Connecting AudioCodes' SBC to Microsoft Teams Direct Routing
Enterprise Model

Version 7.2
Table of Contents

1 Introduction ..................................................................................................................11
  1.1 About Teams Direct Routing .............................................................................11
  1.2 Validated AudioCodes Version .......................................................................11
  1.3 About AudioCodes SBC Product Series ............................................................11
  1.4 Infrastructure Prerequisites .............................................................................12

2 Configuring AudioCodes' SBC ...........................................................................13
  2.1 Prerequisites ......................................................................................................14
    2.1.1 About the SBC Domain Name ....................................................................14
  2.2 Validate AudioCodes' License .........................................................................15
  2.3 Configure LAN and WAN IP Interfaces ............................................................16
    2.3.1 Validate Configuration of Physical Ports and Ethernet Groups ..............17
    2.3.2 Configure LAN and WAN VLANs ............................................................18
    2.3.3 Configure Network Interfaces ...................................................................18
  2.4 Configure TLS Context .....................................................................................20
    2.4.1 Configure the NTP Server Address ..........................................................20
    2.4.2 Create a TLS Context for Teams Direct Routing ....................................20
    2.4.3 Generate a CSR and Obtain the Certificate from a Supported CA ..........22
    2.4.4 Deploy the SBC and Root / Intermediate Certificates on the SBC ..........25
  2.5 Method of Generating and Installing the Wildcard Certificate .........................27
  2.6 Deploy Baltimore Trusted Root Certificate .....................................................27
  2.7 Configure Media Realm ....................................................................................28
  2.8 Configure a SIP Signaling Interface ...................................................................29
  2.9 Configure Proxy Sets and Proxy Address .........................................................30
    2.9.1 Configure Proxy Sets ..................................................................................30
    2.9.2 Configure a Proxy Address ........................................................................31
  2.10 Configure a Coder Group ...............................................................................33
  2.11 Configure an IP Profile ....................................................................................34
  2.12 Configure an IP Groups ..................................................................................36
  2.13 Configure SRTP ...............................................................................................38
  2.14 Configuring Message Condition Rules ............................................................39
  2.15 Configuring Classification Rules .....................................................................40
  2.16 Configure IP-to-IP Call Routing Rules .............................................................41
  2.17 Configuring Firewall Settings .........................................................................42

3 Verify the Pairing Between the SBC and Direct Routing .......................................43

4 Make a Test Call ......................................................................................................45

A Syntax Requirements for SIP Messages 'INVITE' and 'OPTIONS' .....................47
  A.1 Terminology ......................................................................................................47
  A.2 Syntax Requirements for 'INVITE' Messages ..................................................47
  A.3 Requirements for 'OPTIONS' Messages Syntax .............................................47
  A.4 Connectivity Interface Characteristics .........................................................49

B SIP Proxy Direct Routing Requirements ...............................................................51
  B.1 Failover Mechanism .......................................................................................51
List of Figures

Figure 2-1: Connection Topology with SIP Trunk on the LAN ...............................................................13
Figure 2-2: Example of Registered DNS Names....................................................................................15
Figure 2-3: Network Interfaces in the Topology with SIP Trunk on the LAN ........................................16
Figure 2-4: Network Interfaces in the Topology with SIP Trunk on the WAN ........................................16
Figure 2-5: Physical Ports Configuration Interface ...............................................................................17
Figure 2-6: Ethernet Groups Configuration Interface ...........................................................................17
Figure 2-7: Configured VLAN IDs in Ethernet Device ...........................................................................18
Figure 2-8: Configuration Example of the Network Interface Table ......................................................19
Figure 2-9: Configuring NTP Server Address.........................................................................................20
Figure 2-10: Configuration of TLS Context for Direct Routing .............................................................21
Figure 2-11: Configured TLS Context for Direct Routing and Interface to Manage the Certificates ..22
Figure 2-12: Example of Certificate Signing Request – Creating CSR ..................................................23
Figure 2-13: Uploading the Certificate Obtained from the Certification Authority ..................................25
Figure 2-14: Message Indicating Successful Upload of the Certificate ..................................................25
Figure 2-15: Certificate Information Example .......................................................................................26
Figure 2-16: Example of Configured Trusted Root Certificates .............................................................26
Figure 2-17: Configuration Example Media Realms in Media Realm Table ..........................................28
Figure 2-18: Configuration Example of SIP Signaling Interfaces ..........................................................29
Figure 2-19: Configuration Example Proxy Sets in Proxy Sets Table ....................................................30
Figure 2-20: Configuring Proxy Address for SIP Trunk .........................................................................31
Figure 2-21: Configuring Proxy Address for Teams Direct Routing Interface .......................................31
Figure 2-22: Configuring Coder Group for Teams Direct Routing ..........................................................33
Figure 2-23: Configured IP Groups in IP Group Table ..........................................................................37
Figure 2-24: Configuring Media Security Parameter ..............................................................................38
Figure 2-25: Configuring Condition Table .............................................................................................39
Figure 2-26: Configuring Classification Rule ..........................................................................................40
Figure 2-27: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table ............................................41
Figure 3-1: Proxy Set Status ..................................................................................................................43
Figure A-1: Example of an 'INVITE' Message .........................................................................................47
Figure A-2: Example of 'OPTIONS' message .........................................................................................47
List of Tables

Table 1-1: Infrastructure Prerequisites ...................................................................................................12
Table 2-1: DNS Names Registered by an Administrator for a Tenant ...................................................14
Table 2-2: Configuration Example of the Network Interface Table ......................................................18
Table 2-3: New TLS Context ..................................................................................................................21
Table 2-4: Configuration Example Media Realms in Media Realm Table .............................................28
Table 2-5: Configuration Example of SIP Signaling Interfaces .............................................................29
Table 2-6: Configuration Example Proxy Sets in Proxy Sets Table .......................................................30
Table 2-7: Configuration Proxy Address for SIP Trunk ......................................................................31
Table 2-8: Configuration Proxy Address for Teams Direct Routing .....................................................32
Table 2-9: Configuration Example: Teams IP Profile ..........................................................................34
Table 2-10: Configuration Example: SIP Trunk IP Profile ..................................................................34
Table 2-11: Firewall Table Rules ..........................................................................................................42
Table A-1: Syntax Requirements for an 'OPTIONS' Message ..............................................................48
Table A-2: Teams Direct Routing Interface - Technical Characteristics ...........................................49
This page is intentionally left blank.
Notice

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

This document is subject to change without notice.

Date Published: August-26-2019

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Stay in the Loop with AudioCodes

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.
Related Documentation

<table>
<thead>
<tr>
<th>Document Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mediant 500 E-SBC User's Manual</td>
</tr>
<tr>
<td>Mediant 800B E-SBC User's Manual</td>
</tr>
<tr>
<td>Mediant 2600 E-SBC User's Manual</td>
</tr>
<tr>
<td>Mediant 4000 SBC User's Manual</td>
</tr>
<tr>
<td>Mediant 9000 SBC User's Manual</td>
</tr>
<tr>
<td>Mediant Software SBC User's Manual</td>
</tr>
<tr>
<td>Gateway and SBC CLI Reference Guide</td>
</tr>
<tr>
<td>SIP Message Manipulation Reference Guide</td>
</tr>
<tr>
<td>AudioCodes Configuration Notes</td>
</tr>
</tbody>
</table>

Document Revision Record

<table>
<thead>
<tr>
<th>LTRT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12771</td>
<td>Baltimore certificate import requirement: pem/pfx format</td>
</tr>
<tr>
<td>12772</td>
<td>Corrected the .pem certificate path</td>
</tr>
<tr>
<td>12773</td>
<td>MSFT and customer feedback</td>
</tr>
<tr>
<td>12774</td>
<td>Fixes from customer feedback</td>
</tr>
<tr>
<td>12775</td>
<td>Fixes from customer feedback. Title change: Enterprise Model</td>
</tr>
<tr>
<td>12776</td>
<td>Fixes</td>
</tr>
<tr>
<td>12777</td>
<td>Configuration Example: IP Profile; new IP-to-IP routing rules; Configuration Example: Refer Terminate; removed figure 'Configured IP-to-IP Routing'. Appendix B.</td>
</tr>
<tr>
<td>12778</td>
<td>Fixes</td>
</tr>
<tr>
<td>12779</td>
<td>SIP I/F parameter deleted. IP Profile modified description. Message Manipulations. OPTIONS Terminate.</td>
</tr>
<tr>
<td>12785</td>
<td><strong>From Firmware Version 7.20A.204.015 and later:</strong></td>
</tr>
<tr>
<td></td>
<td>The new ‘Proxy Keep-Alive using IP Group settings’ parameter was added in the IP Group Table. Due to this, Message Manipulation Set for OPTIONS was removed.</td>
</tr>
<tr>
<td>12786</td>
<td>Updates to the Proxy Sets configuration</td>
</tr>
<tr>
<td>12787</td>
<td>Fix mismatch in the Proxy Sets configuration</td>
</tr>
<tr>
<td>12788</td>
<td>Added ‘Source IP Address’ to Classification Table</td>
</tr>
<tr>
<td>12789</td>
<td>Step descriptions updates</td>
</tr>
<tr>
<td>12791</td>
<td>Added NTP Server configuration, SIP Trunk configuration example and Firewall Settings; updated certified firmware version and links to Microsoft documents.</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 website at https://online.audiocodes.com/documentation-feedback.
This page is intentionally left blank.
1 Introduction

This document describes how to connect AudioCodes' SBC to Teams Direct Routing and refers to the AudioCodes SBC configuration only. For configuring the Office 365 side, please refer to https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure. This document is intended for IT or telephony professionals.

Note: To zoom in on screenshots of example Web interface configurations, press Ctrl and +.

1.1 About Teams Direct Routing

Teams Direct Routing allows connecting a customer-provided SBC to Microsoft Phone System. The customer-provided SBC can be connected to almost any telephony trunk, or connect with third-party PSTN equipment. The connection allows:

- Using virtually any PSTN trunk with Microsoft Phone System
- Configuring interoperability between customer-owned telephony equipment, such as third-party PBXs, analog devices, and Microsoft Phone System

1.2 Validated AudioCodes Version

Microsoft has successfully conducted validation tests with AudioCodes' Mediant SBC Ver. 7.20A.250. Previous firmware versions may run successfully; however, Microsoft did not test such versions. For an updated list, refer to List of Session Border Controllers certified for Direct Routing. Note the following:

- Validate that you have the correct License key. Refer to AudioCodes' device's User's Manual for more information on how to view the device's License Key including licensed features and capacity. If you don’t have the correct License key, contact your AudioCodes representative to obtain one.
- The main AudioCodes licenses required by the SBC are as follows:
  - SW/TEAMS
  - Number of SBC sessions [Based on requirements]
  - Transcoding sessions [If media transcoding is needed]

1.3 About AudioCodes SBC Product Series

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

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

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

AudioCodes’ SBC is available as an integrated solution running on top of its field-proven Mediant Media Gateway and Multi-Service Business Router platforms, or as a software-only
solution for deployment with third-party hardware. The SBC can be offered as a Virtualized SBC, supporting the following platforms: Hyper-V, AWS, AZURE, AWP, KVM and VMWare.

1.4 **Infrastructure Prerequisites**

The table below shows the list of infrastructure prerequisites for deploying Direct Routing.

**Table 1-1: Infrastructure Prerequisites**

<table>
<thead>
<tr>
<th>Infrastructure Prerequisite</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certified Session Border Controller (SBC)</td>
<td></td>
</tr>
<tr>
<td>SIP Trunks connected to the SBC</td>
<td></td>
</tr>
<tr>
<td>Office 365 tenant</td>
<td></td>
</tr>
<tr>
<td>Domains</td>
<td></td>
</tr>
<tr>
<td>Public IP address for the SBC</td>
<td></td>
</tr>
<tr>
<td>Fully Qualified Domain Name (FQDN) for the SBC</td>
<td></td>
</tr>
<tr>
<td>Public DNS entry for the SBC</td>
<td></td>
</tr>
<tr>
<td>Public trusted certificate for the SBC</td>
<td></td>
</tr>
<tr>
<td>Firewall ports for Direct Routing signaling</td>
<td></td>
</tr>
<tr>
<td>Firewall IP addresses and ports for Direct Routing media</td>
<td></td>
</tr>
<tr>
<td>Media Transport Profile</td>
<td></td>
</tr>
<tr>
<td>Firewall ports for client media</td>
<td></td>
</tr>
</tbody>
</table>

See Microsoft's [Plan Direct Routing](#) document.
2 Configuring AudioCodes' SBC

This section shows how to configure AudioCodes' SBC for internetworking with Teams Direct Routing.

The figures below show examples of the connection topology. Multiple connection entities are shown in the figure:

- Third-party IP-PBX, analog devices and the administrator's management station, located on the LAN
- Teams Phone Systems Direct Routing Interface on the WAN
- SIP trunk from a third-party provider, which can be located on the LAN or on the WAN

Figure 2-1: Connection Topology with SIP Trunk on the LAN

![Connection Topology with SIP Trunk on the LAN]

Figure 2-2: Connection Topology with SIP Trunk on the WAN

![Connection Topology with SIP Trunk on the WAN]
2.1 Prerequisites

Before you begin the configuration, make sure you have the following for every SBC you want to pair:

- Public IP address
- FQDN name matching SIP addresses of the users
- Public certificate, issued by one of the supported CAs

2.1.1 About the SBC Domain Name

The SBC domain name must be from one of the names registered in 'Domains' of the tenant. You cannot use the *.onmicrosoft.com tenant for the domain name. For example, in Figure 2-2, the administrator registered the following DNS names for the tenant:

<table>
<thead>
<tr>
<th>DNS name</th>
<th>Can be used for SBC FQDN</th>
<th>Examples of FQDN names</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACeducation.info</td>
<td>Yes</td>
<td>Valid names:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- sbc.ACeducation.info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ussbscs15.ACeducation.info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- europe.ACeducation.info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Invalid name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- sbc1.europe.ACeducation.info (requires registering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- domain name europe.atatum.biz in 'Domains' first)</td>
</tr>
<tr>
<td>adatumbiz.onmicrosoft.com</td>
<td>No</td>
<td>Using *.onmicrosoft.com domains is not supported for SBC</td>
</tr>
<tr>
<td>hybridvoice.org</td>
<td>Yes</td>
<td>names</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid names:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- sbc1.hybridvoice.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ussbscs15.hybridvoice.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- europe.hybridvoice.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Invalid name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- sbc1.europe.hybridvoice.org (requires registering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- domain name europe.hybridvoice.org in 'Domains' first</td>
</tr>
</tbody>
</table>

Users can be from any SIP domain registered for the tenant. For example, you can provide users user@ACeducation.info with the SBC FQDN sbc1.hybridvoice.org so long as both names are registered for this tenant.
Figure 2-2: Example of Registered DNS Names

The following IP address and FQDN are used as examples in this guide:

<table>
<thead>
<tr>
<th>Public IP</th>
<th>FQDN Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>195.189.192.157</td>
<td>sbc.ACeducation.info</td>
</tr>
</tbody>
</table>

The certificate in the example is from DigiCert.

### 2.2 Validate AudioCodes’ License

The following licenses are required on AudioCodes’ device:

1. **Enable Microsoft** (licensing MSFT) [All AudioCodes media gateways and SBCs are by default shipped with this license. Exceptions: MSBR products and Mediant 500 SBC or Media Gateways]
2. **Enable TEAMS** (licensing SW/TEAMS)
3. **Number of SBC sessions** [based on requirements]
4. **Transcoding sessions** [if media transcoding is needed]
5. **Coders** [based on requirements]
2.3 Configure LAN and WAN IP Interfaces

This section describes how to configure the SBC’s IP network interfaces. There are several ways to deploy the SBC:

- SBC interfaces with the following IP entities:
  - Teams Direct Routing, located on the WAN
  - SIP Trunk - located on the LAN (or WAN)
- SBC connects to the WAN through a DMZ network
- Physical connection: The type of physical connection depends on the method used to connect to the Enterprise’s network. In the interoperability test topology, SBC connects to the LAN and DMZ using dedicated Ethernet ports (i.e., two ports and two network cables are used).
- SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - DMZ (VLAN ID 2)

![Figure 2-3: Network Interfaces in the Topology with SIP Trunk on the LAN](image)

![Figure 2-4: Network Interfaces in the Topology with SIP Trunk on the WAN](image)

This Configuration Notes document give example of topology with SIP Trunk on the LAN.
2.3.1 Validate Configuration of Physical Ports and Ethernet Groups

The physical ports are automatically detected by the SBC. The Ethernet groups are also auto-assigned to the ports. In this step, only parameter validation is necessary.

➢ To validate physical ports:

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

2. Validate that you have at least two physical ports detected by the SBC, one for LAN and the other for WAN. Make sure both ports are in Enabled mode.

Note: Based on your hardware configuration, you might have more than two ports.

➢ To validate Ethernet Groups:

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

2. Validate that you have at least two Ethernet Groups detected by the SBC, one for LAN and the other for WAN.
2.3.2 Configure LAN and WAN VLANs

This section 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.

Figure 2-7: Configured VLAN IDs in Ethernet Device

2.3.3 Configure Network Interfaces

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

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

To configure network parameters for both LAN and WAN interfaces:

1. Open the IP Interfaces table (Setup menu > IP Network tab > Core Entities folder > IP Interfaces).
2. Configure the IP interfaces as follows (your network parameters might be different):

Table 2-2: Configuration Example of the Network Interface Table

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

**Figure 2-8: Configuration Example of the Network Interface 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 IP</td>
<td>OAMP + Media</td>
<td>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>vlan1</td>
</tr>
<tr>
<td>1</td>
<td>WAN IP</td>
<td>Media + Control</td>
<td>IPv4 Manual</td>
<td>196.180.192.197</td>
<td>25</td>
<td>196.180.102.126</td>
<td>80.179.52.100</td>
<td>80.179.55.100</td>
<td>vlan2</td>
</tr>
</tbody>
</table>
2.4 Configure TLS Context

The Microsoft Phone System Direct Routing Interface only allows TLS connections from SBCs for SIP traffic with a certificate signed by one of the trusted Certification Authorities. Currently, supported Certification Authorities can be found in the following link:
https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc

2.4.1 Configure the NTP Server Address

This section describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or another global server) to ensure that the SBC receives the current date and time. This is necessary for validating certificates of remote parties. It is important, that NTP Server will locate on the OAMP IP Interface (LAN_IF in our case) or will be accessible through it.

➢ To configure the NTP server address:

1. Open the Time & Date page (Setup menu > Administration tab > Time & Date).
2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., 10.15.28.1).

   Figure 2-9: Configuring NTP Server Address

3. Click Apply.

2.4.2 Create a TLS Context for Teams Direct Routing

The section below shows how to request a certificate for the SBC WAN interface and to configure it based on the example of DigiCert Global Root CA. The certificate is used by the SBC to authenticate the connection with Teams Direct Routing.

The procedure involves the following main steps:

a. Create a TLS Context for Teams Direct Routing
b. Generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority
c. Deploy the SBC and Root/Intermediate certificates on the SBC

➢ To create a TLS Context for Teams Direct Routing:

1. Open the TLS Contexts page (Setup menu > IP Network tab > Security folder > TLS Contexts).
2. Create a new TLS Context by clicking +New at the top of the interface, and then configure the parameters using the table below as reference.
Table 2-3: New TLS Context

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>TLS Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Teams (arbitrary descriptive name)</td>
<td>TLSv1.2</td>
</tr>
</tbody>
</table>

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

Note: The table above exemplifies configuration focusing on interconnecting SIP and media. You might want to configure additional parameters according to your company's policies. For example, you might want to configure Online Certificate Status Protocol (OCSP) to check if SBC certificates presented in the online server are still valid or revoked. For more information on the SBC's configuration, see the User's Manual, available for download from https://www.audioCodes.com/library/technical-documents.

Figure 2-10: Configuration of TLS Context for Direct Routing

3. Click **Apply**; you should see the new TLS Context and option to manage the certificates at the bottom of 'TLS Context' table.
2.4.3 Generate a CSR and Obtain the Certificate from a Supported CA

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

To generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority:

1. Open the TLS Contexts page (Setup menu > IP Network tab > Security folder > TLS Contexts).
2. In the TLS Contexts page, select the Teams TLS Context index row, and then click the Change Certificate link located below the table; the Context Certificates page appears.
3. Under the Certificate Signing Request group, do the following:
   a. In the 'Common Name [CN]' field, enter the SBC FQDN name (based on example above, ACeducation.info).
   b. In the '1st Subject Alternative Name [SAN]' field, change the type to 'DNS', and then enter the SBC FQDN name (based on the example above, ACeducation.info).
   c. Change the 'Private Key Size' based on the requirements of your Certification Authority. Many CAs do not support private key of size 1024. In this case, you must change the key size to 2048.

Note: The domain portion of the Common Name [CN] and 1st Subject Alternative Name [SAN] must match the SIP suffix configured for Office 365 users.
d. To change the key size on TLS Context, go to: **Generate New Private Key and Self-Signed Certificate**, change the 'Private Key Size' to **2048** and then click **Generate Private-Key**. To use **1024** as a Private Key Size value, you can click **Generate Private-Key** without changing the default key size value.

e. Enter the rest of the request fields according to your security provider’s instructions.

f. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 2-12: Example of Certificate Signing Request – Creating CSR
4. Copy the CSR from the line "----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, for example `certreq.txt`.

5. Send `certreq.txt` file to the Certified Authority Administrator for signing.
2.4.4 Deploy the SBC and Root / Intermediate Certificates on the SBC

After obtaining the SBC signed and Trusted Root/Intermediate Certificate from the CA, install the following:

- SBC certificate
- Root / Intermediate certificates

➢ To install the SBC certificate:

1. In the SBC's Web interface, return to the TLS Contexts page and do the following:
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the Change Certificate link located below the table; the Context Certificates page appears.
   b. Scroll down to the Upload certificates files from your computer group, click the Choose File button corresponding to the 'Send Device Certificate...' field, navigate to the certificate file obtained from the CA, and then click Load File to upload the certificate to the SBC.

Figure 2-13: Uploading the Certificate Obtained from the Certification Authority

2. Validate that the certificate was uploaded correctly: A message indicating that the certificate was uploaded successfully is displayed in blue on the lower part of the page.

Figure 2-14: Message Indicating Successful Upload of the Certificate
3. In the SBC’s Web interface, return to the **TLS Contexts** page, select the required TLS Context index row, and then click the **Certificate Information** link, located at the bottom of the TLS. Then validate the Key size, certificate status and Subject Name:

   **Figure 2-15: Certificate Information Example**

![Certificate Information Example](image)

4. In the SBC’s Web interface, return to the **TLS Contexts** page.
   
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Trusted Root Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
   
   b. Click the **Import** button, and then select all Root/Intermediate Certificates obtained from your Certification Authority to load.

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

   **Figure 2-16: Example of Configured Trusted Root Certificates**

![Trusted Root Certificates](image)
2.5 Method of Generating and Installing the Wildcard Certificate

To use the same certificate on multiple devices, you may prefer using 3rd party application (e.g. DigiCert Certificate Utility for Windows) to process the certificate request from your Certificate Authority on another machine, with this utility installed.

After you've processed the certificate request and response using the DigiCert utility, test the certificate private key and chain and then export the certificate with private key and assign a password.

➢ To install the 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. Scroll down to the Upload certificates files from your computer group and do the following:
   a. Enter the password assigned during export with the DigiCert utility in the 'Private key pass-phrase' field.
   b. Click the Choose File button corresponding to the 'Send Private Key...' field and then select the SBC certificate file exported from the DigiCert utility.

2.6 Deploy Baltimore Trusted Root Certificate


To trust this certificate, your SBC must have the certificate in Trusted Certificates storage. Download the certificate from https://cacert.omniroot.com/bc2025.pem and follow the steps above to import the certificate to the Trusted Root storage.

Note: Before importing the Baltimore root certificate into AudioCodes' SBC, make sure it's in .PEM or .PFX format. If it isn't, you need to convert it to .PEM or .PFX format, otherwise the 'Failed to load new certificate' error message is displayed. To convert to PEM format, use Windows local store on any Windows OS and then export it as 'Base-64 encoded X.509 (.CER) certificate'.
2.7 Configure Media Realm

Media Realms allow dividing the UDP port ranges for use on different interfaces. In the example below, two Media Realms are configured:

- One for the LAN interface, with the UDP port starting at 6000 and the number of media session legs 100 (you need to calculate number of media session legs based on your usage)
- One for the WAN interface, with the UDP port range starting at 7000 and the number of media session legs 100

To configure Media Realms:

1. Open the Media Realms table (Setup menu > Signaling & Media tab > Core Entities folder > Media Realms).
2. Configure Media Realms as follows (you can use the default Media Realm (Index 0), but modify it):

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Topology Location</th>
<th>IPv4 Interface Name</th>
<th>Port Range Start</th>
<th>Number of Media Session Legs</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>MRLan</td>
<td>LAN_IF</td>
<td></td>
<td>6000</td>
<td>100 (media sessions assigned with port range)</td>
</tr>
<tr>
<td>1</td>
<td>MRWan</td>
<td>Up</td>
<td>WAN_IF</td>
<td>7000</td>
<td>100 (media sessions assigned with port range)</td>
</tr>
</tbody>
</table>

The configured Media Realms are shown in the figure below:

Figure 2-17: Configuration Example Media Realms in Media Realm Table
2.8 Configure a SIP Signaling Interface

This section shows how to configure a SIP Signaling Interfaces. A SIP Interface defines a listening port and type (UDP, TCP, or TLS) for SIP signaling traffic on a specific logical IP network interface (configured in the Interface Table above) and Media Realm.

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

AudioCodes also offers a comprehensive suite of documents covering the interconnection between different trunks and equipment.

To configure a SIP Interfaces:

1. Open the SIP Interfaces table (Setup menu > Signaling & Media tab > Core Entities folder > SIP Interfaces).
2. Configure SIP Interfaces. You can use the default SIP Interface (Index 0), but modify it as shown in the table below. The table below shows an example of the configuration. You can change some parameters according to your requirements.

Note: The Direct Routing interface can only use TLS for a SIP port. It does not support using TCP due to security reasons. The SIP port might be any port of your choice. When pairing the SBC with Office 365, the chosen port is specified in the pairing command.

Table 2-5: Configuration Example of SIP Signaling Interfaces

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Network Interface</th>
<th>Application Type</th>
<th>UDP Port</th>
<th>TCP Port</th>
<th>TLS Port</th>
<th>Enable TCP Keepalive</th>
<th>Classification Failure Response Type</th>
<th>Media Realm</th>
<th>TLS Context Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SIPTrunk</td>
<td>LAN_IF</td>
<td>SBC</td>
<td>5060</td>
<td>0</td>
<td>0</td>
<td>Disable</td>
<td>500 (leave default value)</td>
<td>MRLan</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>(arbitrary name)</td>
<td></td>
<td></td>
<td>(according to Service Provider requirement)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Teams</td>
<td>WAN_IF</td>
<td>SBC</td>
<td>0</td>
<td>0</td>
<td>5061</td>
<td>Enable</td>
<td>0 (Recommended to prevent DoS attacks)</td>
<td>MRWan</td>
<td>Teams</td>
</tr>
<tr>
<td></td>
<td>(arbitrary name)</td>
<td></td>
<td></td>
<td>(Phone System does not use UDP or TCP for SIP signaling)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The configured SIP Interfaces are shown in the figure below:

Figure 2-18: Configuration Example of SIP Signaling Interfaces
2.9 Configure Proxy Sets and Proxy Address

2.9.1 Configure Proxy Sets

The Proxy Set and Proxy Address defines TLS parameters, IP interfaces, FQDN and the remote entity’s port. Proxy Sets can also be used to configure load balancing between multiple servers. The example below covers configuration of a Proxy Set for Teams Direct Routing and SIP Trunk. Note that the configuration of a Proxy Set for the SIP Trunk shows as an example and your configuration might be different. For specific configuration of interfaces pointing to SIP trunks and/or the third-party PSTN environment connected to the SBC, see the trunk/environment vendor’s documentation. AudioCodes also offers a comprehensive suite of documents covering the interconnection between different trunks and the equipment.

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

➢ To configure a Proxy Sets:

1. Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets).
2. Configure Proxy Sets as shown in the table below:

Table 2-6: Configuration Example Proxy Sets in Proxy Sets Table

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>SBC IPv4 SIP Interface</th>
<th>TLS Context Name</th>
<th>Proxy Keep-Alive</th>
<th>Proxy Hot Swap</th>
<th>Proxy Load Balancing Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SITrunk (arbitrary name)</td>
<td>SITrunk</td>
<td>Default</td>
<td>Using Options</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Teams (arbitrary name)</td>
<td>Teams</td>
<td>Teams</td>
<td>Using Options</td>
<td>Enable</td>
<td>Random Weights</td>
</tr>
</tbody>
</table>

The configured Proxy Sets are shown in the figure below:

Figure 2-19: Configuration Example Proxy Sets in Proxy Sets Table
2.9.2 Configure a Proxy Address

This section shows how to configure a Proxy Address.

➢ To configure a Proxy Address for SIP Trunk:

1. Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets) and then click the Proxy Set SIPTrunk, and then click the Proxy Address link located below the table; the Proxy Address table opens.
2. Click +New; the following dialog box appears:

Figure 2-20: Configuring Proxy Address for SIP Trunk

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

Table 2-7: Configuration Proxy Address for SIP Trunk

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

4. Click Apply.

➢ To configure a Proxy Address for Teams:

1. Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets) and then click the Proxy Set Teams, and then click the Proxy Address link located below the table; the Proxy Address table opens.
2. Click +New; the following dialog box appears:

Figure 2-21: Configuring Proxy Address for Teams Direct Routing Interface
3. Configure the address of the Proxy Set according to the parameters described in the table below:

**Table 2-8: Configuration Proxy Address for Teams Direct Routing**

<table>
<thead>
<tr>
<th>Index</th>
<th>Proxy Address</th>
<th>Transport Type</th>
<th>Proxy Priority</th>
<th>Proxy Random Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>sip.pstnhub.microsoft.com:5061</td>
<td>TLS</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>sip2.pstnhub.microsoft.com:5061</td>
<td>TLS</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>sip3.pstnhub.microsoft.com:5061</td>
<td>TLS</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

4. Click **Apply** and then save your settings to flash memory.
2.10 Configure a Coder Group

This section describes how to configure coders (known as Coder Groups). Teams Direct Routing supports the SILK and OPUS coders while the network connection to the SIP Trunk may restrict operation with a dedicated coders list. You need to add a Coder Group with the supported coders for each of the following leg, the Teams Direct Routing and the SIP Trunk. Note that the Coder Group ID for this entity will be assigned to its corresponding IP Profile in the next section.

➢ To configure a Coder Group:

1. Open the Coder Groups table (Setup menu > Signaling & Media tab > Coders & Profiles folder > Coder Groups).

2. From the ‘Coder Group Name’ dropdown, select 1:Does Not Exist and add the required codecs as shown in the figure below.

Figure 2-22: Configuring Coder Group for Teams Direct Routing

3. Click Apply, and then confirm the configuration change in the prompt that pops up.
2.11 Configure an IP Profile

This section describes how to configure IP Profiles. An IP Profile is a set of parameters with user-defined settings related to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder type). An IP Profile needs to be assigned to the specific IP Group.

To configure an IP Profile:

1. Open the Proxy Sets table (Setup > Signaling and Media > Coders and Profiles > IP Profiles).
2. Click +New to add the IP Profile for the Direct Routing interface. Configure the parameters using the table below as reference.

Table 2-9: Configuration Example: Teams IP Profile

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Teams (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Media Security</td>
<td></td>
</tr>
<tr>
<td>SBC Media Security Mode</td>
<td>SRTP</td>
</tr>
<tr>
<td>SBC Early Media</td>
<td></td>
</tr>
<tr>
<td>Remote Early Media RTP Detection Mode</td>
<td>By Media (required, as Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18x response)</td>
</tr>
<tr>
<td>SBC Media</td>
<td></td>
</tr>
<tr>
<td>Extension Coders Group</td>
<td>AudioCodersGroups_1</td>
</tr>
<tr>
<td>RTCP Mode</td>
<td>Generate Always (required, as some ITSPs do not send RTCP packets during Hold, but Microsoft expects them)</td>
</tr>
<tr>
<td>ICE Mode</td>
<td>Lite (required only when Media Bypass enabled on Teams)</td>
</tr>
<tr>
<td>SBC Signaling</td>
<td></td>
</tr>
<tr>
<td>Remote Update Support</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Remote re-INVITE Support</td>
<td>Supported Only With SDP</td>
</tr>
<tr>
<td>Remote Delayed Offer Support</td>
<td>Not Supported</td>
</tr>
<tr>
<td>SBC Forward and Transfer</td>
<td></td>
</tr>
<tr>
<td>Remote REFER Mode</td>
<td>Handle Locally</td>
</tr>
<tr>
<td>Remote 3xx Mode</td>
<td>Handle Locally</td>
</tr>
<tr>
<td>SBC Hold</td>
<td></td>
</tr>
<tr>
<td>Remote Hold Format</td>
<td>Inactive (some SIP Trunk may answer with a=inactive and IP=0.0.0.0 in response to the Re-Invite with Hold request from Teams. Microsoft Media Stack doesn’t support this format. So, SBC will replace 0.0.0.0 with its IP address)</td>
</tr>
</tbody>
</table>

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

3. Click Apply, and then save your settings to flash memory.
4. Click +New to add the IP Profile for the SIP Trunk. Configure the parameters using the table below as a reference.

Table 2-10: Configuration Example: SIP Trunk IP Profile

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>
### General

| Name         | SIPTrunk |

### Media Security

| SBC Media Security Mode | RTP |

### SBC Signaling

| P-Asserted-Identity Header Mode | Add (required for anonymous calls) |

### SBC Forward and Transfer

<table>
<thead>
<tr>
<th>Remote REFER Mode</th>
<th>Handle Locally</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Replaces Mode</td>
<td>Handle Locally</td>
</tr>
<tr>
<td>Remote 3xx Mode</td>
<td>Handle Locally</td>
</tr>
</tbody>
</table>

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

5. Click **Apply**, and then save your settings to flash memory.
2.12 Configure an IP Groups

This section describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the SBC communicates. This can be a server (e.g., IP-PBX or SIP Trunk) 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.

➢ To configure an IP Groups:

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

2. Configure the IP Group for the SIP Trunk:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>SIPTrunk</td>
</tr>
<tr>
<td>Type</td>
<td>Server</td>
</tr>
<tr>
<td>Proxy Set</td>
<td>SIPTrunk</td>
</tr>
<tr>
<td>IP Profile</td>
<td>SIPTrunk</td>
</tr>
<tr>
<td>Media Realm</td>
<td>MRLan or MRWan (according to your network environment)</td>
</tr>
<tr>
<td>Classify by Proxy Set</td>
<td>Disable</td>
</tr>
<tr>
<td>SIP Group Name</td>
<td>(according to ITSP requirement)</td>
</tr>
</tbody>
</table>

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

3. Configure IP Group for the Teams Direct Routing:
### Parameter | Value
--- | ---
Name | Teams
Topology Location | Up
Type | Server
Proxy Set | Teams
IP Profile | Teams
Media Realm | MRWan
Classify by Proxy Set | Disable
Local Host Name | `<FQDN name of the SBC in the enterprise tenant>`
(For example, `sbc.ACeducation.info` defines the host name (string) that the device uses in the SIP message's Via and Contact headers. This is typically used to define an FQDN as the host name. The device uses this string for Via and Contact headers in outgoing INVITE messages sent to a specific IP Group, and the Contact header in SIP 18x and 200 OK responses for incoming INVITE messages received from a specific IP Group.
More information about the requirements for the various parts of SIP messages can be found in Appendix A.2 on page 47.)
Always Use Src Address | Yes
Proxy Keep-Alive using IP Group settings | Enable

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

The configured IP Groups are shown in the figure below:

**Figure 2-23: Configured IP Groups in IP Group Table**
2.13 Configure SRTP

This section describes how to configure media security. The Direct Routing Interface requires the use of SRTP only, so you need to configure the SBC to operate in the same manner.

➢ To configure media security:

1. Open the Media Security page (Setup menu > Signaling & Media tab > Media folder > Media Security).
2. From the ‘Media Security’ drop-down list, select Enable to enable SRTP.

Figure 2-24: Configuring Media Security Parameter

3. Click Apply.
2.14 Configuring Message Condition Rules

This section describes how to configure the Message Condition Rules. A Message Condition defines special conditions (requisites) for incoming SIP messages. These rules can be used as additional matching criteria for the IP-to-IP routing rules in the IP-to-IP Routing table. The following condition verifies that the Contact header contains Teams FQDN.

➢ To configure a Message Condition rule:

1. Open the Message Conditions table (Setup menu > Signaling & Media tab > Message Manipulation folder > Message Conditions).
2. Click New, and then configure the parameters as follows:

<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>Teams-Contact (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Condition</td>
<td>header.contact.url.host contains 'pstnhub.microsoft.com'</td>
</tr>
</tbody>
</table>

Figure 2-25: Configuring Condition Table

3. Click Apply.
2.15 Configuring Classification Rules

This section describes how to configure Classification rules. A Classification rule classifies incoming SIP dialog-initiating requests (e.g., INVITE messages) to a "source" IP Group. The source IP Group is the SIP entity that sends the SIP dialog request. Once classified, the device uses the IP Group to process the call (manipulation and routing).

You can also use the Classification table for employing SIP-level access control for successfully classified calls, by configuring Classification rules with whitelist and blacklist settings. If a Classification rule is configured as a whitelist ("Allow"), the device accepts the SIP dialog and processes the call. If the Classification rule is configured as a blacklist ("Deny"), the device rejects the SIP dialog.

➢ To configure a Classification rule:

1. Open the Classification table (Setup menu > Signaling & Media tab > SBC folder > Classification Table).

2. 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>Teams</td>
</tr>
<tr>
<td>Source SIP Interface</td>
<td>Teams</td>
</tr>
<tr>
<td>Source IP Address</td>
<td>52.114.<em>.</em></td>
</tr>
<tr>
<td>Destination Host</td>
<td>sbc.ACeducation.info (example)</td>
</tr>
<tr>
<td>Message Condition</td>
<td>Teams-Contact</td>
</tr>
<tr>
<td>Action Type</td>
<td>Allow</td>
</tr>
<tr>
<td>Source IP Group</td>
<td>Teams</td>
</tr>
</tbody>
</table>

Figure 2-26: Configuring Classification Rule

3. Click Apply.
2.16 Configure IP-to-IP Call Routing Rules

This section describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected.

The example shown below only covers IP-to-IP routing, though you can route the calls from SIP Trunk to Teams and vice versa. See AudioCodes’ SBC documentation for more information on how to route in other scenarios.

The following IP-to-IP Routing Rules will be defined:

- Terminate SIP OPTIONS messages on the SBC
- Terminate REFER messages to Teams Direct Routing
- Calls from Teams Direct Routing to SIP Trunk
- Calls from SIP Trunk to Teams Direct Routing

To configure IP-to-IP routing rules:

1. Open the IP-to-IP Routing table (Setup menu > Signaling & Media tab > SBC folder > Routing > IP-to-IP Routing).
2. Configure routing rules as shown in the table below:

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Source IP Group</th>
<th>Request Type</th>
<th>Call Trigger</th>
<th>ReRoute IP Group</th>
<th>Dest Type</th>
<th>Dest IP Group</th>
<th>Dest Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Terminate OPTIONS</td>
<td>Any</td>
<td>OPTIONS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>internal</td>
</tr>
<tr>
<td>1</td>
<td>Refer from Teams (arbitrary name)</td>
<td>Any</td>
<td>REFER</td>
<td>Teams</td>
<td></td>
<td>Request URI</td>
<td>Teams</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Teams to SIP Trunk (arbitrary name)</td>
<td>Teams</td>
<td></td>
<td></td>
<td>IP Group</td>
<td></td>
<td>SIPTrunk</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>SIP Trunk to Teams (arbitrary name)</td>
<td>SIPTrunk</td>
<td></td>
<td></td>
<td>IP Group</td>
<td></td>
<td>Teams</td>
<td></td>
</tr>
</tbody>
</table>

The configured routing rules are shown in the figure below:

**Figure 2-27: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table**

**Note:** The routing configuration may change according to your specific deployment topology.
2.17 Configuring Firewall Settings

**Note:** AudioCodes highly advised to configure firewall with network traffic filtering rules in front of WAN interface of the SBC. For detailed list of ports, which needed to be open please refer to: https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sip-signaling-fqdns-and-firewall-ports.

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

➢ **To configure a firewall rule:**

1. Open the Firewall table (Setup menu > IP Network tab > Security folder> Firewall).
2. Configure the following Access list rules for Teams Direct Rout IP Interface:

<table>
<thead>
<tr>
<th>Index</th>
<th>Source IP</th>
<th>Subnet Prefix</th>
<th>Start Port</th>
<th>End Port</th>
<th>Protocol</th>
<th>Use Specific Interface</th>
<th>Interface ID</th>
<th>Allow Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>&lt;Public DNS Server IP&gt; (e.g. 8.8.8.8)</td>
<td>32</td>
<td>0</td>
<td>65535</td>
<td>Any</td>
<td>Enable</td>
<td>WAN_IF</td>
<td>Allow</td>
</tr>
<tr>
<td>1</td>
<td>52.114.148.0</td>
<td>32</td>
<td>0</td>
<td>65535</td>
<td>TCP</td>
<td>Enable</td>
<td>WAN_IF</td>
<td>Allow</td>
</tr>
<tr>
<td>2</td>
<td>52.114.132.46</td>
<td>32</td>
<td>0</td>
<td>65535</td>
<td>TCP</td>
<td>Enable</td>
<td>WAN_IF</td>
<td>Allow</td>
</tr>
<tr>
<td>3</td>
<td>52.114.75.24</td>
<td>32</td>
<td>0</td>
<td>65535</td>
<td>TCP</td>
<td>Enable</td>
<td>WAN_IF</td>
<td>Allow</td>
</tr>
<tr>
<td>4</td>
<td>52.114.76.76</td>
<td>32</td>
<td>0</td>
<td>65535</td>
<td>TCP</td>
<td>Enable</td>
<td>WAN_IF</td>
<td>Allow</td>
</tr>
<tr>
<td>5</td>
<td>52.114.7.24</td>
<td>32</td>
<td>0</td>
<td>65535</td>
<td>TCP</td>
<td>Enable</td>
<td>WAN_IF</td>
<td>Allow</td>
</tr>
<tr>
<td>6</td>
<td>52.114.14.70</td>
<td>32</td>
<td>0</td>
<td>65535</td>
<td>TCP</td>
<td>Enable</td>
<td>WAN_IF</td>
<td>Allow</td>
</tr>
<tr>
<td>49</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>65535</td>
<td>Any</td>
<td>Enable</td>
<td>WAN_IF</td>
<td>Block</td>
</tr>
</tbody>
</table>

**Note:** Be aware, that if in your configuration, connectivity to SIP Trunk (or other entities) is performed through the same IP Interface as Teams (WAN_IF in our example), you must add rules to allow traffic from these entities.
3 Verify the Pairing Between the SBC and Direct Routing

After you have paired the SBC with Direct Routing using the `New-CsOnlinePSTNGateway` PowerShell command, validate that the SBC can successfully exchange OPTIONS with Direct Routing.

➢ To validate the pairing using SIP OPTIONS:

1. Open the Proxy Set Status page (Monitor menu > VoIP Status tab > Proxy Set Status).
2. Find the Direct SIP connection and verify that 'Status' is online. If you see a failure, you need to troubleshoot the connection first, before configuring voice routing.

![Figure 3-1: Proxy Set Status](image-url)
This page is intentionally left blank.
4 Make a Test Call

After installation is complete, you can run a test call from the SBC to a registered user, and in the other direction as well. Running a test call will help to perform diagnostics and to check the connectivity for future support calls or setup automation.

Test calls can be performed using the Test Agent, integral to AudioCodes’ SBC. The Test Agent gives you the ability to remotely verify connectivity, voice quality and SIP message flow between SIP UAs.

A simulated endpoint can be configured on the SBC to test SIP signaling of calls between the SBC and a remote destination. This feature is useful because it can remotely verify SIP message flow without involving the remote end in the debug process. The SIP test call simulates the SIP signaling process: Call setup, SIP 1xx responses, through to completing the SIP transaction with a 200 OK.

The test call sends Syslog messages to a Syslog server, showing the SIP message flow, tone signals (e.g., DTMF), termination reasons, as well as voice quality statistics and thresholds (e.g., MOS).

➢ To configure the Test Agent:

1. Open the Test Call Rules table (Troubleshooting menu > Troubleshooting tab > Test Call > Test Call Rules).
2. Configure a test call according to the parameters of your network. For a detailed description, refer to the AudioCodes User Manual documents.

➢ To start, stop and restart a test call:

1. In the Test Call Rules table, select the required test call entry.
2. From the Action drop-down list, choose the required command:
   - **Dial**: Starts the test call (applicable only if the test call party is the caller).
   - **Drop Call**: Stops the test call.
   - **Restart**: Ends all established calls and then starts the test call session again.
A Syntax Requirements for SIP Messages 'INVITE' and 'OPTIONS'

The syntax of SIP messages must conform with Direct Routing requirements. This section covers the high-level requirements for the SIP syntax used in 'INVITE' and 'OPTIONS' messages. You can use the information presented here as a first step when troubleshooting unsuccessful calls. AudioCodes has found that most errors are related to incorrect syntax in SIP messages.

A.1 Terminology

| Must | Strictly required. The deployment does not function correctly without the correct configuration of these parameters. |

A.2 Syntax Requirements for 'INVITE' Messages

Figure A-1: Example of an 'INVITE' Message

```
INVITE sip:+97249888108@10.15.40.55;user=phone SIP/2.0
Via: SIP/2.0/TLS sbc.aceducation.info:5068;alias;branch=z9hG4bKac496289557
Max-Forwards: 69
From: <sip:+97239762000@10.15.77.12>;tag=1c5242854d32
To: <sip:+97249888108@10.15.40.55;user=phone>
Call-ID: 116795307629520192217@aceducation.info
CSeq: 1 INVITE
Contact: <sip:+97239762000@sbc.aceducation.info:5068;transport=tls>
Supported: en,100rel,time,replace,PATH,resource-priority,sdp-mux
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: 10.15.40.55/v.7.10A.250.273
Content-Type: application/sdp
Content-Length: 1114
```

- **Contact** header
  - **MUST**: When placing calls to the Direct Routing interface, the 'CONTACT' header must have the SBC FQDN in the URI hostname
  - Syntax: Contact: <phone number>@<FQDN of the SBC>;<SBC Port>;<transport type>
  - If the parameter is not configured correctly, calls are rejected with a '403 Forbidden' message.

A.3 Requirements for 'OPTIONS' Messages Syntax

Figure A-2: Example of 'OPTIONS' message

```
OPTIONS sip:195.189.192.171 SIP/2.0
Via: SIP/2.0/TLS sbc.aceducation.info:5068;alias;branch=z9hG4bKac1895438539
Max-Forwards: 70
From: <sip:195.189.192.171>;tag=1c1890481146
To: <sip:195.189.192.171>
Call-ID: 59585523229520193103@sbc.aceducation.info
CSeq: 1 OPTIONS
Contact: <sip:sbc.aceducation.info:5068;transport=tls>
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: 10.15.40.55/v.7.20A.250.273
Accept: application/sdp, application/simple-message-summary, message/sipfrag
Content-Length: 0
```
Contact header

- **MUST**: When sending OPTIONS to the Direct Routing interface, the 'CONTACT' header must have the SBC FQDN in the URI hostname
- **Syntax**: Contact: <phone number>@<FQDN of the SBC>:<SBC Port>;<transport type>
- If the parameter is not configured correctly, the calls are rejected with a '403 Forbidden' message

The table below shows where in the Web interface the parameters are configured and where in this document you can find the configuration instructions.

**Table A-1: Syntax Requirements for an 'OPTIONS' Message**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Where Configured</th>
<th>How to Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact</td>
<td>Setup &gt; Signaling and Media &gt; Core Entities &gt; IP Groups &gt; &lt;Group Name&gt; &gt; Local Host Name</td>
<td>See Section 2.12.</td>
</tr>
<tr>
<td></td>
<td>In IP Group, 'Contact' must be configured. In this field ('Local Host Name'), define the local host name of the SBC as a string, for example, sbc.ACeducation.info. The name changes the host name in the call received from the IP Group.</td>
<td></td>
</tr>
</tbody>
</table>
A.4 Connectivity Interface Characteristics

The table below shows the technical characteristics of the Direct Routing interface.

In most cases, Microsoft uses RFC standards as a guide during development, but does not guarantee interoperability with SBCs - even if they support all the parameters in the table below - due to the specifics of the implementation of the standards by SBC vendors.

Microsoft has a partnership with some SBC vendors and guarantees their devices’ interoperability with the interface. All validated devices are listed on Microsoft’s website. Microsoft only supports devices that are validated in order to connect to the Direct Routing interface.

AudioCodes is one of the vendors who are in partnership with Microsoft. AudioCodes' SBCs are validated by Microsoft to connect to the Direct Routing interface.

<table>
<thead>
<tr>
<th>Category</th>
<th>Parameter</th>
<th>Value</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports and IP ranges</td>
<td>SIP Interface FQDN Name</td>
<td>See Microsoft's document Deploying Direct Routing Guide.</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>IP Addresses range for SIP interfaces</td>
<td>See Microsoft's document Deploying Direct Routing Guide.</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>SIP Port</td>
<td>5061</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>IP Address range for Media</td>
<td>See Microsoft's document Deploying Direct Routing Guide.</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Media port range on Media Processors</td>
<td>See Microsoft's document Deploying Direct Routing Guide.</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Media Port range on the client</td>
<td>See Microsoft's document Deploying Direct Routing Guide.</td>
<td>-</td>
</tr>
<tr>
<td>Transport and Security</td>
<td>SIP transport</td>
<td>TLS</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Media Transport</td>
<td>SRTP</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>SRTP Security Context</td>
<td>DTLS, SIPS</td>
<td>Note: Support for DTLS is pending. Currently, SIPS must be configured. When support for DTLS will be announced, it will be the recommended context.</td>
</tr>
<tr>
<td></td>
<td>Crypto Suite</td>
<td>AES_CM_128_HMAC_SH A1_80, non-MKI</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Control protocol for media transport</td>
<td>SRTCP (SRTCP-Mux recommended)</td>
<td>Using RTCP MUX helps reduce the number of required ports</td>
</tr>
<tr>
<td></td>
<td>Supported Certification Authorities</td>
<td>See the Deployment Guide</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Transport for Media Bypass (of configured)</td>
<td>• ICE-lite (RFC5245) – recommended</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Client also has Transport Relays</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Audio codecs</td>
<td>• G711</td>
<td>-</td>
</tr>
<tr>
<td>Category</td>
<td>Parameter</td>
<td>Value</td>
<td>Comments</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td>Silk (Teams clients)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Opus (WebRTC clients) - only if Media Bypass is used</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>G729</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Codecs</td>
<td>Other codecs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CN</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Required narrowband and wideband</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RED - Not required</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DTMF - Required</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Events 0-16</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Silence Suppression - Not required</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

-
B  SIP Proxy Direct Routing Requirements

Teams Direct Routing has three FQDNs:

- **sip.pstnhub.microsoft.com** [Global FQDN. The SBC attempts to use it as the first priority region. When the SBC sends a request to resolve this name, the Microsoft Azure DNS server returns an IP address pointing to the primary Azure datacenter assigned to the SBC. The assignment is based on performance metrics of the datacenters and geographical proximity to the SBC. The IP address returned corresponds to the primary FQDN.]

- **sip2.pstnhub.microsoft.com** [Secondary FQDN. Geographically maps to the second priority region.]

- **sip3.pstnhub.microsoft.com** [Tertiary FQDN. Geographically maps to the third priority region.]

These three FQDNs must be placed in the order shown above to provide optimal quality of experience (less loaded and closest to the SBC datacenter assigned by querying the first FQDN).

The three FQDNs provide a failover if a connection is established from an SBC to a datacenter that is experiencing a temporary issue.

B.1 Failover Mechanism

The SBC queries the DNS server to resolve **sip.pstnhub.microsoft.com**. The primary datacenter is selected based on geographical proximity and datacenters performance metrics.

If during the connection the primary datacenter experiences an issue, the SBC will attempt **sip2.pstnhub.microsoft.com** which resolves to the second assigned datacenter, and in rare cases if datacenters in two regions are unavailable, the SBC retries the last FQDN (**sip3.pstnhub.microsoft.com**) which provides the tertiary datacenter IP address.

The SBC must send SIP OPTIONS to all IP addresses that are resolved from the three FQDNs, that is, **sip.pstnhub.microsoft.com**, **sip2.pstnhub.microsoft.com** and **sip3.pstnhub.microsoft.com**.