop-down list, select Include Extensions.

8. Click Apply.
4.7 **Step 7: 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
- QSC AG SIP trunk - to operate in non-secure mode using RTP or in secure mode using SRTP

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>1</td>
</tr>
<tr>
<td>Name</td>
<td>S4B</td>
</tr>
<tr>
<td><strong>Media Security</strong></td>
<td></td>
</tr>
<tr>
<td>SBC Media Security Mode</td>
<td>SRTP</td>
</tr>
<tr>
<td>Symmetric MKI</td>
<td>Enable</td>
</tr>
<tr>
<td>MKI Size</td>
<td>1</td>
</tr>
<tr>
<td>Enforce MKI Size</td>
<td>Enforce</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>
<tr>
<td><strong>SBC Early Media</strong></td>
<td></td>
</tr>
<tr>
<td>Remote Early Media RTP Detection Mode</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><strong>SBC Media</strong></td>
<td></td>
</tr>
<tr>
<td>Extension Coders Group</td>
<td>AudioCodersGroups_1</td>
</tr>
<tr>
<td><strong>SBC Signaling</strong></td>
<td></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>
</tbody>
</table>
**SBC Forward and Transfer**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Handle Locally (required, as Skype for Business Server 2015 does not support receipt of SIP REFER)</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

Figure 4-20: Configuring IP Profile for Skype for Business Server 2015

![IP Profile Configuration](image)

3. **Click Apply.**
To configure an IP Profile for the QSC AG SIP Trunk:

1. Click **New**, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>2</td>
</tr>
<tr>
<td>Name</td>
<td>QSC</td>
</tr>
<tr>
<td><strong>Media Security</strong></td>
<td></td>
</tr>
<tr>
<td>SBC Media Security Mode</td>
<td>RTP (for non-secure connection) or SRTP (for secure connection)</td>
</tr>
<tr>
<td>Symmetric MKI</td>
<td>Enable (for secure connection)</td>
</tr>
<tr>
<td>Enforce MKI Size</td>
<td>Enforce (for secure connection)</td>
</tr>
<tr>
<td><strong>SBC Media</strong></td>
<td></td>
</tr>
<tr>
<td>Extension Coders Group</td>
<td>AudioCodersGroups_2</td>
</tr>
<tr>
<td>Allowed Audio Coders</td>
<td>QSC-Allowed-Coders</td>
</tr>
<tr>
<td>Allowed Coders Mode</td>
<td>Restriction and Preference (lists Allowed Coders only and re-arranges the priority of the coders according to Allowed Audio Coders Group order)</td>
</tr>
<tr>
<td><strong>SBC Signaling</strong></td>
<td></td>
</tr>
<tr>
<td>P-Asserted-Identity Header Mode</td>
<td>Add (required for anonymous calls)</td>
</tr>
<tr>
<td>Diversion Header Mode</td>
<td>Add (required for forwarded calls)</td>
</tr>
<tr>
<td>History-Info Header Mode</td>
<td>Remove</td>
</tr>
<tr>
<td>Session Expires Mode</td>
<td>Not Supported</td>
</tr>
<tr>
<td><strong>SBC Forward and Transfer</strong></td>
<td></td>
</tr>
<tr>
<td>Remote REFER Mode</td>
<td>Handle Locally (required, as Microsoft send SIP REFER in proprietary format)</td>
</tr>
<tr>
<td>Play RBT To Transferee</td>
<td>Yes</td>
</tr>
</tbody>
</table>
2. Click **Apply**.
4.8 **Step 8: Configure IP Groups**

This step describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the E-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
- QSC AG SIP Trunk located on WAN

➢ **To configure IP Groups:**

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Add an IP Group for the Skype for Business Server 2015:

<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>S4B</td>
</tr>
<tr>
<td>Type</td>
<td>Server</td>
</tr>
<tr>
<td>Proxy Set</td>
<td>S4B</td>
</tr>
<tr>
<td>IP Profile</td>
<td>S4B</td>
</tr>
<tr>
<td>Media Realm</td>
<td>MRLan</td>
</tr>
<tr>
<td>SIP Group Name</td>
<td>sipconnect.qsc.de (according to ITSP requirement)</td>
</tr>
</tbody>
</table>

3. Configure an IP Group for the QSC AG 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>QSC</td>
</tr>
<tr>
<td>Topology Location</td>
<td>Up</td>
</tr>
<tr>
<td>Type</td>
<td>Server</td>
</tr>
<tr>
<td>Proxy Set</td>
<td>QSC</td>
</tr>
<tr>
<td>IP Profile</td>
<td>QSC</td>
</tr>
<tr>
<td>Media Realm</td>
<td>MRWan</td>
</tr>
<tr>
<td>SIP Group Name</td>
<td>sipconnect.qsc.de (according to ITSP requirement)</td>
</tr>
</tbody>
</table>
The configured IP Groups are shown in the figure below:

**Figure 4-22: Configured IP Groups in IP Group Table**
4.9  **Step 9: SIP TLS Connection Configuration**

This section describes how to configure the E-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 E-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 Time & Date page (Setup menu > Administration tab > Time & Date).
2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., 10.15.27.1).

![Figure 4-23: Configuring NTP Server Address](image)

3. Click **Apply**.
4.9.2 **Step 9b: Configure the TLS version**

This step describes how to configure the E-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 table (Setup menu > IP Network tab > Security folder > 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 4-24: Configuring TLS version](image)

4. Click Apply.
4.9.3 Step 9c: Configure a Certificate for Operation with Microsoft Skype for Business Server 2015

This step describes how to exchange a certificate with Microsoft Certificate Authority (CA). The certificate is used by the E-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 E-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).

➢ To configure a certificate:

1. Open the TLS Contexts page (Setup menu > IP Network tab > Security folder > TLS Contexts).
2. In the TLS Contexts page, select the required TLS Context index row, and then click the Change Certificate link located below the table; the Context Certificates page appears.
3. Under the Certificate Signing Request group, do the following:
   a. In the ‘Subject Name [CN]’ field, enter the E-SBC FQDN name (e.g., ITSP.S4B.interop).
   b. Fill in the rest of the request fields according to your security provider's instructions.
   c. Click the Create CSR button; a textual certificate signing request is displayed in the area below the button:
4. Configuring AudioCodes E-SBC

Version 7.2

Figure 4-25: Certificate Signing Request – Creating CSR

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


Figure 4-26: Microsoft Certificate Services Web Page
6. Click **Request a certificate**.

![Figure 4-27: Request a Certificate Page](image)

7. Click **advanced certificate request**, and then click **Next**.

![Figure 4-28: Advanced Certificate Request Page](image)
8. Click **Submit a certificate request** ..., and then click **Next**.

**Figure 4-29: Submit a Certificate Request or Renewal Request Page**

9. Open the `certreq.txt` file that you created and saved in Step 4, and then copy its contents to the 'Saved Request' field.

10. From the 'Certificate Template' drop-down list, select **Web Server**.

11. Click **Submit**.

**Figure 4-30: Certificate Issued Page**

12. Select the **Base 64 encoded** option for encoding, and then click **Download certificate**.

13. Save the file as `gateway.cer` to a folder on your computer.

14. Click the **Home** button or navigate to the certificate server at http://<Certificate Server>/CertSrv.

15. Click **Download a CA certificate, certificate chain, or CRL**.
16. Under the "Encoding method" group, select the **Base 64** option for encoding.
17. Click **Download CA certificate**.
18. Save the file as `certroot.cer` to a folder on your computer.
19. In the E-SBC’s Web interface, return to the **TLS Contexts** page and do the following:
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
   b. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the ‘Send Device Certificate...’ field, navigate to the `gateway.cer` certificate file that you saved on your computer in Step 13, and then click **Send File** to upload the certificate to the E-SBC.

   ![Figure 4-32: Upload Device Certificate Files from your Computer Group](image)

20. In the E-SBC’s Web interface, return to the **TLS Contexts** page.
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Trusted Root Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
   b. Click the **Import** button, and then select the certificate file to load.

   ![Figure 4-33: Importing Root Certificate into Trusted Certificates Store](image)

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

22. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 84).
4.9.4 Step 9d: Configure a Certificate for work with QSC AG SIP Trunk

This step describes how to exchange a certificate with QSC AG Certificate Authority (CA). The certificate is used by the E-SBC to authenticate the connection with QSC AG SIP Trunk.

Note: This step is required only for secure connection.

The procedure involves the following main steps:

a. Generating a Private Key and Self-Signed Certificate.
b. Obtaining Trusted Root Certificate from QSC AG CA.
c. Deploying Trusted Root Certificates on E-SBC.

➢ To configure a certificate:

1. Open the TLS Contexts table (Setup menu > IP Network tab > Security folder > TLS Contexts).
2. Click Add and configure new record in the TLS Contexts table (with name e.g., QSC).
3. In the TLS Contexts page, select the nearly added TLS Context index row, and then click the Change Certificate link located below the table; the Context Certificates page appears.
4. Under the Certificate Signing Request group, in the 'Subject Name [CN]' field, enter the E-SBC name (e.g., audc).
5. Under the Generate new private key and self-signed certificate group, do the following:
   a. Click the Generate Private Key button.
   b. Click the Generate Self-Signed Certificate button.
6. In the E-SBC's Web interface, return to the TLS Contexts page.
   a. In the TLS Contexts page, select the QSC TLS Context index row, and then click the Trusted Root Certificates link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears. The QSC are signed with the Thawte primary root CA, which can be found here: https://www.thawte.com/roots/
   b. Click the Import button, and then select the certificate file to load.
   c. Click OK; the certificate is loaded to the device and listed in the Trusted Certificates store.
7. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 84).
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 E-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 47).

➢ To configure media security:

1. Open the Media Security page (Setup menu > Signaling & Media tab > Media folder > Media Security).

Figure 4-34: Configuring SRTP

2. From the 'Media Security' drop-down list, select Enable to enable SRTP.
3. Click Apply.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 84).
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 E-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 Media Settings page (Setup menu > Signaling & Media tab > Media folder > Media Settings).

   ![Figure 4-35: Configuring Number of Media Channels](image)

2. In the 'Number of Media Channels' field, enter the number of media channels according to your environment's transcoding calls (e.g., 100).

3. Click **Apply**.

4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 84).
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 E-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 (as configured in Section 4.8 on page 46,) to denote the source and destination of the call.

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 QSC AG SIP Trunk (DMZ):

- Terminate SIP OPTIONS messages on the E-SBC that are received from the both LAN and DMZ
- Calls from Skype for Business Server 2015 to QSC AG SIP Trunk
- Calls from QSC AG SIP Trunk to Skype for Business Server 2015
To configure IP-to-IP routing rules:

1. Open the IP-to-IP Routing table (Setup menu > Signaling & Media tab > SBC folder > Routing > IP-to-IP Routing).
2. Configure a rule to terminate SIP OPTIONS messages received from both LAN and DMZ:
   a. Click New, and then configure the parameters as follows:

<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>Terminate OPTIONS (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Source IP Group</td>
<td>Any</td>
</tr>
<tr>
<td>Request Type</td>
<td>OPTIONS</td>
</tr>
<tr>
<td>Destination Type</td>
<td>Dest Address</td>
</tr>
<tr>
<td>Destination Address</td>
<td>internal</td>
</tr>
</tbody>
</table>

![Figure 4-36: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS](image)

   b. Click Apply.
3. Configure a rule to route calls from Skype for Business Server 2015 to QSC AG SIP Trunk:
   a. Click **New**, 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>S4B to ITSP (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Source IP Group</td>
<td>S4B</td>
</tr>
<tr>
<td>Destination Type</td>
<td>IP Group</td>
</tr>
<tr>
<td>Destination IP Group</td>
<td>QSC</td>
</tr>
</tbody>
</table>

   ![Figure 4-37: Configuring IP-to-IP Routing Rule for S4B to ITSP](image)

   b. Click **Apply**.
4. Configure rule to route calls from QSC AG SIP Trunk to Skype for Business Server 2015:
   a. Click New, 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>ITSP to S4B (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Source IP Group</td>
<td>QSC</td>
</tr>
<tr>
<td>Destination Type</td>
<td>IP Group</td>
</tr>
<tr>
<td>Destination IP Group</td>
<td>S4B</td>
</tr>
</tbody>
</table>

   ![Figure 4-38: Configuring IP-to-IP Routing Rule for ITSP to S4B](image)

   b. Click Apply.
The configured routing rules are shown in the figure below:

**Figure 4-39: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table**

![Routing Table Image]

**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 (Setup menu > Signaling & Media tab > Message Manipulation folder > Message Manipulations).

2. Configure a new manipulation rule (Manipulation Set 4) for the QSC AG SIP Trunk. This rule applies to messages sent to the QSC AG SIP Trunk IP Group in a call forward scenario. This replaces the host part of the SIP Diversion Header with the value configured in the ‘SIP Group Name’ parameter for the QSC AG SIP Trunk IP Group.

<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>Change Diversion Host</td>
</tr>
<tr>
<td>Manipulation Set ID</td>
<td>4</td>
</tr>
<tr>
<td>Message Type</td>
<td>invite.request</td>
</tr>
<tr>
<td>Condition</td>
<td>header.diversion exists</td>
</tr>
<tr>
<td>Action Subject</td>
<td>header.diversion.url.host</td>
</tr>
<tr>
<td>Action Type</td>
<td>Modify</td>
</tr>
<tr>
<td>Action Value</td>
<td>param.ipg.dst.host</td>
</tr>
</tbody>
</table>
3. Configure another manipulation rule (Manipulation Set 4) for QSC AG SIP Trunk. This rule applies to messages sent to the QSC AG SIP Trunk IP Group in a Call Forward scenario. This replaces the user part of the SIP P-Asserted Identity Header with the value from the user part of the SIP 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>Call Forward</td>
</tr>
<tr>
<td>Manipulation Set ID</td>
<td>4</td>
</tr>
<tr>
<td>Message Type</td>
<td>invite.request</td>
</tr>
<tr>
<td>Condition</td>
<td>header.diversion exists</td>
</tr>
<tr>
<td>Action Subject</td>
<td>header.p-asserted-identity.url.user</td>
</tr>
<tr>
<td>Action Type</td>
<td>Modify</td>
</tr>
<tr>
<td>Action Value</td>
<td>header.diversion.url.user</td>
</tr>
</tbody>
</table>
4. Configure another manipulation rule (Manipulation Set 4) for QSC AG SIP Trunk. This rule applies to messages sent to the QSC AG SIP Trunk IP Group during Call Transfer initiated by the Skype for Business Server 2015 IP Group. This replaces the host part of the SIP Referred-By Header with the value configured in the ‘SIP Group Name’ parameter for the QSC AG SIP Trunk IP Group.

<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>Call Transfer</td>
</tr>
<tr>
<td>Manipulation Set ID</td>
<td>4</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.referred-by.url.host</td>
</tr>
<tr>
<td>Action Type</td>
<td>Modify</td>
</tr>
<tr>
<td>Action Value</td>
<td>param.ipg.dst.host</td>
</tr>
</tbody>
</table>
5. Configure another manipulation rule (Manipulation Set 4) for QSC AG SIP Trunk, which will be executed if the manipulation rule Index 2 (above) is executed. This rule applies to messages sent to the QSC AG SIP Trunk IP Group during Call Transfer initiated by the Skype for Business Server 2015 IP Group. This replaces the user part of the SIP P-Asserted Identity Header with the value from the SIP Referred-By Header.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>3</td>
</tr>
<tr>
<td>Name</td>
<td>Call Transfer</td>
</tr>
<tr>
<td>Manipulation Set ID</td>
<td>4</td>
</tr>
<tr>
<td>Row Role</td>
<td>Use Previous Condition</td>
</tr>
<tr>
<td>Action Subject</td>
<td>header.p-asserted-identity.url.user</td>
</tr>
<tr>
<td>Action Type</td>
<td>Modify</td>
</tr>
<tr>
<td>Action Value</td>
<td>header.referred-by.url.user</td>
</tr>
</tbody>
</table>

Figure 4-42: Configuring SIP Message Manipulation Rule 2 (for QSC AG SIP Trunk)
6. Configure another manipulation rule (Manipulation Set 4) for QSC AG SIP Trunk. This rule is applied to response messages sent to the QSC AG SIP Trunk IP Group for Rejected Calls initiated by the Skype for Business Server 2015 IP Group. This replaces the method types ‘488’, ‘503’ and ‘603’ with the value ‘486’, because QSC AG SIP Trunk does not recognize these method types.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>4</td>
</tr>
<tr>
<td>Name</td>
<td>Reject Cause</td>
</tr>
<tr>
<td>Manipulation Set ID</td>
<td>4</td>
</tr>
<tr>
<td>Message Type</td>
<td>any.response</td>
</tr>
<tr>
<td>Condition</td>
<td>header.request-uri.methodtype==’603’ OR header.request-uri.methodtype==’503’ OR header.request-uri.methodtype==’488’</td>
</tr>
<tr>
<td>Action Subject</td>
<td>header.request-uri.methodtype</td>
</tr>
<tr>
<td>Action Type</td>
<td>Modify</td>
</tr>
<tr>
<td>Action Value</td>
<td>‘486’</td>
</tr>
</tbody>
</table>
4. Configuring AudioCodes E-SBC

Figure 4-44: Configuring SIP Message Manipulation Rule 4 (for QSC AG SIP Trunk)

Figure 4-45: Example of Configured SIP Message Manipulation Rules
The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set ID 4 and which are executed for messages sent to the QSC AG SIP Trunk IP Group. These rules are specifically required to enable proper interworking between QSC AG SIP Trunk and Skype for Business Server 2015. Refer to the User’s Manual for further details concerning the full capabilities of header manipulation.

<table>
<thead>
<tr>
<th>Rule Index</th>
<th>Rule Description</th>
<th>Reason for Introducing Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>This rule applies to messages sent to the QSC AG SIP Trunk IP Group. This replaces the host part of the SIP Diversion Header with the value configured in the ‘SIP Group Name’ parameter for the QSC AG SIP Trunk IP Group.</td>
<td>For Call Forward scenarios, QSC AG SIP Trunk needs that Host part in SIP Diversion Header will be pre-defined.</td>
</tr>
<tr>
<td>1</td>
<td>This rule applies to messages sent to the QSC AG SIP Trunk IP Group. This replaces the user part of the SIP P-Asserted Identity Header with the value from the user part of the SIP Diversion Header.</td>
<td>For Call Forward scenarios, QSC AG SIP Trunk needs that User part in SIP P-Asserted Identity Header will be defined number. In order to do this, the User part of the SIP P-Asserted Identity Header is replaced with the value from the Diversion Header.</td>
</tr>
<tr>
<td>2</td>
<td>This rule applies to messages sent to the QSC AG SIP Trunk IP Group. This replaces the host part of the SIP Referred-By Header with the value configured in the ‘SIP Group Name’ parameter for the QSC AG SIP Trunk IP Group.</td>
<td>For Call Transfer initiated by Skype for Business Server 2015, QSC AG SIP Trunk needs to replace the Host part of the SIP Referred-By Header with the pre-defined value.</td>
</tr>
<tr>
<td>3</td>
<td>If the manipulation rule Index 2 (above) is executed, then the following rule is also executed. It replaces the user part of the SIP P-Asserted Identity Header with the value from the SIP Referred-By Header.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>This rule is applied to response messages sent to the QSC AG SIP Trunk IP Group for Rejected Calls initiated by the Skype for Business Server 2015 IP Group. This replaces the method types ‘488’, ‘503’ and ‘603’ with the value ‘486’.</td>
<td>QSC AG SIP Trunk does not recognize these method types and continues to send an INVITE message (meaning it tries to setup another call).</td>
</tr>
</tbody>
</table>
7. Assign Manipulation Set ID 4 to the QSC AG SIP trunk IP Group:
   a. Open the IP Groups table ([Setup menu > Signaling & Media tab > Core Entities folder > IP Groups]).
   b. Select the row of the QSC AG SIP trunk IP Group, and then click Edit.
   c. Set the 'Outbound Message Manipulation Set' field to 4.

   Figure 4-46: Assigning Manipulation Set 4 to the QSC AG SIP Trunk IP Group

   d. Click Apply.
4.14 **Step 14: Configure Registration Accounts**

This step describes how to configure SIP registration accounts. This is required so that the E-SBC can register with the QSC AG SIP Trunk on behalf of Skype for Business Server 2015. The QSC AG SIP Trunk requires registration and authentication to provide service. In the interoperability test topology, the Served IP Group is Skype for Business Server 2015 IP Group and the Serving IP Group is QSC AG SIP Trunk IP Group.

➢ **To configure a registration account:**

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Served IP Group</td>
<td>S4B</td>
</tr>
<tr>
<td>Application Type</td>
<td>SBC</td>
</tr>
<tr>
<td>Serving IP Group</td>
<td>QSC</td>
</tr>
<tr>
<td>Host Name</td>
<td>As provided by the SIP Trunk provider</td>
</tr>
<tr>
<td>Register</td>
<td>Regular</td>
</tr>
<tr>
<td>Contact User</td>
<td>1234567890 (trunk main line)</td>
</tr>
<tr>
<td>Username</td>
<td>As provided by the SIP Trunk provider</td>
</tr>
<tr>
<td>Password</td>
<td>As provided by the SIP Trunk provider</td>
</tr>
</tbody>
</table>
4. Click **Apply**.
4.15 **Step 15: Miscellaneous Configuration**

This section describes miscellaneous E-SBC configuration.

4.15.1 **Step 15a: Configure Call Forking Mode**

This step describes how to configure the E-SBC's handling of SIP 18x responses received for call forking of INVITE messages. For the interoperability test topology, if a SIP 18x response with SDP is received, the E-SBC opens a voice stream according to the received SDP. The E-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.

➢ **To configure call forking:**

1. Open the SBC General Settings page (Setup menu > Signaling & Media tab > SBC folder > SBC General Settings).
2. From the ‘SBC Forking Handling Mode’ drop-down list, select **Sequential**.

   **Figure 4-48: Configuring Forking Mode**

3. Click **Apply**.
4.15.2 Step 15b: Configure SBC Alternative Routing Reasons

This step describes how to configure the E-SBC's handling of SIP 503 responses received for outgoing SIP dialog-initiating methods, e.g., INVITE, OPTIONS, and SUBSCRIBE messages. In this case E-SBC attempts to locate an alternative route for the call.

- **To configure SIP reason codes for alternative IP routing:**
  1. Open the Alternative Routing Reasons table (Setup menu > Signaling & Media tab > SBC folder > Routing > Alternative Reasons).
  2. Click New.
  3. From the 'Release Cause' drop-down list, select 503 Service Unavailable.

*Figure 4-49: SBC Alternative Routing Reasons Table*

4. Click **Apply**.
4.16 Step 16: Reset the E-SBC

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

➢ To reset the device through Web interface:

1. Open the Maintenance Actions page (Setup menu > Administration tab > Maintenance folder > Maintenance Actions).

   ![Figure 4-50: Resetting the E-SBC](image)

   Maintenance Actions

<table>
<thead>
<tr>
<th>RESET DEVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset Device</td>
</tr>
<tr>
<td>Save To Flash</td>
</tr>
<tr>
<td>Graceful Option</td>
</tr>
</tbody>
</table>

2. Ensure that the 'Save To Flash' field is set to Yes (default).

3. Click the Reset button; a confirmation message box appears, requesting you to confirm.

4. Click OK to confirm device reset.
A AudioCodes INI File

The ini configuration file of the E-SBC, corresponding to the secure mode (TLS/SRTP) Web-based configuration as described in Section 4 on page 31, is shown below:

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

```
;**************
;** Ini File **
;**************
;Board: Mediant 800B
;HW Board Type: 69  FK Board Type: 72
;Serial Number: 5299378
;Slot Number: 1
;Software Version: 7.20A.002
;DSP Software Version: 5014AE3_R => 720.25
;Board IP Address: 10.15.17.77
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 512M   Flash size: 64M   Core speed: 500Mhz
;Num of DSP Cores: 3  Num DSP Channels: 30
;Num of physical LAN ports: 4
;Profile: NONE
;;Key features:
;Board Type: Mediant 800B ;IP Media: Conf VXML CALEA TrunkTesting ;PSTN FALLBACK Supported ;E1Trunks=1 ;T1Trunks=1 ;FXSPorts=4 ;FXOPorts=0 ;BRITrunks=4 ;DATA features: ;Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol ;Channel Type: DspCh=30 IPMediaDspCh=30 ;HA ;DSP Voice features: RTCP-XR ;Coders: G723 G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB G722 EG711 MS_RTA_NB MS_RTA_WP SILK_NB SILK_WP SPEEX_NB SPEEX_WP OPUS_NB OPUS_WP ;QOE features: VoiceQualityMonitoring MediaEnhancement ;Control Protocols: MSFT FEU=100 TestCall=100 MGCP SIP SASurvivability SBC=250 ;Default features::;Coders: G711 G726;

------- HW components------
;
; Slot # : Module type : # of ports
;---------------------------------------------------------------
;    1 : FALC56   : 1
;    2 : FXS      : 4
;    3 : BRI      : 4
;---------------------------------------------------------------

[System Params]

SyslogServerIP = 10.15.77.100
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCoffset = 7200
TelnetServerEnable = 0
;VpFileLastUpdateTime is hidden but has non-default value
```

Version 7.2
85
AudioCodes Mediant E-SBC
NTPServerIP = '10.15.27.1'
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSUBSCRIBEDialogs is hidden but has non-default value
;PM_gwSBCRegisteredUsers is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value

[BSP Params]
PCMLawSelect = 3
INIFileVersion = 10482
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]

[ControlProtocols Params]

[MGCP Params]

[MEGACO 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]
ENABLEMEDIASECURITY = 1

[WEB Params]
LogoWidth = '145'
UseProductName = 1
;HTTPSPKeyFileName is hidden but has non-default value

[SIP Params]
MEDIACHANNELS = 100
GWDEBUGLEVEL = 5
ENABLESBCAPPLICATION = 1
MSLDAPPRIIMARYKEY = 'telephoneNumber'
SBCMAXFORWARDSLIMIT = 70
A. AudioCodes INI File

SBCPREFERENCESMODE = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
SBCSESSIONREFRESHINGPOLICY = 1
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[SCTP 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_4_1", 1, 4, "LAN Port#1", "GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_4_2", 1, 4, "LAN Port#2", "GROUP_1", "Redundant";
PhysicalPortsTable 2 = "GE_4_3", 1, 4, "WAN Port#1", "GROUP_2", "Active";
PhysicalPortsTable 3 = "GE_4_4", 1, 4, "WAN Port#2", "GROUP_2", "Redundant";

[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";

[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName,
DeviceTable_Tagging, DeviceTable_MTU;
DeviceTable 0 = 1, "GROUP_1", "LAN_DEV", 0, 1500;
DeviceTable 1 = 2, "GROUP_2", "WAN_DEV", 0, 1500;
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes, InterfaceTable_InterfaceMode, InterfaceTable_IPAddress, InterfaceTable_PrefixLength, InterfaceTable_Gateway, InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress, InterfaceTable_SecondaryDNSServerIPAddress, InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.77.55, 16, 10.15.0.1, "LAN_IF", 10.15.27.1, 0.0.0.0, "LAN_DEV";
InterfaceTable 1 = 5, 10, 195.189.192.157, 25, 195.189.192.129, "WAN_IF", 80.179.52.100, 80.179.55.100, "WAN_DEV";

WebUsers 0 = "Admin", "$1$LE0VGBxUAQFSUAJXUQANXwoPDwtaeSNwInB2c3B+eihzKSgvfDfzMDI1YgC0YWhub2h1P GpUVwVBlNBgpRXV4="", 1, 0, 2, 15, 60, 200, "62cabed5276f6d59432fca295a1346";
WebUsers 1 = "User", "$1$fRwcHLO4tOHmvOKy701ys7m5vrbzpqfyokL0r6v7q/iv/P35kpmUwcxBkZWy5iaz8+Wm NGBoFXhdTR14yDj94="", 3, 0, 2, 15, 60, 50, "e124fc45691a62316416e055a60ed6f";

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion, TLSContexts_DTLSVersion, TLSContexts_ServerCipherString, TLSContexts_ClientCipherString, TLSContexts.RequireStrictCert, TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary, TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort, TLSContexts_OcspDefaultResponse, TLSContexts_DHKeySize;
TLSContexts 0 = "default", 7, 0, "RC4:EXP", "ALL:!ADH", 0, 0, 0.0.0.0, 0.0.0.0, 2560, 0, 1024;
TLSContexts 1 = "QSC", 7, 0, "RC4:AES128", "ALL:!aNULL", 0, 0, 0.0.0.0, 0.0.0.0, 2560, 0, 1024;
[ AudioCodersGroups ]

FORMAT AudioCodersGroups_Index = AudioCodersGroups_Name;
AudioCodersGroups 0 = "AudioCodersGroups_0"
AudioCodersGroups 1 = "AudioCodersGroups_1"
AudioCodersGroups 2 = "AudioCodersGroups_2"

[

AllowedAudioCodersGroups

FORMAT AllowedAudioCodersGroups_Index = AllowedAudioCodersGroups_Name;
AllowedAudioCodersGroups 0 = "QSC-Allowed-Coders"

[

IpProfile

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupName, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_CNGmode,
IpProfile_VxXTransportType, IpProfile_NSEMode, IpProfile_IsDTMFUsed,
IpProfile_CallLimit, IpProfile_DisconnectOnBrokenConnection,
IpProfile_FirstTxDTmfOption, IpProfile_SecondTxDTmfOption,
IpProfile_CallDTMFOption, IpProfile_EnableDTMF,
IpProfile_CallDTMFAnswerMode, IpProfile_CallDTMFAnswerModeOnHold,
IpProfile_CallDTMFAnswerModeOnHoldOnHold, IpProfile_CallDTMFAnswerModeOnHoldOnHangUp,
IpProfile_CallDTMFAnswerModeOnHoldOnHangUpOnHold,
IpProfile_CallDTMFAnswerModeOnHoldOnHangUpOnHangUp,
IpProfile_CallDTMFAnswerModeOnHoldOnHangUpOnHangUpOnHold,
IpProfile_EnableHold, IpProfile_InputGain,
IpProfile_VoiceVolume, IpProfile_AddIEInSetup,
IpProfile_SBCExtensionCodersGroupName,
IpProfile_SBCIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedAudioCodersGroupName,
IpProfile_SBCAllowedVideoCodersGroupName, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDASensitivityParameterSuit, IpProfile_AMDASensitivityLevel,
IpProfile_AMDAMaxGreetingTime, IpProfile_AMDAMaxPostSilenceGreetingTime,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
Microsoft Skype for Business & QSC AG SIP Trunk

IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay,
IpProfile_SBCUserBehindUpdNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCSDPHandleTCPAttribute,
IpProfile_SBCRemoveCryptoLifetimeInSDP, IpProfile_SBCIceMode,
IpProfile_SBCRTCPMPux, IpProfile_SCCMediaSecurityMethod,
IpProfile_SBCHandleDTXdetect, IpProfile_SBCRTCPFeedback,
IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders,
IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCRemoteMultipleEarlyDialogs,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag,
IpProfile_SBCAdaptRFC2833BWToVoiceCoderBW,
IpProfile_CreatedByRoutingServer, IpProfile_SBCFaxReroutingMode,
IpProfile_SBCMaxCallDuration, IpProfile_SBCGenerateRTP,
IpProfile_SBCISUPBodyHandling, IpProfile_SBCISUPVariant,
IpProfile_SBCVoiceQualityEnhancement, IpProfile_SBCMaxOpusBW;

IpProfile 1 = "S4B", 1, "", 0, 10, 10, 46, 24, 0, 0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", "AudioCodersGroups_1", 0, 0, "", "", 0, 1, 0, 0, 0, 0, 300, 400, 0, 0, 0, "", 0, 1, 3, 3, 1, 1, 0, 3, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0;

IpProfile 2 = "QSC", 1, "", 0, 10, 10, 46, 24, 0, 0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", "AudioCodersGroups_2", 0, 0, "", "QSC-Allowed-Coders", 2, 1, 0, 0, 0, 1, 0, 8, 300, 400, 1, 2, 0, "", 0, 0, 1, 3, 2, 2, 1, 3, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0;
SRD UsedByRoutingServer, SRD_SBCOperationMode, SRD_SBCRoutingPolicyName, 
SRD_SBCDialPlanName;
SRD 0 = "DefaultSRD", 0, -1, 0, 0, 0, "defaultSBCRoutingPolicy", "";

[ \SRD ]

[ MessagePolicy ]

FORMAT MessagePolicy_Index = MessagePolicy_Name, 
MessagePolicy_MaxMessageLength, MessagePolicy_MaxHeaderLength, 
MessagePolicy_MaxBodyLength, MessagePolicy_MaxNumHeaders, 
MessagePolicy_SendRejection, MessagePolicy_MethodList, MessagePolicy_MethodListType, 
MessagePolicy_BodyList, MessagePolicy_BodyListType, 
MessagePolicy_UseMaliciousSignatureDB;
MessagePolicy 0 = "Malicious Signature DB Protection", -1, -1, -1, -1, -1, 
1, 1, "", 0, "", 0, 1;

[ \MessagePolicy ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName, 
SIPInterface_NetworkInterface, SIPInterface_ApplicationType, 
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_TopologyLocation;
SIPInterface 0 = "S4B", "LAN_IF", 2, 0, 0, 5067, "DefaultSRD", "", 
"default", -1, 0, 500, -1, -1, -1, 0, 0;
SIPInterface 1 = "QSC", "WAN_IF", 2, 5060, 0, 5061, "DefaultSRD", "", 
"default", -1, 0, 500, -1, -1, -1, 0, 1;

[ \SIPInterface ]

[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName, 
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime, 
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, 
ProxySet_SRDNName, ProxySet_ClassificationInput, ProxySet_TLSContextName, 
ProxySet_RedundancyMode, ProxySet_DNSResolveMethod, 
ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName, 
ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv4SIPInterfaceName, 
ProxySet_SBCIPv6SIPInterfaceName, ProxySet_MinActiveServersLB, 
ProxySet_SuccessDetectionRetries, ProxySet_SuccessDetectionInterval, 
ProxySet_FailureDetectionRetransmissions;
ProxySet 0 = "ProxySet_0", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", 
"", "S4B", "", "", 1, 1, 10, -1;
ProxySet 1 = "S4B", 1, 60, 1, 1, "DefaultSRD", 0, "default", 1, -1, "", 
"", "S4B", "", "", 1, 1, 10, -1;
ProxySet 2 = "QSC", 1, 60, 0, 0, "DefaultSRD", 0, "QSC", -1, 1, "", "", 
"QSC", "", "", 1, 1, 10, -1;
FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRVName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCLoading, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_AgentUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_TopologyLocation, IPGroup_SBCDialPlanName,
IPGroup_CallSetupRulesSetId;

IPGroup 0 = 0, "Default_IPG", "ProxySet_0", "", "", -1, 0, "DefaultSRD",
"", 0, 0, 0, 0, 0; IPGroup 1 = 0, "S4B", "S4B", "sipconnect.qsc.de", "S4B",
"", 0, 0, 0, 0, 0, 0, 0; IPGroup 2 = 0, "QSC", "QSC", "sipconnect.qsc.de", "QSC",
"", 0, 0, 0, 0, 0, 0, 0; SBCAlternativeRoutingReasons 0 = 503;

FORMAT SBCAlternativeRoutingReasons_Index =
SBCAlternativeRoutingReasons_ReleaseCause;
SBCAlternativeRoutingReasons 0 = 503;

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 1 = "1", 0, "FE.S4B.interop:5067", 2;
ProxyIp 2 = "2", 0, "secure-sipconnect.qsc.de", 2;

FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroupName, Account_ServingIPGroupName, Account_Username,
Account_Password, Account_HostName, Account_Register, Account_ContactUser, Account_ApplicationType;
Account 0 = -1, "S4B", "QSC", "100066588364", "$1$KWhfTx0dB9UAhE=",
"sip.qsc.de", 1, "100066588364", 2;

[ \Account ]

[ 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_IPGroupSetName;
IP2IPRouting 0 = "Terminate OPTIONS", "defaultSBCRoutingPolicy", "Any", 
"", ",", ",", ",", ",", ",", 0, "", 1, "", "internal", 0, "", 0, 
"", ",", "";
IP2IPRouting 1 = "S4B to ITSP", "defaultSBCRoutingPolicy", "S4B", ",", ",", ",", ",", 0, "", "Any", 0, "", 0, "QSC", ",", 0, "", 1, 0, "", 
"", "", 0, 0, "";
IP2IPRouting 2 = "ITSP to S4B", "defaultSBCRoutingPolicy", "QSC", ",", ",", ",", ",", 0, "", "Any", 0, "", 0, "S4B", ",", 0, "", 1, 0, "", 
"", "", 0, 0, "";

[ \IP2IPRouting ]

[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index = IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_RoutingPolicyName, IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupName, IPOutboundManipulation_SrcIPGroupName,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcUsernamePrefix,
IPOutboundManipulation_DestUsernamePrefix, IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_CallingNamePrefix, IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageConditionName, IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupName, IPOutboundManipulation_Trigger,
IPOutboundManipulation_ManipulatedURI, IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight, IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_ManipulatedURI,
[ MessageManipulations ]

FORMAT MessageManipulations_Index = MessageManipulations_ManipulationName, MessageManipulations_ManSetID, MessageManipulations_ActionSubject, MessageManipulations_ActionType, MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Change Diversion Host", 4, "invite.request", "header.diversion exists", "header.diversion.url.host", 2, "param.ipg.dst.host", 0;
MessageManipulations 1 = "Call Forward", 4, "invite.request", "header.diversion exists", "header.p-asserted-identity.url.user", 2, "header.diversion.url.user", 0;
MessageManipulations 2 = "Call Transfer", 4, "invite.request", "header.referred-by exists", "header.referred-by.url.host", 2, "param.ipg.dst.host", 0;
MessageManipulations 3 = "Call Transfer", 4, "", "", "header.p-asserted-identity.url.user", 2, "header.referred-by.url.user", 1;
MessageManipulations 4 = " Reject Cause", 4, "any.response", "header.request-uri.methodtype=='603' OR header.request-uri.methodtype=='503' OR header.request-uri.methodtype=='488'"", "header.request-uri.methodtype", 2, "'486'", 0;

[ \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 ]

[ MaliciousSignatureDB ]

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

[ \MaliciousSignatureDB ]

[ AllowedAudioCoders ]

FORMAT AllowedAudioCoders_Index =
AllowedAudioCoders_AllowedAudioCodersGroupName,
AllowedAudioCoders_AllowedAudioCodersIndex, AllowedAudioCoders_CoderID,
AllowedAudioCoders_UserDefineCoder;
AllowedAudioCoders 0 = "QSC-Allowed-Coders", 0, 2, "";
AllowedAudioCoders 1 = "QSC-Allowed-Coders", 1, 1, "";
AllowedAudioCoders 2 = "QSC-Allowed-Coders", 2, 3, "";
AllowedAudioCoders 3 = "QSC-Allowed-Coders", 3, 20, "";

[ \AllowedAudioCoders ]

[ AudioCoders ]

FORMAT AudioCoders_Index = AudioCoders_AudioCodersGroupId,
AudioCoders_AudioCodersIndex, AudioCoders_Name, AudioCoders_pTime,
AudioCoders_rate, AudioCoders_PayloadType, AudioCoders_Sce,
AudioCoders_CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 0, 1, 2, 90, -1, 0, "";
AudioCoders 1 = "AudioCodersGroups_1", 0, 2, 2, 90, -1, 1, "";
AudioCoders 2 = "AudioCodersGroups_1", 1, 1, 2, 90, -1, 1, "";
AudioCoders 3 = "AudioCodersGroups_2", 0, 3, 2, 19, -1, 0, "";

[ \AudioCoders ]