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 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 in Hosting Model ........................................... 15
    2.1.1.1 SBC Domain Name in a Carrier's Tenant ................................................. 15
    2.1.1.2 SBC Domain Name in a Customer's Tenant ............................................. 16
  2.2 Validate AudioCodes' License .......................................................................... 17
  2.3 SBC Configuration Concept ............................................................................ 17
  2.4 Call Flows ........................................................................................................ 18
    2.4.1 Incoming Call to the Teams Client ............................................................... 18
    2.4.2 Outgoing Call from the Teams Client ......................................................... 19
    2.4.3 Transfer Call .............................................................................................. 20
  2.5 Configure LAN and WAN IP Interfaces ............................................................ 20
    2.5.1 Validate Configuration of Physical Ports and Ethernet Groups ...................... 20
    2.5.2 Configure LAN and WAN VLANS .............................................................. 21
    2.5.3 Configure Network Interfaces .................................................................. 22
  2.6 Configure TLS Context .................................................................................... 24
    2.6.1 Create a TLS Context for Teams Direct Routing ........................................... 25
    2.6.2 Generate a CSR and Obtain the Certificate from a Supported CA ................. 27
    2.6.3 Deploy the SBC and Root / Intermediate Certificates on the SBC ............... 28
  2.7 Alternative Method of Generating and Installing the Certificate ....................... 30
  2.8 Deploy Baltimore Trusted Root Certificate ...................................................... 31
  2.9 Configure Media Realm .................................................................................... 31
  2.10 Configure a SIP Signaling Interfaces ............................................................... 34
  2.11 Configure Proxy Sets and Proxy Address ....................................................... 35
    2.11.1 Configure Proxy Set for Teams Direct Routing ........................................... 35
    2.11.2 Configure a Proxy Address ....................................................................... 36
  2.12 Configure the Dial Plan Table (Customer DID Only) ......................................... 37
  2.13 Configuring Call Setup Rules ......................................................................... 38
    2.13.1 Configuring Call Setup Rules Based on Customer DID Range (Dial Plan) ....... 38
    2.13.2 Configuring Call Setup Rules based on Host name ..................................... 39
  2.14 Configure a Coder Group .............................................................................. 40
  2.15 Configure an IP Profile .................................................................................. 41
  2.16 Configure an IP Group (per Tenant) ............................................................... 43
  2.17 Configure SRTP ............................................................................................ 44
  2.18 Configure SIP OPTIONS ............................................................................. 45
    2.18.1 Configure FQDN in Contact Header of OPTIONS Message using Message Manipulations Sets .............................................................................. 45
  2.19 Configuring Message Condition Rules ........................................................... 47
  2.20 Configuring Classification Rules .................................................................. 48
  2.21 Configure IP to IP Routing ............................................................................ 49
  2.22 Configuring Firewall Settings ....................................................................... 53
  2.23 Configuring an SBC to Suppress Call Line ID (Optional) ................................ 54

Version 7.2 3 AudioCodes SBCs
3 Verify the Pairing between the SBC and Direct Routing.................................55
4 Make a Test Call ..........................................................................................57
5 Tenant Provisioning Script............................................................................59
A Syntax Requirements for SIP Messages 'INVITE' and 'OPTIONS'..............61
   A.1 Terminology .........................................................................................61
   A.2 Syntax Requirements for 'INVITE' Messages ........................................61
   A.3 Requirements for 'OPTIONS' Messages Syntax ....................................62
   A.4 Connectivity Interface Characteristics ..............................................63
B SIP Proxy Direct Routing Requirements ......................................................65
   B.1 Failover Mechanism .............................................................................65
C SBC Dashboard Example: SBC with Two Office 365 Teams Tenants ..........67
List of Figures

Figure 2-1: Connection Topology - Network Interfaces.................................................................13
Figure 2-2: Tenants Domain Structure .......................................................................................13
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: Incoming Call to the Teams Client .............................................................................18
Figure 2-9: Outgoing Call from the Teams Client .......................................................................19
Figure 2-10: Call Transfer ..........................................................................................................20
Figure 2-11: Physical Ports Configuration Interface .................................................................21
Figure 2-12: Ethernet Groups Configuration Interface ..............................................................21
Figure 2-13: Configured VLANs in the Ethernet Device Table ....................................................22
Figure 2-14: Configured IP Interfaces ..........................................................................................23
Figure 2-15: Tenants Domain Structure .....................................................................................24
Figure 2-16: Configuration of TLS Context for Direct Routing ....................................................25
Figure 2-17: Configured TLS Context for Direct Routing and Interface to Manage the Certificates 26
Figure 2-18: Example of Certificate Signing Request Page .........................................................28
Figure 2-19: Uploading the Certificate Obtained from the Certification Authority .......................29
Figure 2-20: Certificate Information Example .............................................................................29
Figure 2-21: Configured Trusted Certificates Page ....................................................................30
Figure 2-22: Configuring Media Realm for LAN .......................................................................32
Figure 2-23: Configuring Media Realm for WAN .....................................................................33
Figure 2-24: Configured Media Realms in Media Realm Table ...................................................33
Figure 2-25: Configuring Proxy Set for Teams Direct Routing ......................................................35
Figure 2-26: Configuring Proxy Address for Teams Direct Routing Interface .............................36
Figure 2-27: Dial Plan Rule Table - Add Dialog Box ..................................................................37
Figure 2-28: Call Setup Rules Table - Add Dialog Box ................................................................38
Figure 2-29: Call Setup Rules Table - Add Dialog Box ................................................................39
Figure 2-30: Configuring Coder Group for Teams Direct Routing .............................................40
Figure 2-31: Configured Media Security Parameter .....................................................................44
Figure 2-32: Configuring SIP Message Manipulation Rule 0 (for Teams) .................................46
Figure 2-33: Activating 'OPTIONS' Manipulation Set ...............................................................46
Figure 2-34: Configuring Condition Table ...................................................................................47
Figure 2-35: Configuring Condition Table ...................................................................................47
Figure 2-36: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS ........................50
Figure 2-37: Configuring IP-to-IP Routing Rule for Destination Tag Routing ..............................51
Figure 2-38: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table .................................52
Figure 2-39: Privacy Restriction Mode ........................................................................................54
Figure 2-40: P-Asserted-Identity Header Mode ..........................................................................54
Figure 3-1: Proxy Set Status .......................................................................................................55
Figure A-1: Example of an 'INVITE' Message ............................................................................61
Figure A-2: Example of 'OPTIONS' message ............................................................................62
Figure C-1: SBC with Two Office 365 Teams Tenants with a Single SIP Interface .................67
List of Tables

Table 1-1: Infrastructure Prerequisites ...................................................................................................12
Table 2-1: DNS Names Registered by an Administrator for a Carrier’s Tenant ..............................15
Table 2-2: Adding VLAN ID 2 for the WAN Side ..................................................................................21
Table 2-3: Configuration Example: Network Interfaces .......................................................................22
Table 2-4: Adding a Network Interface for the WAN for Teams .............................................................23
Table 2-5: New TLS Context ................................................................................................................25
Table 2-6: Configuration Example: Teams SIP Interface .......................................................................34
Table 2-7: Configuration Proxy Address for Teams Direct Routing .......................................................36
Table 2-8: Dial Plan Teams Tenants ...................................................................................................37
Table 2-9: Call Setup Rules Table .........................................................................................................38
Table 2-10: Call Setup Rules Table ......................................................................................................39
Table 2-11: Configuration Example: Teams IP Profile .........................................................................41
Table 2-12: Configuration Example: SIP Trunk IP Profile ..................................................................42
Table 2-13: Configuration Example: IP Group - Teams Global FQDNs ................................................43
Table 2-14: Configuration Example: Message Manipulation for Options .........................................45
Table 2-15: Activating 'OPTIONS' Manipulation Set ...........................................................................46
Table 2-16: Classification Rules ..........................................................................................................48
Table 2-17: Firewall Table Rules ..........................................................................................................53
Table A-1: Syntax Requirements for an 'INVITE' Message ................................................................62
Table A-2: Teams Direct Routing Interface - Technical Characteristics ..............................................63
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: July-08-2019

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>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>
<tr>
<td>13202</td>
<td><strong>Firmware version 7.20A.204.015 and later:</strong></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Modified: ‘Query Target’ parameter was added to Call Setup Rule #2</td>
</tr>
<tr>
<td></td>
<td>A link was added to Microsoft’s official list of supported Trusted Certificate Authorities in section “Configure TLS Context”.</td>
</tr>
<tr>
<td>13203</td>
<td>Updated CLI script – removed SIP Interface.</td>
</tr>
<tr>
<td></td>
<td>Removed DTLS Context from IP Group configuration.</td>
</tr>
<tr>
<td></td>
<td>Updated the configuration to support Tag-based Classification (Fix Dial Plan tags, Added CSR, SIP Interface)</td>
</tr>
<tr>
<td>LTRT</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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 |
| 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                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 13208 | **Modified due to changes in the Microsoft concept of Hosting Model. For more details refer to** [https://docs.microsoft.com/en-us/microsoftteams/direct-routing-sbc-multiple-tenants#create-a-trunk-and-provision-users](https://docs.microsoft.com/en-us/microsoftteams/direct-routing-sbc-multiple-tenants#create-a-trunk-and-provision-users)                                                                                     |

**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).
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 Web interface configuration examples, click 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.204.222. Previous firmware versions may run successfully; however, Microsoft did not test such versions. 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>See Microsoft's document <em>Deploying Direct Routing Guide.</em></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>
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

This guide covers how to configure the connection between AudioCodes' SBC and the Microsoft Phone Systems Direct Routing Interface. The interconnection of Service Provider SIP Trunk is outside the scope of this guide. Information about how to configure connections like these is available in other guides produced by AudioCodes.

Figure 2-1: Connection Topology - Network Interfaces

Note: This document shows how to configure the AudioCodes SBC to communicate with Teams Direct Routing. To configure 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).

Figure 2-2: Tenants Domain Structure
2.1 Prerequisites

Before you begin configuration, make sure you have these for every Hosting 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 in Hosting Model

2.1.1.1 SBC Domain Name in a Carrier’s 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 Figure 2-3, the administrator registered the following DNS names for the tenant:

Table 2-1: DNS Names Registered by an Administrator for a Carrier’s 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>• ussbcs15.Customers.aceducation.info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• europe.Customers.aceducation.info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Invalid name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sbc1.europe.Customers.aceducation.info</td>
</tr>
<tr>
<td>adatumbiz.onmicrosoft.com</td>
<td>No</td>
<td>Using *.onmicrosoft.com domains is not supported for SBC names.</td>
</tr>
</tbody>
</table>

For activating the domain, the Hosting Provider needs to add at least one user from the SIP domain registered for the tenant. For example, you can provide users sbc@Customers.aceducation.info with the Domain FQDN Customers.aceducation.info as long as 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’s Tenant

For each Customer’s 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 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>96.66.240.132</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.aceducation.info` with the Domain FQDN `SBC2.Customers.aceducation.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.
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, except for 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 SBC Configuration Concept

The figure below illustrates the concept behind the configuration of AudioCodes’ SBC device. Each tenant has an IP Group which uses the same Teams Direct Routing Proxy Set.

*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 or Host name, and uses Tag base Route.

For more information, see AudioCodes’ documentation suite.

2.4 Call Flows

The section illustrates the following flows:

- Incoming call to the Teams Client (see Section 2.4.1 below)
- Outgoing call from the Teams Client (see Section 2.4.2 below)
- Call transfer performed by Teams client (see Section 2.4.3 below)

2.4.1 Incoming Call to the Teams Client

The figure below shows an inbound call from the carrier’s SIP trunk to the Teams client.

*Figure 2-8: Incoming Call to the Teams Client*
2.4.2 Outgoing Call from the Teams Client

The figure below shows an outbound call from the Teams client to the carrier’s SIP trunk.

Figure 2-9: Outgoing Call from the Teams Client

Outgoing call from Teams

Classifies call by Classification table (Tag)

Call rejected

Yes

IP Group - Call Setup Rule (#0)
Sets Dest tag to ‘SIPTrunk’.
Saves Src tenant tag in session variable

Routes call to tenant using Dest tag
2.4.3 Transfer Call

The figure below shows a call transfer performed by the Teams client.

Figure 2-10: Call Transfer

- Teams sends REFER
- SBC terminates the REFER and issues a new INVITE
- IP Group - Call Setup Rule (#1)
  - Sets the Dest tenant tag according the session variable
- Routes call to tenant using Dest tag

2.5 Configure LAN and WAN IP Interfaces

2.5.1 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. Go to Setup > IP Network > Core Entities > 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 configuration, you might have more than two ports.
To validate Ethernet Groups:
1. Go to Setup > IP Network > Core Entities > Ethernet Groups.
2. Validate that you have at least two Ethernet Groups detected by the SBC, one for LAN and the other for WAN.

To configure VLANs:
1. Open the Ethernet Device Page (Setup > IP Network > Core Entities > Ethernet Devices); there'll be a VLAN ID for the underlying interface Group 1 (LAN).
2. Add VLAN ID 2 for the WAN side as follows:

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

This step shows how to configure network parameters for both LAN and WAN interfaces.

- To configure network parameters for both LAN and WAN interfaces:
  1. Open the IP Interfaces Table (Setup > IP Network > Core Entities > IP Interfaces)
  2. Configure network parameters for LAN interface.
     - Open O+M+C interface.
     - Configure the network parameters.

The table below shows a configuration example; your network parameters might be different.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>LAN_IF (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Application type</td>
<td>OAMP + Media + Control (this interface points to the internal network where the network administrator's station is located, so enabling OAMP is necessary)</td>
</tr>
<tr>
<td>Ethernet Device</td>
<td>vlan 1</td>
</tr>
<tr>
<td>Interface Mode</td>
<td>IPv4 Manual (if you use IPv4)</td>
</tr>
<tr>
<td>IP address</td>
<td>192.168.1.165 (example)</td>
</tr>
<tr>
<td>Prefix length</td>
<td>24 (example)</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>192.168.1.1 (example)</td>
</tr>
<tr>
<td>Primary DNS</td>
<td>192.168.1.130 (example)</td>
</tr>
</tbody>
</table>
3. Add a network interface for the WAN side for Teams. Use the table below as reference.

**Table 2-4: Adding a Network Interface for the WAN for Teams**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>WAN_IF (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Application type</td>
<td>Media + Control (as this interface points to the internet, enabling OAMP is not recommended)</td>
</tr>
<tr>
<td>Ethernet Device</td>
<td>vlan 2</td>
</tr>
<tr>
<td>Interface Mode</td>
<td>IPv4 Manual (if you use IPv4)</td>
</tr>
<tr>
<td>IP address</td>
<td>96.66.240.132 (Public IP example)</td>
</tr>
<tr>
<td>Prefix length</td>
<td>24 (example)</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>96.66.240.134 (example)</td>
</tr>
<tr>
<td>Primary DNS</td>
<td>According to your Internet provider’s instructions</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td>According to your Internet provider’s instructions</td>
</tr>
</tbody>
</table>

**Figure 2-14: Configured IP Interfaces**
2.6 Configure TLS Context

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
- **SAN**: *.customers.ACeducation.info

This certificate module is based on the Service Provider's own TLS Certificate. For more certificate structure options, see Teams Direct Routing documentation.

![Figure 2-15: Tenants Domain Structure](image)

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:


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:

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

1. Open TLS Contexts (Setup > IP Network > Security > TLS Contexts).
2. Create a new TLS Context by clicking +New, and then configure the parameters using the table below as reference.

Table 2-5: New TLS Context

<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>Teams (arbitrary descriptive name)</td>
</tr>
<tr>
<td>TLS Version</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.

3. Click Apply; you should see the new TLS Context and option to manage the certificates at the bottom of ‘TLS Context’ table.
Figure 2-17: Configured TLS Context for Direct Routing and Interface to Manage the Certificates
2.6.2 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 required TLS Context index row, and then click the Change Certificate link located below the table; the Context Certificates page appears.

Note: The domain portion of the Common Name [CN] must match the SIP suffix configured for Office 365 users.

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, customers.ACeducation.info).
   b. In the ‘1st Subject Alternative Name [SAN]’ field, change the type to ‘DNS’ and enter the wildcard FQDN name (based on example above, *.customers.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.
   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. Fill in 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:
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.

2.6.3 Deploy the SBC and Root / Intermediate Certificates on the SBC

After obtaining an SBC signed and Trusted Root/Intermediate Certificate from the CA, in the SBC’s Web interface, return to the TLS Contexts page and do the following:

- To install the SBC 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, 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.
4. Confirm that the certificate was uploaded correctly. A message indicating that the certificate was uploaded successfully is displayed in blue in the lower part of the page.

5. 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 2-20: Certificate Information Example**

   ![Certificate Information Example](image)

   **PRIVATE KEY**

   - **Key size:** 2048 bits
   - **Status:** OK

   **CERTIFICATE**

   - **Certificate:**
     - **Data:**
       - **Version:** 3 (0x2)
       - **Serial Number:** 06:5d:38:c2:00:17:01:7a:17:db:fe:ac:e1
     - **Signature Algorithm:** sha256WithRSAEncryption
     - **Issuer:** C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL RSA CA 2018
     - **Not Before:** May 22 00:00:00 2018 GMT
     - **Not After:** May 22 12:00:00 2019 GMT
     - **Subject:** CN=Cisco%auddc4c44d3c4cedcategor hotmail.com
     - **Subject Public Key Info:**
       - **Public Key Algorithm:** rsaEncryption
       - **Public-Key:** (2048 bit)
     - **Modulus:**
       - **00:5d:38:c2:00:17:01:7a:17:db:fe:ac:e1**

   **Figure 2-19: Uploading the Certificate Obtained from the Certification Authority**

6. 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.

7. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store:
2.7 Alternative Method of Generating and Installing the Certificate

To use the same certificate on multiple devices, you may prefer using 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.

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.
2.8 Deploy Baltimore Trusted Root Certificate

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:7b:db:28:52:ca:e4:74.

To trust this certificate, your SBC must have the certificate in Trusted Certificates storage. Download the certificate from [https://cacert.omniroot.com/bc2025.pem](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'.

2.9 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. Add a Media Realm for the LAN interface. You can use the default Media Realm (Index 0), but modify it as shown below:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>0</td>
</tr>
<tr>
<td>Name</td>
<td>MRLan (descriptive name)</td>
</tr>
<tr>
<td>IPv4 Interface Name</td>
<td>LAN_IF</td>
</tr>
<tr>
<td>Port Range Start</td>
<td>6000 (represents lowest UDP port number used for media on LAN)</td>
</tr>
<tr>
<td>Number of Media Session Legs</td>
<td>100 (media sessions assigned with port range)</td>
</tr>
</tbody>
</table>
Figure 2-22: Configuring Media Realm for LAN
3. Configure a Media Realm for WAN traffic:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>1</td>
</tr>
<tr>
<td>Name</td>
<td>MRWan (arbitrary name)</td>
</tr>
<tr>
<td>Topology Location</td>
<td>Up</td>
</tr>
<tr>
<td>IPv4 Interface Name</td>
<td>WAN_IF</td>
</tr>
<tr>
<td>Port Range Start</td>
<td>7000 (represents lowest UDP port number used for media on WAN)</td>
</tr>
<tr>
<td>Number of Media Session Legs</td>
<td>100 (media sessions assigned with port range)</td>
</tr>
</tbody>
</table>

The configured Media Realms are shown in the figure below:

Figure 2-23: Configuring Media Realm for WAN

Figure 2-24: Configured Media Realms in Media Realm Table
2.10 Configure a SIP Signaling Interfaces

This section shows how to configure a SIP signaling interface pointing to the Direct Routing interface.

Note that the configuration of a SIP interface for the PSTN trunk and the third-party IP-PBX is also required but not covered in this guide. 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 interface:

1. Open the SIP Interface table (Setup menu > Signaling & Media tab > Core Entities folder > SIP Interfaces).
2. Click +New to add a SIP Interface for the WAN interface pointing to the Direct Routing service. 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 2-6: Configuration Example: Teams SIP Interface

<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>Teams (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Network Interface</td>
<td>WAN_IF</td>
</tr>
<tr>
<td>Application Type</td>
<td>SBC</td>
</tr>
<tr>
<td>UDP and TCP Port</td>
<td>0</td>
</tr>
<tr>
<td>TLS Port</td>
<td>5061 (as configured in the Office 365)</td>
</tr>
<tr>
<td>Enable TCP Keepalive</td>
<td>Enable</td>
</tr>
<tr>
<td>Classification Failure Response Type</td>
<td>0 (Recommended to prevent DoS attacks)</td>
</tr>
<tr>
<td>Call Setup Rules Set ID</td>
<td>2</td>
</tr>
<tr>
<td>Media Realm</td>
<td>MRWan</td>
</tr>
<tr>
<td>TLS Context Name</td>
<td>Teams</td>
</tr>
</tbody>
</table>

All other parameters leave unchanged with their default values.

3. Click Apply and then save your settings to flash memory.

Note: Remember to configure SIP interfaces for the other SIP Trunks you may have.
2.11 Configure Proxy Sets and Proxy Address

2.11.1 Configure Proxy Set for Teams Direct Routing

The Proxy Set and Proxy Address defines TLS parameters, IP interfaces, FQDN and the remote entity's port. The example below covers configuration of a Proxy Set for Teams Direct Routing. Note that configuration of a Proxy Set for the PSTN trunk and the third-party PBX is also necessary, but isn't covered in this guide. 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.

➢ To configure a Proxy Set:

1. Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets).
2. Click +New to add the Proxy Set for the Teams Direct Routing Service.
3. Add a Proxy Set for the Teams Direct Routing as shown below:

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

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

4. Click Apply and then save your settings to flash memory.
2.11.2 Configure a Proxy Address

This section shows how to configure a Proxy Address. The Proxy Address must be the same for all Proxy Sets.

➢ To configure a Proxy Address:

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:

![Proxy Address dialog box]

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

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 and then save your settings to flash memory.

Note: Proxy Set and Proxy Address must be configured for the SIP Trunk Proxy Set too.
2.12 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 (TeamsTenants) will be configured with a tenant 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 (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]

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Prefix</th>
<th>Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise1</td>
<td>+1909xxxxx</td>
<td>Tenant1</td>
</tr>
<tr>
<td>Enterprise2</td>
<td>+1709xxxxx</td>
<td>Tenant2</td>
</tr>
<tr>
<td>Enterprise3</td>
<td>+1809xxxxx</td>
<td>Tenant3</td>
</tr>
</tbody>
</table>

7. Click Apply and then save your settings to flash memory.
2.13 Configuring Call Setup Rules

This section describes how to configure Call Setup Rules. 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.

2.13.1 Configuring Call Setup Rules Based on Customer DID Range (Dial Plan)

➢ To configure a Call Setup rule 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:

![Call Setup Rules Table - Add Dialog Box](image)

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

<table>
<thead>
<tr>
<th>Index</th>
<th>Rules Set ID</th>
<th>Request Type</th>
<th>Request Target</th>
<th>Request 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></td>
<td></td>
<td>var.session.0 == &quot;&quot;</td>
<td>var.session.0</td>
<td>Modify</td>
<td>Param.IPG.Src.Tags.Tenant</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Dial Plan</td>
<td>Teams Tenants</td>
<td>Param.Call. Dst.User</td>
<td>var.session.0 == &quot;&quot;</td>
<td>var.session.0</td>
<td>Modify</td>
<td>DialPlan.Result</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>Dial Plan</td>
<td>Teams Tenants</td>
<td>var(session.0 != &quot;&quot;</td>
<td>DstTags.Tenant</td>
<td>Modify</td>
<td>Var.Session.0</td>
<td></td>
</tr>
</tbody>
</table>

4. Click Apply and then save your settings to flash memory.

⚠️ Note: Make sure that “ForwardPai” is set to “True” using Get-CsOnlinePSTNGateway
2.13.2 Configuring Call Setup Rules based on Host name

- To configure a Call Setup rule based on Host name:
  1. Open the Call Setup Rules table (Setup menu > Signaling & Media tab > SIP Definitions folder > Call Setup Rules).
  2. Click New.

![Figure 2-29: Call Setup Rules Table - Add Dialog Box](image)

3. Configure a Call Setup rule using the following table as reference.

<table>
<thead>
<tr>
<th>Index</th>
<th>Rules Set ID</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>var.session.0 == ''</td>
<td>var.session.0</td>
<td>Modify</td>
<td>Param.IPG.Src.Tags.Tenant</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>DstTags.Tenant</td>
<td>var.session.0</td>
<td>Modify</td>
<td>‘SIPTrunk’</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>var.session.0 == ''</td>
<td>var.session.0</td>
<td>Modify</td>
<td>Header.Request-URI.URL.Host</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>var.session.0 != ''</td>
<td>DstTags.Tenant</td>
<td>Modify</td>
<td>Var.Session.0</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>SrcTags.Tenant</td>
<td></td>
<td>Modify</td>
<td>Header.Request-URI.URL.Host</td>
</tr>
</tbody>
</table>

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

This section describes how to configure coders (termed Coder Groups). As 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 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 step.

➢ 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 2-30: Configuring Coder Group for Teams Direct Routing

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 can later be assigned to specific IP calls (inbound and/or outbound).

➢ 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>SRTP</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>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><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 Trunk. 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>SIPTrunk (arbitrary descriptive name)</td>
</tr>
<tr>
<td><strong>Media Security</strong></td>
<td></td>
</tr>
<tr>
<td>SBC Media Security Mode</td>
<td>RTP</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 an IP Group (per Tenant)

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.

This section shows how to configure one.

➢ To configure an IP Group:

1. Open the IP Groups table (Setup > Signaling and Media > Core Entities > IP Group).

2. Click +New to add an IP Group for the Direct Routing interface. Configure the parameters using the table below as reference.

Note: Press Ctrl and + to zoom in and view the following table.

### Table 2-13: Configuration Example: IP Group - Teams Global FQDNs

<table>
<thead>
<tr>
<th>Ind</th>
<th>IP Group Name</th>
<th>Media Realm</th>
<th>Classify by ProxySet</th>
<th>Proxy Set ID</th>
<th>Local Host Name</th>
<th>Call Setup Rules Set ID</th>
<th>Tags</th>
<th>Always Use Src Address</th>
<th>IP Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Not Used</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>SIP Trunk</td>
<td>MRLan</td>
<td>Enable</td>
<td>SIPTrunk</td>
<td>1</td>
<td>Tenant=SIPTrunk</td>
<td></td>
<td></td>
<td>SIPTrunk</td>
</tr>
<tr>
<td>2</td>
<td>Teams-Tenant-1 (arbitrary descriptive name)</td>
<td>MRWan</td>
<td>Disable</td>
<td>Teams</td>
<td><code>&lt;FQDN name of your tenant in SBC&gt;</code>. For example, <code>sbc1.customers.ACeducation.info</code></td>
<td>0</td>
<td>Tenant=Tenant1 or Tenant=sbc1.customers.ACeducation.info</td>
<td>Yes</td>
<td>Teams</td>
</tr>
<tr>
<td>3</td>
<td>Teams-Tenant-2</td>
<td>MRWan</td>
<td>Disable</td>
<td>Teams</td>
<td><code>&lt;FQDN name of your tenant in SBC&gt;</code>. For example, <code>sbc2.customers.ACeducation.info</code></td>
<td>0</td>
<td>Tenant=Tenant2 or Tenant=sbc2.customers.ACeducation.info</td>
<td>Yes</td>
<td>Teams</td>
</tr>
<tr>
<td>4</td>
<td>Teams-Tenant-3</td>
<td>MRWan</td>
<td>Disable</td>
<td>Teams</td>
<td><code>&lt;FQDN name of your tenant in SBC&gt;</code>. For example, <code>sbc3.customers.ACeducation.info</code></td>
<td>0</td>
<td>Tenant=Tenant3 or Tenant=sbc3.customers.ACeducation.info</td>
<td>Yes</td>
<td>Teams</td>
</tr>
</tbody>
</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 2-31: Configured Media Security Parameter**

3. Click **Apply**.

   ![Media Security Configuration](image-url)

   **Figure 2-31: Configured Media Security Parameter**
2.18  Configure SIP OPTIONS

SIP OPTIONS is an important mechanism used to monitor the connection from the AudioCodes SBC to the Teams Direct Routing. Teams Direct Routing requires the FQDN of the trunk sent in the 'CONTACT' field of SIP OPTIONS. The FQDN of the trunk is the name that was specified during the pairing that was performed in the service provider’s tenant, for example:

New-CSOnlinePSTNGateway -FQDN customers.aceducation.info

The IP address of the SBC is by default sent in the 'CONTACT' field:

Contact: <sip:96.66.240.133>;tag=1c153541232

It's mandatory, however, that the 'CONTACT' field contains the FQDN of the SBC. More information about the requirements can be found at Requirements for 'OPTIONS' Messages Syntax.

Use the Message Manipulation Rules to configure sending the FQDN in the 'CONTACT' header of SIP OPTIONS.

2.18.1 Configure FQDN in Contact Header of OPTIONS Message using Message Manipulations Sets

This method allows manipulation of the 'CONTACT' header based on the Destination address of the entity. For example,

- SIP OPTIONS going to sip.pstnhub.microsoft.com should be in the format:

  Contact:123456789@customers.aceducation.info

The method will not function if you need to send a different FQDN in the 'Contact' header to multiple entities.

➢ To configure the Message Manipulations Table:

1. Open the Message Manipulations page (Setup menu > Signaling & Media tab > Message Manipulation folder > Message Manipulations).
2. Configure a new Message Manipulation Set as shown below:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>0</td>
</tr>
<tr>
<td>Name</td>
<td>Teams Options</td>
</tr>
<tr>
<td>Manipulation Set ID</td>
<td>1</td>
</tr>
<tr>
<td>Message Type</td>
<td>Options</td>
</tr>
<tr>
<td>Condition</td>
<td>Param.Message.Address.Dst.SIPInterface == '1'</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>'customers.aceducation.info' (FQDN of the SBC)</td>
</tr>
</tbody>
</table>
These rules will not apply automatically. For them to work, you must activate this set.

➢ **To activate this set:**

1. Open https://<SBC FQDN or IP >/AdminPage.
2. Go to 'ini Parameters'.

**Table 2-15: Activating 'OPTIONS' Manipulation Set**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GWOutboundManipulationSet</td>
<td>1 (Message Manipulation Set ID configured in the previous step)</td>
</tr>
</tbody>
</table>

3. Click **Apply New Value**.

**Figure 2-33: Activating 'OPTIONS' Manipulation Set**
2.19 Configuring 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>

3. Click Apply.
4. Click New, and then configure additional rule as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>1</td>
</tr>
<tr>
<td>Name</td>
<td>Teams-Options (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Condition</td>
<td>Header.Contact.URL.Host contains 'pstnhub.microsoft.com' AND Header.Request-URL.MethodType == '8'</td>
</tr>
</tbody>
</table>

5. Click Apply.
2.20 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 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 configure the Classification rule according to the parameters described in the table below.

Table 2-16: Classification Rules

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Source SIP Interface</th>
<th>Source IP Address</th>
<th>Message Condition</th>
<th>IP Group Selection</th>
<th>Action Type</th>
<th>IP Group Tag Name</th>
<th>Source IP Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Teams</td>
<td>Options</td>
<td>52.114.<em>.</em></td>
<td>Teams-Options</td>
<td>Source IP Group</td>
<td>Allow</td>
<td>&lt;Choose Any Teams IP Group&gt;</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Teams</td>
<td>Teams</td>
<td>52.114.<em>.</em></td>
<td>Teams-Contact</td>
<td>Tagged IP Group</td>
<td>Allow</td>
<td>Tenant</td>
<td></td>
</tr>
</tbody>
</table>

3. Click Apply.
2.21 Configure IP to IP Routing

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 routing rules use the configured IP Groups to denote the source and destination of the call.

The example shown in the table below only covers IP to IP routing, though you can route calls between Teams Direct Routing and SIP Trunk:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity
- Destination Tag based Routing (from/to Teams Direct Routing or AudioCodes SBC SIP Trunk)

See AudioCodes' SBC documentation for more information on how to route in other scenarios.

➢ To configure a route rule:

1. Open the IP-to-IP Routing table (Setup menu > Signaling & Media tab > SBC folder > Routing > IP-to-IP Routing).
2. Click +New and configure the rule using the example in the table below as reference:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>0</td>
</tr>
<tr>
<td>Name</td>
<td>Terminate OPTIONS (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Source IP Group</td>
<td>Any</td>
</tr>
<tr>
<td>Request Type</td>
<td>OPTIONS</td>
</tr>
<tr>
<td>Destination Type</td>
<td>Dest Address</td>
</tr>
<tr>
<td>Destination Address</td>
<td>internal</td>
</tr>
</tbody>
</table>
3. Click Apply.
4. Configure a rule to route calls based on Destination Tag Routing:
   a. Click **New**, and then configure the parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>1</td>
</tr>
<tr>
<td>Route Name</td>
<td><strong>Dest Tag Based Routing</strong> (arbitrary descriptive name)</td>
</tr>
<tr>
<td>Source IP Group</td>
<td>Any</td>
</tr>
<tr>
<td>Destination Type</td>
<td>Destination Tag</td>
</tr>
<tr>
<td>Routing Tag Name</td>
<td>Tenant</td>
</tr>
</tbody>
</table>

   **Figure 2-37: Configuring IP-to-IP Routing Rule for Destination Tag Routing**

   b. Click **Apply**.
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**

![Table of configured IP-to-IP routing rules](image)

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

As the SBC’s Teams Direct Routing IP Address interfaces with the public Internet, to increase the security from hacking, there is a need to define network traffic filtering rules (access list) for incoming traffic. 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 2-17: Firewall Table Rules

<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;</td>
<td>8.8.8.8</td>
<td>0</td>
<td>65535</td>
<td>Any</td>
<td>Enable</td>
<td>WAN_IF</td>
<td>Allow</td>
</tr>
<tr>
<td>0</td>
<td>(e.g. 8.8.8.8)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>sip.pstnhub.microsoft.com</td>
<td>0</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>sip2.pstnhub.microsoft.com</td>
<td>0</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>sip3.pstnhub.microsoft.com</td>
<td>0</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>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.
2.23 Configuring an SBC to Suppress Call Line ID (Optional)

This section shows how to configure an SBC in two steps when Forward P-Asserted-Identity header is included with the Privacy ID header (the configuration is optional). This allows:

- Suppressing all IDs
- Suppressing only the Forward P-Asserted-Identity header and allowing the From header

To override the Privacy:

- Use Outbound Manipulations: Set their 'Privacy Restriction Mode' to **Remove Restriction**; the P-Asserted-Identity header will remain and no privacy will apply.

To suppress the Forward P-Asserted-Identity header if required by the customer:

- (In addition to the previous step above) Use Teams’ IP Profile to set the ‘P-Asserted-Identity Header Mode’ to **Remove**.

---

**Figure 2-39: Privacy Restriction Mode**

**Figure 2-40: P-Asserted-Identity Header Mode**
3 Verify the Pairing between the SBC and Direct Routing

After you've 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 > 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.
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:

- Open the Test Call Rules table (Troubleshooting > Troubleshooting > Test Call > Test Call Rules).

➢ 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’ dropdown, 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 Tenant Provisioning Script

The CLI script below implements a Direct Routing Tenant based on this Configuration Note.

- The script is based on the assumption that a permanent configuration, not unique to a specific Direct Routing Tenant, is already configured (for example, Proxy Sets Table, Condition Table, IP-to-IP Routing, etc.).
- **Red** = variables that must be set/changed for each tenant.
- **Green** = constants unique to this Configuration Note; may vary per customer setup.

Access the CLI using Telnet and then log in with user credentials (Default: Admin/Admin).

```
en
Admin (Password)
configure voip

ip-group new
name <TBD-IPGroup> (e.g. Teams-Tenant-1)
proxy-set-name "Teams"
ip-profile-name "Teams"
sip-group-name "sbc1.customers.aceducation.info"
local-host-name "sbc1.customers.aceducation.info"
always-use-source-addr enable
sbc-dial-plan-name TeamsTenants
tags Tenant=<TBD-Tenant> (e.g. Tenant1 or sbc1.customers.ACeducation.info)
classify-by-proxy-set disable
call-setup-rules-set-id 0
proxy-keepalive-use-ipg enable
activate
exit
```

**Note:** The following script should be executed if the customer uses a Direct Inward Dialing (DID) service.

```
sbc dial-plan 0 (e.g. TeamsTenants)
    #(the below should repeat if the tenant has multiple DID ranges)
    dial-plan-rule new
    name <Customer/Tenant>
    prefix "+123456"
    tag "Tenant=Tenant1"
    exit
    #(repeat)
exit
do write
```
This page is intentionally left blank.
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

<table>
<thead>
<tr>
<th>Recommended</th>
<th>Must</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not required, but to simplify troubleshooting it’s recommended to configure as shown in the examples below.</td>
<td>Strictly required. The deployment does not function correctly without the correct configuration of these parameters.</td>
</tr>
</tbody>
</table>

A.2 Syntax Requirements for 'INVITE' Messages

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

```
INVITE sip:+97239764559@sbc.Aeducation.info;user=phone SIP/2.0
Via: SIP/2.0/TLS sbc.Aeducation.info:5060;branch=x-96496-Kac1922410385
Max-Forwards: 60
From: "Tel Shl" <sip:+97239764559@sbc.Aeducation.info;user=phone>;tag=1c1337768236;puid=C418C3B49
To: <sip:+97239764559@sbc.Aeducation.info;user=phone>
Call-ID: 562864536526917150168@sbc.Aeducation.info
CSeq: 1 INVITE
Contact: <sip:sbc.Aeducation.info:5060;transport=tl;ms-opaque=253493350fd81f9>
Supported: 100rel,sdp-verify
Allow: CANCEL, BYE, INVITE, PRACK, UPDATE
Request-URI
- Recommended: Configure the SBC FQDN in the URI hostname when sending calls to the Direct Routing interface
  - Syntax: INVITE sip: <phone number>@<FQDN of the SBC> SIP/2.0

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.
```
To header

- Recommended: When placing calls to the Direct Routing interface, the 'To' header can have the SBC FQDN in the URI hostname
- Syntax: To: INVITE sip: <phone number>@<FQDN of the SBC>

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 'INVITE' Message

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Where configured</th>
<th>How to configure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Request-URI</strong></td>
<td>Setup &gt; Signaling and Media &gt; Core Entities &gt; IP Group&gt; &lt;Group Name&gt; &gt; SIP Group Name</td>
<td>See AudioCodes' SIP Message Manipulation Reference Guide.</td>
</tr>
<tr>
<td><strong>To</strong></td>
<td>Signaling and Media &gt; Message Manipulations &gt; Manipulation Set Note that the Manipulation Set must be applied to the Teams IP Group as an Outbound Message Manipulation Set.</td>
<td>See AudioCodes' SIP Message Manipulation Reference Guide.</td>
</tr>
</tbody>
</table>
| **Contact** | Setup > Signaling and Media > Core Entities > IP Group> <Group Name> > Local Host Name  
In IP Groups, 'Contact' must also be configured. In this field, 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. For outbound calls, configure 'Local Host Name' in the IP Group setting. | See Section 2.16. |

### A.3 Requirements for 'OPTIONS' Messages Syntax

Figure A-2: Example of 'OPTIONS' message

```
OPTIONS sip:sbc.ACeducation.info SIP/2.0
Via: SIP/2.0/TLS 105.189.192.150:5068;branch=z9hG4bKac1404080305
Max-Forwards: 70
From: <sip:sbc.ACeducation.info>;tag=1c386866573
To: <sip:sbc.ACeducation.info>
Call-ID: 188403163931122917223428@195.189.192.150
CSeq: 1 OPTIONS
Contact: <sip:sbc.ACeducation.info:5068;transport=TLS>
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,REGISTER,UPDATE
```

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, the calls are rejected with a '403 Forbidden' message
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_HMA C_SHA1_80, non-MKI</td>
<td><a href="https://tools.ietf.org/html/rfc5763">https://tools.ietf.org/html/rfc5763</a></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>Control protocol for media</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>transport</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Certification</td>
<td>Supported Certification Authorities</td>
<td>See the Deployment Guide</td>
<td></td>
</tr>
<tr>
<td>Authorities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport for Media Bypass</td>
<td>Transport for Media Bypass (of configured)</td>
<td>• ICE-lite (RFC 5245) – recommended</td>
<td></td>
</tr>
<tr>
<td>(of configured)</td>
<td></td>
<td>• Client also has Transport Relays</td>
<td></td>
</tr>
<tr>
<td>Audio codecs</td>
<td>Audio codecs</td>
<td>• G.711</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Silk (Teams clients)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Opus (WebRTC clients) - only if Media Bypass is used</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• G.729</td>
<td></td>
</tr>
<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>
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.
This page is intentionally left blank.
C. SBC Dashboard Example: SBC with Two Office 365 Teams Tenants

The figure below exemplifies an SBC dashboard showing an SBC with two Office 365 Teams tenants, where:

- On the SBC Teams represented by one SIP Interface and each Teams site tenant is represented by an IP Group

Figure C-1: SBC with Two Office 365 Teams Tenants with a Single SIP Interface