Configuration Note

AudioCodes Mediant™ Family of Media Gateways & Session Border Controllers

Connecting AudioCodes' SBC to Microsoft Teams Direct Routing Hosting Model

Version 7.2

audiocodes

Table of Contents

List of Figures

List of Tables

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: April-30-2019

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

Document Name
Mediant 500 E-SBC User's Manual
Mediant 500L E-SBC User's Manual
Mediant 800B E-SBC User’s Manual
Mediant 2600 E-SBC User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
Gateway and SBC CLI Reference Guide
SIP Message Manipulation Reference Guide
AudioCodes Configuration Notes

Document Revision Record

LTRT	Description
12885	Initial document release for Version 7.2. Hosting Model.
12886	Fixes
12887	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.
12888	Call Flows. Configuration Concept.
12889	Parameter ‘Request Type’. SIP I/F-Index entry deleted. Parameter ‘SBC Media Security Method’.
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)

LTRT	Description
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

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

This page is intentionally left blank.

1 Introduction

This *Configuration Note* describes how to connect AudioCodes' SBC to Microsoft Teams Direct Routing. The 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 Microsoft Teams Direct Routing

Microsoft 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

Infrastructure Prerequisite	Details
Certified Session Border Controller (SBC)	See Microsoft's document *Deploying Direct Routing Guide.*
SIP Trunks connected to the SBC	
Office 365 tenant	
Domains	
Public IP address for the SBC	
Fully Qualified Domain Name (FQDN) for the SBC	
Public DNS entry for the SBC	
Public trusted certificate for the SBC	
Firewall ports for Direct Routing signaling	
Firewall IP addresses and ports for Direct Routing media	
Media Transport Profile	
Firewall ports for client media	

2 Configuring AudioCodes' SBC

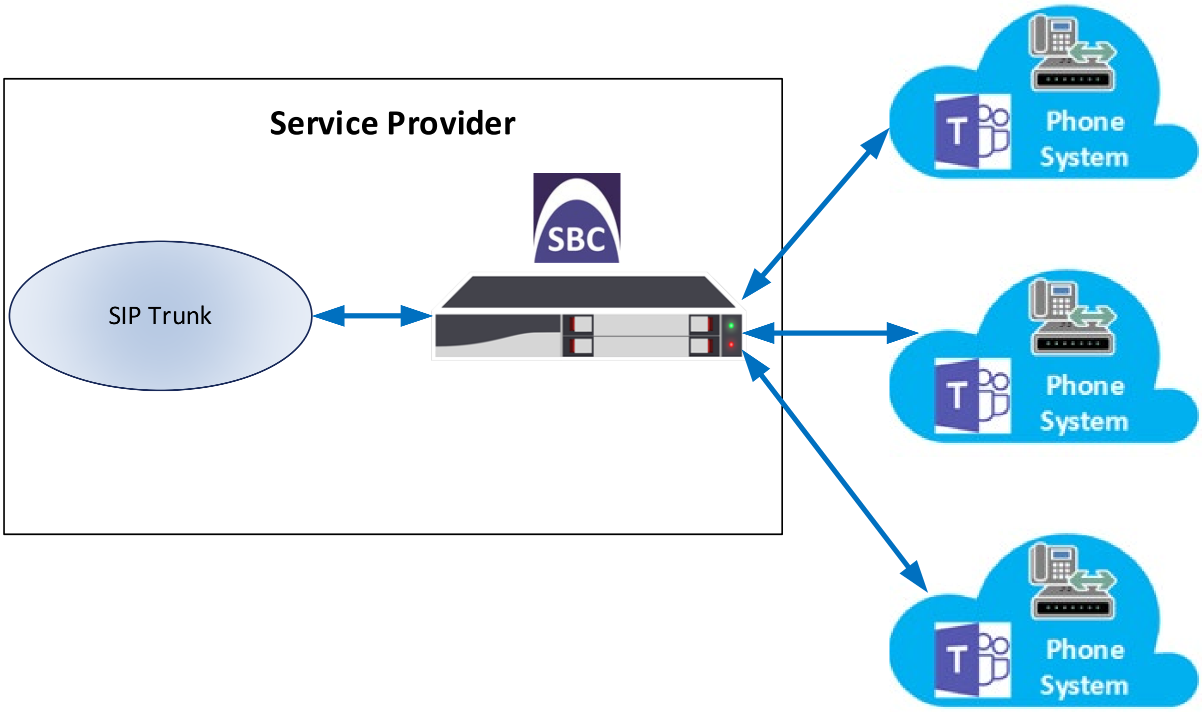
This section shows how to configure AudioCodes' SBC for internetworking with Microsoft Teams Direct Routing.

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

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

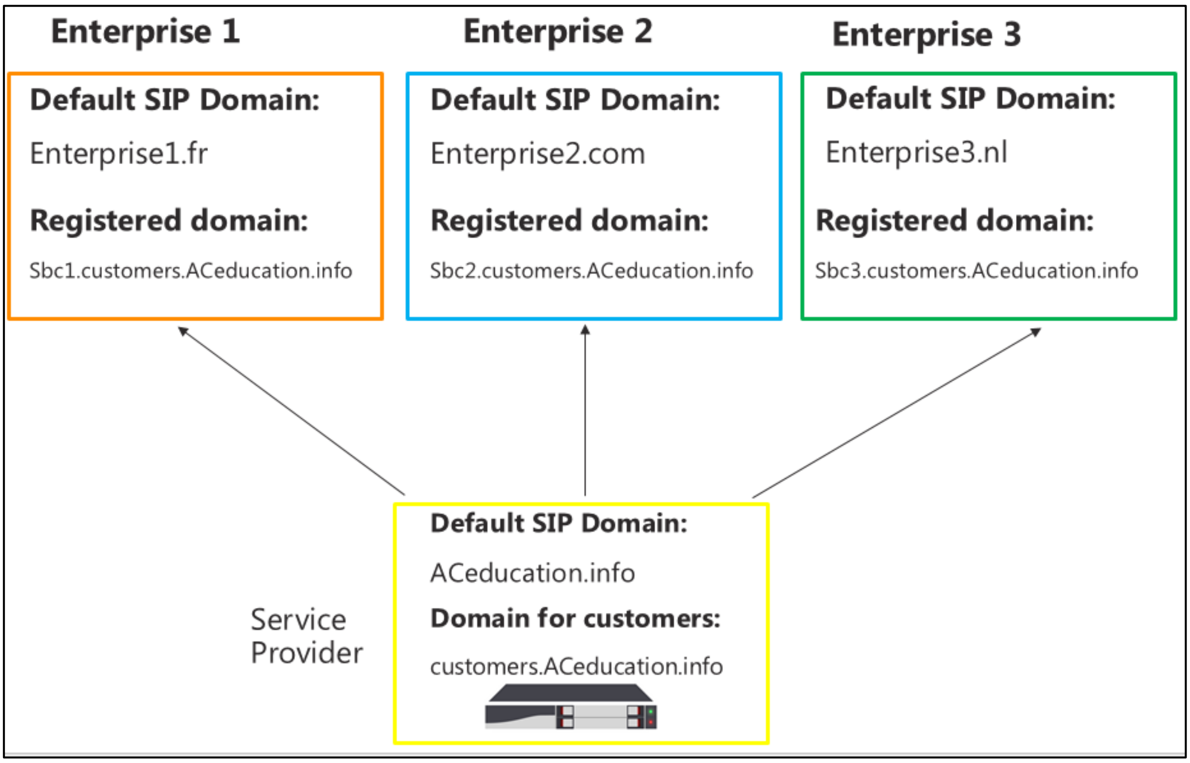
This guide covers how to configure the connection between AudioCodes' SBC and the Microsoft Phone Systems Direct Routing Interface. The interconnection of Service Provider SIP Trunk is outside the scope of this guide. Information about how to configure connections like these is available in other guides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

Figure 2-1: Connection Topology - Network Interfaces



> **Note:** This document shows how to configure the Microsoft Teams side. 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

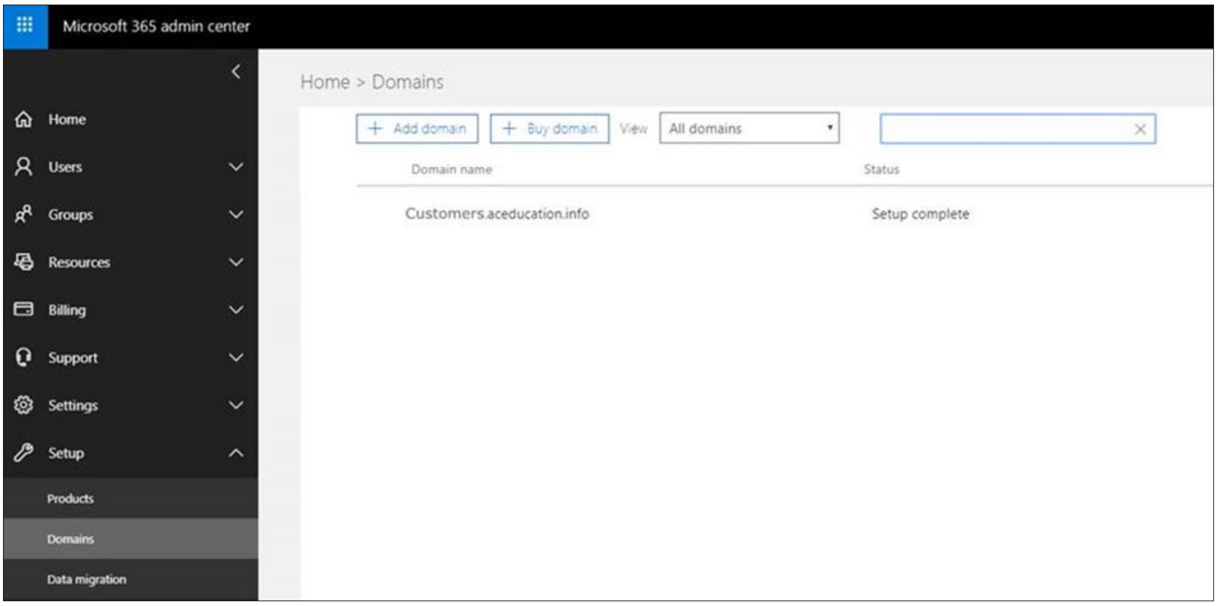
2.1.1.1 SBC Domain Name in a Carrier's Tenant

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

DNS name	Can be used for SBC FQDN	Examples of FQDN names for Hosting Customers
Customers.aceducation.info	Yes	**Valid names**: ▪ sbc.Customers.aceducation.info ▪ ussbcs15.Customers.aceducation.info ▪ europe.Customers.aceducation.info **Invalid name:** sbc1.europe.Customers.aceducation.info
adatumbiz.onmicrosoft.com	No	Using ***.onmicrosoft.com** domains is not supported for SBC names.

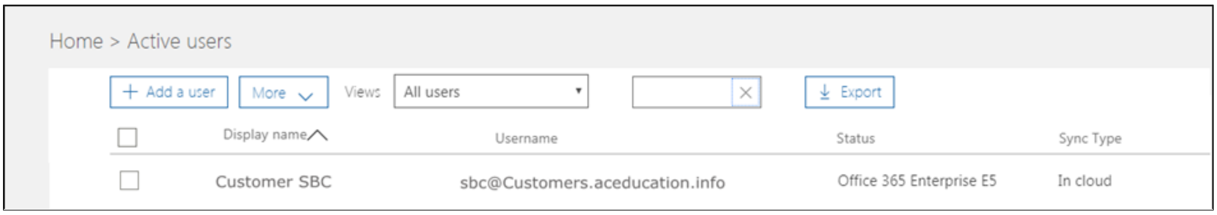
Figure 2-3: Example of Registered DNS Names



Domain name	Status
Customers.aceducation.info	Setup complete

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.

Figure 2-4: Example of User Belonging to SBC Carrier's Domain

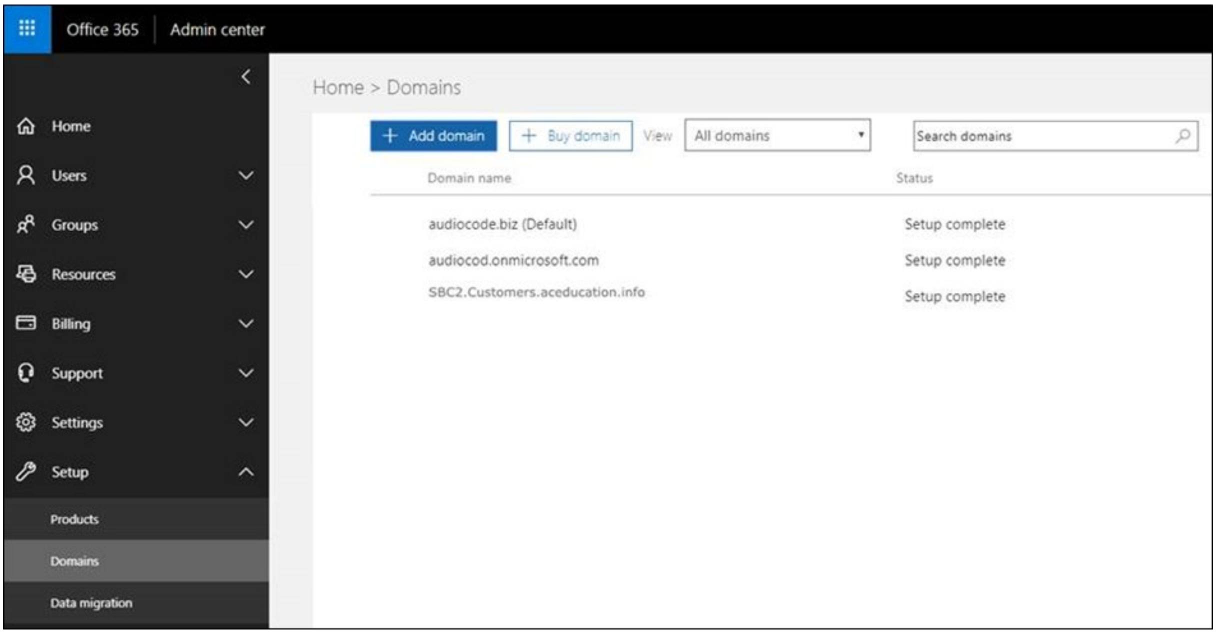


☐	Display name	Username	Status	Sync Type
☐	Customer SBC	sbc@Customers.aceducation.info	Office 365 Enterprise E5	In cloud

2.1.1.2 SBC Domain Name in a Customer's Tenant

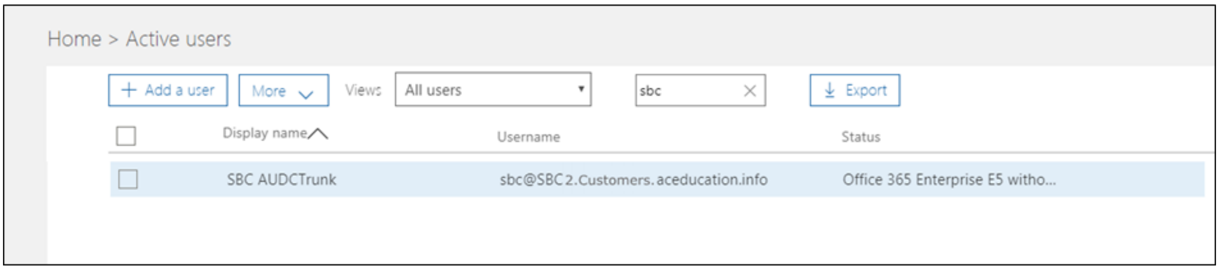
For each Customer's tenant, you should add a domain belonging to a carrier that points to a customer tenant as in Figure 2-5 and create at least one licensed user belonging to your SBC domain as in Figure 2-6.

Figure 2-5: Example of Domain for Carrier SBC in Customer Domain



Domain name	Status
audiocode.biz (Default)	Setup complete
audiocod.onmicrosoft.com	Setup complete
SBC2.Customers.aceducation.info	Setup complete

Figure 2-6: Example of User for Carrier SBC in Customer Domain



☐	Display name	Username	Status
☐	SBC AUDCTrunk	sbc@SBC2.Customers.aceducation.info	Office 365 Enterprise E5 witho...

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

Public IP	FQDN Name of Carrier's SBC for a customer
96.66.240.132	Sbc2.Customers.ACeducation.info

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

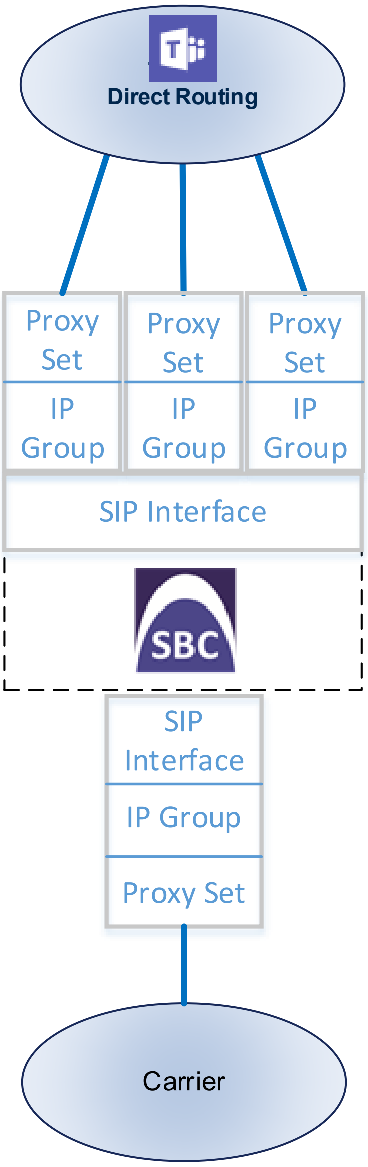
The following licenses are required on AudioCodes' device:

1. **Microsoft TEAMS License**
2. **Number of SBC sessions** [Based on requirements]
3. **Transcoding sessions** [If media transcoding is needed]
4. **Coders** [Based on requirements - licenses for SILK and OPUS]

2.3 SBC Configuration Concept

The figure below illustrates the concept behind the configuration of AudioCodes' SBC device. Each tenant has an IP Group and a 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

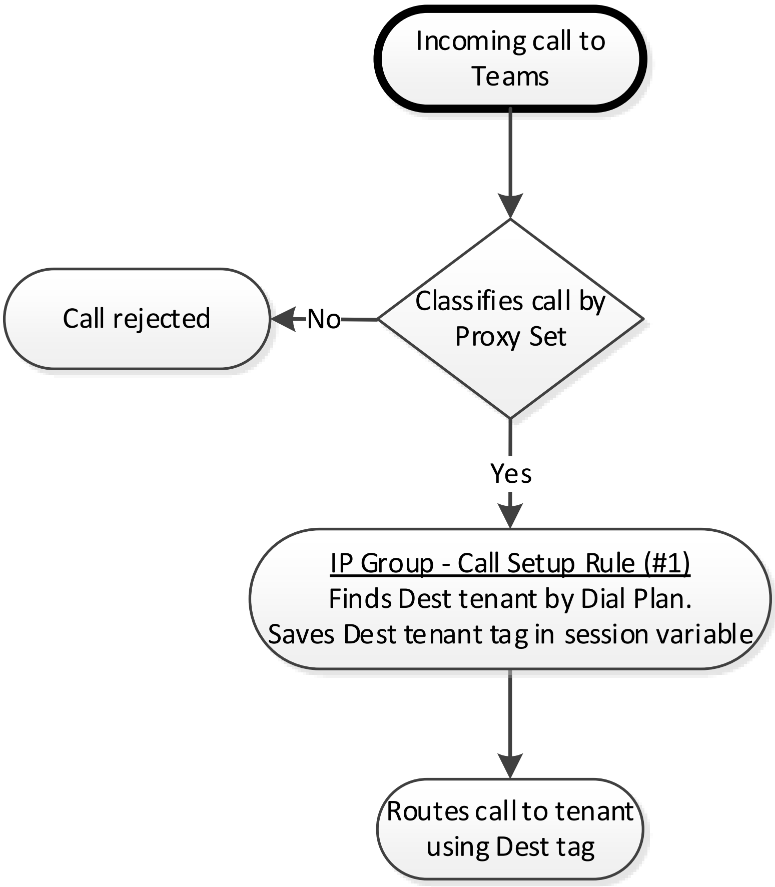
The section illustrates the following flows:

- an incoming call to the Teams Client (see Section 2.4.1 below)
- an outgoing call from the Teams Client (see Section 2.4.2 below)
- a 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.

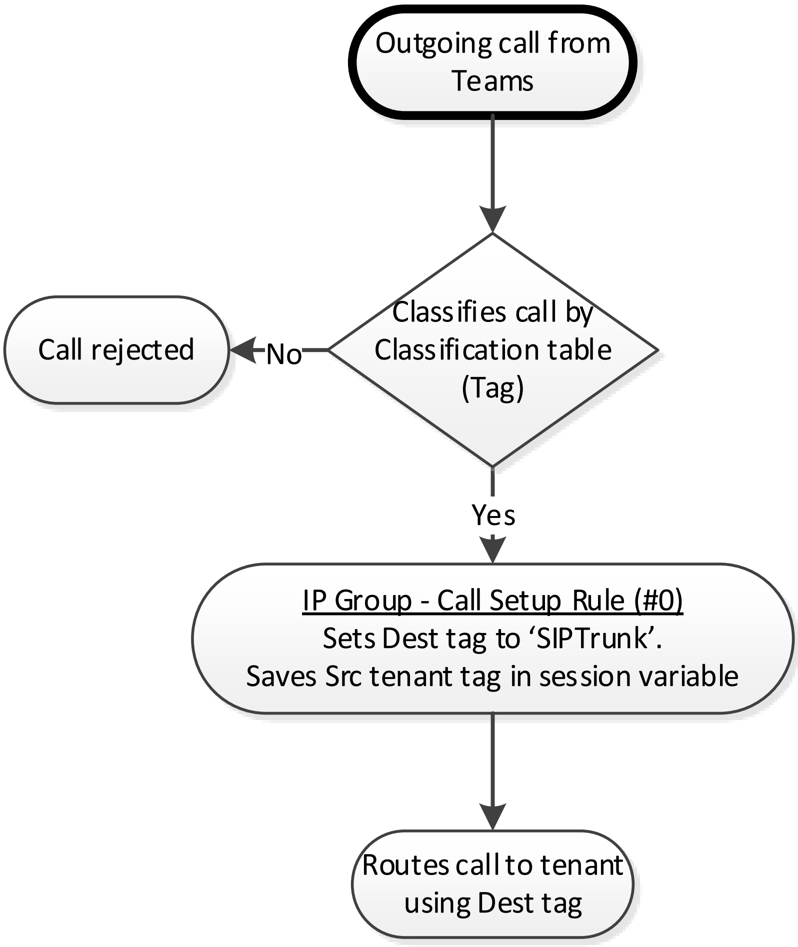
Figure 2-8: Incoming Call to the Teams Client


Incoming call to Teams
Classifies call by Proxy Set
No
Call rejected
Yes
IP Group - Call Setup Rule (#1)
Finds Dest tenant by Dial Plan.
Saves Dest tenant tag in session variable
Routes call to tenant using Dest tag

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.

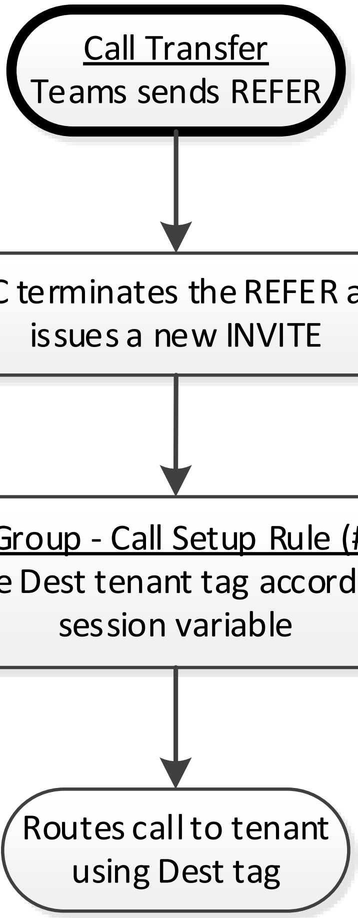
Figure 2-9: Outgoing Call from the Teams Client


Outgoing call from Teams
Classifies call by Classification table (Tag)
No
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


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

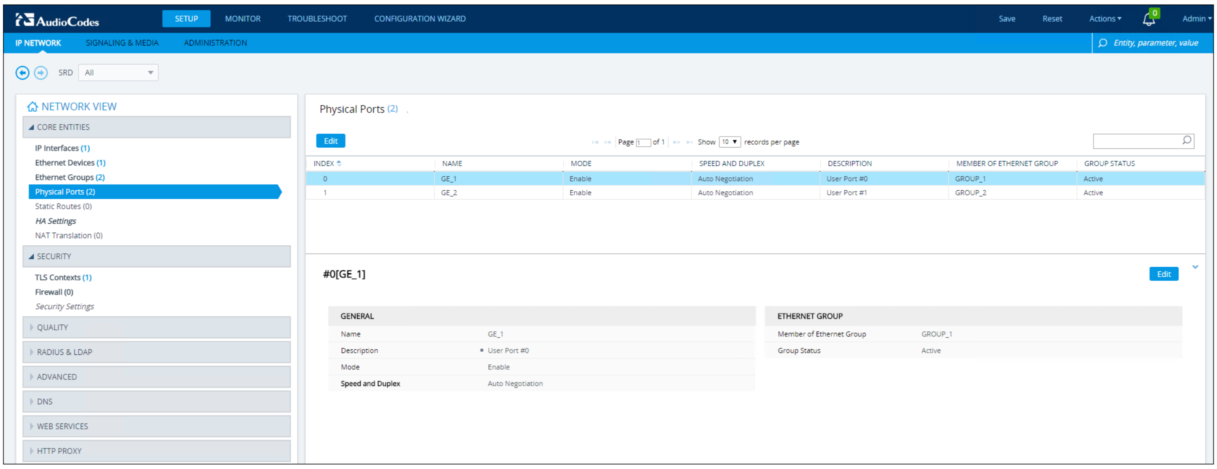
The physical ports are automatically detected by the SBC. The Ethernet groups are also auto-assigned to the ports. In this step, only parameter validation is necessary.

➢ **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.

Figure 2-11: Physical Ports Configuration Interface



Physical Ports (2)

INDEX	NAME	MODE	SPEED AND DUPLEX	DESCRIPTION	MEMBER OF ETHERNET GROUP	GROUP STATUS
0	GE_1	Enable	Auto Negotiation	User Port #0	GROUP_1	Active
1	GE_2	Enable	Auto Negotiation	User Port #1	GROUP_2	Active

#0[GE_1]

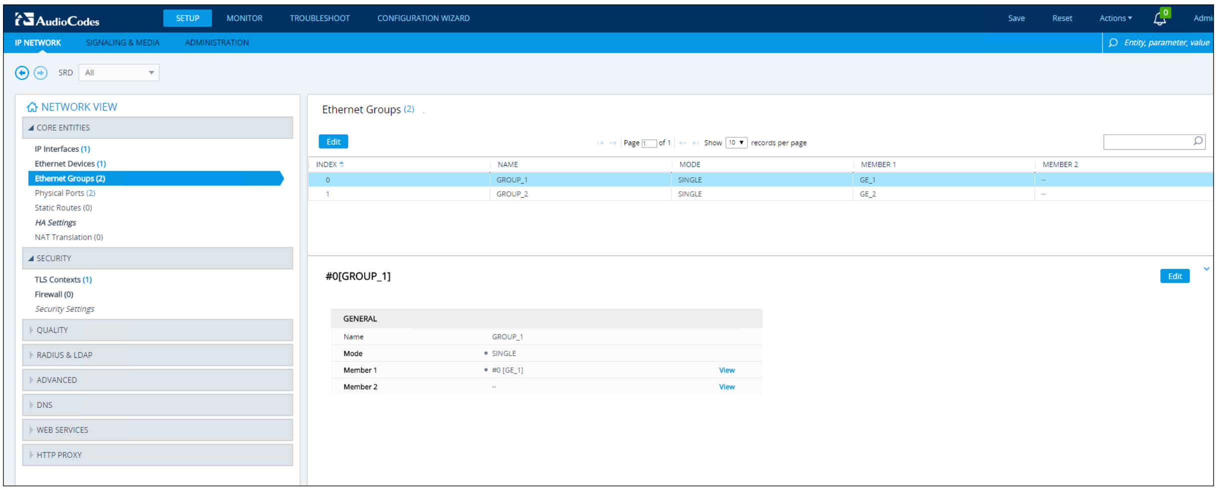
GENERAL	
Name	GE_1
Description	• User Port #0
Mode	Enable
Speed and Duplex	Auto Negotiation

ETHERNET GROUP	
Member of Ethernet Group	GROUP_1
Group Status	Active

➢ 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.

Figure 2-12: Ethernet Groups Configuration Interface



Ethernet Groups (2)

INDEX	NAME	MODE	MEMBER 1	MEMBER 2
0	GROUP_1	SINGLE	GE_1	--
1	GROUP_2	SINGLE	GE_2	--

#0[GROUP_1]

GENERAL		
Name	GROUP_1	
Mode	• SINGLE	
Member 1	• #0 [GE_1]	View
Member 2	--	View

2.5.2 Configure LAN and WAN VLANs

This step shows how to configure VLANs for LAN and WAN interfaces.

➢ To configure VLANs:

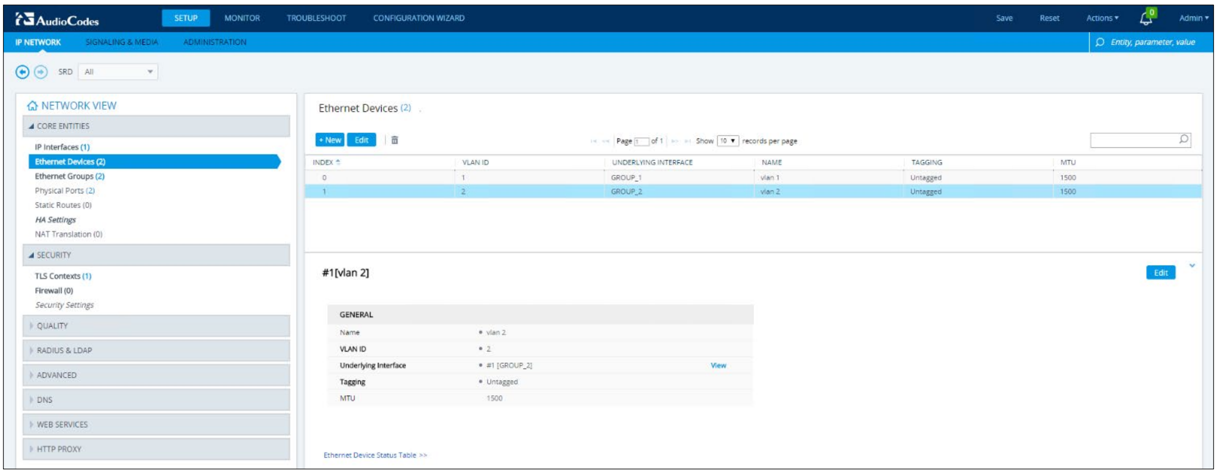
1. Open the Ethernet Device Page (**Setup** > **IP Network** > **Core Entities** > **Ethernet Devices**); there'll be a VLAN ID for the underlying interface Group 1 (LAN).
2. Add VLAN ID 2 for the WAN side as follows:

Table 2-2: Adding VLAN ID 2 for the WAN Side

Parameter	Value
Index	1
Name	vlan 2
VLAN ID	2

Underlying Interface	GROUP_2 (Ethernet port group)
Tagging	Untagged

Figure 2-13: Configured VLANs in the Ethernet Device Table



Ethernet Devices (2)

INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING	MTU
0	1	GROUP_1	vlan 1	Untagged	1500
1	2	GROUP_2	vlan 2	Untagged	1500

#1[vlan 2]

GENERAL

Name	vlan 2
VLAN ID	2
Underlying Interface	#1 [GROUP_2]
Tagging	Untagged
MTU	1500

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**) – see
2. Figure 2-14 below.
3. 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 2-3: Configuration Example: Network Interfaces

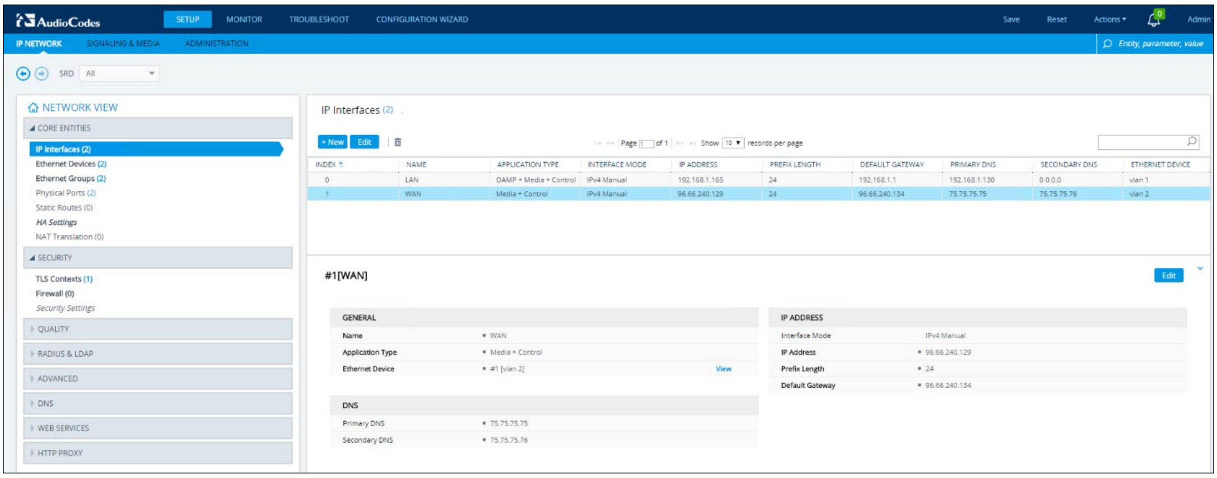
Parameter	Value
Name	LAN_IF (arbitrary descriptive name)
Application type	OAMP + Media + Control (this interface points to the internal network where the network administrator's station is located, so enabling OAMP is necessary)
Ethernet Device	#0[vlan 1]
Interface Mode	IPv4 Manual (if you use IPv4)
IP address	192.168.1.165 (example)
Prefix length	24 (example)
Default Gateway	192.168.1.1 (example)
Primary DNS	192.168.1.130 (example)
Secondary DNS	192.168.1.131 (example)

4. 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

Parameter	Value
Name	WAN_IF (arbitrary descriptive name)
Application type	Media + Control (as this interface points to the internet, enabling AMP is not recommended)
Ethernet Device	#1[vlan 2]
Interface Mode	IPv4 Manual (if you use IPv4)
IP address	96.66.240.132 (Public IP example)
Prefix length	24 (example)
Default Gateway	96.66.240.134 (example)
Primary DNS	According to your Internet provider's instructions
Secondary DNS	According to your Internet provider's instructions

Figure 2-14: Configured IP Interfaces



IP Interfaces (2)

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	LAN	OAMP + Media + Control	IPv4 Manual	192.168.1.165	24	192.168.1.1	192.168.1.130	0.0.0.0	vlan 1
1	WAN	Media + Control	IPv4 Manual	96.66.240.129	24	96.66.240.134	75.75.75.75	75.75.75.76	vlan 2

#1[WAN]

GENERAL

- Name: WAN
- Application Type: Media + Control
- Ethernet Device: #1 [vlan 2]

DNS

- Primary DNS: 75.75.75.75
- Secondary DNS: 75.75.75.76

IP ADDRESS

- Interface Mode: IPv4 Manual
- IP Address: 96.66.240.129
- Prefix Length: 24
- Default Gateway: 96.66.240.134

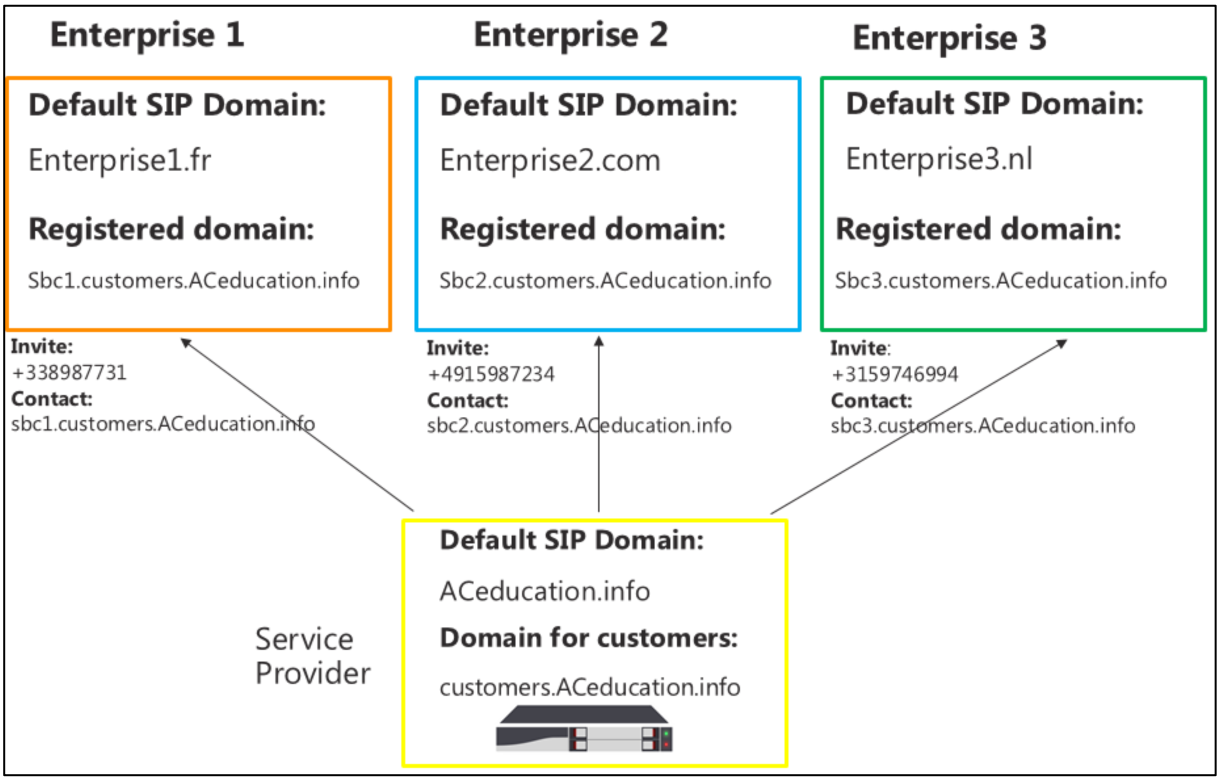
2.6 Configure TLS Context

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 Microsoft Teams Direct Routing documentation.

Figure 2-15: Tenants Domain Structure



The Microsoft Phone System 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

The step below shows how to request a certificate for the SBC WAN interface and to configure it based on an example using DigiCert Global Root CA.

This step includes the following stages:

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

2.6.1 Create a TLS Context for Microsoft Phone System Direct Routing

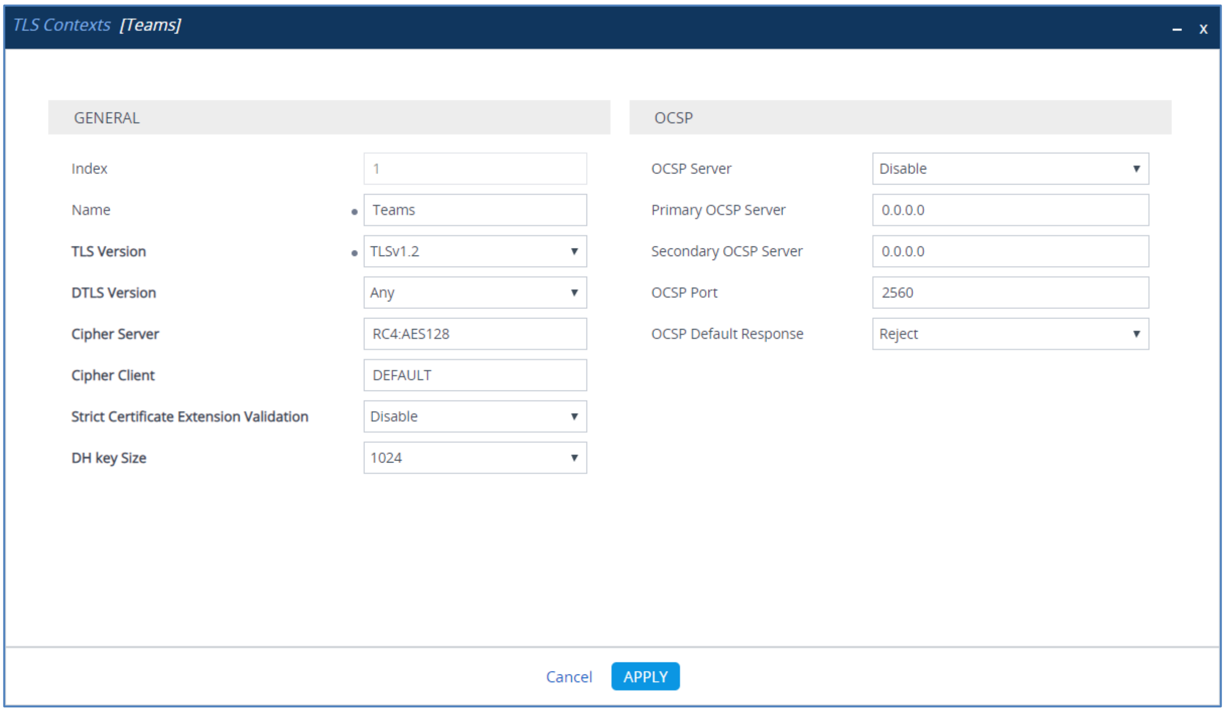
1. Open TLS Contexts (**Setup** > **IP Network** >**Security**>**TLS Contexts**).
2. Create a new TLS Context by clicking **+New**, and then configure the parameters using the table below as reference.

Table 2-5: New TLS Context

Parameter	Value
Index	1
Name	Teams (arbitrary descriptive name)
TLS Version	TLSv1.2
All other parameters leave unchanged at their default values	

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

Figure 2-16: Configuration of TLS Context for Direct Routing



TLS Contexts *[Teams]*

GENERAL

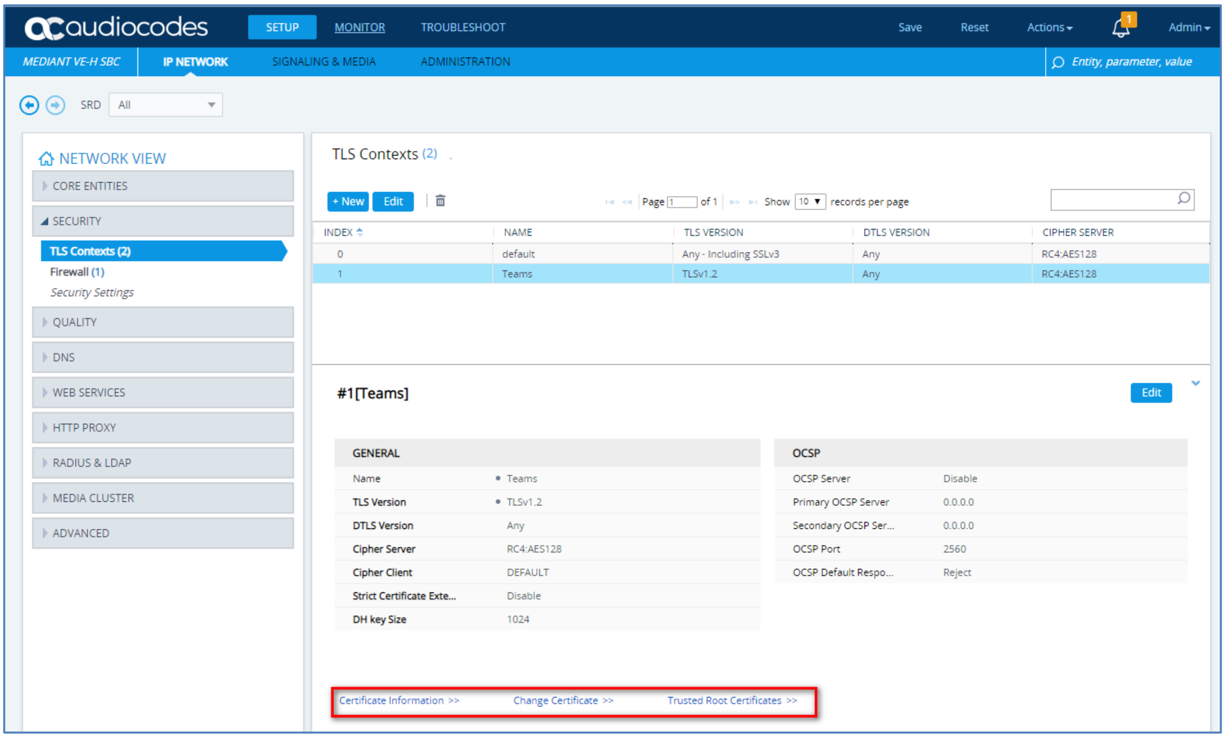
Index	1
Name	Teams
TLS Version	TLSv1.2
DTLS Version	Any
Cipher Server	RC4:AES128
Cipher Client	DEFAULT
Strict Certificate Extension Validation	Disable
DH key Size	1024

OCSP

OCSP Server	Disable
Primary OCSP Server	0.0.0.0
Secondary OCSP Server	0.0.0.0
OCSP Port	2560
OCSP Default Response	Reject

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



TLS Contexts (2)

INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	default	Any - Including SSLv3	Any	RC4:AES128
1	Teams	TLSv1.2	Any	RC4:AES128

#1[Teams]

GENERAL	
Name	• Teams
TLS Version	• TLSv1.2
DTLS Version	Any
Cipher Server	RC4:AES128
Cipher Client	DEFAULT
Strict Certificate Exte...	Disable
DH key Size	1024

OCSP	
OCSP Server	Disable
Primary OCSP Server	0.0.0.0
Secondary OCSP Ser...	0.0.0.0
OCSP Port	2560
OCSP Default Respo...	Reject

Certificate Information >> Change Certificate >> Trusted Root 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.

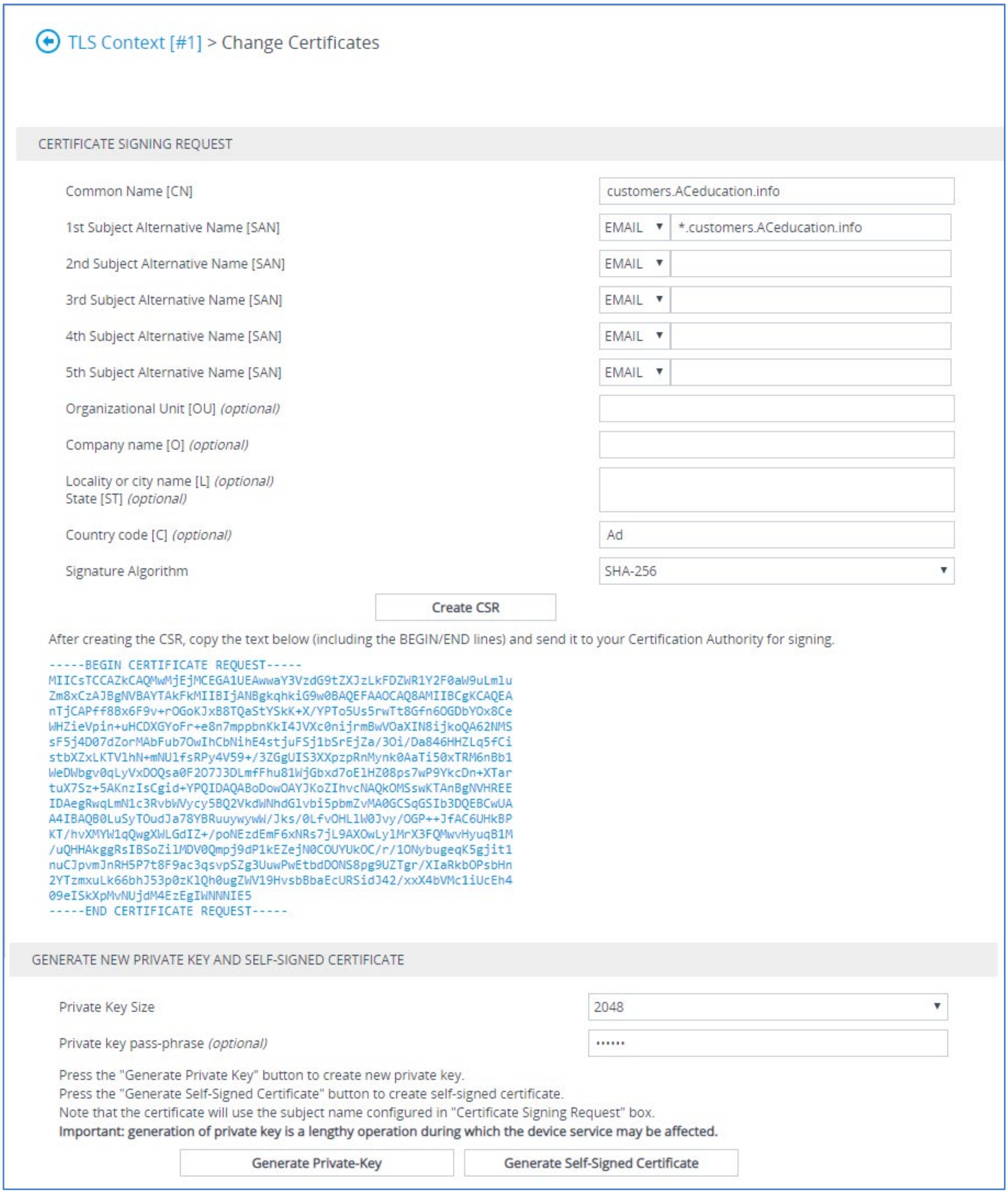
➢ **To generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority:**

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 SN must match the SIP suffix configured for Office 365 users.

3. Under the **Certificate Signing Request** group, do the following:
   a. In the 'Subject Name [CN]' field, enter the SBC FQDN name (based on example above, **customers.ACeducation.info**).
   b. In the '1st Subject Alternative Name [SAN]' field, 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:

Figure 2-18: Example of Certificate Signing Request Page



TLS Context [#1] > Change Certificates

CERTIFICATE SIGNING REQUEST

Common Name [CN]	customers.ACeducation.info
1st Subject Alternative Name [SAN]	EMAIL ▼ *.customers.ACeducation.info
2nd Subject Alternative Name [SAN]	EMAIL ▼
3rd Subject Alternative Name [SAN]	EMAIL ▼
4th Subject Alternative Name [SAN]	EMAIL ▼
5th Subject Alternative Name [SAN]	EMAIL ▼
Organizational Unit [OU] *(optional)*	
Company name [O] *(optional)*	
Locality or city name [L] *(optional)* State [ST] *(optional)*	
Country code [C] *(optional)*	Ad
Signature Algorithm	SHA-256 ▼

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICsTCCAZkCAQMwMjEjMCEGA1UEAwwaY3VzdG9tZXJzLkFDZWR1Y2F0aW9uLmlu
Zm8xCzAJBgNVBAYTAkFkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
nTjCAPff8Bx6F9v+rOGoKJxB8TQaStYSkK+X/YPTo5Us5rwTt8Gfn6OGDbYOx8Ce
WHZieVpin+uHCDXGYoFr+e8n7mppbnKkI4JVXc0nijrmBwVOaXIN8ijkoQA62NMS
sF5j4D07dZorMAbFub7OwIhCbNihE4stjuFSj1bSrEjZa/3Oi/Da846HHZLq5fCi
stbXZxLKTVlhN+mNUlfsRPy4V59+/3ZGgUIS3XXpzpRnMynk0AaTi50xTRM6nBb1
WeDWbgv0qLyVxDOQsa0F2O7J3DLmfFhu81WjGbxd7oElHZ08ps7wP9YkcDn+XTar
tuX7Sz+5AKnzIsCgid+YPQIDAQABoDowOAYJKoZIhvcNAQkOMSswKTAnBgNVHREE
IDAegRwqLmN1c3RvbWVycy5BQ2VkdWNhdGlvbi5pbmZvMA0GCSqGSIb3DQEBCwUA
A4IBAQB0LuSyTOudJa78YBRuuywywW/Jks/0LfvOHLlW0Jvy/OGP++JfAC6UHkBP
KT/hvXMYW1qQwgXWLGdIZ+/poNEzdEmF6xNRs7jL9AXOwLylMrX3FQMwvHyuqB1M
/uQHHAkggRsIBSoZilMDV0Qmpj9dP1kEZejN0COUYUkOC/r/1ONybugeqK5gjit1
nuCJpvmJnRH5P7t8F9ac3qsvpSZg3UuwPwEtbdDONS8pg9UZTgr/XIaRkbOPsbHn
2YTzmxuLk66bhJ53p0zKlQh0ugZWV19HvsbBbaEcURSidJ42/xxX4bVMc1iUcEh4
09eISkXpMvNUjdM4EzEgIWNNNIE5
-----END CERTIFICATE REQUEST-----
```

GENERATE NEW PRIVATE KEY AND SELF-SIGNED CERTIFICATE

Private Key Size	2048 ▼
Private key pass-phrase *(optional)*	••••••

Press the "Generate Private Key" button to create new private key.
Press the "Generate Self-Signed Certificate" button to create self-signed certificate.
Note that the certificate will use the subject name configured in "Certificate Signing Request" box.
Important: generation of private key is a lengthy operation during which the device service may be affected.

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

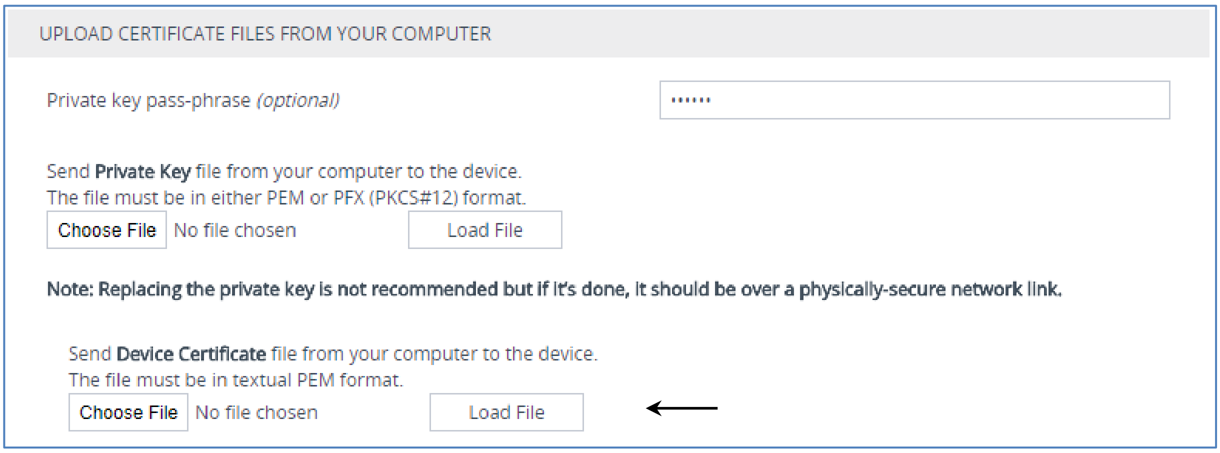
5. Send *certreq.txt* file to the Certified Authority Administrator for signing.

6. 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:

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



UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase *(optional)* ••••••

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

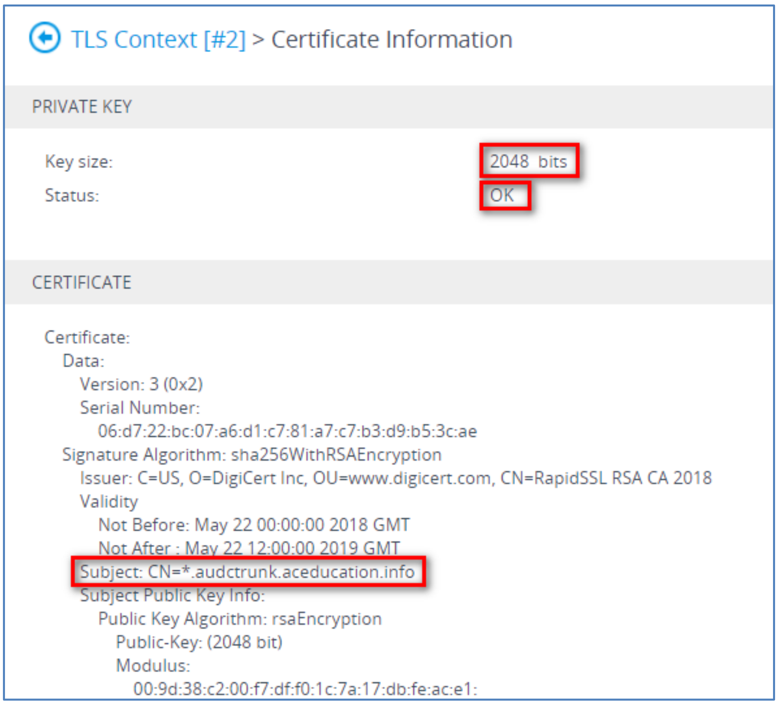
Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.

7. 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.

8. 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



TLS Context [#2] > Certificate Information

PRIVATE KEY

Key size: 2048 bits

Status: OK

CERTIFICATE

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      06:d7:22:bc:07:a6:d1:c7:81:a7:c7:b3:d9:b5:3c:ae
  Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL RSA CA 2018
    Validity
      Not Before: May 22 00:00:00 2018 GMT
      Not After : May 22 12:00:00 2019 GMT
    Subject: CN=*.audctrunk.aceducation.info
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
          00:9d:38:c2:00:f7:df:f0:1c:7a:17:db:fe:ac:e1:
```

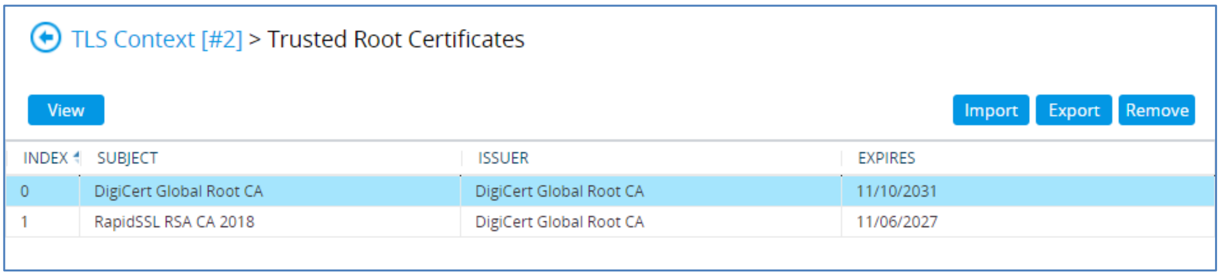
9. In the SBC's Web interface, return to the **TLS Contexts** page.

c. 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.

d. Click the **Import** button, and then select all Root/Intermediate Certificates obtained from your Certification Authority to load.

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

Figure 2-21: Example of Configured Trusted Root Certificates



INDEX	SUBJECT	ISSUER	EXPIRES
0	DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031
1	RapidSSL RSA CA 2018	DigiCert Global Root CA	11/06/2027

11. Reset the SBC with a burn to flash for your settings to take effect.

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

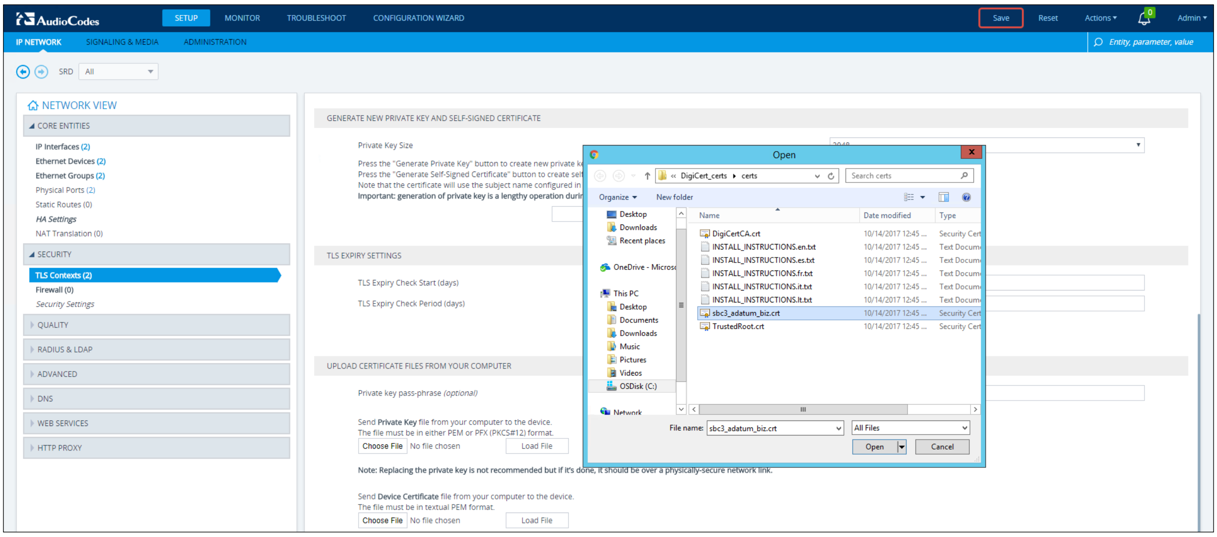
After receiving the certificates from the Certification Authority, install the

- SBC certificate
- Root / Intermediate certificates

➢ To install the SBC certificate:

1. Open the Change Certificate page (**Setup** > **IP Network** > **Security** > **TLS Contexts** > **Direct Connect** > **Change Certificate**.
2. Under 'Upload Certificate Files From Your Computer', click **Choose File** below 'Device Certificate' and then select the SBC certificate file obtained from your Certification Authority.

Figure 2-22: Uploading the Certificate Obtained from the Certification Authority



GENERATE NEW PRIVATE KEY AND SELF-SIGNED CERTIFICATE

Private Key Size: 2048

Press the "Generate Private Key" button to create new private ke
Press the "Generate Self-Signed Certificate" button to create self
Note that the certificate will use the subject name configured in
Important: generation of private key is a lengthy operation durir

TLS EXPIRY SETTINGS

TLS Expiry Check Start (days)

TLS Expiry Check Period (days)

UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase *(optional)*

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.
Choose File No file chosen

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

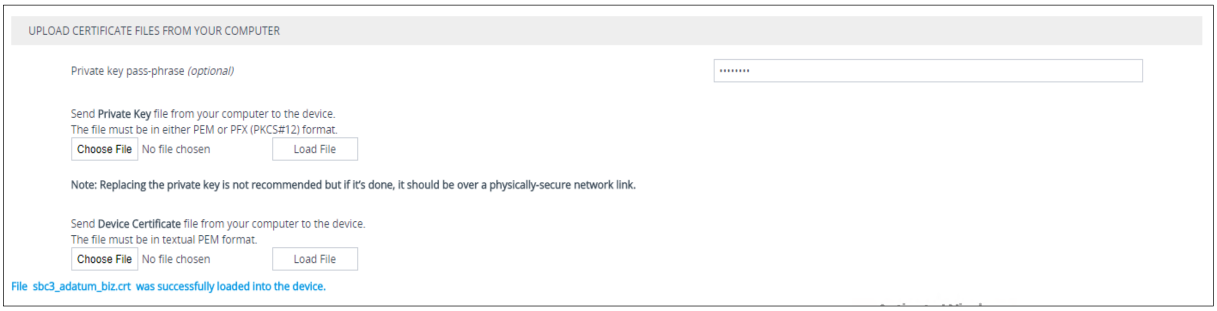
Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.
Choose File No file chosen

Name	Date modified	Type
DigiCertCA.crt	10/14/2017 12:45 ...	Security Cert
INSTALL_INSTRUCTIONS.en.txt	10/14/2017 12:45 ...	Text Docum
INSTALL_INSTRUCTIONS.es.txt	10/14/2017 12:45 ...	Text Docum
INSTALL_INSTRUCTIONS.fr.txt	10/14/2017 12:45 ...	Text Docum
INSTALL_INSTRUCTIONS.it.txt	10/14/2017 12:45 ...	Text Docum
INSTALL_INSTRUCTIONS.lt.txt	10/14/2017 12:45 ...	Text Docum
sbc3_adatum_biz.crt	10/14/2017 12:45 ...	Security Cert
TrustedRoot.crt	10/14/2017 12:45 ...	Security Cert

File name: sbc3_adatum_biz.crt

a. Validate that the certificate was uploaded correctly: A message indicating that the certificate was uploaded successfully is displayed lowermost in the page.

Figure 2-23: Message Indicating Successful Upload of the Certificate



UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase *(optional)*: ••••••••

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

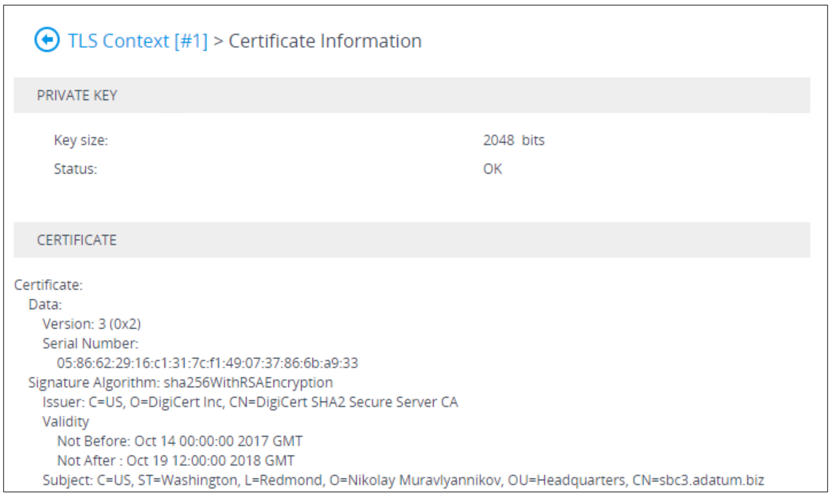
Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.

File sbc3_adatum_biz.crt was successfully loaded into the device.

b. Go to **Setup** > **IP Network** > **Security** > **TLS Contexts** > **Direct Connect** > **Certificate Information** and then validate the certificate Subject Name.

Figure 2-24: Certificate Information



TLS Context [#1] > Certificate Information

PRIVATE KEY

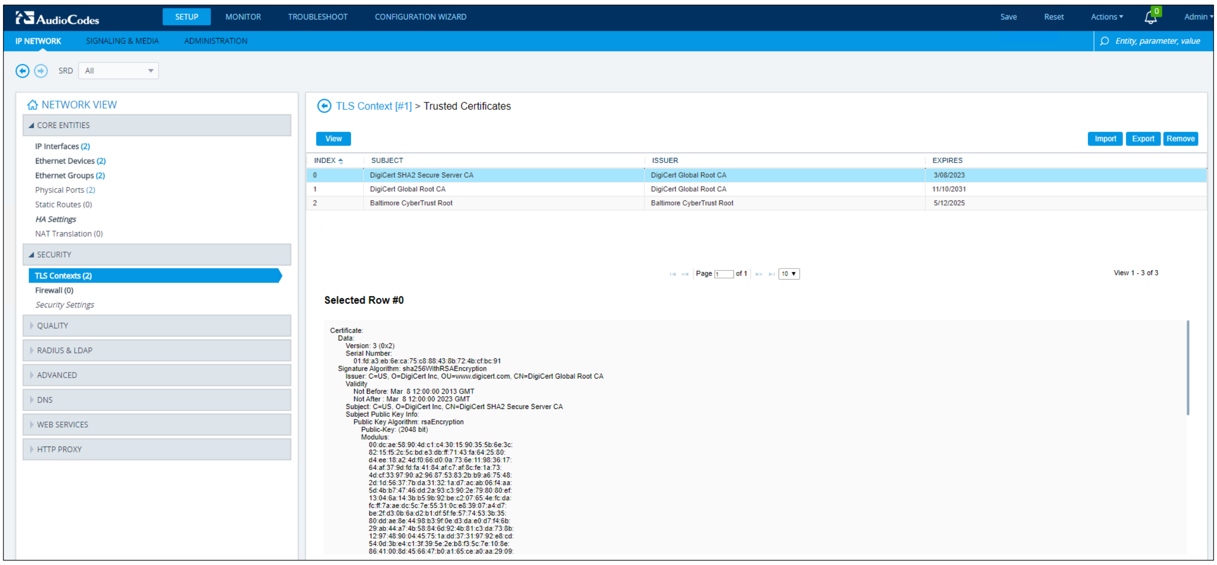
Key size:	2048 bits
Status:	OK

CERTIFICATE

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      05:86:62:29:16:c1:31:7c:f1:49:07:37:86:6b:a9:33
  Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
    Validity
      Not Before: Oct 14 00:00:00 2017 GMT
      Not After : Oct 19 12:00:00 2018 GMT
    Subject: C=US, ST=Washington, L=Redmond, O=Nikolay Muravlyannikov, OU=Headquarters, CN=sbc3.adatum.biz
```

3. To install the root and the intermediate certificate, go to **Setup** > **IP Network** > **Security** > **TLS Contexts** > **Direct Connect** > **Trusted Root Certificates** and then click **Import** and upload all root and intermediate certificates obtained from your Certification Authority.

Figure 2-25: Configured Trusted Certificates Page



TLS Context [#1] > Trusted Certificates

INDEX	SUBJECT	ISSUER	EXPIRES
0	DigiCert SHA2 Secure Server CA	DigiCert Global Root CA	3/08/2023
1	DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031
2	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025

Page 1 of 1 10 ▼ View 1 - 3 of 3

Selected Row #0

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      01:fd:a3:eb:6e:ca:75:c8:88:43:8b:72:4b:cf:bc:91
  Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA
    Validity
      Not Before: Mar  8 12:00:00 2013 GMT
      Not After : Mar  8 12:00:00 2023 GMT
    Subject: C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
          00:dc:ae:58:90:4d:c1:c4:30:15:90:35:5b:6e:3c:
          82:15:f5:2c:5c:bd:e3:db:ff:71:43:fa:64:25:80:
          d4:ee:18:a2:4d:f0:66:d0:0a:73:6e:11:98:36:17:
          64:af:37:9d:fd:fa:41:84:af:c7:af:8c:fe:1a:73:
          4d:cf:33:97:90:a2:96:87:53:83:2b:b9:a6:75:48:
          2d:1d:56:37:7b:da:31:32:1a:d7:ac:ab:06:f4:aa:
          5d:4b:b7:47:46:dd:2a:93:c3:90:2e:79:80:80:ef:
          13:04:6a:14:3b:b5:9b:92:be:c2:07:65:4e:fc:da:
          fc:ff:7a:ae:dc:5c:7e:55:31:0c:e8:39:07:a4:d7:
          be:2f:d3:0b:6a:d2:b1:df:5f:fe:57:74:53:3b:35:
          80:dd:ae:8e:44:98:b3:9f:0e:d3:da:e0:d7:f4:6b:
          29:ab:44:a7:4b:58:84:6d:92:4b:81:c3:da:73:8b:
          12:97:48:90:04:45:75:1a:dd:37:31:97:92:e8:cd:
          54:0d:3b:e4:c1:3f:39:5e:2e:b8:f3:5c:7e:10:8e:
          86:41:00:8d:45:66:47:b0:a1:65:ce:a0:aa:29:09:
```

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 **Setup** > **IP Network** > **Security** > **TLS Contexts** > **Direct Connect** > **Change Certificate**.
2. Enter the password assigned during export with the DigiCert utility in the 'Private key pass-phrase' field.
3. Under 'Upload Certificate Files From Your Computer', click **Choose File** from under 'Private Key' and then select the SBC certificate file exported from the DigiCert utility.

2.8 Deploy Baltimore Trusted Root Certificate

The DNS name of the Microsoft 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.

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'.

2.9 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

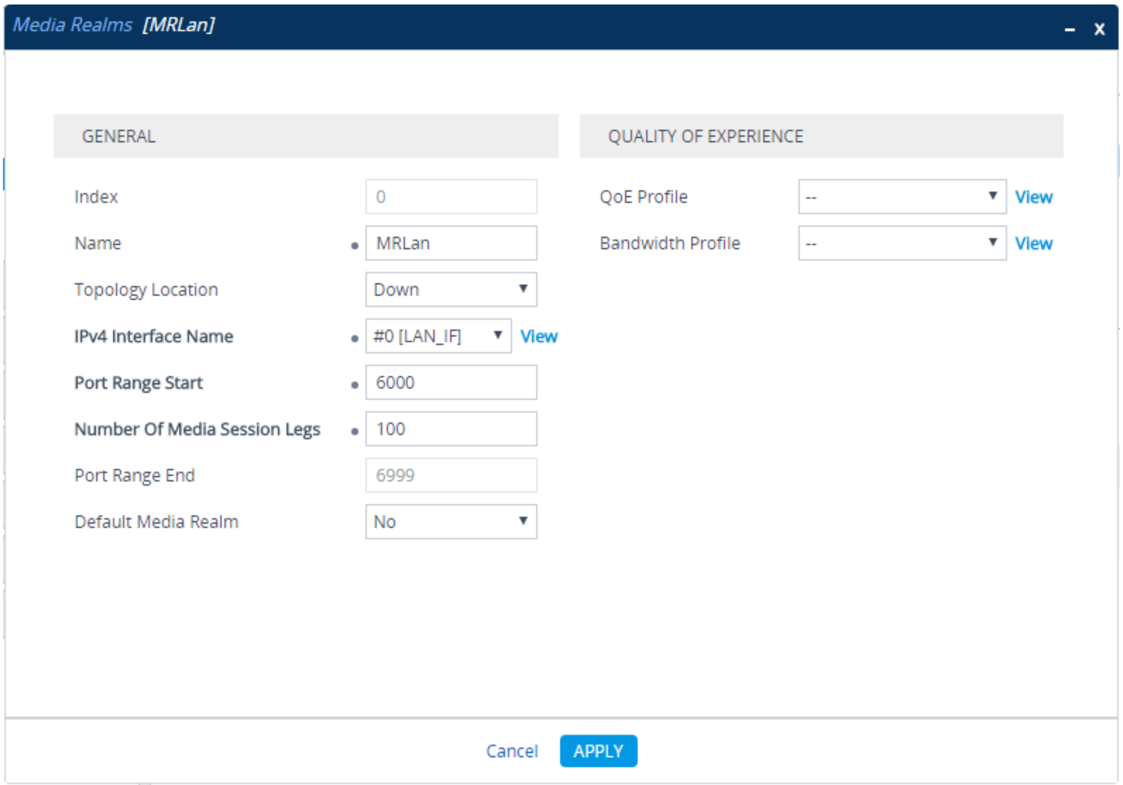
➢ **To configure Media Realms:**

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:

Parameter	Value

Index	**0**
Name	**MRLan** (descriptive name)
IPv4 Interface Name	**LAN_IF**
Port Range Start	**6000** (represents lowest UDP port number used for media on LAN)
Number of Media Session Legs	**100** (media sessions assigned with port range)

Figure 2-26: Configuring Media Realm for LAN

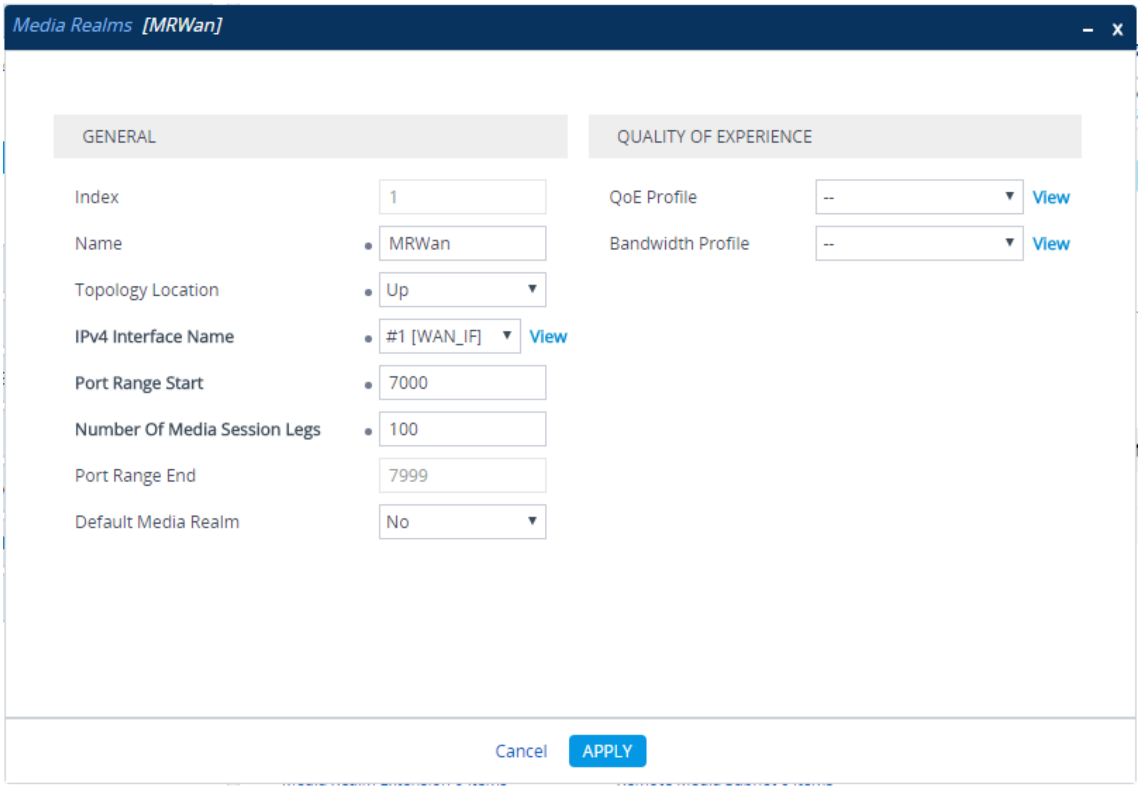


Index	0
Name	MRLan
Topology Location	Down
IPv4 Interface Name	#0 [LAN_IF]
Port Range Start	6000
Number Of Media Session Legs	100
Port Range End	6999
Default Media Realm	No
QoE Profile	--
Bandwidth Profile	--

3. Configure a Media Realm for WAN traffic:

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

Figure 2-27: Configuring Media Realm for WAN



Media Realms [MRWan]

GENERAL

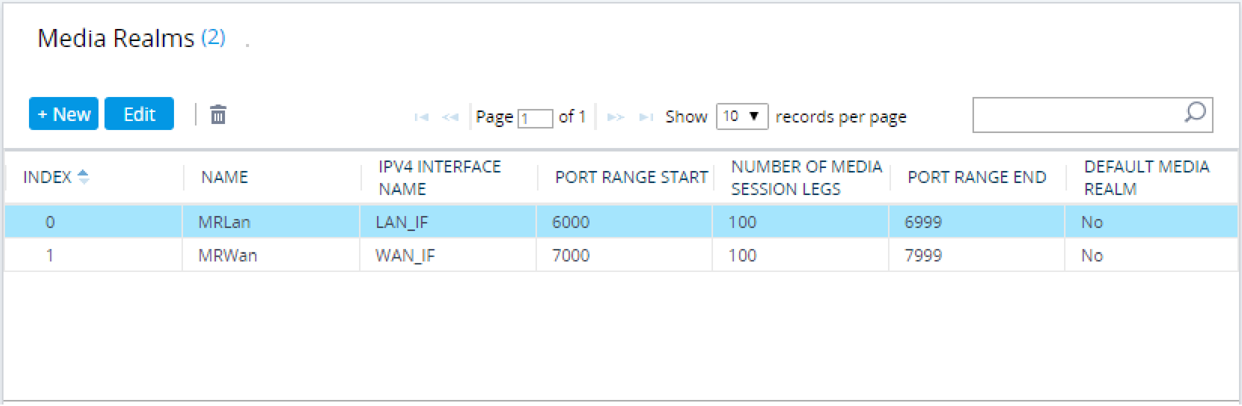
Index	1
Name	MRWan
Topology Location	Up
IPv4 Interface Name	#1 [WAN_IF]
Port Range Start	7000
Number Of Media Session Legs	100
Port Range End	7999
Default Media Realm	No

QUALITY OF EXPERIENCE

QoE Profile	--
Bandwidth Profile	--

The configured Media Realms are shown in the figure below:

Figure 2-28: Configured Media Realms in Media Realm Table



Media Realms (2)

INDEX	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	MRLan	LAN_IF	6000	100	6999	No
1	MRWan	WAN_IF	7000	100	7999	No

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.

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

Table 2-6: Configuration Example: Teams SIP Interface

Parameter	Value
Index	**1**
Name	**Teams** (arbitrary descriptive name)
Network Interface	**WAN_IF**
Application Type	**SBC**
UDP and TCP Port	**0**
TLS Port	**5061** (as configured in the Office 365)
Enable TCP Keepalive	**Enable**
Classification Failure Response Type	**0** (Recommended to prevent DoS attacks)
Call Setup Rules Set ID	**2**
Media Realm	**MRWan**
TLS Context Name	**Teams**

Note:

- All other parameters can be left unchanged at their default values.
- 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 Sets (per Tenant)

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 Microsoft 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 Direct Routing Service.
3. Add a Proxy Set (***per each Tenant***) for the Microsoft Teams Direct Routing as shown below:

Parameter	Value
Index	**2**
Name	**Teams-Tenant-1** (arbitrary descriptive name)
SBC IPv4 SIP Interface	**Teams**
TLS Context Name	**Teams**
Proxy Keep-Alive	**Using Options**
Proxy Hot Swap	**Enable**
Proxy Load Balancing Method	**Random Weights**
DNS Resolve Method	**SRV**

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

Following table shows an example of the configuration. You can change parameters according to requirements.

Table 2-7: Configuration Example: Proxy Set - Teams - Global FQDNs

ID	Name	SBC IPv4 SIP Interface	Proxy Keep Alive	Proxy Hot Swap	Proxy Load Balancing Method	DNS Resolve Method
1	SIP Trunk	SIPTrunk	Using OPTIONS	Enable		
2	Teams-Tenant-1	Teams	Using OPTIONS	Enable	Random Weights	SRV
3	Teams-Tenant-2	Teams	Using OPTIONS	Enable	Random Weights	SRV
4	Teams-Tenant-3	Teams	Using OPTIONS	Enable	Random Weights	SRV

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

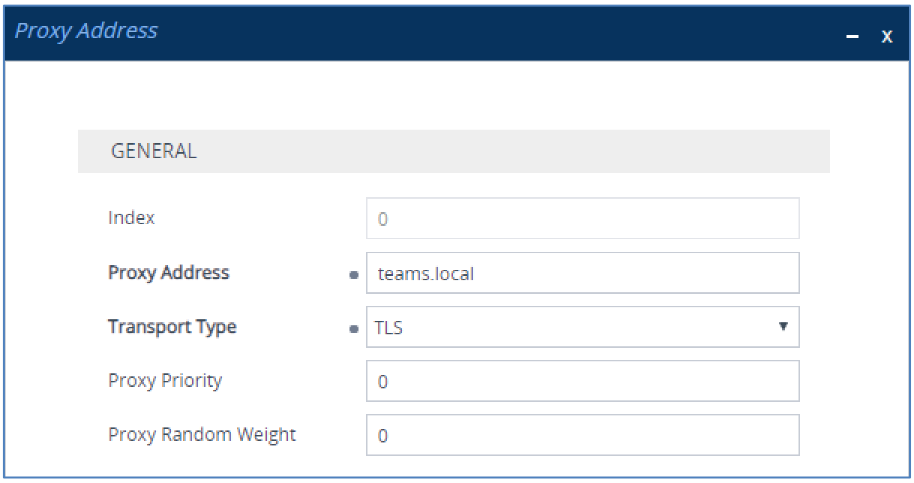
2.11.2 Configure a Proxy Address

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:

Figure 2-29: Configuring Proxy Address for Microsoft Teams Direct Routing Interface



Index	0
Proxy Address ●	teams.local
Transport Type ●	TLS ▾
Proxy Priority	0
Proxy Random Weight	0

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

Table 2-8: Configuration Example: Proxy Address

Parameter	Value
Index	**0**
Name	**teams.local**
Transport Type	**TLS**

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

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

Note: Proxy Address must be configured for the SIP Trunk Proxy Set too.

2.12 Configure the Internal SRV Table

The Internal SRV table resolves host names to DNS A-Records. Three different A-Records can be assigned to each host name, where each A-Record contains the host name, priority, weight, and port.

➢ **To configure the internal SRV Table:**

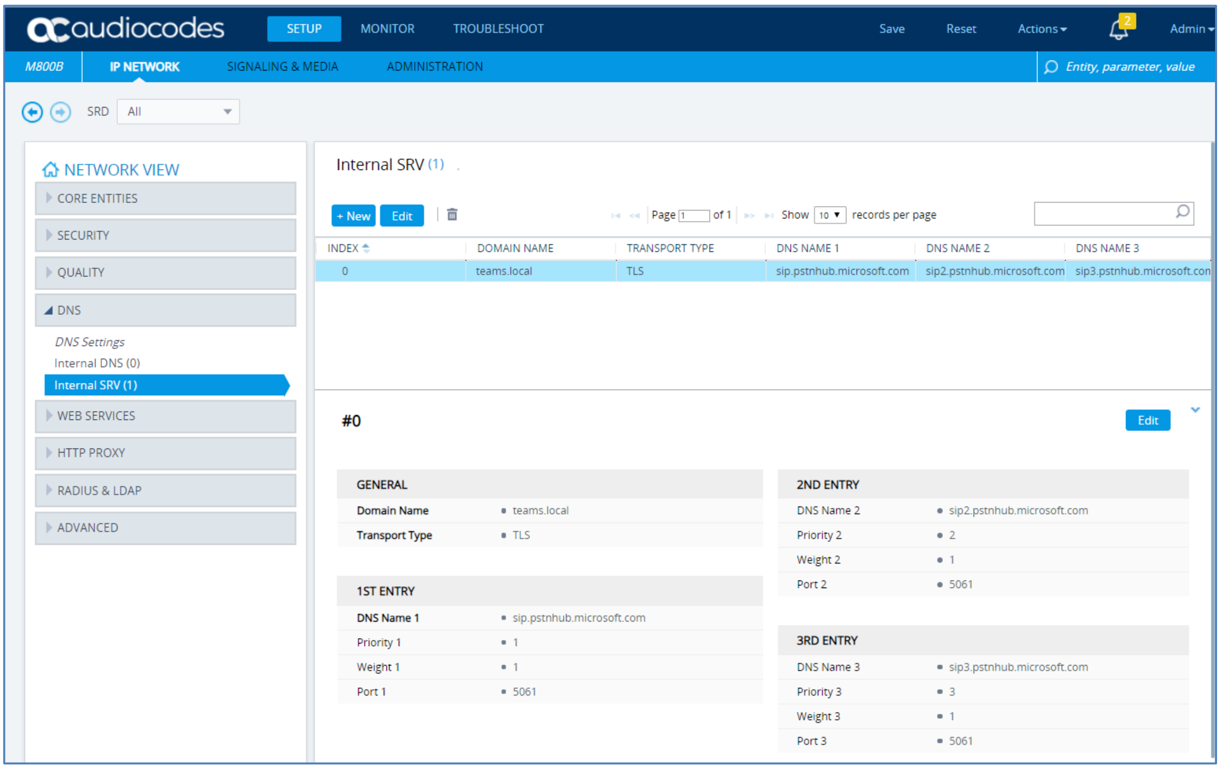
1. Open the Internal SRV table (**Setup** menu > **IP Network** tab > **DNS** folder > **Internal SRV**).
2. Click **+New** to add the SRV record for **teams.local** and use the table below as configuration reference.

Table 2-9: Configuration Example: Internal SRV Table

Parameter	Value
Domain Name	**teams.local** (FQDN is case-sensitive; configure in line with the configuration of the Teams Proxy Set)
Transport Type	**TLS**
1st ENTRY	
DNS Name 1	**sip.pstnhub.microsoft.com**
Priority 1	**1**
Weight 1	**1**
Port 1	**5061**
2nd ENTRY	
DNS Name 2	**sip2.pstnhub.microsoft.com**
Priority 2	**2**
Weight 2	**1**
Port 2	**5061**
3rd ENTRY	
DNS Name 3	**sip3.pstnhub.microsoft.com**
Priority 3	**3**
Weight 3	**1**
Port 3	**5061**

Use the figure below as reference.

Figure 2-30: Configured Internal SRV Table



Internal SRV (1)

INDEX	DOMAIN NAME	TRANSPORT TYPE	DNS NAME 1	DNS NAME 2	DNS NAME 3
0	teams.local	TLS	sip.pstnhub.microsoft.com	sip2.pstnhub.microsoft.com	sip3.pstnhub.microsoft.con

#0

GENERAL

Domain Name	teams.local
Transport Type	TLS

1ST ENTRY

DNS Name 1	sip.pstnhub.microsoft.com
Priority 1	1
Weight 1	1
Port 1	5061

2ND ENTRY

DNS Name 2	sip2.pstnhub.microsoft.com
Priority 2	2
Weight 2	1
Port 2	5061

3RD ENTRY

DNS Name 3	sip3.pstnhub.microsoft.com
Priority 3	3
Weight 3	1
Port 3	5061

2.13 Configure the Dial Plan Table (Customer DID Only)

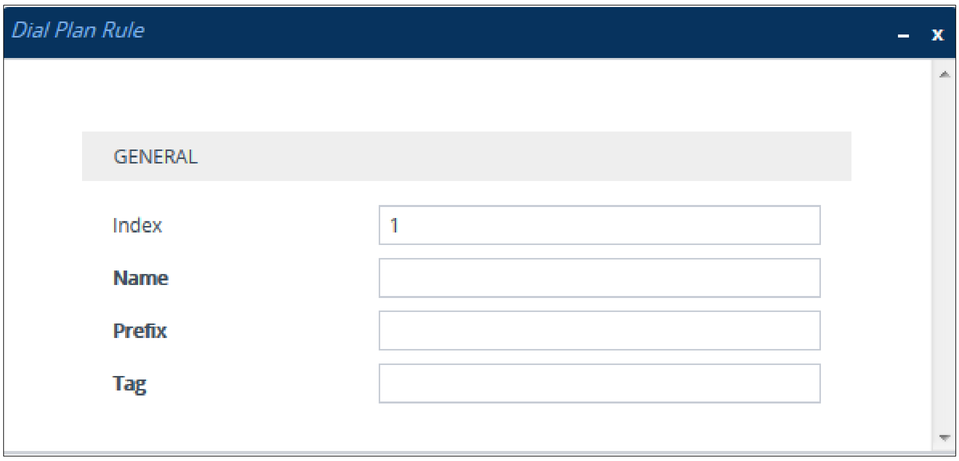
For deployments requiring hundreds of routing rules (which may exceed the maximum number of rules that can be configured in the IP-to-IP Routing table), you can employ tags to represent the many different calling (source URI user name) and called (destination URI user name) prefix numbers in your routing 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 2-31: Dial Plan Rule Table - Add Dialog Box



Dial Plan Rule

GENERAL

Index: 1

Name:

Prefix:

Tag:

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

Table 2-10: Dial Plan Teams Tenants

Name	Prefix	Tag
Enterprise1	+1909xxxxx	Tenant1
Enterprise2	+1709xxxxx	Tenant2
Enterprise3	+1809xxxxx	Tenant3

7. Click **Apply** and then save your settings to flash memory.

2.14 Configuring Call Setup Rules

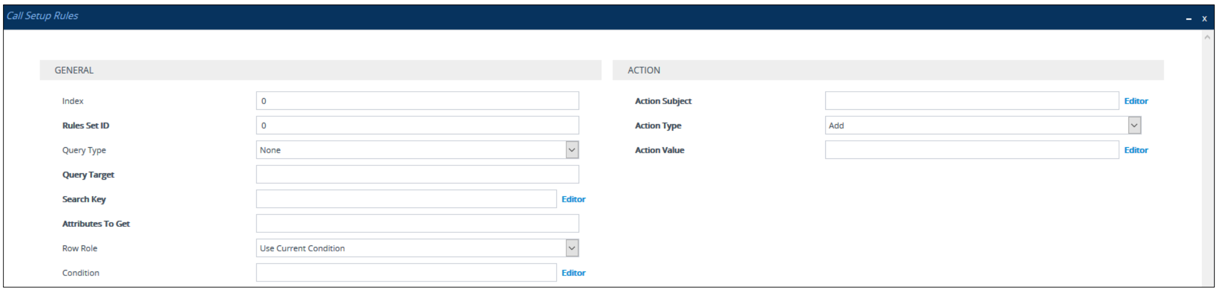
This section describes how to configure Call Setup Rules. Call Setup rules define various sequences that are run upon receipt of an incoming call (dialog) at call setup, before the device routes the call to its destination.

2.14.1 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:

Figure 2-32: Call Setup Rules Table - Add Dialog Box



Call Setup Rules

GENERAL

Index: 0
Rules Set ID: 0
Query Type: None
Query Target:
Search Key: Editor
Attributes To Get:
Row Role: Use Current Condition
Condition: Editor

ACTION

Action Subject: Editor
Action Type: Add
Action Value: Editor

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

Table 2-11: Call Setup Rules Table

Index	Rules Set ID	Query Type	Query Target	Search Key	Condition	Action Subject	Action Type	Action Value
0	0				var.session.0 == ''	var.session.0	Modify	Param.IPG.Src.Tags.Tenant
1	0					DstTags.Tenant	Modify	‘SIPTrunk’
2	1	Dial Plan	TeamsTenants	Param.Call.Dst.User	var.session.0 == ''	var.session.0	Modify	DialPlan.Result
3	1				var.session.0 != ''	DstTags.Tenant	Modify	Var.Session.0
4	2	Dial Plan	TeamsTenants	Param.Call.Src.User		SrcTags.Tenant	Modify	DialPlan.Result
5	2	Dial Plan	TeamsTenants	Header.P-Asserted-Identity.URL.User	DialPlan.Found exists	SrcTags.Tenant	Modify	DialPlan.Result

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

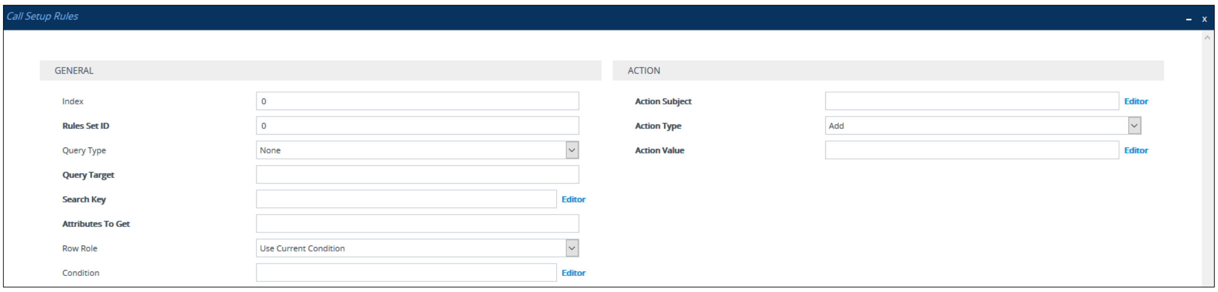
Note: Make sure that “ForwardPai” is set to “True” using Get-CsOnlinePSTNGateway

2.14.2 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 2-33: Call Setup Rules Table - Add Dialog Box



Call Setup Rules

GENERAL

Index	0
Rules Set ID	0
Query Type	None
Query Target	
Search Key	
Attributes To Get	
Row Role	Use Current Condition
Condition	

ACTION

Action Subject	
Action Type	Add
Action Value	

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

Table 2-12: Call Setup Rules Table

Index	Rules Set ID	Condition	Action Subject	Action Type	Action Value
0	0	var.session.0 == ''	var.session.0	Modify	Param.IPG.Src.Tags.Tenant
1	0		DstTags.Tenant	Modify	'SIPTrunk'
2	1	var.session.0 == ''	var.session.0	Modify	Header.Request-URI.URL.Host
3	1	var.session.0 != ''	DstTags.Tenant	Modify	Var.Session.0
4	2		SrcTags.Tenant	Modify	Header.Request-URI.URL.Host

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

2.15 Configure a Coder Group

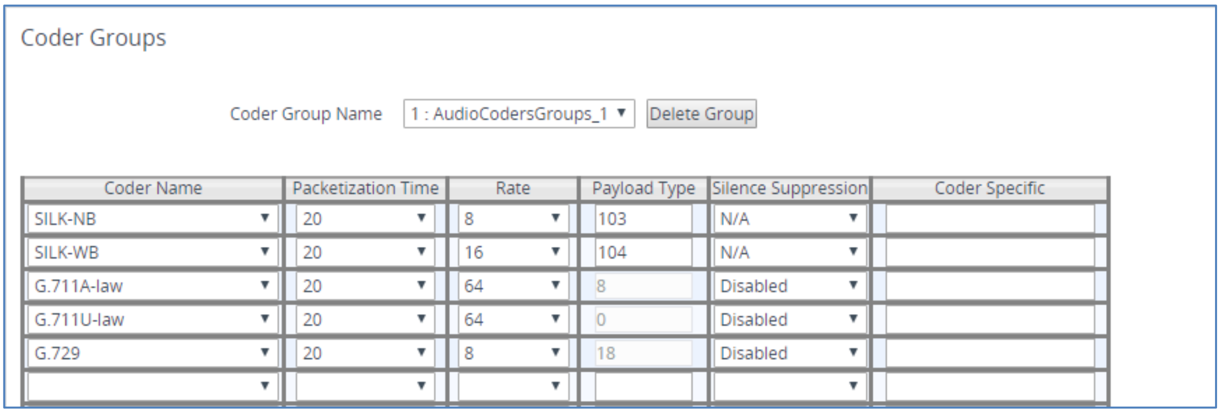
This section describes how to configure coders (termed *Coder Group*). As Microsoft Teams Direct Routing supports the SILK and OPUS coders while the network connection to the SIP Trunk may restrict operation with a dedicated coders list, you need to add a Coder Group with the supported coders for each leg, the Microsoft 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 2-34: Configuring Coder Group for Microsoft Teams Direct Routing



Coder Groups

Coder Group Name: 1 : AudioCodersGroups_1

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
SILK-NB	20	8	103	N/A	
SILK-WB	20	16	104	N/A	
G.711A-law	20	64	8	Disabled	
G.711U-law	20	64	0	Disabled	
G.729	20	8	18	Disabled	

3. Click **Apply** and confirm the configuration change in the prompt that pops up.

2.16 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 2-13: Configuration Example: Teams IP Profile

Parameter	Value
General	
Name	**Teams** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**SRTP**
SBC Early Media	
Remote Early Media RTP Detection Mode	**By Media** (required, as Microsoft Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18x response)
SBC Media	
Extension Coders Group	**AudioCodersGroups_1**
ICE Mode	**Lite** (required only when Media Bypass enabled on Microsoft Teams)
SBC Signaling	
Remote Update Support	**Not Supported**
Remote re-INVITE Support	**Supported Only With SDP**
Remote Delayed Offer Support	**Not Supported**
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally**
Remote 3xx Mode	**Handle Locally**
SBC Hold	
Remote Hold Format	**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)

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

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

Table 2-14: Configuration Example: SIP Trunk IP Profile

Parameter	Value
General	
Name	**SIPTrunk** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**RTP**
SBC Signaling	
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally**
Remote Replaces Mode	**Handle Locally**
Remote 3xx Mode	**Handle Locally**

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

2.17 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 2-15: Configuration Example: IP Group - Teams Global FQDNs

Ind	IP Group Name	Media Realm	Classify by ProxySet	Proxy Set ID	Local Host Name	Call Setup Rules Set ID	Tags	Always Use Src Address	IP Profile	Proxy Keep-Alive using IP Group settings
0	Not Used									
1	SIP Trunk	MRLan	Enable	SIPTrunk		1	Tenant=SIPTrunk		SIPTrunk	
2	Teams-Tenant-1 (arbitrary descriptive name)	MRWan	Disable	Teams-Tenant-1	<FQDN name of your tenant in SBC>. For example, sbc1.customers.ACeducation.info	0	Tenant=Tenant1 or Tenant=sbc1.customers.ACeducation.info	Yes	Teams	Enable
3	Teams-Tenant-2	MRWan	Disable	Teams-Tenant-2	<FQDN name of your tenant in SBC>. For example, sbc2.customers.ACeducation.info	0	Tenant=Tenant2 or Tenant=sbc2.customers.ACeducation.info	Yes	Teams	Enable
4	Teams-Tenant-3	MRWan	Disable	Teams-Tenant-3	<FQDN name of your tenant in SBC>. For example, sbc3.customers.ACeducation.info	0	Tenant=Tenant3 or Tenant=sbc3.customers.ACeducation.info	Yes	Teams	Enable

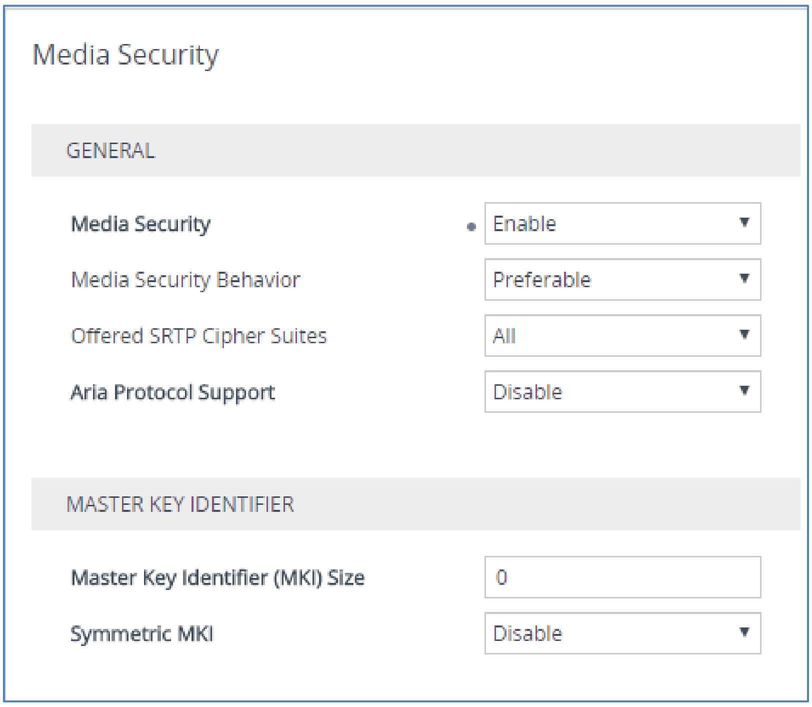
2.18 Configure SRTP

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: Configured Media Security Parameter



Media Security

GENERAL

Media Security: Enable

Media Security Behavior: Preferable

Offered SRTP Cipher Suites: All

Aria Protocol Support: Disable

MASTER KEY IDENTIFIER

Master Key Identifier (MKI) Size: 0

Symmetric MKI: Disable

3. Click **Apply**.

2.19 Configuring Message Condition Rules

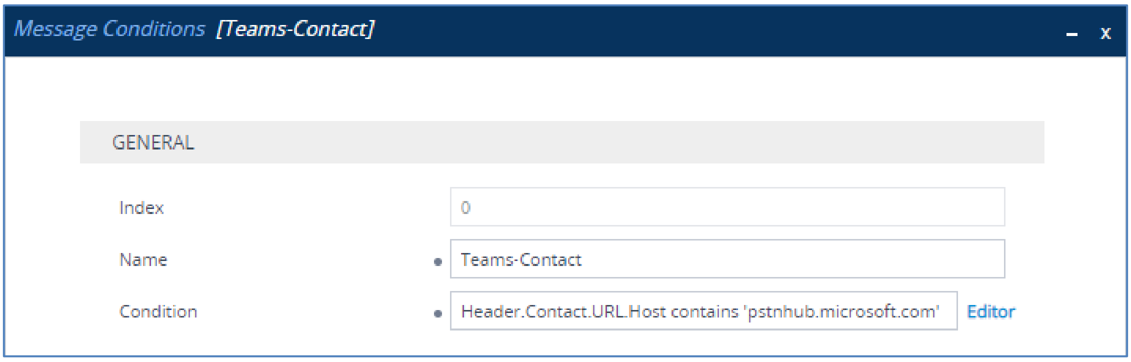
This section describes how to configure the Message Condition Rules. A Message Condition defines special conditions (pre-requisites) for incoming SIP messages. These rules can be used as additional matching criteria for the IP-to-IP routing rules in the IP-to-IP Routing table.

➢ **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:

Parameter	Value
Index	**0**
Name	**Teams-Contact** (arbitrary descriptive name)
Condition	**Header.Contact.URL.Host contains 'pstnhub.microsoft.com'**

Figure 2-36: Configuring Condition Table



Message Conditions [Teams-Contact]

GENERAL

Index: 0

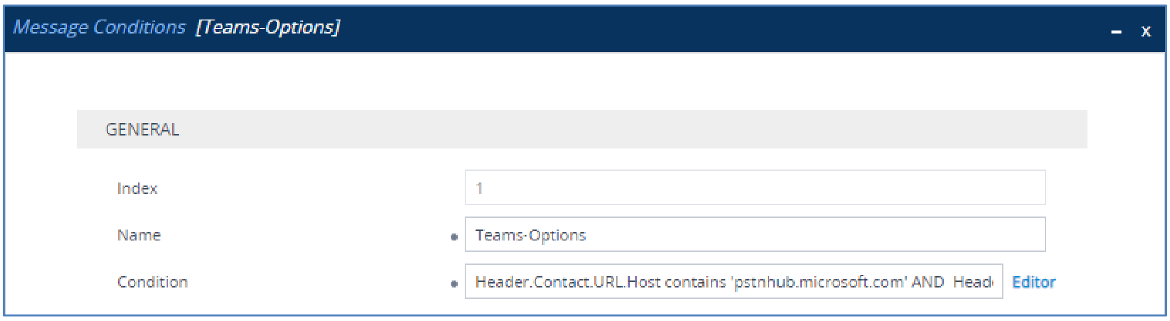
Name: Teams-Contact

Condition: Header.Contact.URL.Host contains 'pstnhub.microsoft.com'

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

Parameter	Value
Index	**1**
Name	**Teams-Options** (arbitrary descriptive name)
Condition	**Header.Contact.URL.Host contains 'pstnhub.microsoft.com' AND Header.Request-URI.MethodType == ‘8’**

Figure 2-37: Configuring Condition Table



Message Conditions [Teams-Options]

GENERAL

Index: 1

Name: Teams-Options

Condition: Header.Contact.URL.Host contains 'pstnhub.microsoft.com' AND Head

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

Index	Name	Source SIP Interface	Message Condition	IP Group Selection	Action Type	IP Group Tag Name	Source IP Group
1	Teams Options	Teams	Teams-Options	Source IP Group	Allow		<Choose Any Teams IP Group>
2	Teams	Teams	Teams-Contact	Tagged IP Group	Allow	Tenant	

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 Microsoft 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 Microsoft Teams Direct Routing or AudioCodes SBC SIP Trunk)

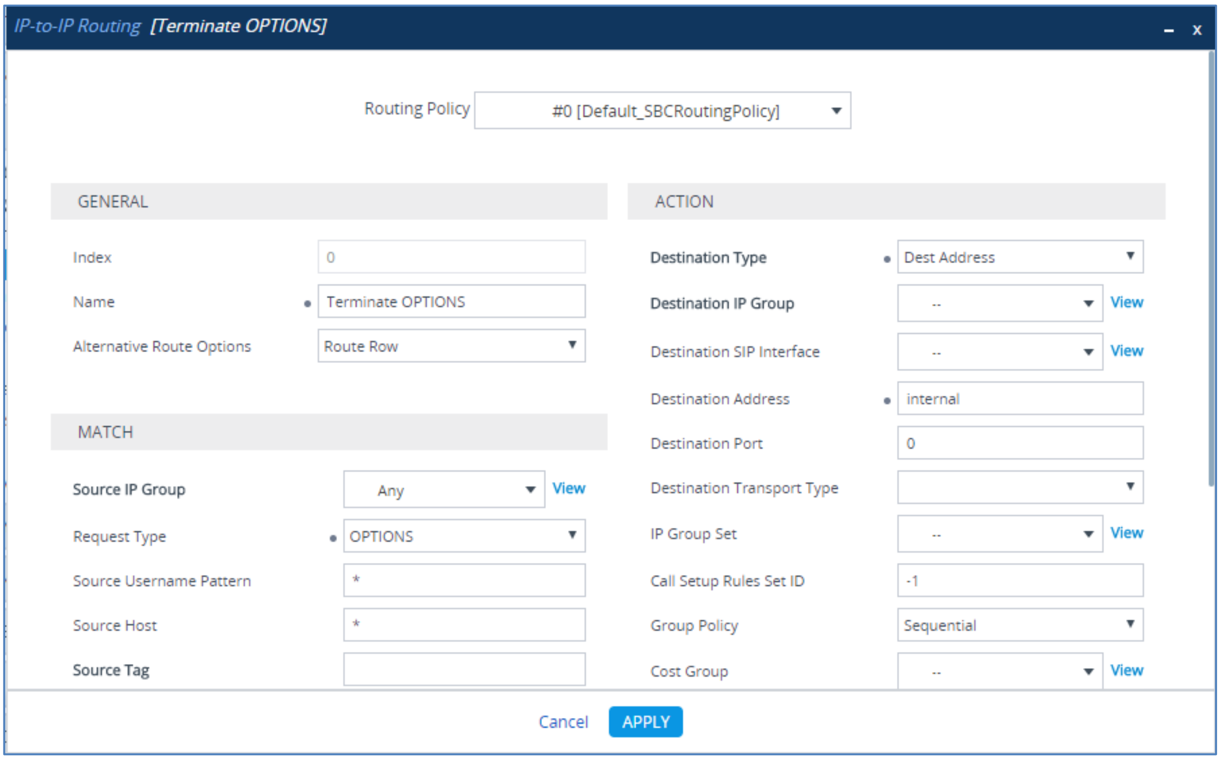
See AudioCodes' SBC documentation for more information on how to route in other scenarios.

➢ **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:

Parameter	Value
Index	**0**
Name	**Terminate OPTIONS** (arbitrary descriptive name)
Source IP Group	**Any**
Request Type	**OPTIONS**
Destination Type	**Dest Address**
Destination Address	**internal**

Figure 2-38: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS



IP-to-IP Routing [Terminate OPTIONS]

Routing Policy: #0 [Default_SBCRoutingPolicy]

GENERAL

Index	0
Name ●	Terminate OPTIONS
Alternative Route Options	Route Row

MATCH

Source IP Group	Any
Request Type ●	OPTIONS
Source Username Pattern	*
Source Host	*
Source Tag	

ACTION

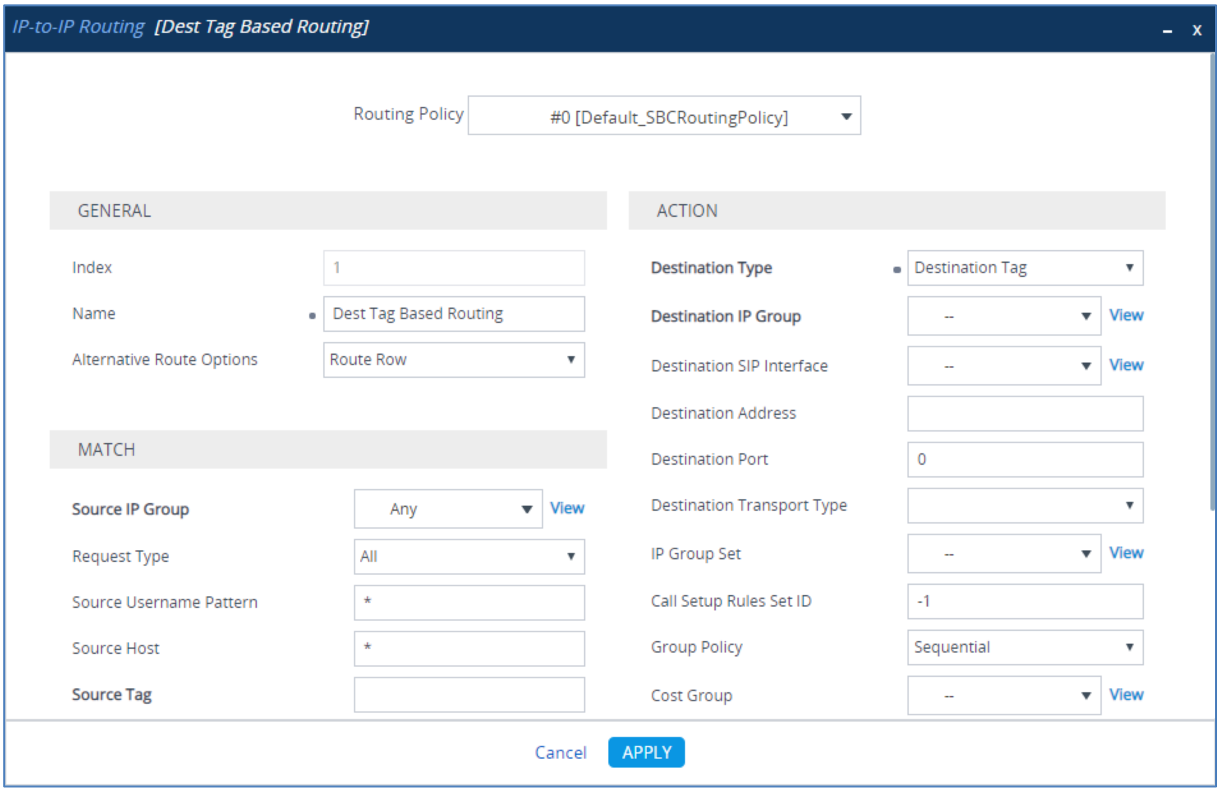
Destination Type ●	Dest Address
Destination IP Group	--
Destination SIP Interface	--
Destination Address ●	internal
Destination Port	0
Destination Transport Type	
IP Group Set	--
Call Setup Rules Set ID	-1
Group Policy	Sequential
Cost Group	--

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:

Parameter	Value
Index	**1**
Route Name	**Dest Tag Based Routing** (arbitrary descriptive name)
Source IP Group	**Any**
Destination Type	**Destination Tag**
Routing Tag Name	**Tenant**

Figure 2-39: Configuring IP-to-IP Routing Rule for Destination Tag Routing



IP-to-IP Routing [Dest Tag Based Routing]

Routing Policy: #0 [Default_SBCRoutingPolicy]

GENERAL

Index	1
Name	Dest Tag Based Routing
Alternative Route Options	Route Row

MATCH

Source IP Group	Any
Request Type	All
Source Username Pattern	*
Source Host	*
Source Tag	

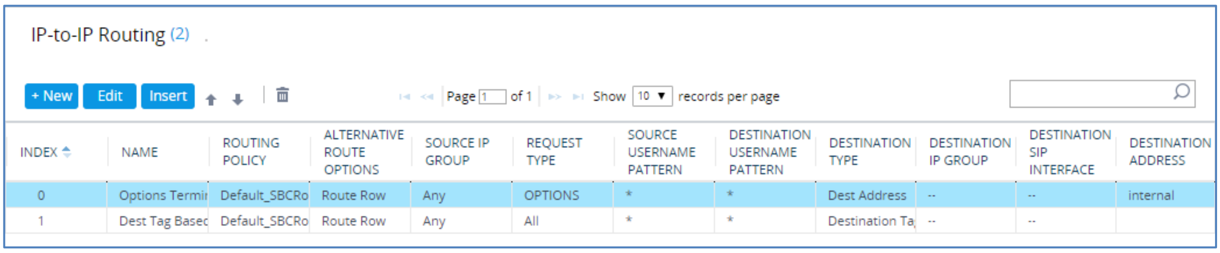
ACTION

Destination Type	Destination Tag
Destination IP Group	--
Destination SIP Interface	--
Destination Address	
Destination Port	0
Destination Transport Type	
IP Group Set	--
Call Setup Rules Set ID	-1
Group Policy	Sequential
Cost Group	--

   b. Click **Apply**.

The configured routing rules are shown in the figure below:

Figure 2-40: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	Options Termi	Default_SBCRo	Route Row	Any	OPTIONS	*	*	Dest Address	--	--	internal
1	Dest Tag Basec	Default_SBCRo	Route Row	Any	All	*	*	Destination Ta	--	--	

Note: The routing configuration may change according to your specific deployment topology.

2.22 Configuring an SBC to Suppress Call Line ID (Optional)

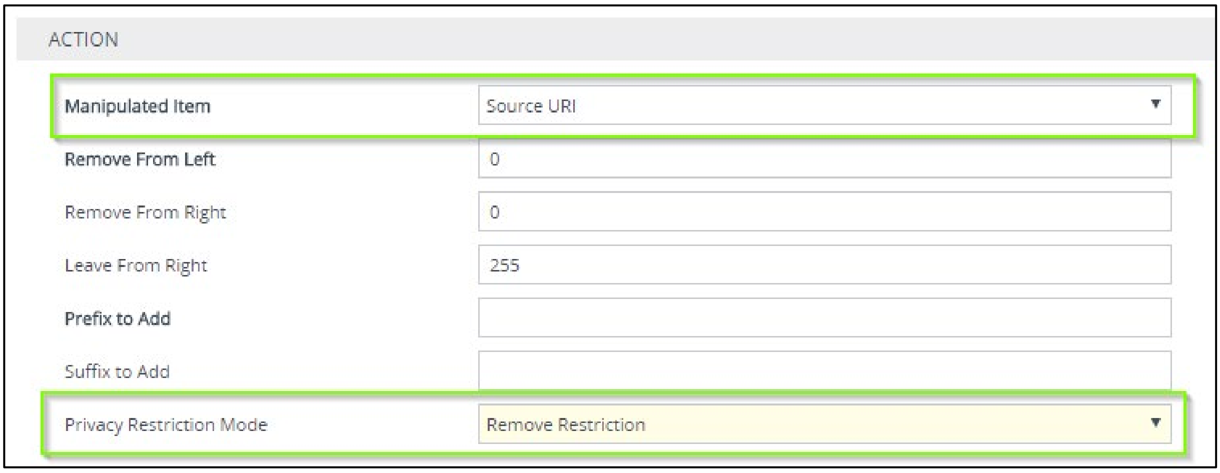
This section shows how to configure an SBC in two steps when Forward P-Asserted-Identity header is included with the Privacy ID header (the configuration is optional). This allows:

- 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.

Figure 2-41: Privacy Restriction Mode



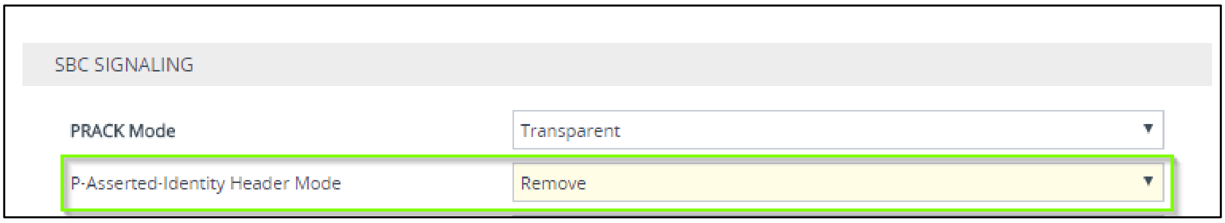
ACTION

Manipulated Item	Source URI
Remove From Left	0
Remove From Right	0
Leave From Right	255
Prefix to Add	
Suffix to Add	
Privacy Restriction Mode	Remove Restriction

➢ 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 2-42: P-Asserted-Identity Header Mode



SBC SIGNALING

PRACK Mode	Transparent
P-Asserted-Identity Header Mode	Remove

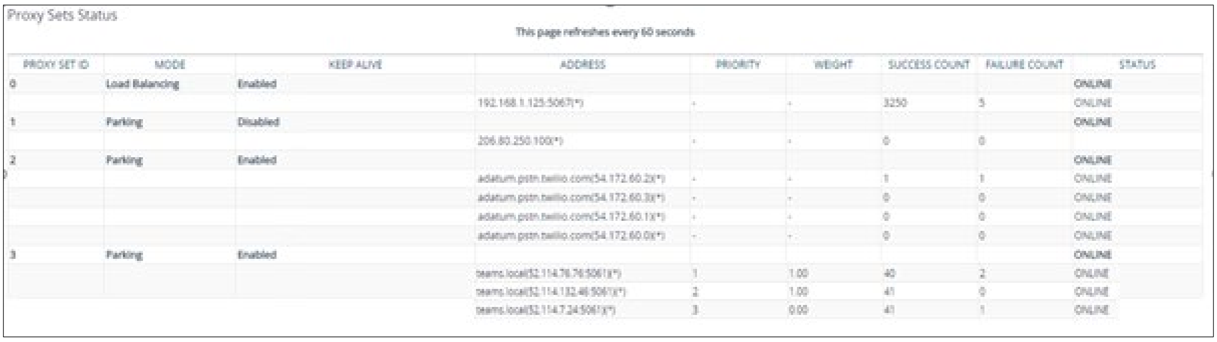
3 Verify the Pairing between the SBC and Direct Routing

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



Proxy Sets Status

This page refreshes every 60 seconds

PROXY SET ID	MODE	KEEP ALIVE	ADDRESS	PRIORITY	WEIGHT	SUCCESS COUNT	FAILURE COUNT	STATUS
0	Load Balancing	Enabled						ONLINE
			192.168.1.125:5067(*)	-	-	3250	5	ONLINE
1	Parking	Disabled						ONLINE
			206.80.250.100(*)	-	-	0	0	
2	Parking	Enabled						ONLINE
			adatum.pstn.twilio.com(54.172.60.2)(*)	-	-	1	1	ONLINE
			adatum.pstn.twilio.com(54.172.60.3)(*)	-	-	0	0	ONLINE
			adatum.pstn.twilio.com(54.172.60.1)(*)	-	-	0	0	ONLINE
			adatum.pstn.twilio.com(54.172.60.0)(*)	-	-	0	0	ONLINE
3	Parking	Enabled						ONLINE
			teams.local(52.114.76.76:5061)(*)	1	1.00	40	2	ONLINE
			teams.local(52.114.132.46:5061)(*)	2	1.00	41	0	ONLINE
			teams.local(52.114.7.24:5061)(*)	3	0.00	41	1	ONLINE

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, 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

proxy-set new
proxy-name <TBD-PrSet>  (e.g. "Teams-Tenant-1")
sbcipv4-sip-int-name "Teams"
proxy-enable-keep-alive using-options
proxy-load-balancing-method random-weights
is-proxy-hot-swap enable
dns-resolve-method srv
proxy-ip new
proxy-address "teams.local"
transport-type tls
exit
activate
exit

ip-group new
name <TBD-IPGroup> (e.g. Teams-Tenant-1)
proxy-set-name <TBD-PrSet> (e.g. Teams-Tenant-1)
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

exit
do write
```

A Syntax Requirements for SIP Messages 'INVITE' and 'OPTIONS'

The syntax of SIP messages must conform with Direct Routing requirements.

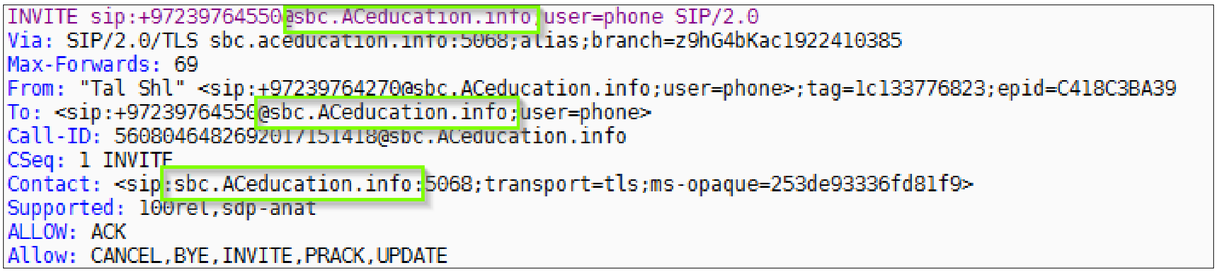
This section covers the high-level requirements for the SIP syntax used in 'INVITE' and 'OPTIONS' messages. You can use the information presented here as a first step when troubleshooting unsuccessful calls. AudioCodes has found that most issues are related to incorrect syntax in SIP messages.

A.1 Terminology

Recommended	Not required, but to simplify troubleshooting it's recommended to configure as shown in the examples below.
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:+97239764550@sbc.ACeducation.info;user=phone SIP/2.0
Via: SIP/2.0/TLS sbc.aceducation.info:5068;alias;branch=z9hG4bKac1922410385
Max-Forwards: 69
From: "Tal Shl" <sip:+97239764270@sbc.ACeducation.info;user=phone>;tag=1c133776823;epid=C418C3BA39
To: <sip:+97239764550@sbc.ACeducation.info;user=phone>
Call-ID: 5608046482692017151418@sbc.ACeducation.info
CSeq: 1 INVITE
Contact: <sip:sbc.ACeducation.info:5068;transport=tls;ms-opaque=253de93336fd81f9>
Supported: 100rel,sdp-anat
ALLOW: ACK
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>*

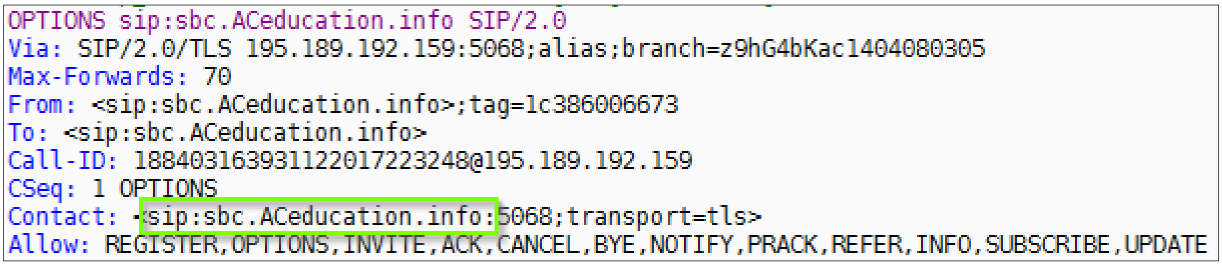
The table below shows where in the Web interface the parameters are configured and where in this document you can find the configuration instructions.

Table A-1: Syntax Requirements for an 'INVITE' Message

Parameter	Where configured	How to configure
Request-URI	Setup > Signaling and Media > Core Entities > IP Group> <Group Name> > SIP Group Name	See AudioCodes' *SIP Message Manipulation Reference Guide*.
To	Signaling and Media > Message Manipulations > Manipulation Set Note that the Manipulation Set must be applied to the Teams IP Group as an Outbound Message Manipulation Set.	See AudioCodes' *SIP Message Manipulation Reference Guide*.
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 2.17.

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 195.189.192.159:5068;alias;branch=z9hG4bKac1404080305
Max-Forwards: 70
From: <sip:sbc.ACeducation.info>;tag=1c386006673
To: <sip:sbc.ACeducation.info>
Call-ID: 188403163931122017223248@195.189.192.159
CSeq: 1 OPTIONS
Contact: <sip:sbc.ACeducation.info:5068;transport=tls>
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,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 A-2: Teams Direct Routing Interface - Technical Characteristics

Category	Parameter	Value	Comments
Ports and IP ranges	SIP Interface FQDN Name	See Microsoft's document *Deploying Direct Routing Guide.*	
	IP Addresses range for SIP interfaces	See Microsoft's document *Deploying Direct Routing Guide.*	
	SIP Port	5061	
	IP Address range for Media	See Microsoft's document *Deploying Direct Routing Guide.*	
	Media port range on Media Processors	See Microsoft's document *Deploying Direct Routing Guide.*	
	Media Port range on the client	See Microsoft's document *Deploying Direct Routing Guide.*	
Transport and Security	SIP transport	TLS	
	Media Transport	SRTP	
	SRTP Security Context	DTLS, SIPS Note: Support for DTLS is pending. Currently, SIPS must be configured. When support for DTLS will be announced, it will be the recommended context.	https://tools.ietf.org/html/rfc5763
	Crypto Suite	AES_CM_128_HMAC_SHA1_80, non-MKI	

Category	Parameter	Value	Comments
	Control protocol for media transport	SRTCP (SRTCP-Mux recommended)	Using RTCP MUX helps reduce the number of required ports
	Supported Certification Authorities	See the *Deployment Guide*	
	Transport for Media Bypass (of configured)	▪ ICE-lite (RFC 5245) – recommended ▪ Client also has Transport Relays	
	Audio codecs	▪ G.711 ▪ Silk (Teams clients) ▪ Opus (WebRTC clients) - only if Media Bypass is used ▪ G.729	
Codecs	Other codecs	▪ CN ▪ Required narrowband and wideband ▪ RED - Not required ▪ DTMF - Required ▪ Events 0-16 ▪ Silence Suppression - Not required	

B SIP Proxy Direct Routing Requirements

Microsoft 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**.

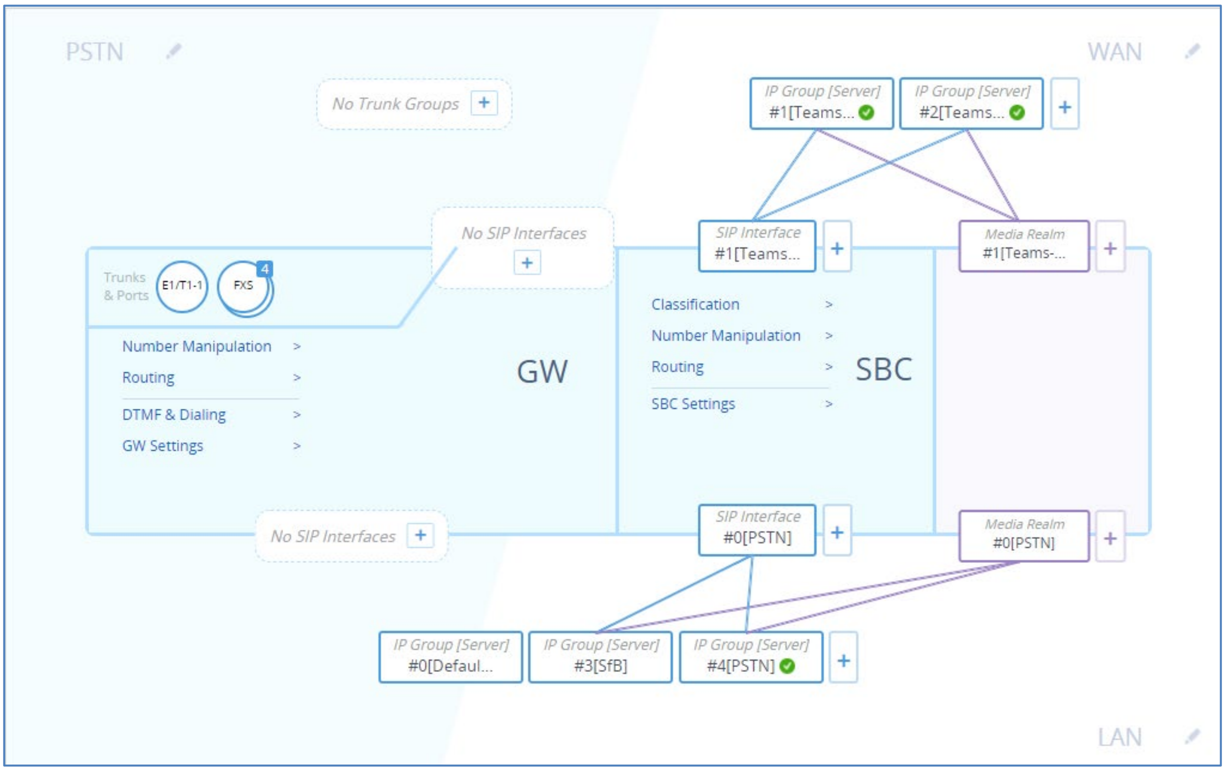
This page is intentionally left blank.

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



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/

Document #: LTRT-13206