Connecting AudioCodes' SBC to Microsoft Teams Direct Routing

Hosting Model

Version 7.2
Table of Contents

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

2 Configuring AudioCodes' SBC ........................................................................ 13
   2.1 Prerequisites ...................................................................................................... 14
      2.1.1 About the SBC Domain Name in Hosting Model ............................................. 15
         2.1.1.1 SBC Domain Name in a Carrier Office 365 Tenant .................................. 15
         2.1.1.2 SBC Domain Name in a Customer Office 365 Tenant .............................. 16
   2.2 Validate AudioCodes SBC License ..................................................................... 17
   2.3 SBC Configuration Concept .............................................................................. 17
   2.4 Configure LAN and WAN IP Interfaces ............................................................. 18
      2.4.1 Validate Configuration of Physical Ports and Ethernet Groups ....................... 18
      2.4.2 Configure LAN and WAN VLANs ................................................................. 20
      2.4.3 Configure Network Interfaces ....................................................................... 21
   2.5 Configure TLS Context for Teams .................................................................... 22
      2.5.1 Configure the NTP Server Address ................................................................ 23
      2.5.2 Create a TLS Context for Teams Direct Routing ............................................. 23
      2.5.3 Generate a CSR and Obtain the Certificate from a Supported CA ................. 25
      2.5.4 Deploy the SBC and Root / Intermediate Certificates on the SBC .................. 27
   2.6 Method of Generating and Installing the Wildcard Certificate ......................... 29
   2.7 Deploy Baltimore Trusted Root Certificate ..................................................... 29
   2.8 Configure Media Realms .................................................................................. 30
   2.9 Configure SIP Signaling Interfaces ................................................................... 31
   2.10 Configure Proxy Sets and Proxy Address ......................................................... 33
      2.10.1 Configure Proxy Sets ................................................................................... 33
      2.10.2 Configure a Proxy Address ......................................................................... 34
   2.11 Configure the Dial Plan Table (Customer DID Only) ........................................ 36
   2.12 Configure Call Setup Rules ........................................................................... 37
   2.13 Configure Message Manipulation Rules .......................................................... 38
   2.14 Configure a Coder Group .............................................................................. 42
   2.15 Configure an IP Profile .................................................................................. 43
   2.16 Configure IP Groups ...................................................................................... 45
   2.17 Configure SRTP ............................................................................................. 47
   2.18 Configure Message Condition Rules ................................................................. 48
   2.19 Configure Classification Rules ........................................................................ 49
   2.20 Configure IP-to-IP Call Routing Rules .............................................................. 50
   2.21 Configure Firewall Settings (Optional) ............................................................. 51

3 Verify the Pairing between the SBC and Direct Routing .................................. 52

4 Make a Test Call ................................................................................................. 54

5 Configure via UMP 365 (Optional) .................................................................. 56

A Syntax Requirements for SIP Messages 'INVITE' and 'OPTIONS' ...................... 58
   A.1 Terminology .................................................................................................... 58
A.2 Syntax Requirements for 'INVITE' Messages ..............................................................58
A.3 Requirements for 'OPTIONS' Messages Syntax.........................................................59
A.4 Connectivity Interface Characteristics.....................................................................60

B SIP Proxy Direct Routing Requirements ....................................................................63
B.1 Failover Mechanism ..............................................................................................63
List of Figures

Figure 2-1: Connection Topology - Network Interfaces ................................................................. 13
Figure 2-2: Carrier Office 365 Tenant Domain Structure ............................................................... 14
Figure 2-3: Example of Registered DNS Names ............................................................................ 15
Figure 2-4: Example of User Belonging to SBC Carrier’s Domain ............................................... 16
Figure 2-5: Example of Domain for Carrier SBC in Customer Domain ........................................ 16
Figure 2-6: Example of User for Carrier SBC in Customer Domain ............................................. 16
Figure 2-7: SBC Configuration Concept ....................................................................................... 17
Figure 2-8: Network Interfaces in the Topology with SIP Trunk on the LAN .................................... 18
Figure 2-9: Physical Ports Configuration Interface ........................................................................ 19
Figure 2-10: Ethernet Groups Configuration Interface ................................................................. 19
Figure 2-11: Configured VLANs in the Ethernet Device Table ..................................................... 20
Figure 2-12: Configuration Example of the Network Interface Table .......................................... 21
Figure 2-13: Carriers’ Office 365 Tenants Domain Structure ....................................................... 22
Figure 2-14: Configuring NTP Server Address ............................................................................. 23
Figure 2-15: Configuration of TLS Context for Direct Routing ................................................... 24
Figure 2-16: Configured TLS Context for Direct Routing and Interface to Manage the Certificates 25
Figure 2-17: Example of Certificate Signing Request Page ......................................................... 26
Figure 2-18: Uploading the Certificate Obtained from the Certification Authority ......................... 27
Figure 2-19: Message Indicating Successful Upload of the Certificate ........................................ 27
Figure 2-20: Certificate Information Example ................................................................................ 28
Figure 2-21: Configured Trusted Certificates Page ..................................................................... 28
Figure 2-22: Configuration Example Media Realms in Media Realm Table ................................ 30
Figure 2-23: Configuration Example of SIP Signaling Interfaces ................................................. 32
Figure 2-24: Configuration Example Proxy Sets in Proxy Sets Table ......................................... 33
Figure 2-25: Configuring Proxy Address for Teams Direct Routing Interface ............................... 34
Figure 2-26: Configuring Proxy Address for SIP Trunk ................................................................. 35
Figure 2-27: Dial Plan Rule Table - Add Dialog Box ................................................................. 36
Figure 2-28: Call Setup Rules Table - Add Dialog Box ................................................................. 37
Figure 2-29: Configuring SIP Message Manipulation Rule 0 (for Teams IP Group) ....................... 38
Figure 2-30: Configuring SIP Message Manipulation Rule 1 (for Teams IP Group) ..................... 39
Figure 2-31: Configuring SIP Message Manipulation Rule 2 (for Teams IP Group) ..................... 40
Figure 2-30: Configuring SIP Message Manipulation Rule 1 (for Teams IP Group) Disable Forwarding Example ................................................................. 41
Figure 2-32: Configuring Coder Group for Teams Direct Routing ................................................ 42
Figure 2-33: Configuration Example IP Groups in IP Group Table ............................................. 46
Figure 2-34: Configuring Media Security Parameter ................................................................... 47
Figure 2-35: Configuring Condition Table .................................................................................... 48
Figure 2-36: Configuring Classification Rule ................................................................................ 49
Figure 2-37: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table ..................................... 50
Figure 3-1: Proxy Set Status ........................................................................................................ 52
Figure 5-1: Provider Main Screen View ....................................................................................... 56
Figure 5-2: Customer Tenant view – User List ............................................................................. 57
Figure A-1: Example of an ’INVITE’ Message ............................................................................. 58
Figure A-2: Example of ’OPTIONS’ message ............................................................................. 59
Teams Direct Routing Hosting Model

List of Tables

Table 1-1: Infrastructure Prerequisites ...................................................................................................12
Table 2-1: DNS Names Registered by an Administrator for a Carriers’ Office 365 Tenant .................15
Table 2-2: Configuration Example of the Network Interface Table ....................................................21
Table 2-3: New TLS Context ....................................................................................................................23
Table 2-4: Configuration Example Media Realms in Media Realm Table ...........................................30
Table 2-5: Configuration Example of SIP Signaling Interfaces ............................................................31
Table 2-6: Configuration Example Proxy Sets in Proxy Sets Table .....................................................33
Table 2-7: Configuration Proxy Address for Teams Direct Routing ....................................................34
Table 2-8: Configuration Proxy Address for SIP Trunk .......................................................................35
Table 2-9: Dial Plan Carriers’ Office 365 Teams Tenants ..................................................................36
Table 2-10: Call Setup Rules Table ......................................................................................................37
Table 2-11: Configuration Example: Teams IP Profile ......................................................................43
Table 2-12: Configuration Example: SIP Trunk IP Profile .................................................................44
Table 2-13: Firewall Table Rules .........................................................................................................51
Table A-1: Syntax Requirements for an ‘OPTIONS’ Message ...............................................................59
Table A-2: Teams Direct Routing Interface - Technical Characteristics .............................................60
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: May-06-2021

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 Gateway &amp; E-SBC User's Manual</td>
</tr>
<tr>
<td>Mediant 800 Gateway &amp; E-SBC User's Manual</td>
</tr>
<tr>
<td>Mediant 1000B Gateway &amp; 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>
</tbody>
</table>
Document Name

AudioCodes Configuration Notes
AudioCodes User Management Pack 365 SP Edition Installation and Administration Guide

Document Revision Record

<table>
<thead>
<tr>
<th>LTRT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12886</td>
<td>Fixes</td>
</tr>
<tr>
<td>12887</td>
<td>New: Configure the Dial Plan Table; Configuring Call Setup Rules; Note about Proxy Address; Tenant Provisioning Script; Note under IP Profile. Modified: Configuration Example: IP Profile; Configuration Example: IP Group - Teams Global FQDNs; Configuration Example: SIP Interface; Configuration Example: Proxy Set - Teams - Global FQDNs; the note under SIP Interfaces, About the SBC Domain Name in Hosting Model, Classification rule, Route rule, IP-to-IP Routing. Appendix B.</td>
</tr>
<tr>
<td>12888</td>
<td>Call Flows. Configuration Concept.</td>
</tr>
<tr>
<td>12889</td>
<td>Parameter ‘Request Type’. SIP I/F-Index entry deleted. Parameter ‘SBC Media Security Method’.</td>
</tr>
</tbody>
</table>
| 13202  | **Firmware version 7.20A.204.015 and later:**
  New parameter ‘Proxy Keep-Alive using IP Group settings’ added in the IP Group Table. Due to this, Message Manipulation Set for OPTIONS was removed and now only one SIP Interface is required for Teams Direct Routing.
  Modified: ‘Query Target’ parameter was added to Call Setup Rule #2
  A link was added to Microsoft’s official list of supported Trusted Certificate Authorities in section "Configure TLS Context". |
| 13203  | Updated CLI script – removed SIP Interface.
  Removed DTLS Context from IP Group configuration.
  Updated the configuration to support Tag-based Classification (Fix Dial Plan tags, Added CSR, SIP Interface)                                                                                                                                 |
| 13204  | Modified sections: Prerequisites; SBC Configuration Concept; Outgoing Call from the Teams Client (figure); licenses required on device; Configure the Dial Plan Table (Customer DID Only); Configuring Call Setup Rules Based on Customer DID Range (Dial Plan); Call Setup rule (step 1); Configuration Example: IP Group - Teams Global FQDNs (table); Configuring an SBC to Suppress Call Line ID (Optional); Teams IP Profile
  Modified parameters: IP address (parameter – adding NI for WAN); Routing from SIP Trunk to Direct Routing (Name); srctag name; Options Classification; DialPlan tag update
  New section: Add Routing option based on Host name                                                                                                                                                          |
<p>| 13205  | Modified sections: Configure a SIP Signaling Interface; Configure a Proxy Address; Configure an IP Group (per Tenant)                                                                                                                                                 |
| 13206  | Modified sections: TLS Context Generation procedure                                                                                                                                                           |
| 13207  | Add ‘Source IP Address’ to Classification Table                                                                                                                                                              |</p>
<table>
<thead>
<tr>
<th>LTRT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13209</td>
<td>Added a configuration example for SIP Trunk. Configuration is simplified by moving to one IP Group for Teams and changing Call Setup Rules. Updated NTP Server configuration. Updated certified firmware version and links to Microsoft documents.</td>
</tr>
<tr>
<td>13210</td>
<td>Modified sections: Deploy Baltimore Trusted Root Certificate (added note for Baltimore Trusted Root Certificate and MTLS implementation); Configure SIP Signaling Interfaces; Configure Call Setup Rules; Configure Message Manipulation Rules; Configure IP Groups;</td>
</tr>
<tr>
<td>13211</td>
<td>Note removed regarding external firewall.</td>
</tr>
<tr>
<td>13212</td>
<td>License update (typo)</td>
</tr>
<tr>
<td>13213</td>
<td>Update to topology figures and correction for parameter “Remote Update Support” to “SIP UPDATE Support”.</td>
</tr>
<tr>
<td>13214</td>
<td>Update to the “Related Documentation” table to include the Mediant 1000B Gateway &amp; E-SBC product.</td>
</tr>
<tr>
<td>13215</td>
<td>Update in configuration concept. Modified sections: SBC Configuration Concept; Configure Proxy Sets and Proxy Address; Configure IP Groups; Configure IP-to-IP Call Routing Rules. Section “Tenant Provisioning Script” replaced with “UMP Configuration”. An Additional 2 IP addresses were added to firewall per Microsoft request.</td>
</tr>
<tr>
<td>13216</td>
<td>Update for Message Manipulation rule towards Microsoft Teams.</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](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 Hosting model 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 and https://docs.microsoft.com/en-us/microsoftteams/direct-routing-sbc-multiple-tenants.

This document is intended for IT or telephony professionals.

Note: To zoom in on screenshots of Web interface configuration examples, 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 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.
1.3 Validated AudioCodes SBC Version

Microsoft has successfully conducted validation tests with AudioCodes' Mediant SBC Ver. 7.20A.258. 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: For implementing Microsoft Teams Direct Routing based on the configuration described in this document, AudioCodes SBC must be installed with a License Key that includes the following features:

- **MSFT** (general Microsoft license)
  - Note: By default, all AudioCodes media gateways and SBCs are shipped with this license (except MSBR products, Mediant 500 SBC, and Mediant 500 Media Gateway).
- **SW/TEAMS** (Microsoft Teams license)
- **Number of SBC sessions** (based on requirements)
- **Transcoding sessions** (only if media transcoding is needed)
- **Coders** (based on requirements)

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

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 carrier tenant and customer 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>See Microsoft's Plan Direct Routing document.</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>
2 Configuring AudioCodes' SBC

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

The figure below shows an example of the connection topology for the hosting model. Multiple connection entities are shown in the figure:

- Teams Phone Systems Direct Routing Interface on the WAN
- Service Provider SIP Trunk

Figure 2-1: Connection Topology - Network Interfaces

Note: This document shows how to configure the connection between AudioCodes’ SBC and the Teams Direct Routing with a generic SIP Trunk. For detailed configuration of other entities in the deployment such as the SIP Trunk Provider and the local IP-PBX, see AudioCodes’ SIP Trunk Configuration Notes (in the interoperability suite of documents).
2.1 **Prerequisites**

Before you begin configuration, make sure you have the below for every Hosting SBC you wish to pair:

- Public IP address
- FQDN name matching the SIP addresses of the Teams users
- Public certificate, issued by one of the supported CAs
2.1.1 About the SBC Domain Name in Hosting Model

2.1.1.1 SBC Domain Name in a Carrier Office 365 Tenant

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 the administrator registered the following DNS names for the tenant:

Table 2-1: DNS Names Registered by an Administrator for a Carriers' Office 365 Tenant

<table>
<thead>
<tr>
<th>DNS name</th>
<th>Can be used for SBC FQDN</th>
<th>Examples of FQDN names for Hosting Customers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customers.aceducation.info</td>
<td>Yes</td>
<td>Valid names:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sbc.Customers.aceducation.info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ussbscs15.Customers.aceducation.info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• europe.Customers.aceducation.info</td>
</tr>
<tr>
<td>adatumbiz.onmicrosoft.com</td>
<td>No</td>
<td>Invalid name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sbc1.europe.Customers.aceducation.info</td>
</tr>
</tbody>
</table>

Note: Please check the DNS configuration with TXT and that an A record has been validated.

For activating the domain, the Hosting Provider needs to add at least one user with Microsoft plan as Enterprise or Business with Phone System (e.g. E5 or E1/E3 with Phone System) from the SIP domain registered for the carriers' Office 365 tenant. For example, you can provide users sbc@Customers.aceducation.info with the Domain FQDN Customers.aceducation.info if this name is registered for this tenant. You should create at least one licensed user belonging to the SBC domain you added as described above.
2.1.1.2 SBC Domain Name in a Customer Office 365 Tenant

For each customer tenant, you should add a domain belonging to a carrier that points to a customer tenant as in Figure 2-5 and create at least one licensed user with Microsoft plan as Enterprise or Business with Phone System (e.g. E5 or E1/E3 with Phone System) belonging to your SBC domain as in Figure 2-6.

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

<table>
<thead>
<tr>
<th>Public IP</th>
<th>FQDN Name of Carrier’s SBC for a customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>195.189.192.157</td>
<td>sbc2.Customers.ACeducation.info</td>
</tr>
</tbody>
</table>
Each customer needs to add at least one user from the Carrier’s SIP domain registered for the tenant. For example, you can provide users `sbc@SBC2.Customers.aceduation.info` with the Domain FQDN `sbc2.Customers.aceduation.info` so long as this name is registered for this tenant.

You should create at least one licensed user belonging to your SBC domain that you added in the step above.

**Note:** Microsoft commits for up to 24 hours, before the PSTN gateway is activated.


### 2.2 Validate AudioCodes SBC License

Please refer to Section 1.2 on page 11 for the list of required licenses.

### 2.3 SBC Configuration Concept

The figure below illustrates the concept behind the configuration of AudioCodes’ SBC device.

**Figure 2-7: SBC Configuration Concept**

The routing from the SIP Trunk to Direct Routing is dependent on the Class 4 switch routing method. The routing decision can be based on:

- Customer DID Range
- Trunk Context (TGRP)
- IP Interface
- SIP Interface (UDP/TCP Port)
- Host name
- etc.

The configuration shown in this document is based on Customer DID Range using Dial Plan. For more information, see the AudioCodes’ documentation suite.
2.4 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
- 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 2-8: Network Interfaces in the Topology with SIP Trunk on the LAN

2.4.1 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.

Figure 2-10: Ethernet Groups Configuration Interface
2.4.2 Configure LAN and WAN VLANs

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

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

To configure 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 2-11: Configured VLANs in the Ethernet Device Table](image-url)
2.4.3 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>
<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 2-12: Configuration Example of the Network Interface Table
2.5 Configure TLS Context for Teams

The configuration instructions in this section are based on the following domain structure that must be implemented as part of the certificate which must be loaded to the host SBC:

- **CN:** *.customers.ACeducation.info
- **1st SAN:** customers.ACeducation.info
- **2nd SAN:** *.customers.ACeducation.info

This certificate module is based on the carriers’ own TLS Certificate. For more certificate structure options, see Microsoft Teams Direct Routing documentation.

Figure 2-13: Carriers’ Office 365 Tenants Domain Structure

The Teams Direct Routing Interface only allows TLS connections from SBC devices for SIP traffic with a certificate signed by one of the trusted Certificate Authorities. The currently supported Certification Authorities can be found at:

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc
2.5.1 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 be located 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 2-14: Configuring NTP Server Address](image)

3. Click Apply.

2.5.2 Create a TLS Context for Teams Direct Routing

The section below describes how to request a certificate for the SBC WAN interface and 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:

■ Create a TLS Context for Teams Direct Routing
■ Generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority
■ 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, and then configure the parameters using the table below as reference.

![Table 2-3: New TLS Context](image)

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 displayed 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 2-15: 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.
2.5.3 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 wildcard FQDN name (based on example above, *.customers.ACeducation.info).
   b. In the ‘1st Subject Alternative Name [SAN]' field, change the type to ‘DNS' and enter the SBC FQDN name (based on example above, customers.ACeducation.info).
   c. In the ‘2nd Subject Alternative Name [SAN]' field, change the type to ‘DNS' and enter the wildcard FQDN name (based on example above, *.customers.ACeducation.info).

Note: The domain portion of the Common Name [CN], 1st and 2nd Subject Alternative Name [SAN] must match the SIP suffix configured for carrier Office 365 tenant (see Section 2.1.1.1).
d. Change the 'Private Key Size' based on the requirements of your Certification Authority. Many CAs do not support private key of size 1024.

e. To change the key size on TLS Context, go to: Generate New Private Key and Self-Signed Certificate, change the 'Private Key Size' and then click Generate Private-Key. To use 2048 as a Private Key Size value, you can click Generate Private-Key without changing the default key size value.

f. Fill in the rest of the request fields according to your security provider’s instructions.

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

![Figure 2-17: Example of Certificate Signing Request Page](image)

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

5. Send certreq.txt file to the Certified Authority Administrator for signing.
2.5.4 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 2-18: Uploading the Certificate Obtained from the Certification Authority](image)

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

   ![Figure 2-19: Message Indicating Successful Upload of the Certificate](image)

3. In the SBC's Web interface, return to the TLS Contexts page, select the required TLS Context index row, and then click the Certificate Information link, located at the bottom of the TLS. Then validate the Key size, certificate status and Subject Name:
4. In the SBC’s Web interface, return to the TLS Contexts page.
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the Trusted Root Certificates link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
   b. Click the Import button, and then select all 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 2-21: Configured Trusted Certificates Page**

---

**Note:** The above method creates a signed certificate for an explicit device, on which a Certificate Sign Request was generated (and signed with private key). To be able to use the same wildcard certificate on multiple devices, use following methods.
2.6  **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.

2.7  **Deploy Baltimore Trusted Root Certificate**

**Note:** Loading Baltimore Trusted Root Certificates to AudioCodes' SBC is mandatory for implementing an MTLS connection with the Microsoft Teams network.

The DNS name of the Teams Direct Routing interface is sip.pstnhub.microsoft.com. In this interface, a certificate is presented which is signed by Baltimore Cyber Baltimore CyberTrust Root with Serial Number: 02 00 00 b9 and SHA fingerprint: d4:de:20:d0:5e:66:fc:53:fe:1a:50:88:2c:78:db:28:52:ca:e4:74. For more information on the DNS name, see Appendix B.

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'.
2.8 Configure Media Realms

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 2-4: Configuration Example Media Realms in Media Realm Table

<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>6000</td>
<td>100</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 2-22: Configuration Example Media Realms in Media Realm Table
2.9 Configure SIP Signaling Interfaces

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 Interface 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 (arbitrary name)</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>0</td>
<td>Teams (arbitrary name)</td>
<td>WAN_IF</td>
<td>SBC</td>
<td>0</td>
<td>0</td>
<td>5061</td>
<td>0</td>
<td>0 (Recommended to prevent DoS attacks)</td>
<td>MRWan</td>
<td>Teams</td>
</tr>
</tbody>
</table>

Note: For implementing an MTLS connection with the Microsoft Teams network, configure ‘TLS Mutual Authentication’ to “Enable” for the Teams SIP Interface.

Note: Loading Baltimore Trusted Root Certificates to AudioCodes' SBC is mandatory for implementing an MTLS connection with the Microsoft Teams network. Refer to Section 2.7 on page 29.
The configured SIP Interfaces are shown in the figure below:

**Figure 2-23: Configuration Example of SIP Signaling Interfaces**
2.10 Configure Proxy Sets and Proxy Address

This section describes how to configure Proxy Sets and Proxy addresses.

2.10.1 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 Sets for Teams Direct Routing and SIP Trunks. 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>Teams (arbitrary name)</td>
<td>Teams</td>
<td>Teams</td>
<td>Using Options</td>
<td>Enable</td>
<td>Random Weights</td>
</tr>
<tr>
<td>2</td>
<td>SIPTrunks (arbitrary name)</td>
<td>SIPTrunk</td>
<td>Default</td>
<td>Using Options</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

The configured Proxy Sets are shown in the figure below:

Figure 2-24: Configuration Example Proxy Sets in Proxy Sets Table
2.10.2 Configure a Proxy Address

This section shows how to configure a Proxy Address.

➢ 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 2-25: 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 (for more information, see Appendix B):

Table 2-7: 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.

➢ To configure a Proxy Address for SIP Trunks:

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

2. Click +New; the following dialog box appears:
3. Configure the address of the Proxy Set according to the parameters described in the table below:

Table 2-8: 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</td>
<td>UDP</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

(SIP Trunk IP / FQDN and port)

4. Click Apply.
2.11 Configure the Dial Plan Table (Customer DID Only)

For deployments requiring hundreds of routing rules (which may exceed the maximum number of rules that can be configured in the IP-to-IP Routing table), you can employ tags to represent the many different calling (source URI user name) and called (destination URI user name) prefix numbers in your routing rules. Tags are typically implemented when you have users of many different called and/or calling numbers that need to be routed to the same destination (e.g., IP Group or IP address). In such a scenario, instead of configuring many routing rules to match all the required prefix numbers, you need only to configure a single routing rule using the tag to represent all the possible prefix numbers.

The Dial Plan (e.g., TeamsTenants) will be configured with an Office 365 customer tenant FQDN tag per prefix.

➢ To configure Dial Plans:

1. Open the Dial Plan table (Setup menu > Signaling & Media tab > SIP Definitions folder > Dial Plan).
2. Click New and then configure a Dial Plan name (e.g., TeamsTenants) according to the parameters described in the table below.
3. Click Apply.
4. In the Dial Plan table, select the row for which you want to configure dial plan rules and then click the Dial Plan Rule link located below the table; the Dial Plan Rule table appears.
5. Click New; the following dialog box appears:

   ![Figure 2-27: Dial Plan Rule Table - Add Dialog Box](image)

6. Configure a dial plan rule according to the parameters described in the table below.

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Prefix</th>
<th>Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Enterprise1</td>
<td>+19098[0000-9999]</td>
<td>&lt;FQDN name of the carrier customer 1 tenant in SBC&gt;, For example, sbc1.customers.ACeducation.info</td>
</tr>
<tr>
<td>1</td>
<td>Enterprise2</td>
<td>+17093[0000-9999]</td>
<td>&lt;FQDN name of the carrier customer 2 tenant in SBC&gt;, For example, sbc2.customers.ACeducation.info</td>
</tr>
<tr>
<td>2</td>
<td>Enterprise3</td>
<td>+18097[0000-9999]</td>
<td>&lt;FQDN name of the carrier customer 3 tenant in SBC&gt;, For example, sbc3.customers.ACeducation.info</td>
</tr>
</tbody>
</table>

7. Click Apply and then save your settings to flash memory.
2.12 Configure Call Setup Rules

This section describes how to configure Call Setup Rules based on customer DID range (Dial Plan). Call Setup rules define various sequences that are run upon receipt of an incoming call (dialog) at call setup, before the device routes the call to its destination. Configured Call Setup Rules need be assigned to specific IP Group.

➢ To configure a Call Setup Rules based on customer DID range (Dial Plan):

1. Open the Call Setup Rules table (Setup menu > Signaling & Media tab > SIP Definitions folder > Call Setup Rules).
2. Click New; the following dialog box appears:

Figure 2-28: Call Setup Rules Table - Add Dialog Box

3. Configure a Call Setup rule according to the parameters described in the table below.

Table 2-10: Call Setup Rules Table

<table>
<thead>
<tr>
<th>Index</th>
<th>Rules Set ID</th>
<th>Name</th>
<th>Query Type</th>
<th>Query Target</th>
<th>Search Key</th>
<th>Condition</th>
<th>Action Subject</th>
<th>Action Type</th>
<th>Action Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>TenantFQDN by PAI</td>
<td>Dial Plan</td>
<td>TeamsTenants</td>
<td>Header.P-Asserted-Identity.URL.User</td>
<td>DialPlan.Found exists</td>
<td>var.session.Tenant FQDN</td>
<td>Modify</td>
<td>DialPlan.Result</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>SIP Trunk DstTags</td>
<td></td>
<td></td>
<td>DstTags</td>
<td></td>
<td>var.session.TenantFQDN</td>
<td>Modify</td>
<td>var.session.TenantFQDN</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>Teams DstTags</td>
<td></td>
<td></td>
<td>DstTags</td>
<td></td>
<td>'Teams'</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. Click Apply and then save your settings to flash memory.
2.13 Configure Message Manipulation Rules

This section describes how to configure SIP message manipulation rules. SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Manipulation rules are grouped into Manipulation Sets, enabling you to apply multiple rules to the same SIP message (IP entity).

Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

To configure SIP message manipulation rule for Teams:

1. Open the Message Manipulations page (Setup menu > Signaling & Media tab > Message Manipulation folder > Message Manipulations).
2. Configure a new manipulation rule (Manipulation Set 2) for Teams IP Group. This rule applies to messages sent to the Teams IP Group. This replaces the host part of the SIP Contact Header with the value saved in the session variable ‘TenantFQDN’ during execution of the Call Setup Rule.

<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>TeamsTenants (arbitrary name)</td>
</tr>
<tr>
<td>Manipulation Set ID</td>
<td>2</td>
</tr>
<tr>
<td>Condition</td>
<td>Var.Session.TenantFQDN != &quot;</td>
</tr>
<tr>
<td>Action Subject</td>
<td>Header.Contact.URL.Host</td>
</tr>
<tr>
<td>Action Type</td>
<td>Modify</td>
</tr>
<tr>
<td>Action Value</td>
<td>Var.Session.TenantFQDN</td>
</tr>
</tbody>
</table>

Figure 2-29: Configuring SIP Message Manipulation Rule 0 (for Teams IP Group)
3. Configure another manipulation rule (Manipulation Set 1) for Teams IP Group. This rule applies to messages received from the Teams IP Group. This rule removes the SIP Privacy Header in all messages, except of call with presentation restriction.

<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>Remove Privacy Header</td>
</tr>
<tr>
<td>Manipulation Set ID</td>
<td>1</td>
</tr>
<tr>
<td>Condition</td>
<td>Header.Privacy exists And Header.From.URL !contains 'anonymous'</td>
</tr>
<tr>
<td>Action Subject</td>
<td>Header.Privacy</td>
</tr>
<tr>
<td>Action Type</td>
<td>Remove</td>
</tr>
</tbody>
</table>

Figure 2-30: Configuring SIP Message Manipulation Rule 1 (for Teams IP Group)
4. Configure another manipulation rule (Manipulation Set 1) for Teams IP Group. This rule applies to messages received from the Teams IP Group. This rule removes the SIP P-Asserted-Identity Header.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>2</td>
</tr>
<tr>
<td>Name</td>
<td>Remove PAI</td>
</tr>
<tr>
<td>Manipulation Set ID</td>
<td>1</td>
</tr>
<tr>
<td>Action Subject</td>
<td>Header.P-Asserted-Identity</td>
</tr>
<tr>
<td>Action Type</td>
<td>Remove</td>
</tr>
</tbody>
</table>

Figure 2-31: Configuring SIP Message Manipulation Rule 2 (for Teams IP Group)
5. Configure a new manipulation rule (Manipulation Set 2) for Teams IP Group. This rule applies to messages sent to the Teams IP Group. This rule adds a routing policy rule toward Microsoft for handling different call forwarding scenarios (according to the action values shown below).

<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><strong>Teams Routing Policy</strong> (arbitrary name)</td>
</tr>
<tr>
<td>Manipulation Set ID</td>
<td>2</td>
</tr>
<tr>
<td>Condition</td>
<td>Action Subject: header.X-MS-RoutingPolicies</td>
</tr>
<tr>
<td></td>
<td>Action Type: Add</td>
</tr>
</tbody>
</table>
|                 | Action Value: One of the following values: "none", "no_missed_call", "disable_forwarding", "disable_forwarding_except_phone"

**Note:** Implementation of this Message Manipulation rule with Microsoft Teams is optional according to site deployment requirements.

Figure 2-32: Configuring SIP Message Manipulation Rule 1 (for Teams IP Group) Disable Forwarding Example
2.14 Configure a Coder Group

This section describes how to configure coders (termed Coder Groups). As Teams Direct Routing supports the SILK and G.729 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 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.

3. Click Apply and confirm the configuration change in the prompt that pops up.
2.15 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 need be assigned to specific IP Group.

To configure an IP Profile:

1. Open the Proxy Sets table (Setup menu > Signaling & Media tab > Coders & Profiles folder > 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 2-11: Configuration Example: Teams IP Profile

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Teams (arbitrary descriptive name)</td>
</tr>
<tr>
<td><strong>Media Security</strong></td>
<td></td>
</tr>
<tr>
<td>SBC Media Security Mode</td>
<td>Secured</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 Teams Direct Routing 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>RTCP Mode</td>
<td>Generate Always (required, as some ITSPs do not send RTCP packets while in Hold mode, but Microsoft expected them)</td>
</tr>
<tr>
<td>ICE Mode</td>
<td>Lite (required only when Media Bypass is enabled on Teams)</td>
</tr>
<tr>
<td><strong>SBC Signaling</strong></td>
<td></td>
</tr>
<tr>
<td>SIP 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><strong>SBC Forward and Transfer</strong></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><strong>SBC Hold</strong></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 with 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 Trunks. Configure the parameters using the table below as reference.

**Table 2-12: Configuration Example: SIP Trunk IP Profile**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>SIPTrunks (arbitrary descriptive name)</td>
</tr>
<tr>
<td><strong>Media Security</strong></td>
<td></td>
</tr>
<tr>
<td>SBC Media Security Mode</td>
<td>Not Secured</td>
</tr>
<tr>
<td><strong>SBC Signaling</strong></td>
<td></td>
</tr>
<tr>
<td>P-Asserted-Identity Header Mode</td>
<td>Add (required for anonymous calls)</td>
</tr>
<tr>
<td><strong>SBC Forward and Transfer</strong></td>
<td></td>
</tr>
<tr>
<td>Remote REFER Mode</td>
<td>Handle Locally</td>
</tr>
<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.
2.16 Configure IP Groups

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Teams</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>Teams</td>
</tr>
<tr>
<td>IP Profile</td>
<td>Teams</td>
</tr>
<tr>
<td>Media Realm</td>
<td>MRWan</td>
</tr>
<tr>
<td>Classify By Proxy Set</td>
<td>Disable</td>
</tr>
<tr>
<td>Local Host Name</td>
<td>&lt;FQDN name of the SBC in the carrier tenant&gt; (based on our example, customers.ACeducation.info).</td>
</tr>
<tr>
<td>Teams Direct Routing Mode</td>
<td>Enable (Enables the SBC to include Microsoft's proprietary X-MS-SBC header in outgoing SIP INVITE and OPTIONS messages in a Microsoft Teams Direct Routing environment. The header is used by Microsoft Teams to identify vendor equipment. The header's value is in the format 'AudioCodes/&lt;model&gt;/&lt;firmware&gt;').</td>
</tr>
<tr>
<td>Always Use Src Address</td>
<td>Yes</td>
</tr>
<tr>
<td>Call Setup Rules Set ID</td>
<td>0</td>
</tr>
<tr>
<td>Tags</td>
<td>Teams</td>
</tr>
<tr>
<td>Inbound Message Manipulation Set ID</td>
<td>1</td>
</tr>
<tr>
<td>Outbound Message Manipulation Set</td>
<td>2</td>
</tr>
<tr>
<td>Proxy Keep-Alive using IP Group settings</td>
<td>Enable</td>
</tr>
</tbody>
</table>

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

3. Configure IP Groups for the Enterprise's SIP Trunks (for each enterprise create a dedicated IP Group):

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enterprise1-SIPTrunk (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Type</td>
<td>Server</td>
</tr>
</tbody>
</table>
Proxy Set | SIPTrunks
---|---
IP Profile | SIPTrunks
Media Realm | MRLan or MRWan (according to your network environment)
Call Setup Rules Set ID | 1
Tags | `<FQDN name of the SBC in the customer tenant>`
   
   (For example, `sbc1.customers.ACeducation.info`)

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

The configured IP Groups are shown in the figure below:

**Figure 2-34: Configuration Example IP Groups in IP Group Table**
2.17 Configure SRTP

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

➢ To enable SRTP:

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 2-35: Configuring Media Security Parameter

3. Click Apply.
## 2.18 Configure Message Condition Rules

This section describes how to configure the Message Condition Rules. A Message Condition defines special conditions (pre-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.

- **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 2-36: Configuring Condition Table](image)

3. Click Apply.
2.19 Configure 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 sent 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>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>

3. Click Apply.
### 2.20 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 Trunks 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 that are received from any entity
- Terminate REFER messages to Teams Direct Routing
- Destination Tag based Routing (from/to Microsoft Teams Direct Routing or SIP Trunks)

#### 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></td>
</tr>
<tr>
<td>1</td>
<td>Refer Termination</td>
<td>Any</td>
<td>REFER</td>
<td>Teams</td>
<td>Request URI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Dest Tag Based Routing</td>
<td>Any</td>
<td>Destination Tag</td>
<td></td>
<td>Request URI</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The configured routing rules are shown in the figure below:

**Figure 2-38: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table**

**Note:** The routing configuration may change according to your specific deployment topology.
2.21 Configure Firewall Settings (Optional)

As extra security, there is an option to configure traffic filtering rules (access list) for incoming traffic on AudioCodes SBC. For each packet received on the configured network interface, the SBC searches the table from top to bottom until the first matching rule is found. The matched rule can permit (allow) or deny (block) the packet. Once a rule in the table is located, subsequent rules further down the table are ignored. If the end of the table is reached without a match, the packet is accepted. Please note that the firewall is stateless. The blocking rules 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>7</td>
<td>52.114.16.74</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>8</td>
<td>52.114.20.29</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've paired the SBC with Direct Routing, 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 > VOIP Status > 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
This page is intentionally left blank.
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 detailed description refer to 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.
This page is intentionally left blank.
5 Configure via UMP 365 (Optional)

AudioCodes’ User Management Pack 365 (UMP 365) SP Edition is a software application that simplifies the carriers’ management of its customers (Microsoft Office 365 tenants) onboarding automation, users MACD and lifecycle management of Microsoft Teams, SharePoint and OneDrive policies with Microsoft Direct Routing capabilities.

The application is an asynchronous model. This implies that changes to users will only be applied after replication takes place, either from scheduled tasks or by forcing a replication cycle from within the web application.

The figure below displays an example screen including a list of M365 customers tenants:

Figure 5-1: Provider Main Screen View

- View typical Microsoft 365 Tenant Phone Numbers
- Audit activities
- View queue for tasks status and results
- Update the Microsoft 365 Setting
Figure 5-2: Customer Tenant view – User List

For a detailed description, refer to AudioCodes User Management Pack 365 SP Edition Installation and Administration Guide.
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 issues 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:+97249888.108@10.15.40.55;user=phone SIP/2.0
Via: SIP/2.0/TLS ALDCTrunk;aceducation.info:5068;branch=z9hG4bKac466286557
Max-Forwards: 60
From: <sip:+97239762000@10.15.40.55>;tag=1c1642854452
To: <sip:+97249888108@10.15.40.55;user=phone>
Call-ID: 1167963076289201992217@ALDCTrunk.aceducation.info
CSeq: 1 INVITE
Contact: <sip:+97239762000@SBC1.AUDICTrunk;aceducation.info:5068;transport=tls>
Supported: v=0,100;ref,replace,replacepath,resourcetype,socknat
Allow: REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, PRACK, REFER, INFO, SUBSCRIBE, UPDATE
User-Agent: 10.15.40.55/v7.20A.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 subdomain in 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 AUDCTrunk.aceducation.info:5068;branch=z9hG4bKoc1603870555
Max-Forwards: 70
From: <sip:195.189.192.171>;tag=1c15b1a88696
To: <sip:195.189.192.171>
Call-ID: 123936556259520193103@AUDCTrunk.aceducation.info
CSeq: 1 OPTIONS
Contact: <sip:AUDCTrunk.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 Carrier Trunk FQDN in the URI hostname
  - Syntax: Contact: <phone number>@<Carrier Trunk FQDN>:<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><strong>Contact</strong></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 2.16.</td>
</tr>
</tbody>
</table>

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, `sbc1.AUDCTrunk.ACeducation.info`. The name changes the host name in the call received from the IP Group.
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</td>
<td>See Microsoft's document Deploying Direct Routing Guide.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interfaces</td>
<td></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</td>
<td>See Microsoft's document Deploying Direct Routing Guide.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Processors</td>
<td></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</td>
<td>SRTCP (SRTCP-Mux recommended)</td>
<td>Using RTCP MUX helps reduce the number of required ports</td>
</tr>
<tr>
<td></td>
<td>transport</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Supported Certification</td>
<td>See the Deployment Guide</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authorities</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transport for Media Bypass</td>
<td>▪ ICE-lite (RFC5245) – recommended</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(of configured)</td>
<td>▪ Client also has Transport Relays</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Audio codecs</td>
<td>▪ G711</td>
<td></td>
</tr>
</tbody>
</table>
### A. Syntax Requirements for SIP Messages 'INVITE' and 'OPTIONS'

<table>
<thead>
<tr>
<th>Category</th>
<th>Parameter</th>
<th>Value</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codecs</td>
<td>Other codecs</td>
<td>• CN</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Required narrowband and wideband</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RED - Not required</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DTMF - Required</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Events 0-16</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Silence Suppression - Not required</td>
<td></td>
</tr>
</tbody>
</table>
This page is intentionally left blank.
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**.
International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
200 Cottontail Lane,
Suite A101E, Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
website: https://www.audiocodes.com/

©2021 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant,
Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, AudioCodes Room
Experience and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or
trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-13216