Configuration Note

AudioCodes Mediant™ Family of Media Gateways & Session Border Controllers

Connecting AudioCodes' SBC to Microsoft Teams Direct Routing

Hosting Model

Microsoft Teams

audiocodes

Table of Contents

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: November-20-2024

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

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 Gateway & E-SBC User's Manual
Mediant 500L Gateway & E-SBC User's Manual
Mediant 800 Gateway & E-SBC User's Manual
Mediant 1000B Gateway & E-SBC User's Manual
Mediant 2600 E-SBC User's Manual
Mediant 4000 SBC User's Manual

Document Name
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
Gateway and SBC CLI Reference Guide
SIP Message Manipulation Reference Guide
AudioCodes User Management Pack 365 SP Edition Installation and Administration Guide

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)
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

LTRT	Description
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.
13209	Added a configuration example for SIP Trunk. Configuration is simplified by moving to one IP Group for Teams and changing Call Setup Rules. Added NTP Server configuration. Updated certified firmware version and links to Microsoft documents.
13210	Modified sections: Deploy Baltimore Trusted Root Certificate (added note for Baltimore Trusted Root Certificate and MTLS implementation); Configure SIP Signaling Interfaces; Configure Call Setup Rules ; Configure Message Manipulation Rules; Configure IP Groups;
13211	Note removed regarding external firewall.
13212	License update (typo)
13213	Update to topology figures and correction for parameter “Remote Update Support” to “SIP UPDATE Support”.
13214	Update to the “Related Documentation” table to include the Mediant 1000B Gateway & E-SBC product.
13215	Update in configuration concept. Modified sections: SBC Configuration Concept; Configure Proxy Sets and Proxy Address; Configure IP Groups; Configure IP-to-IP Call Routing Rules. Section “Tenant Provisioning Script” replaced with “UMP Configuration”. An Additional 2 IP addresses were added to firewall per Microsoft request.
13216	Update for Message Manipulation rule towards Microsoft Teams.
13217	Update to the Firewall Table Rules table with two additional IP addresses of the new infrastructure in Japan.
13218	Update to SIP Trunk IP Profile and validated firmware version.
13219	Fix to Call Setup Rule; Added section for overcoming problem of not playing music on hold during conversational transfer.
13330	Remote Replaces Mode parameter with value “Handle Locally” was added to the Teams IP Profile due to new Microsoft requirements. The Classification rule was updated. Update to the Firewall Table Rules table due to new Microsoft requirements.
13333	TLS Root Certificate Authority updated by Microsoft.
13335	Updated Classification Table with stricter rules to only allow for documented Microsoft SIP Proxies.
13337	Note added detailing deployment in Office 365 GCC DoD and GCC High environments.
13338	TLS Private Key size of 1024 was removed. Microsoft subnets were updated in the Classification and Firewall tables.
33524	Teams IP Profile update with RFC 2833 Mode parameter.

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.

1 Introduction

This document describes how to connect AudioCodes' SBC to Teams Direct Routing Hosting model and refers to the AudioCodes SBC configuration only.

For configuring the Office 365 side, please refer to https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure and https://docs.microsoft.com/en-us/microsoftteams/direct-routing-sbc-multiple-tenants.

This document is intended for IT or telephony professionals.

> To zoom in on screenshots of Web interface configuration examples, press **Ctrl** and **+**.

1.1 About Teams Direct Routing

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

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

1.2 About AudioCodes SBC Product Series

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

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

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

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

1.3 Validated AudioCodes SBC Version

Microsoft has successfully conducted validation tests with AudioCodes' Mediant SBC Ver. 7.40A.250. Previous certified firmware versions are 7.20A.258 and 7.40A.100. For an updated list, refer to *List of Session Border Controllers certified for Direct Routing*.

For implementing Microsoft Teams Direct Routing based on the configuration described in this document, AudioCodes SBC must be installed with a License Key that includes the following features:

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

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

1.4 Infrastructure Prerequisites

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

Table 1: Infrastructure Prerequisites

Infrastructure Prerequisite	Details
Certified Session Border Controller (SBC)	See Microsoft's Plan Direct Routing document.
SIP Trunks connected to the SBC	
Office 365 carrier tenant and customer 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	

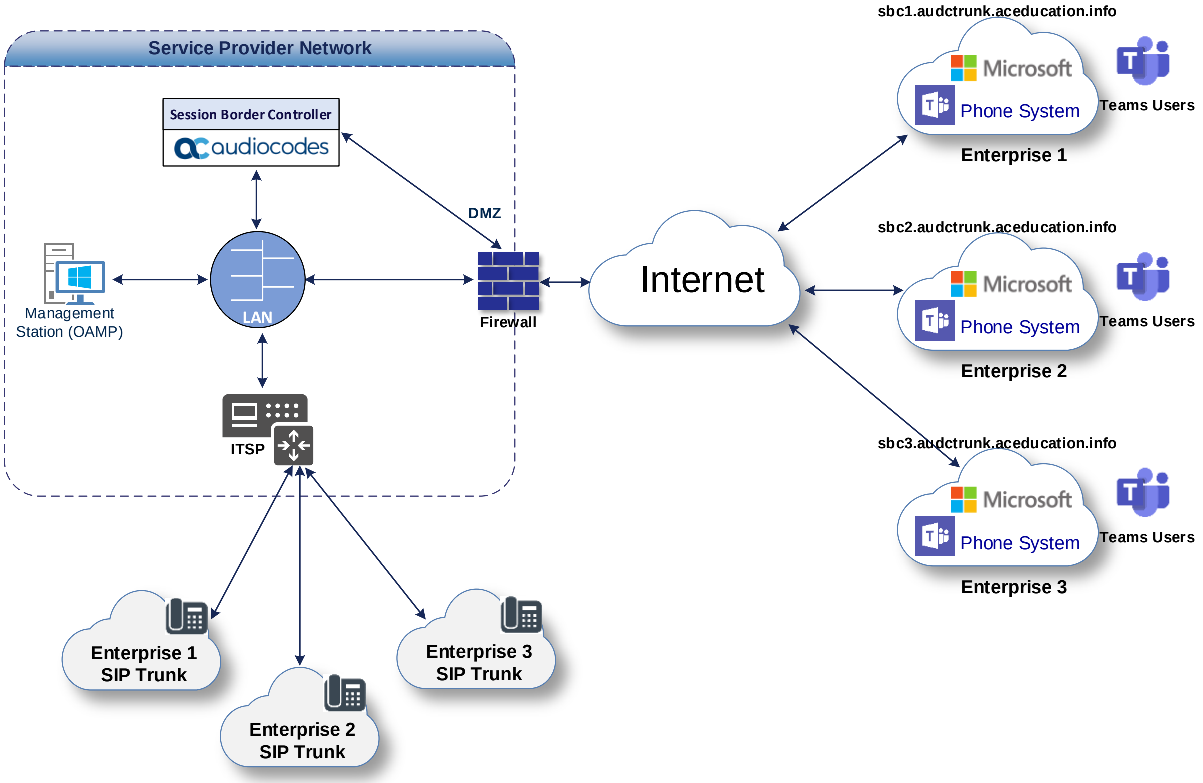
2 Configuring AudioCodes' SBC

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

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

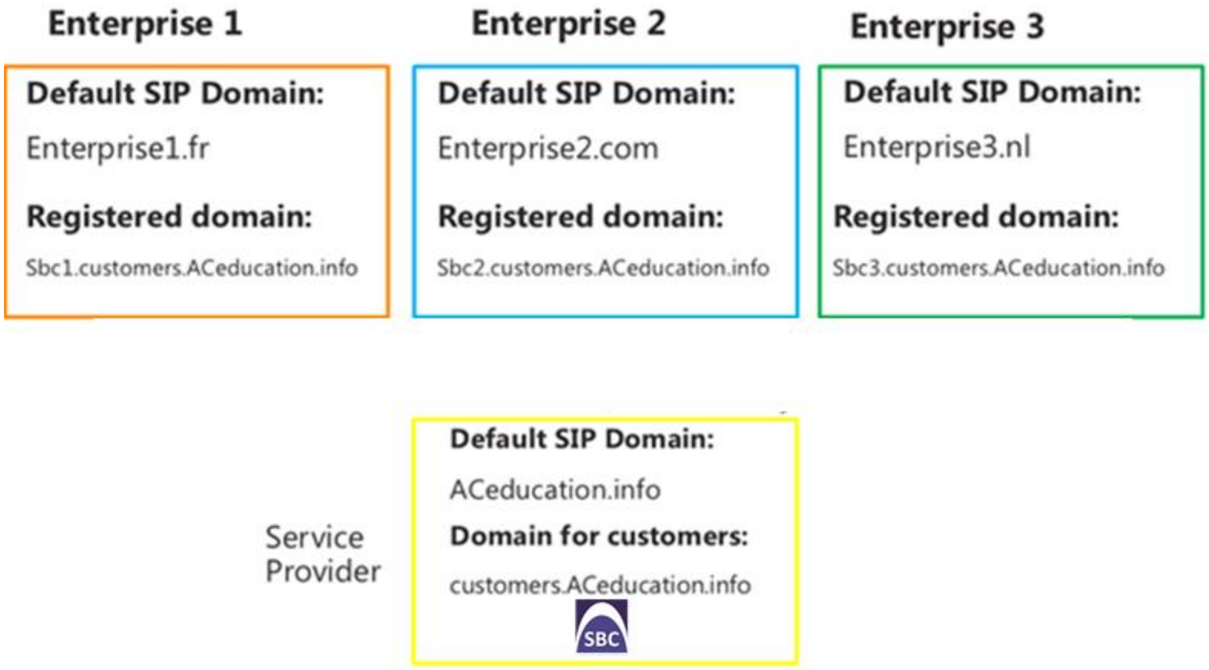
- Teams Phone Systems Direct Routing Interface on the WAN
- Service Provider SIP Trunk

Figure 1: Connection Topology - Network Interfaces



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

Figure 2: Carrier Office 365 Tenant Domain Structure



2.1 Prerequisites

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

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

2.1.1 About the SBC Domain Name in Hosting Model

2.1.1.1 SBC Domain Name in a Carrier Office 365 Tenant

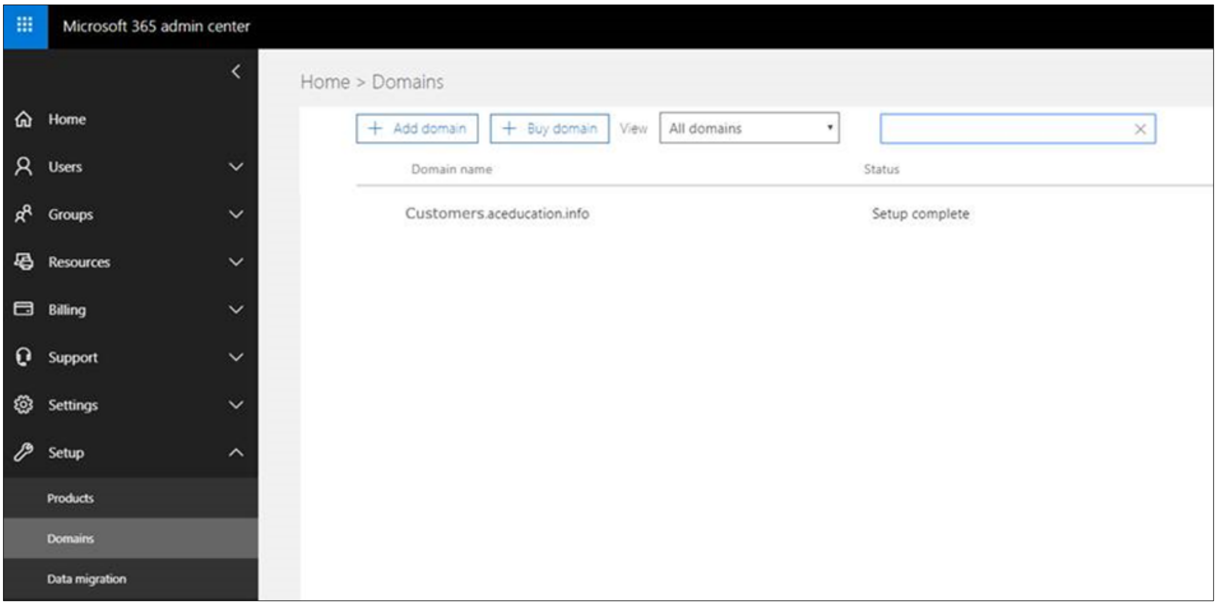
The SBC domain name must be from one of the names registered in 'Domains' of the tenant. You cannot use the ***.onmicrosoft.com** tenant for the domain name. For example, in the administrator registered the following DNS names for the tenant:

Table 2: DNS Names Registered by an Administrator for a Carriers' Office 365 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.

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

Figure 3: Example of Registered DNS Names

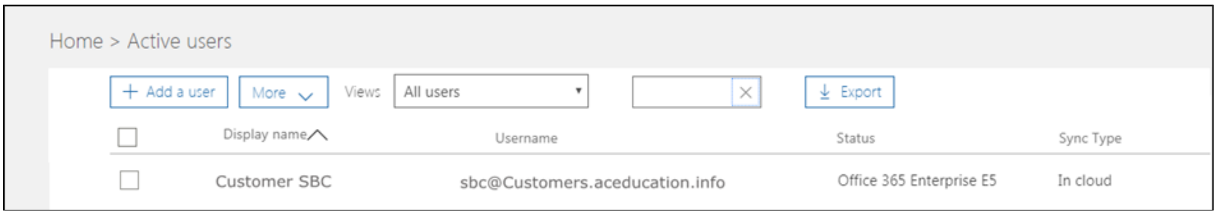


Domain name	Status
Customers.aceducation.info	Setup complete

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

> Microsoft commit for up to 24 Hours, before the PSTN gateway is activate.

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

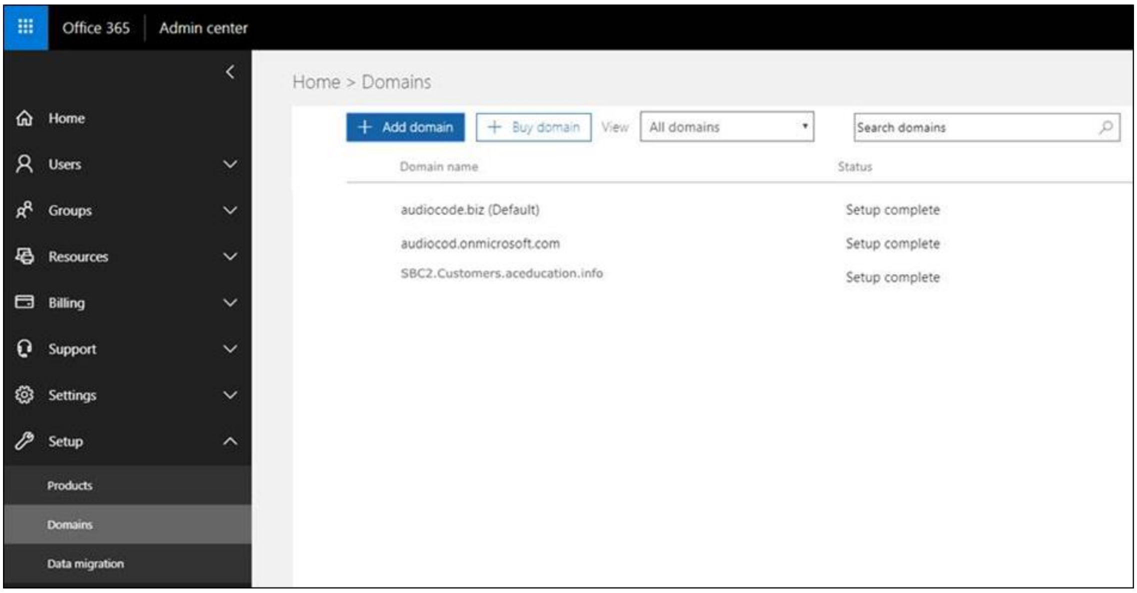


□	Display name	Username	Status	Sync Type
□	Customer SBC	sbc@Customers.aceducation.info	Office 365 Enterprise E5	In cloud

2.1.1.2 SBC Domain Name in a Customer Office 365 Tenant

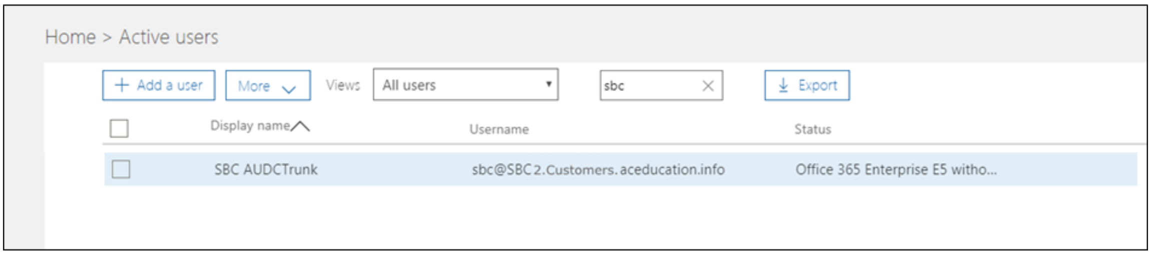
For each customer tenant, you should add a domain belonging to a carrier that points to a customer tenant as in Figure 5 and create at least one licensed user with Microsoft plan as Enterprise or Business with Phone System (e.g. E5 or E1/E3 with Phone System) belonging to your SBC domain as in Figure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

Figure 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 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
195.189.192.157	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.

> Microsoft commits for up to 24 hours, before the PSTN gateway is activated.

> Please refer to Microsoft guidelines "how to Register a subdomain name in a customer tenant" - https://docs.microsoft.com/en-us/microsoftteams/direct-routing-sbc-multiple-tenants#register-a-subdomain-name-in-a-customer-tenant

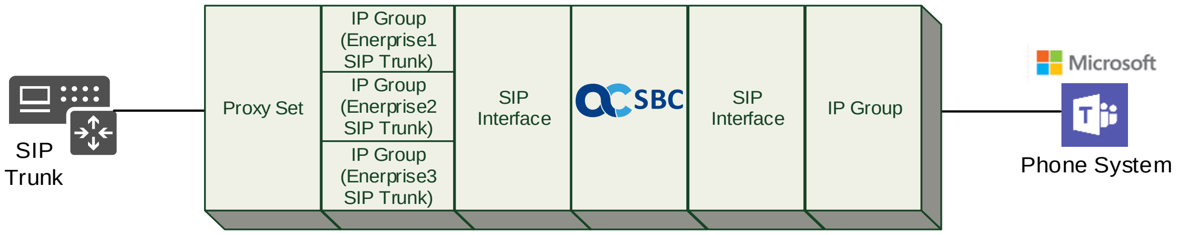
2.2 Validating AudioCodes SBC License

Please refer to Section 1.2 on page 1 for the list of required licenses.

2.3 SBC Configuration Concept

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

Figure 7: SBC Configuration Concept


SIP
Trunk
Proxy Set
IP Group (Enerprise1 SIP Trunk)
IP Group (Enerprise2 SIP Trunk)
IP Group (Enerprise3 SIP Trunk)
SIP Interface
SBC
SIP Interface
IP Group
Microsoft
Phone System

Configuration may be changed per customer request to a dedicated Proxy Set per IP Group (Enterprise's SIP Trunk).

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

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

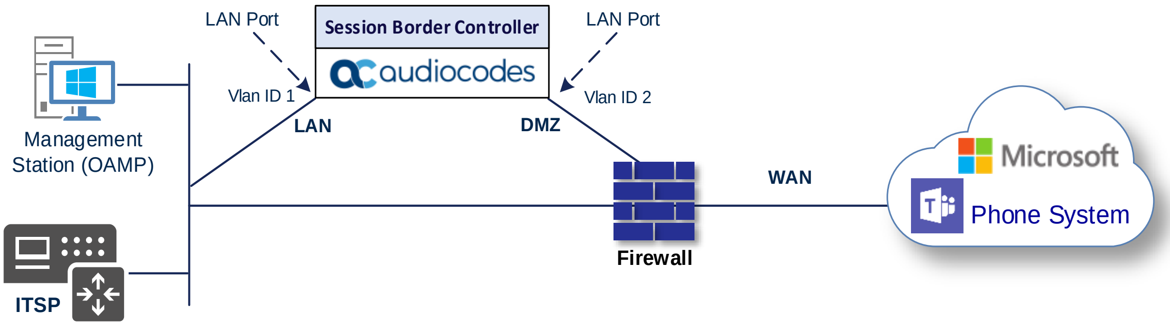
The configuration shown in this document is based on Customer DID Range using Dial Plan. For more information, see the AudioCodes' documentation suite.

2.4 Configuring LAN and WAN IP Interfaces

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

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

Figure 8: Network Interfaces in the Topology with SIP Trunk on the LAN



2.4.1 Validating Configuration of Physical Ports and Ethernet Groups

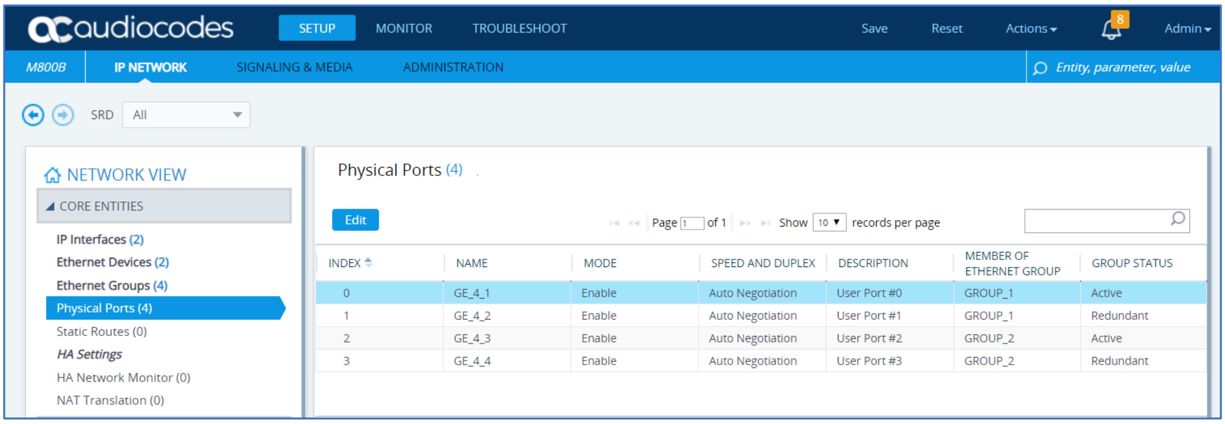
The physical ports are automatically detected by the SBC. The Ethernet groups are also auto-assigned to the ports. In this step, only parameter validation is necessary.

To validate physical ports:

1. Open the Physical Ports table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Physical Ports**).
2. Validate that you have at least two physical ports detected by the SBC, one for LAN and the other for WAN. Make sure both ports are in **Enabled** mode.

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

Figure 9: Physical Ports Configuration Interface

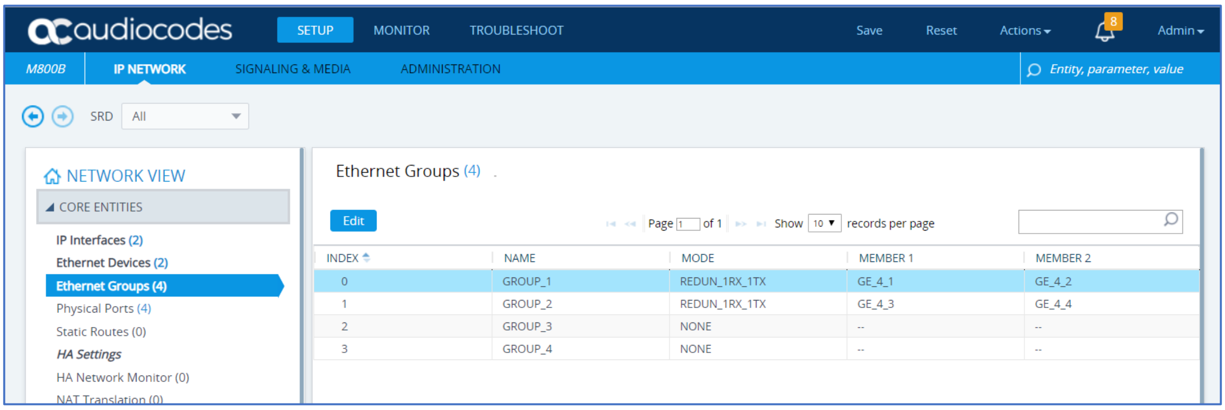


INDEX	NAME	MODE	SPEED AND DUPLEX	DESCRIPTION	MEMBER OF ETHERNET GROUP	GROUP STATUS
0	GE_4_1	Enable	Auto Negotiation	User Port #0	GROUP_1	Active
1	GE_4_2	Enable	Auto Negotiation	User Port #1	GROUP_1	Redundant
2	GE_4_3	Enable	Auto Negotiation	User Port #2	GROUP_2	Active
3	GE_4_4	Enable	Auto Negotiation	User Port #3	GROUP_2	Redundant

To validate Ethernet Groups:

1. Open the Ethernet Groups table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Groups**).
2. Validate that you have at least two Ethernet Groups detected by the SBC, one for LAN and the other for WAN.

Figure 10: Ethernet Groups Configuration Interface



INDEX	NAME	MODE	MEMBER 1	MEMBER 2
0	GROUP_1	REDUN_1RX_1TX	GE_4_1	GE_4_2
1	GROUP_2	REDUN_1RX_1TX	GE_4_3	GE_4_4
2	GROUP_3	NONE	--	--
3	GROUP_4	NONE	--	--

2.4.2 Configure LAN and WAN VLANs

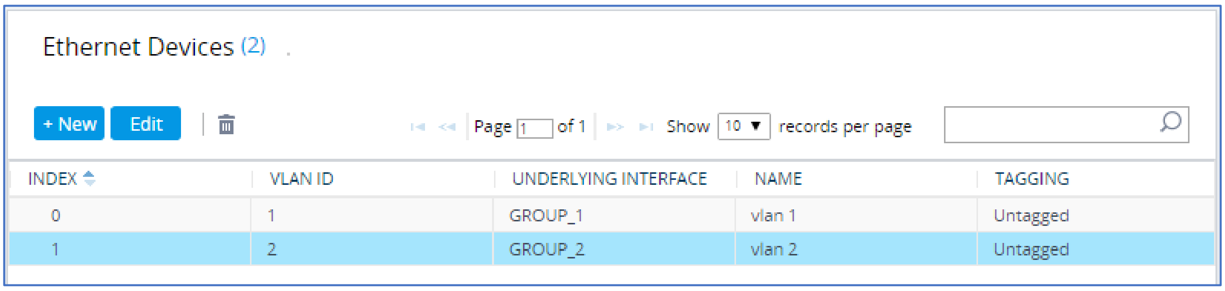
This section describes how to define VLANs for each of the following interfaces:

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

To configure VLANs:

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

Figure 11: Configured VLANs in the Ethernet Device Table



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

2.4.3 Configure Network Interfaces

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

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

To configure network parameters for both LAN and WAN interfaces:

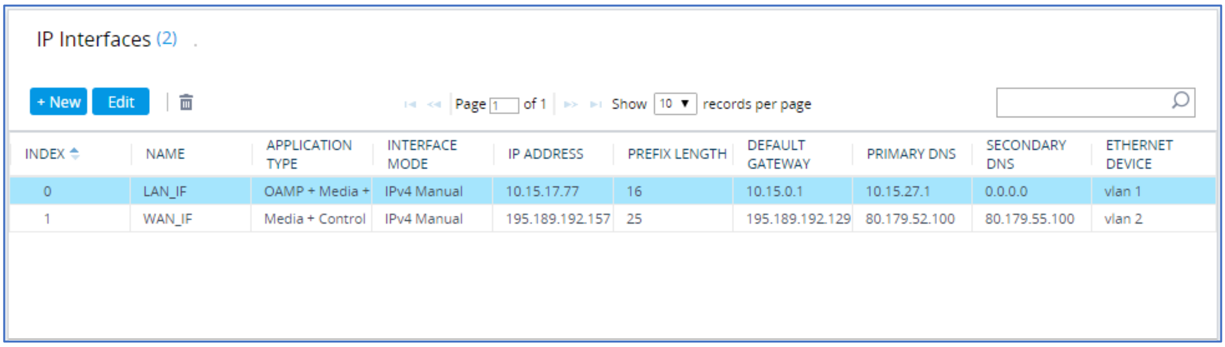
1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Configure the IP interfaces as follows (your network parameters might be different):

Table 3: Configuration Example of the Network Interface Table

Index	Application Types	Interface Mode	IP Address	Prefix Length	Gateway	DNS	I/F Name	Ethernet Device
0	OAMP+ Media + Control	IPv4 Manual	10.15.77.77	16	10.15.0.1	10.15.27.1	LAN_IF	vlan 1
1	Media + Control (as this interface points to the internet, enabling OAMP is not recommended)	IPv4 Manual	195.189.192.157 (DMZ IP address of SBC)	25	195.189.192.129 (router's IP address)	According to your Internet provider's instructions	WAN_IF	vlan 2

The configured IP network interfaces are shown below:

Figure 12: Configuration Example of the Network Interface Table



IP Interfaces (2)

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	LAN_IF	OAMP + Media +	IPv4 Manual	10.15.17.77	16	10.15.0.1	10.15.27.1	0.0.0.0	vlan 1
1	WAN_IF	Media + Control	IPv4 Manual	195.189.192.157	25	195.189.192.129	80.179.52.100	80.179.55.100	vlan 2

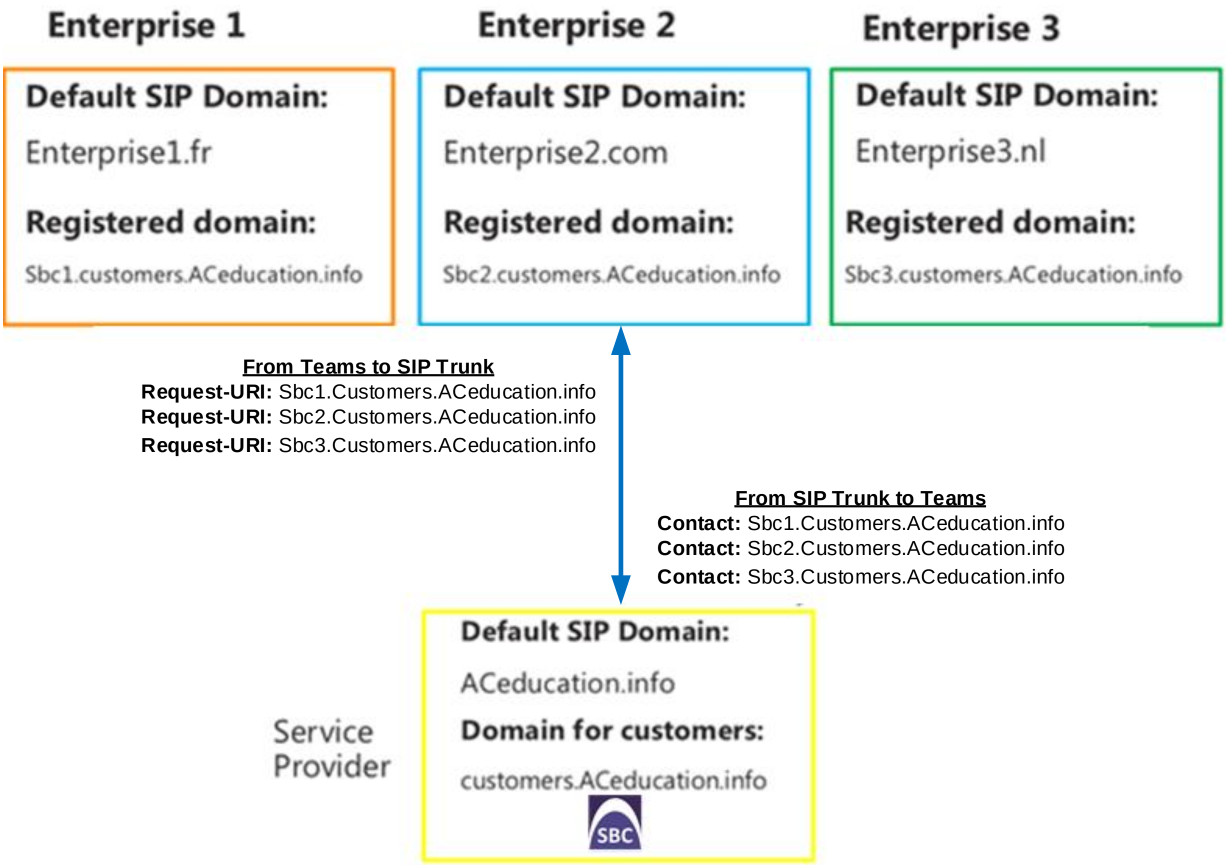
2.5 Configuring TLS Context for Teams

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

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

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

Figure 13: Carriers' Office 365 Tenants Domain Structure



Enterprise 1
Default SIP Domain:
Enterprise1.fr
Registered domain:
Sbc1.customers.ACeducation.info
Enterprise 2
Default SIP Domain:
Enterprise2.com
Registered domain:
Sbc2.customers.ACeducation.info
Enterprise 3
Default SIP Domain:
Enterprise3.nl
Registered domain:
Sbc3.customers.ACeducation.info
From Teams to SIP Trunk
Request-URI: Sbc1.Customers.ACeducation.info
Request-URI: Sbc2.Customers.ACeducation.info
Request-URI: Sbc3.Customers.ACeducation.info
From SIP Trunk to Teams
Contact: Sbc1.Customers.ACeducation.info
Contact: Sbc2.Customers.ACeducation.info
Contact: Sbc3.Customers.ACeducation.info
Service Provider
Default SIP Domain:
ACeducation.info
Domain for customers:
customers.ACeducation.info
SBC

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

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc

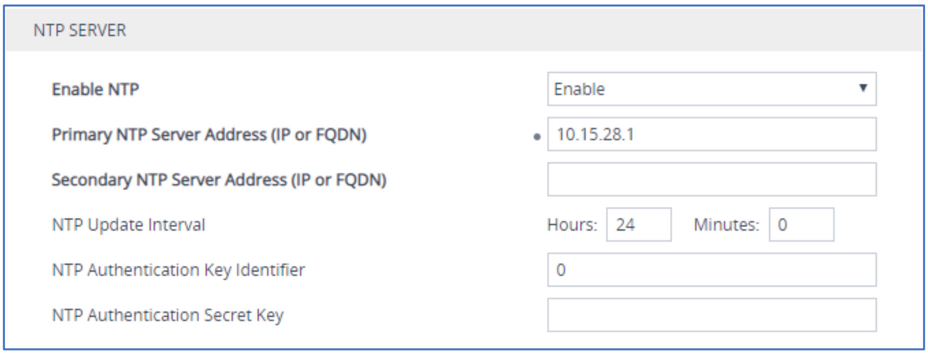
2.5.1 Configuring the NTP Server Address

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

To configure the NTP server address:

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

Figure 14: Configuring NTP Server Address



NTP SERVER

Enable NTP	Enable ▾
Primary NTP Server Address (IP or FQDN)	● 10.15.28.1
Secondary NTP Server Address (IP or FQDN)	
NTP Update Interval	Hours: 24 Minutes: 0
NTP Authentication Key Identifier	0
NTP Authentication Secret Key	

3. Click **Apply**.

2.5.2 Creating a TLS Context for Teams Direct Routing

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

The procedure involves the following main steps:

a. Creating a TLS Context for Teams Direct Routing.

b. Generating a Certificate Signing Request (CSR) and obtaining the certificate from a supported Certification Authority.

c. Deploying the SBC and Root / Intermediate certificates on the SBC.

To create a TLS Context for Teams Direct Routing:

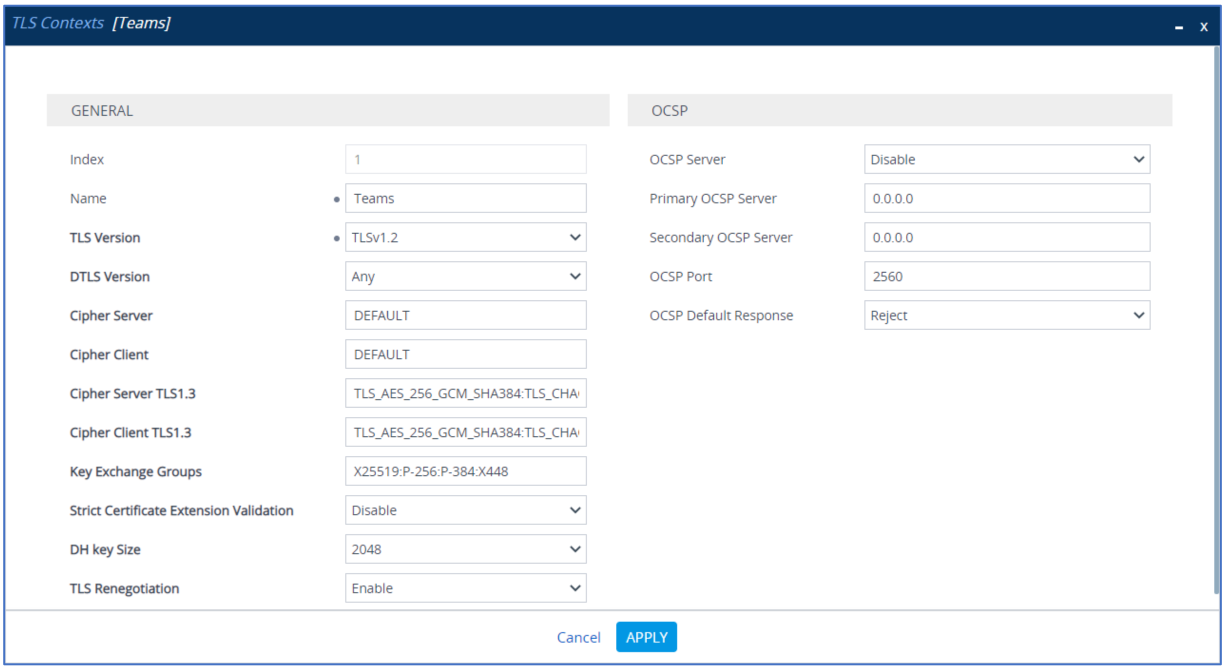
1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. Create a new TLS Context by clicking **+New**, and then configure the parameters using the table below as reference.

Table 4: New TLS Context

Index	Name	TLS Version
1	Teams (arbitrary descriptive name)	TLSv1.2
All other parameters can be left unchanged with their default values.		

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

Figure 15: Configuration of TLS Context for Direct Routing



TLS Contexts [Teams]

GENERAL

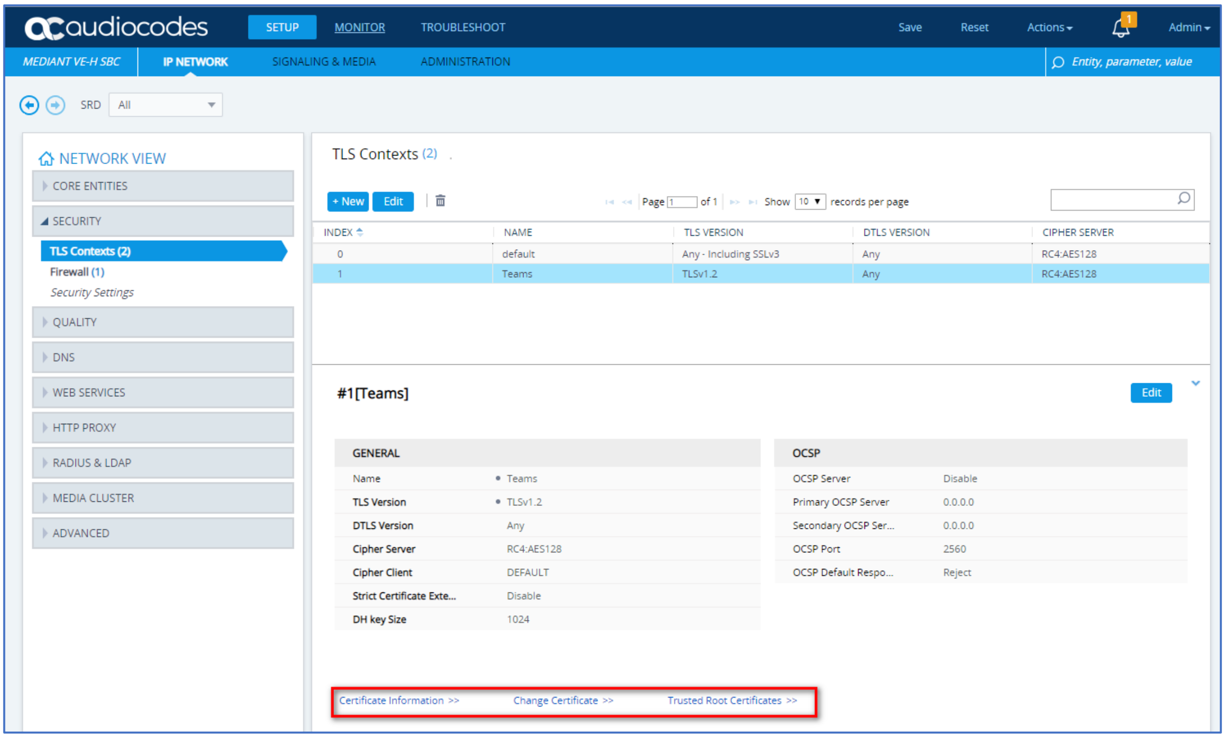
Index	1
Name	Teams
TLS Version	TLSv1.2
DTLS Version	Any
Cipher Server	DEFAULT
Cipher Client	DEFAULT
Cipher Server TLS1.3	TLS_AES_256_GCM_SHA384:TLS_CHA
Cipher Client TLS1.3	TLS_AES_256_GCM_SHA384:TLS_CHA
Key Exchange Groups	X25519:P-256:P-384:X448
Strict Certificate Extension Validation	Disable
DH key Size	2048
TLS Renegotiation	Enable

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 16: 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

2.5.3 Generating a CSR and Obtaining the Certificate from a Supported CA

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

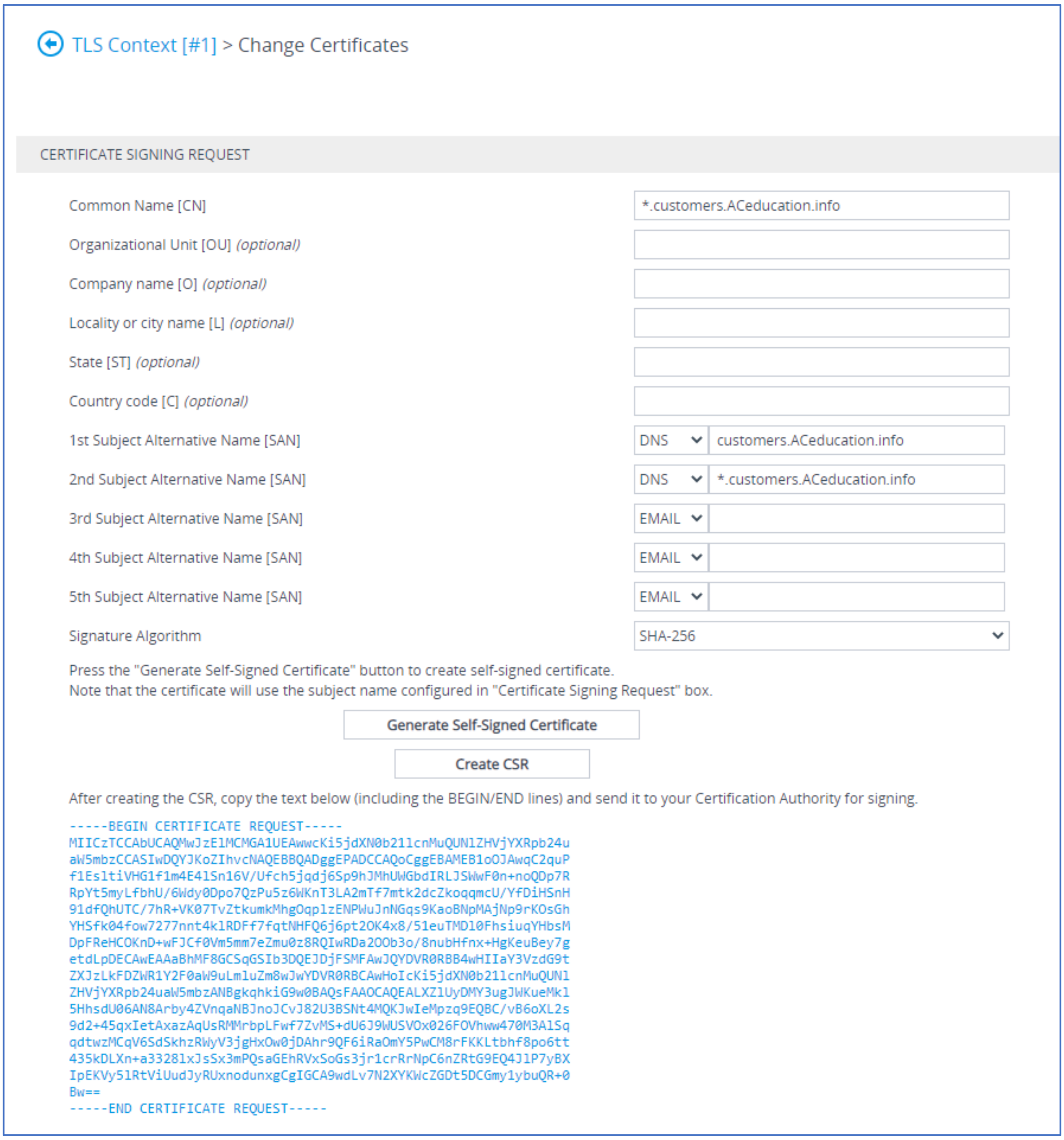
To generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority:

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the Teams TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
3. Under the **Certificate Signing Request** group, do the following:
    a. In the 'Common Name [CN]' field, enter the wildcard FQDN name (based on example above, *.**customers.ACeducation.info**).
    b. In the '1st Subject Alternative Name [SAN]' field, change the type to ‘DNS’ and enter the SBC FQDN name (based on example above, **customers.ACeducation.info**).
    c. In the '2nd Subject Alternative Name [SAN]' field, change the type to ‘DNS’ and enter the wildcard FQDN name (based on example above, ***.customers.ACeducation.info**).

> The domain portion of the Common Name [CN], 1st and 2nd Subject Alternative Name [SAN] must match the SIP suffix configured for carrier Office 365 tenant (see Section 2.1.1.1).

    d. Fill in the rest of the request fields according to your security provider's instructions.
    e. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 17: Example of Certificate Signing Request Page



TLS Context [#1] > Change Certificates

CERTIFICATE SIGNING REQUEST

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

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.

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-----
MIICzTCCAbUCAQMwJzElMCMGA1UEAwwcKi5jdXN0b21lcnMuQUNlZHVjYXRpb24u
aW5mbzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMEB1oOJAwqC2quP
f1EsltiVHG1f1m4E4lSn16V/Ufch5jqdj6Sp9hJMhUWGbdIRLJSWwF0n+noQDp7R
RpYt5myLfbhU/6Wdy0Dpo7QzPu5z6WKnT3LA2mTf7mtk2dcZkoqqmcU/YfDiHSnH
91dfQhUTC/7hR+VK07TvZtkumkMhgOqplzENPWuJnNGqs9KaoBNpMAjNp9rKOsGh
YHSfk04fow7277nnt4klRDFf7fqtNHFQ6j6pt2OK4x8/51euTMD10FhsiuqYHbsM
DpFReHCOKnD+wFJCf0Vm5mm7eZmu0z8RQIwRDa2OOb3o/8nubHfnx+HgKeuBey7g
etdLpDECAwEAAaBhMF8GCSqGSIb3DQEJDjFSMFAwJQYDVR0RBB4wHIIaY3VzdG9t
ZXJzLkFDZWR1Y2F0aW9uLmluZm8wJwYDVR0RBCAwHoIcKi5jdXN0b21lcnMuQUNl
ZHVjYXRpb24uaW5mbzANBgkqhkiG9w0BAQsFAAOCAQEALXZ1UyDMY3ugJWKueMkl
5HhsdU06AN8Arby4ZVnqaNBJnoJCvJ82U3BSNt4MQKJwIeMpzq9EQBC/vB6oXL2s
9d2+45qxIetAxazAqUsRMMrbpLFwf7ZvMS+dU6J9WUSVOx026FOVhww470M3AlSq
qdtwzMCqV6SdSkhzRWyV3jgHxOw0jDAhr9QF6iRaOmY5PwCM8rFKKLtbhf8po6tt
435kDLXn+a3328lxJsSx3mPQsaGEhRVxSoGs3jr1crRrNpC6nZRtG9EQ4J1P7yBX
IpEKVy5lRtViUudJyRUxnodunxgCgIGCA9wdLv7N2XYKWcZGDt5DCGmy1ybuQR+0
Bw==
-----END CERTIFICATE REQUEST-----
```

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

2.5.4 Deploying the SBC and Root / Intermediate Certificates on the SBC

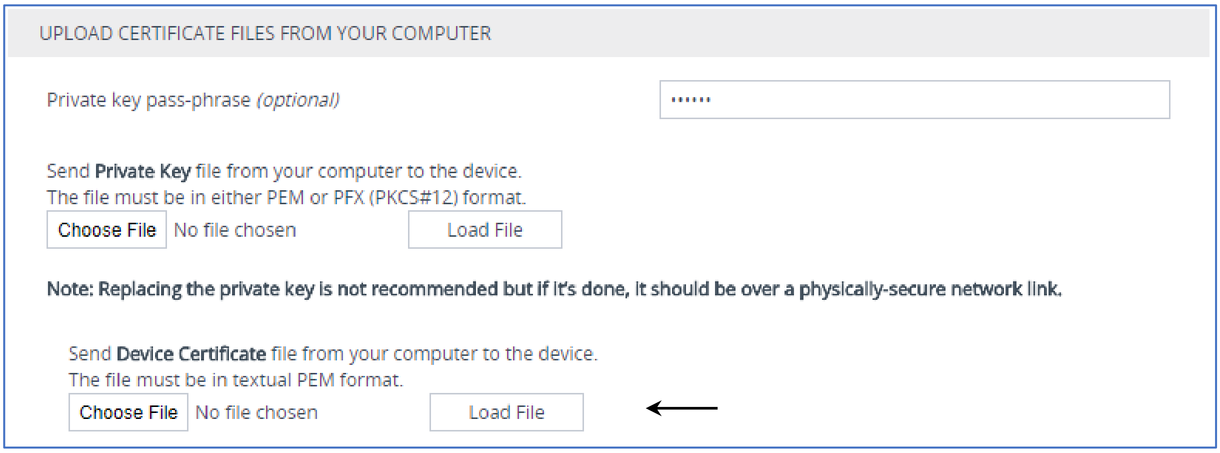
After obtaining the SBC signed and Trusted Root/Intermediate Certificate from the CA, install the following:

- SBC certificate
- Root / Intermediate certificates:

To install the SBC certificate:

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

Figure 18: Uploading the Certificate Obtained from the Certification Authority



UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

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

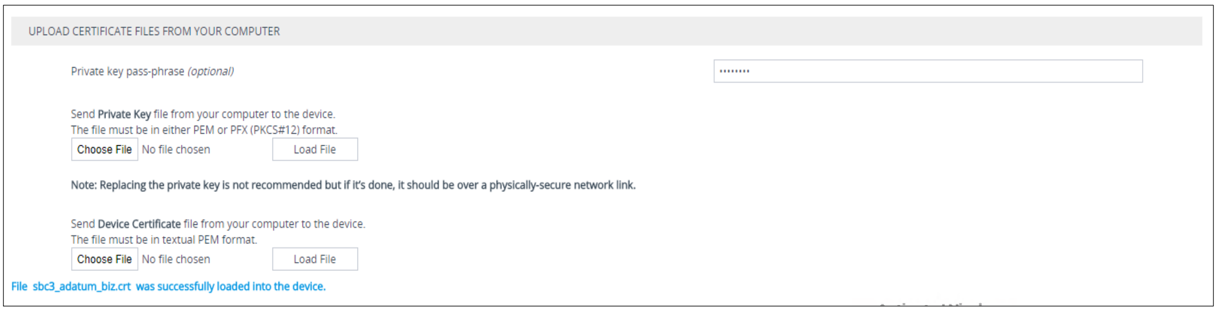
Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.
Choose File No file chosen Load File

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 Load File

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

Figure 19: 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.
Choose File No file chosen Load File

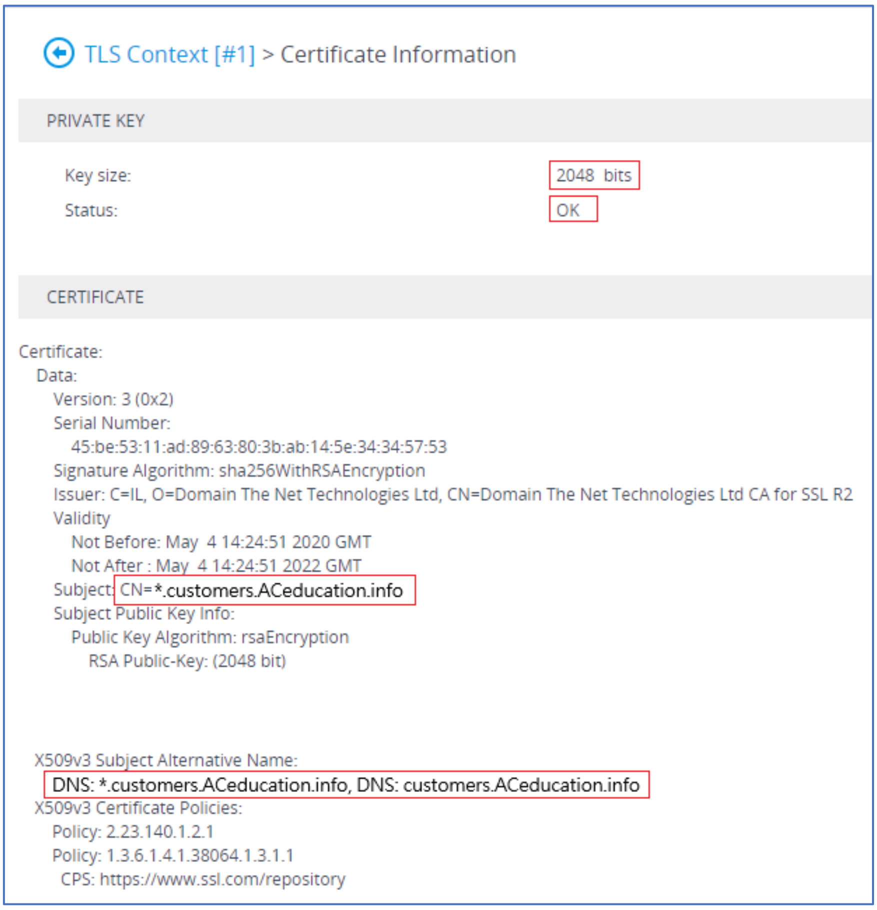
Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

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

File sbc3_adatum_biz.crt was successfully loaded into the device.

3. In the SBC's Web interface, return to the **TLS Contexts** page, select the required TLS Context index row, and then click the **Certificate Information** link, located at the bottom of the TLS. Then validate the Key size, certificate status and Subject Name:

Figure 20: Certificate Information Example



TLS Context [#1] > Certificate Information

PRIVATE KEY

Key size:	2048 bits
Status:	OK

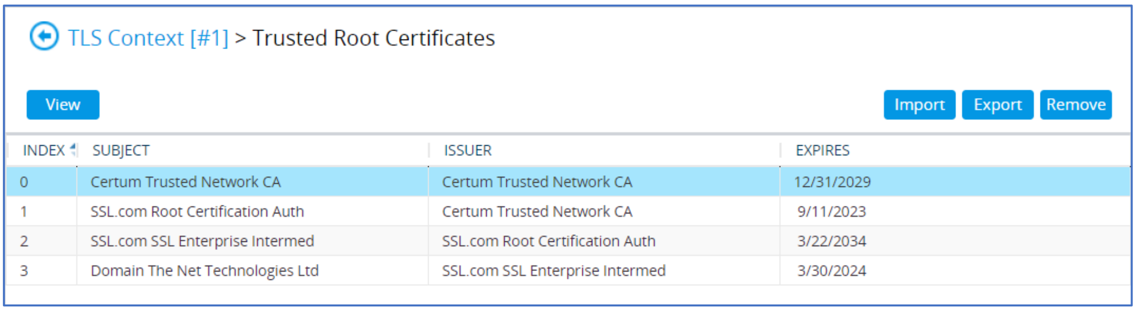
CERTIFICATE

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      45:be:53:11:ad:89:63:80:3b:ab:14:5e:34:34:57:53
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=IL, O=Domain The Net Technologies Ltd, CN=Domain The Net Technologies Ltd CA for SSL R2
    Validity
      Not Before: May  4 14:24:51 2020 GMT
      Not After : May  4 14:24:51 2022 GMT
    Subject: CN=*.customers.ACeducation.info
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        RSA Public-Key: (2048 bit)


  X509v3 Subject Alternative Name:
    DNS: *.customers.ACeducation.info, DNS: customers.ACeducation.info
  X509v3 Certificate Policies:
    Policy: 2.23.140.1.2.1
    Policy: 1.3.6.1.4.1.38064.1.3.1.1
     CPS: https://www.ssl.com/repository
```

4. In the SBC's Web interface, return to the **TLS Contexts** page.
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Trusted Root Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
   b. Click the **Import** button, and then select all Root/Intermediate Certificates obtained from your Certification Authority to load.
5. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store:

Figure 21: Configured Trusted Certificates Page



INDEX	SUBJECT	ISSUER	EXPIRES
0	Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029
1	SSL.com Root Certification Auth	Certum Trusted Network CA	9/11/2023
2	SSL.com SSL Enterprise Intermed	SSL.com Root Certification Auth	3/22/2034
3	Domain The Net Technologies Ltd	SSL.com SSL Enterprise Intermed	3/30/2024

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

2.6 Method of Generating and Installing the Wildcard Certificate

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

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

To install the certificate:

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
3. Scroll down to the **Upload certificates files from your computer** group and do the following:
   a. Enter the password assigned during export with the DigiCert utility in the '**Private key pass-phrase**' field.
   b. Click the **Choose File** button corresponding to the 'Send **Private Key**...' field and then select the SBC certificate file exported from the DigiCert utility.

2.7 Deploying Trusted Root Certificate for MTLS connection

> Loading Trusted Root Certificates to AudioCodes' SBC is mandatory when implementing an MTLS connection with the Microsoft Teams network.

> Microsoft 365 is updating services powering messaging, meetings, telephony, voice, and video to use TLS certificates from a different set of Root Certificate Authorities (CAs). For more details of the new Root CAs, refer to Microsoft technical guidance at Office TLS Certificate Changes. Services began transitioning to the new Root CAs (e.g., DigiCert) beginning in January 2022 and will continue through October 2022. During this migration period, it’s possible to load both the old (Baltimore) and the new (DigiCert) Root certificate to the same TLS Context.

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 **DigiCert** with:

Serial Number: 0x033af1e6a711a9a0bb2864b11d09fae5,
SHA-1 Thumbprint: DF3C24F9BFD666761B268073FE06D1CC8D4F82A4 and
SHA-256 Thumbprint: CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F.

For more information on the DNS name, see Appendix B.

To trust this certificate, your SBC *must* have the certificate in Trusted Certificates storage. Download the **DigiCert Global Root G2** (df3c) certificate in **PEM format** from https://www.digicert.com/kb/digicert-root-certificates.htm and follow the steps above to import the certificate to the Trusted Root storage.

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

2.8 Configuring Media Realms

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

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

To configure Media Realms:

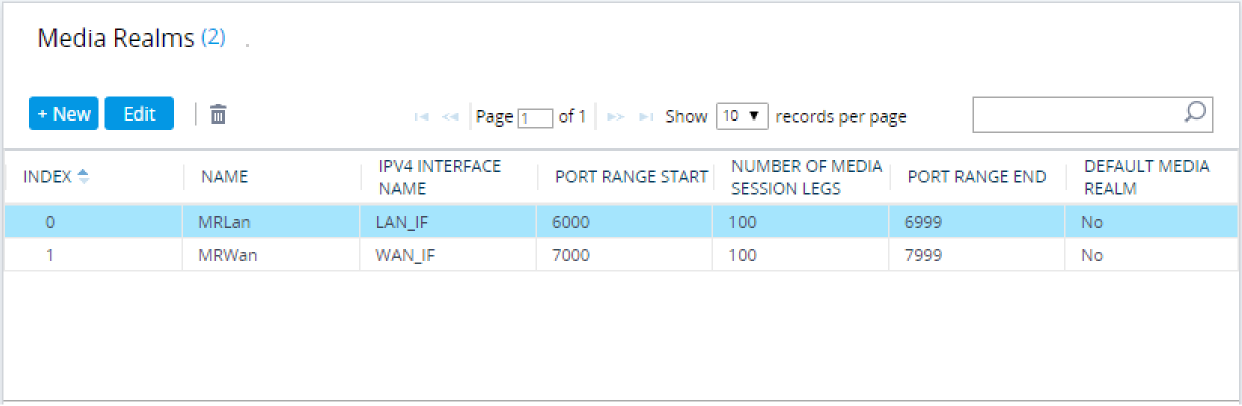
1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Configure Media Realms as follows (you can use the default Media Realm - Index 0 - but modify it):

Table 5: Configuration Example Media Realms in Media Realm Table

Index	Name	Topology Location	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
0	MRLan (arbitrary name)		LAN_IF	6000	100 (media sessions assigned with port range)
1	MRWan (arbitrary name)	Up	WAN_IF	7000	100 (media sessions assigned with port range)

The configured Media Realms are shown in the figure below:

Figure 22: Configuration Example Media Realms in Media Realm Table



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

2.9 Configuring SIP Signaling Interfaces

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

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

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

To configure a SIP interfaces:

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

> 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 6: Configuration Example of SIP Signaling Interfaces

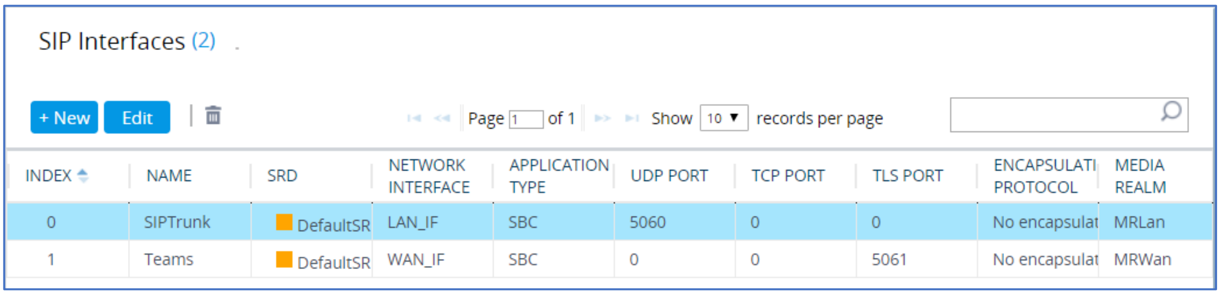
Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepalive	Classification Failure Response Type	Media Realm	TLS Context Name
0	SIPTrunk (arbitrary name)	LAN_IF	SBC	5060 (according to Service Provider requirement)	0	0	Disable (leave default value)	500 (leave default value)	MRLan	-
1	Teams (arbitrary name)	WAN_IF	SBC	0 (Phone System does not use UDP or TCP for SIP signaling)	0	5061 (as configured in the Office 365)	Enable	0 (Recommended to prevent DoS attacks)	MRWan	Teams

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

> Loading DigiCert Trusted Root Certificates to AudioCodes' SBC is mandatory for implementing an MTLS connection with the Microsoft Teams network. Refer to Section 2.7 on page 20.

The configured SIP Interfaces are shown in the figure below:

Figure 23: Configuration Example of SIP Signaling Interfaces



SIP Interfaces (2)

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATI PROTOCOL	MEDIA REALM
0	SIPTrunk	🟧 DefaultSR	LAN_IF	SBC	5060	0	0	No encapsulat	MRLan
1	Teams	🟧 DefaultSR	WAN_IF	SBC	0	0	5061	No encapsulat	MRWan

2.10 Configuring Proxy Sets and Proxy Address

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

2.10.1 Configuring Proxy Sets

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

To configure a Proxy Sets:

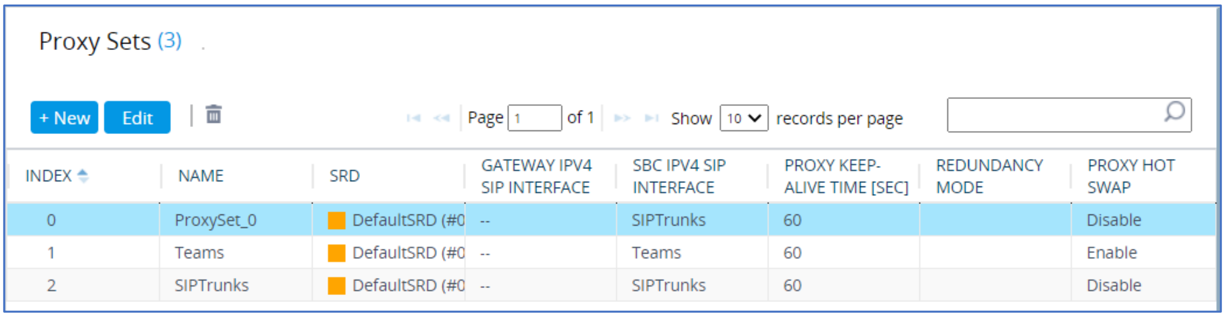
1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Configure Proxy Sets as shown in the table below:

Table 7: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Proxy Hot Swap	Proxy Load Balancing Method
1	Teams (arbitrary name)	Teams	Teams	Using Options	Enable	Random Weights
2	SIPTrunks (arbitrary name)	SIPTrunk	Default	Using Options	-	-

The configured Proxy Sets are shown in the figure below:

Figure 24: Configuration Example Proxy Sets in Proxy Sets Table



Proxy Sets (3)

INDEX	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	🟧 DefaultSRD (#0	--	SIPTrunks	60		Disable
1	Teams	🟧 DefaultSRD (#0	--	Teams	60		Enable
2	SIPTrunks	🟧 DefaultSRD (#0	--	SIPTrunks	60		Disable

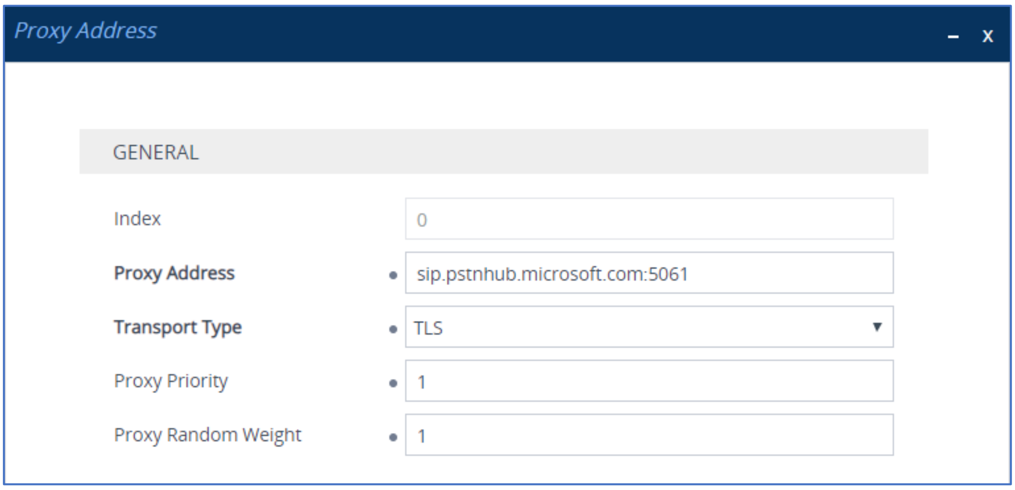
2.10.2 Configuring a Proxy Address

This section shows how to configure a Proxy Address.

To configure a Proxy Address for Teams:

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

Figure 25: Configuring Proxy Address for Teams Direct Routing Interface



Proxy Address

GENERAL

Index: 0

Proxy Address: ● sip.pstnhub.microsoft.com:5061

Transport Type: ● TLS

Proxy Priority: ● 1

Proxy Random Weight: ● 1

3. Configure the address of the Proxy Set according to the parameters described in the table below (for more information, see Appendix B):

Table 8: Configuration Proxy Address for Teams Direct Routing

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	sip.pstnhub.microsoft.com:5061	TLS	1	1
1	sip2.pstnhub.microsoft.com:5061	TLS	2	1
2	sip3.pstnhub.microsoft.com:5061	TLS	3	1

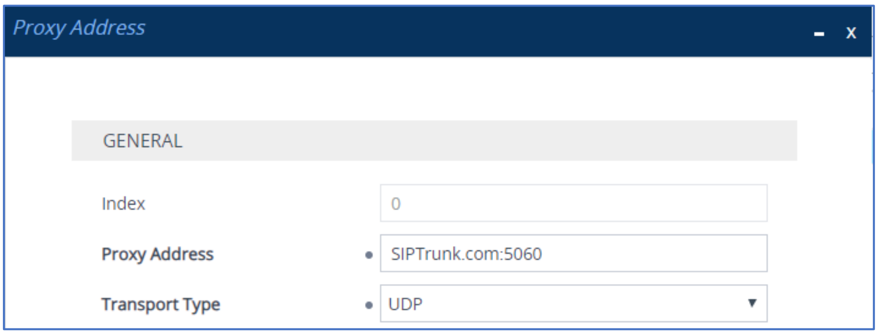
4. Click **Apply**.

> If the SBC is deployed in Office 365 GCC DoD or GCC High environments, please contact AudioCodes deployment services, since these environments have different configurations (FQDNs) than the public Office 365 environment.

To configure a Proxy Address for SIP Trunks:

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

Figure 26: Configuring Proxy Address for SIP Trunk



Index: 0
Proxy Address: SIPTrunk.com:5060
Transport Type: UDP

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

Table 9: Configuration Proxy Address for SIP Trunk

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	SIPTrunk.com:5060 (SIP Trunk IP / FQDN and port)	UDP	0	0

4. Click **Apply**.

2.11 Configuring the Dial Plan Table (Customer DID Only)

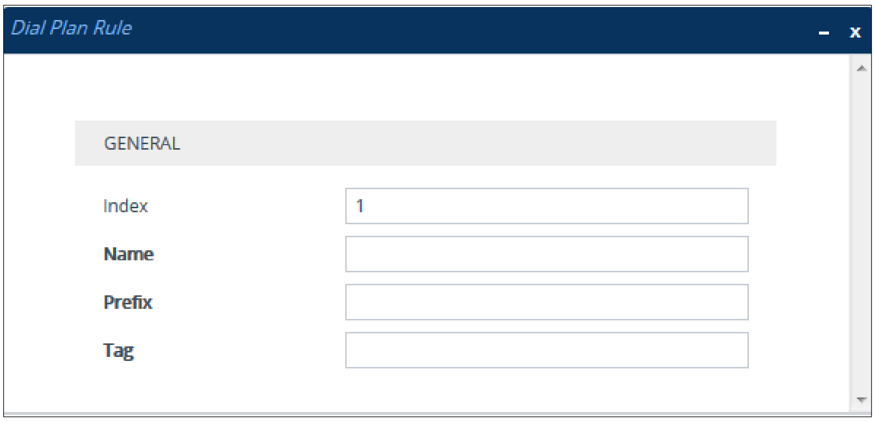
For deployments requiring hundreds of routing rules (which may exceed the maximum number of rules that can be configured in the IP-to-IP Routing table), you can employ tags to represent the many different calling (source URI user name) and called (destination URI user name) prefix numbers in your routing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

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

To configure Dial Plans:

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

Figure 27: Dial Plan Rule Table - Add Dialog Box



Index 1
Name
Prefix
Tag

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

Table 10: Dial Plan Carriers' Office 365 Teams Tenants

Index	Name	Prefix	Tag
0	Enterprise1	+19098[0000-9999]	<FQDN name of the carrier customer 1 tenant in SBC>. For example, ***sbc1.customers.ACeducation.info***
1	Enterprise2	+17093[0000-9999]	<FQDN name of the carrier customer 2 tenant in SBC>. For example, ***sbc2.customers.ACeducation.info***
2	Enterprise3	+18097[0000-9999]	<FQDN name of the carrier customer 3 tenant in SBC>. For example, ***sbc3.customers.ACeducation.info***

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

2.12 Configuring Call Setup Rules

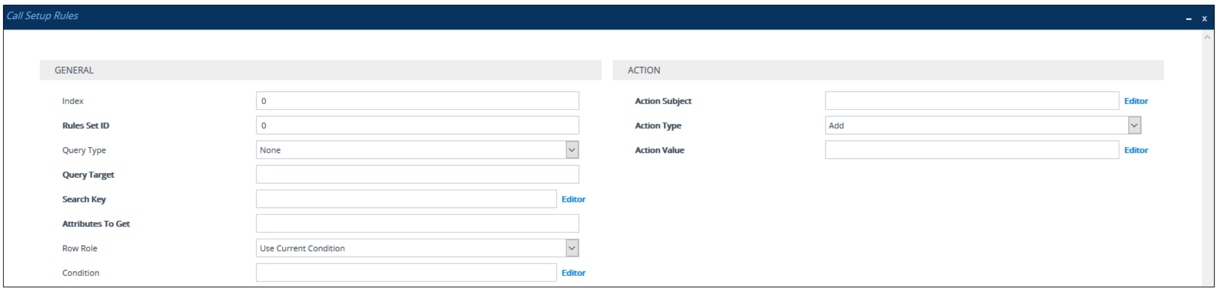
This section describes how to configure Call Setup Rules based on customer DID range (Dial Plan). Call Setup rules define various sequences that are run upon receipt of an incoming call (dialog) at call setup, before the device routes the call to its destination.

Configured Call Setup Rules need be assigned to specific IP Group.

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

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

Figure 28: Call Setup Rules Table - Add Dialog Box



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

Action Subject:
Action Type: Add
Action Value:

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

Table 11: Call Setup Rules Table

Index	Rules Set ID	Name	Query Type	Query Target	Search Key	Condition	Action Subject	Action Type	Action Value
0	0	TenantFQDN by PAI	Dial Plan	TeamsTenants	Header.P-Asserted-Identity.URL.User	DialPlan.Found exists	var.session.TenantFQDN	Modify	DialPlan.Result
1	0	TenantFQDN by From	Dial Plan	TeamsTenants	Param.Call.Src.User	DialPlan.Found exists AND var.session.TenantFQDN == ''	var.session.TenantFQDN	Modify	DialPlan.Result
2	0	SIP Trunk DstTags					DstTags	Modify	var.session.TenantFQDN
3	1	TenantFQDN by R-URI	Dial Plan	TeamsTenants	Param.Call.Dst.User	DialPlan.Found exists	var.session.TenantFQDN	Modify	DialPlan.Result
4	1	Teams DstTags					DstTags	Modify	'Teams'

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

2.13 Configuring Message Manipulation Rules

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

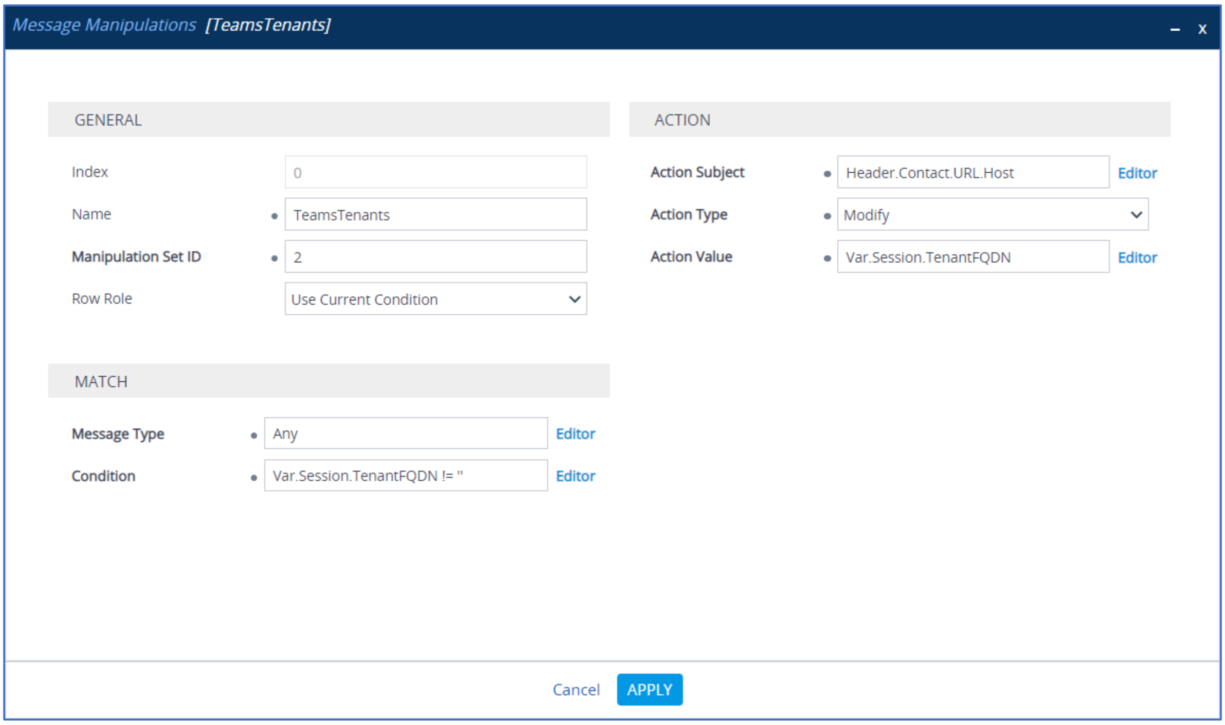
Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

To configure SIP message manipulation rule for Teams:

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

Parameter	Value
Index	**0**
Name	**TeamsTenants** (arbitrary name)
Manipulation Set ID	**2**
Condition	**Var.Session.TenantFQDN != ''**
Action Subject	**Header.Contact.URL.Host**
Action Type	**Modify**
Action Value	**Var.Session.TenantFQDN**

Figure 29: Configuring SIP Message Manipulation Rule 0 (for Teams IP Group)



Message Manipulations [TeamsTenants]

GENERAL

Index	0
Name	TeamsTenants
Manipulation Set ID	2
Row Role	Use Current Condition

MATCH

Message Type	Any
Condition	Var.Session.TenantFQDN != ''

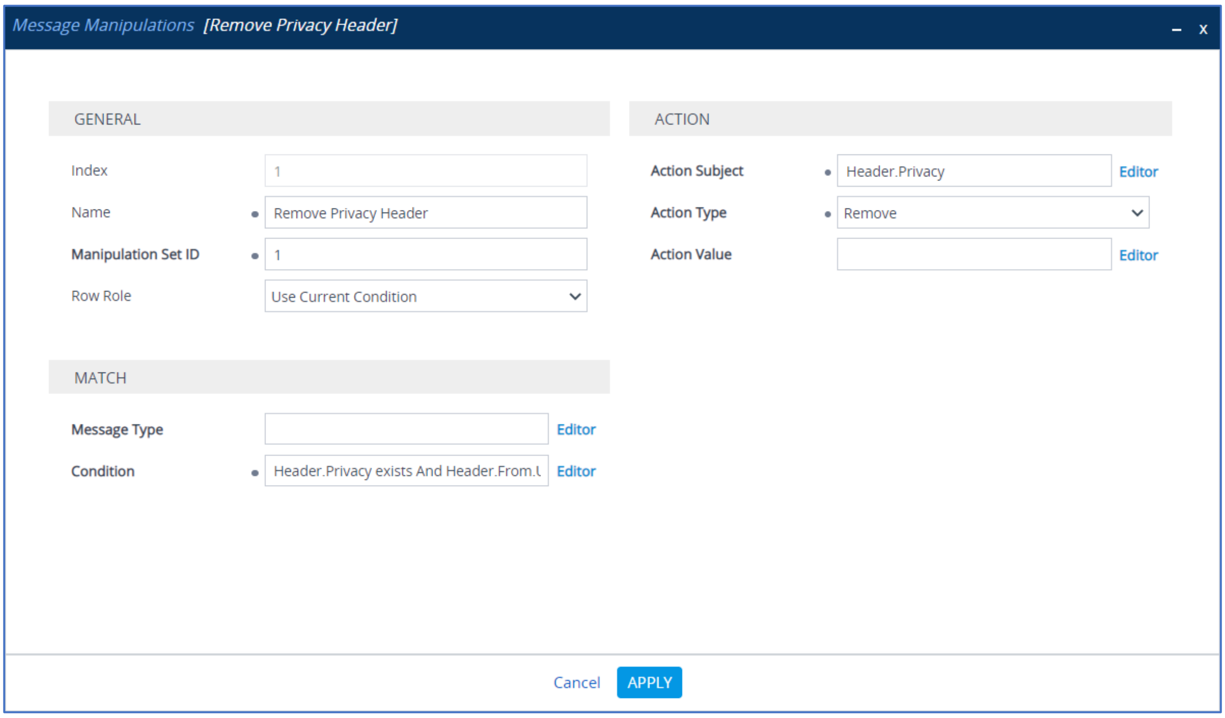
ACTION

Action Subject	Header.Contact.URL.Host
Action Type	Modify
Action Value	Var.Session.TenantFQDN

3. Configure another manipulation rule (Manipulation Set 1) for Teams IP Group. This rule applies to messages received from the Teams IP Group. This rule removes the SIP Privacy Header in all messages, except of call with presentation restriction.

Parameter	Value
Index	**1**
Name	**Remove Privacy Header**
Manipulation Set ID	**1**
Condition	**Header.Privacy exists And Header.From.URL !contains 'anonymous'**
Action Subject	**Header.Privacy**
Action Type	**Remove**

Figure 30: Configuring SIP Message Manipulation Rule 1 (for Teams IP Group)



Message Manipulations [Remove Privacy Header]

GENERAL

Index: 1

Name: Remove Privacy Header

Manipulation Set ID: 1

Row Role: Use Current Condition

MATCH

Message Type:

Condition: Header.Privacy exists And Header.From.U

ACTION

Action Subject: Header.Privacy

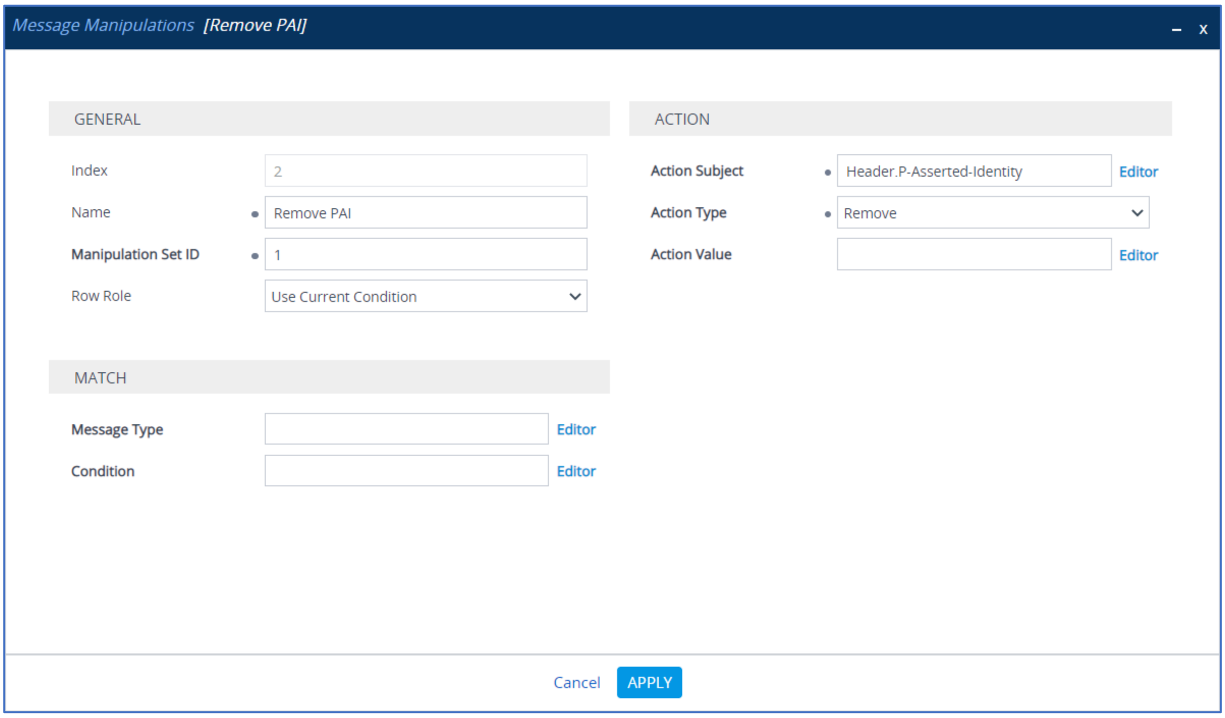
Action Type: Remove

Action Value:

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

Parameter	Value
Index	**2**
Name	**Remove PAI**
Manipulation Set ID	**1**
Action Subject	**Header.P-Asserted-Identity**
Action Type	**Remove**

Figure 31: Configuring SIP Message Manipulation Rule 2 (for Teams IP Group)



Message Manipulations ***[Remove PAI]***

GENERAL

Index	2
Name ●	Remove PAI
Manipulation Set ID ●	1
Row Role	Use Current Condition

MATCH

Message Type	
Condition	

ACTION

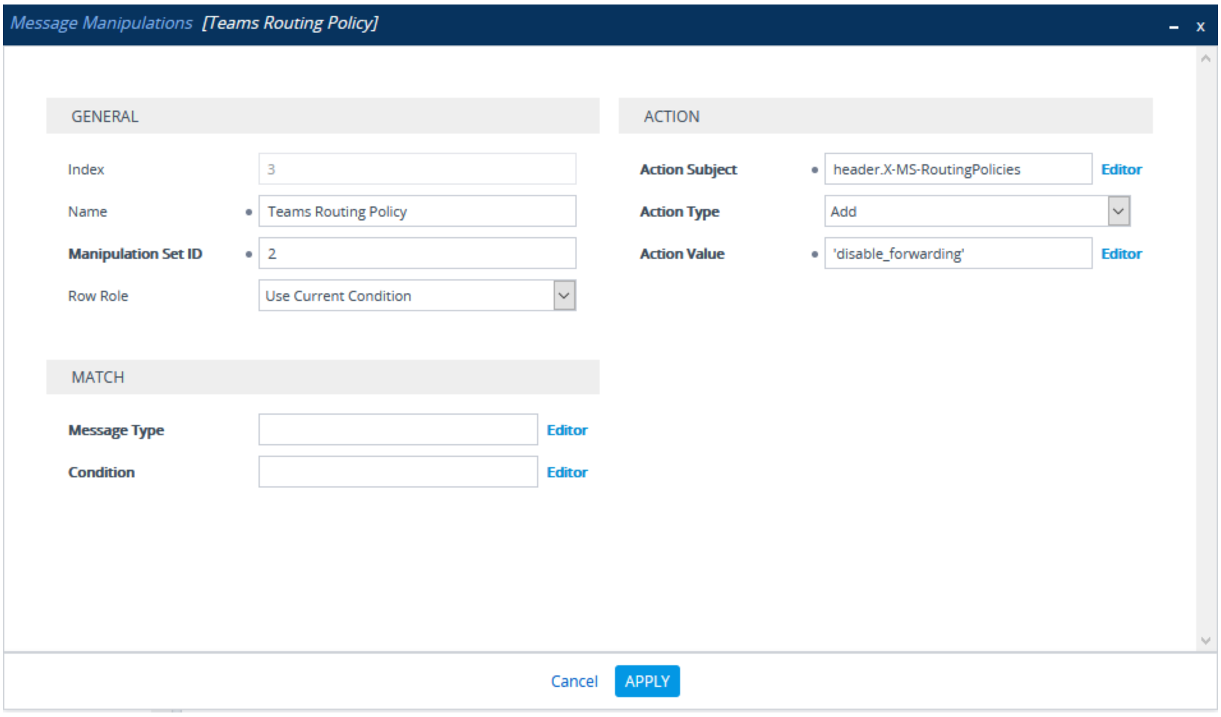
Action Subject ●	Header.P-Asserted-Identity
Action Type ●	Remove
Action Value	

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

Parameter	Value
Index	**3**
Name	**Teams Routing Policy** (arbitrary name)
Manipulation Set ID	**2**
Condition	
Action Subject	**header.X-MS-RoutingPolicies**
Action Type	**Add**
Action Value	One of the following values: **"none", "no_missed_call", "disable_forwarding", "disable_forwarding_except_phone**

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

Figure 32: Configuring SIP Message Manipulation Rule 1 (for Teams IP Group) Disable Forwarding Example



Message Manipulations [Teams Routing Policy]

GENERAL

Index	3
Name	Teams Routing Policy
Manipulation Set ID	2
Row Role	Use Current Condition

MATCH

Message Type	
Condition	

ACTION

Action Subject	header.X-MS-RoutingPolicies
Action Type	Add
Action Value	'disable_forwarding'

2.14 Configuring a Coder Group

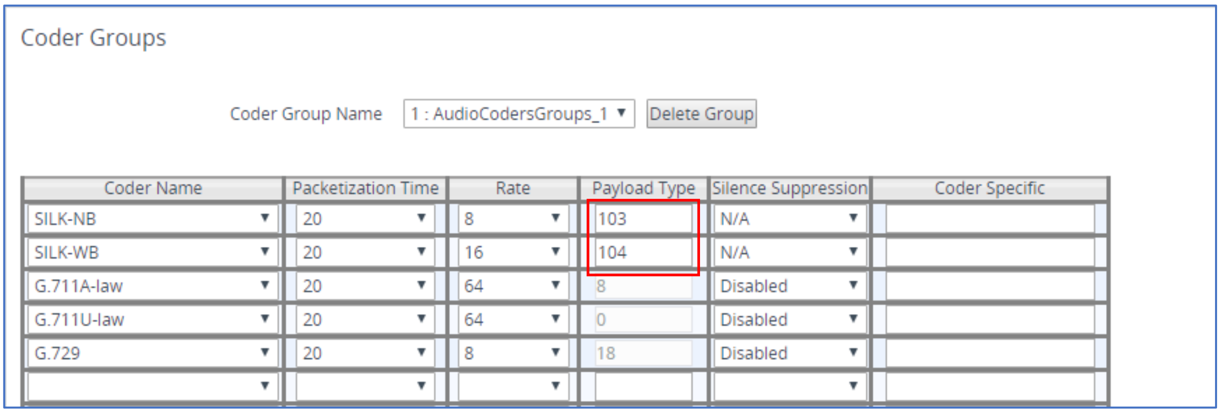
This section describes how to configure coders (termed *Coder Groups*). As Teams Direct Routing supports the SILK and G.729 coders while the network connection to the SIP Trunk may restrict operation with a dedicated coders list, you need to add a Coder Group with the supported coders for each leg, the Teams Direct Routing and the SIP Trunk.

Note that the Coder Group ID for this entity will be assigned to its corresponding IP Profile in the next section.

To configure a Coder Group:

1. Open the Coder Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Coder Groups**).
2. From the 'Coder Group Name' dropdown, select **1:Does Not Exist** and add the required codecs as shown in the figure below.

Figure 33: Configuring Coder Group for 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.

2.15 Configuring an IP Profile

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

To configure an IP Profile:

1. Open the IP Profiles 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 12: Configuration Example: Teams IP Profile

Parameter	Value
General	
Name	**Teams** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Secured**
SBC Early Media	
Remote Early Media RTP Detection Mode	**By Media** (required, as 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**
RFC 2833 Mode	**Extend**
RTCP Mode	**Generate Always** (required, as some ITSPs do not send RTCP packets while in Hold mode, but Microsoft expected them)
ICE Mode	**Lite** (required only when Media Bypass is enabled on Teams)
SBC Signaling	
SIP 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 Replaces 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 with their default values.	

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

4. Click **+New** to add the IP Profile for the SIP Trunks. Configure the parameters using the table below as reference.

Table 13: Configuration Example: SIP Trunk IP Profile

Parameter	Value
General	
Name	**SIPTrunks** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Not Secured**
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**
Play RBT To Transferee	**Yes** (required, as some SIP Trunks do not play ring-back tone during transfer)
Remote 3xx Mode	**Handle Locally**
All other parameters can be left unchanged with their default values.	

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

> Teams Hold music is not supported by Microsoft in consultative transfer of a PSTN call. The transferee will hear silence during the transfer. To overcome this issue, it is possible to configure SBC to play music during a consultative transfer. To do this, refer to Section 2.22.

2.16 Configuring IP Groups

This section describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the SBC communicates. This can be a server (e.g., IP-PBX or SIP Trunk) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

To configure an IP Groups:

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Configure IP Group for the Teams Direct Routing:

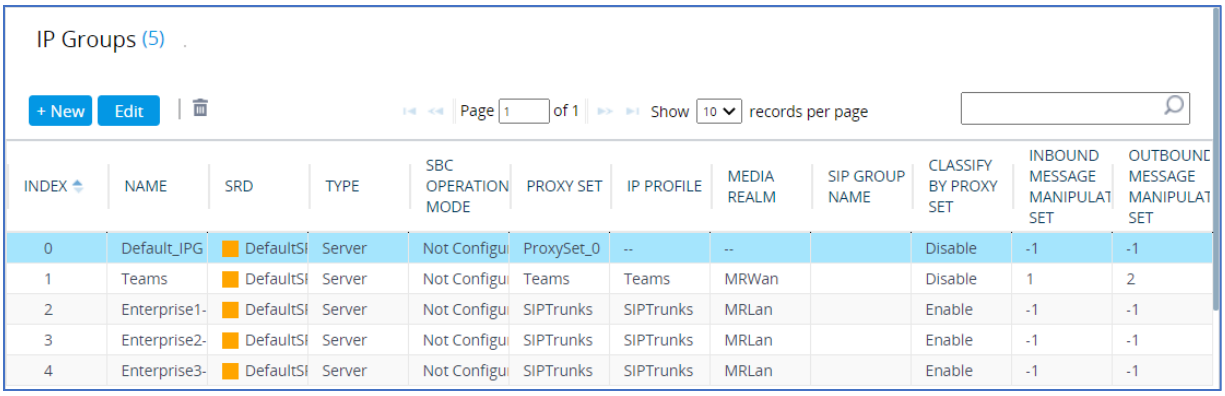
Parameter	Value
Name	**Teams**
Topology Location	**Up**
Type	**Server**
Proxy Set	**Teams**
IP Profile	**Teams**
Media Realm	**MRWan**
Classify By Proxy Set	**Disable**
Local Host Name	**<FQDN name of the SBC in the carrier tenant>** (based on our example, *customers.ACeducation.info)*.
Teams Direct Routing Mode	**Enable** (Enables the SBC to include Microsoft's proprietary X-MS-SBC header in outgoing SIP INVITE and OPTIONS messages in a Microsoft Teams Direct Routing environment. The header is used by Microsoft Teams to identify vendor equipment. The header's value is in the format 'Audiocodes/<model>/<firmware>').
Always Use Src Address	**Yes**
Call Setup Rules Set ID	**0**
Tags	**Teams**
Inbound Message Manipulation Set ID	**1**
Outbound Message Manipulation Set	**2**
Proxy Keep-Alive using IP Group settings	**Enable**
All other parameters can be left unchanged with their default values.	

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

Parameter	Value
Name	**Enterprise1-SIPTrunk** (arbitrary descriptive name)
Type	**Server**
Proxy Set	**SIPTrunks**
IP Profile	**SIPTrunks**
Media Realm	**MRLan** or **MRWan** (according to your network environment)
Call Setup Rules Set ID	**1**
Tags	**<FQDN name of the SBC in the customer tenant>** (For example, *sbc1.customers.ACeducation.info)*
All other parameters can be left unchanged with their default values.	

The configured IP Groups are shown in the figure below:

Figure 34: Configuration Example IP Groups in IP Group Table



IP Groups (5)

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULAT SET	OUTBOUNI MESSAGE MANIPULAT SET
0	Default_IPG	🟧 DefaultSI	Server	Not Configu	ProxySet_0	--	--		Disable	-1	-1
1	Teams	🟧 DefaultSI	Server	Not Configu	Teams	Teams	MRWan		Disable	1	2
2	Enterprise1-	🟧 DefaultSI	Server	Not Configu	SIPTrunks	SIPTrunks	MRLan		Enable	-1	-1
3	Enterprise2-	🟧 DefaultSI	Server	Not Configu	SIPTrunks	SIPTrunks	MRLan		Enable	-1	-1
4	Enterprise3-	🟧 DefaultSI	Server	Not Configu	SIPTrunks	SIPTrunks	MRLan		Enable	-1	-1

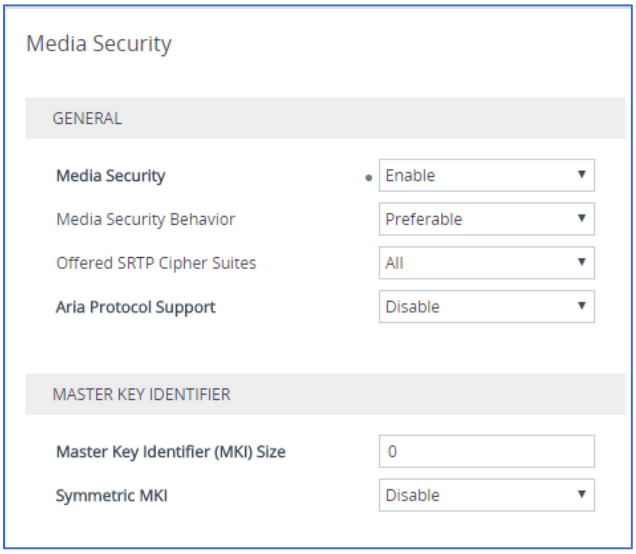
2.17 Configuring SRTP

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 35: Configuring 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**.

2.18 Configuring Message Condition Rules

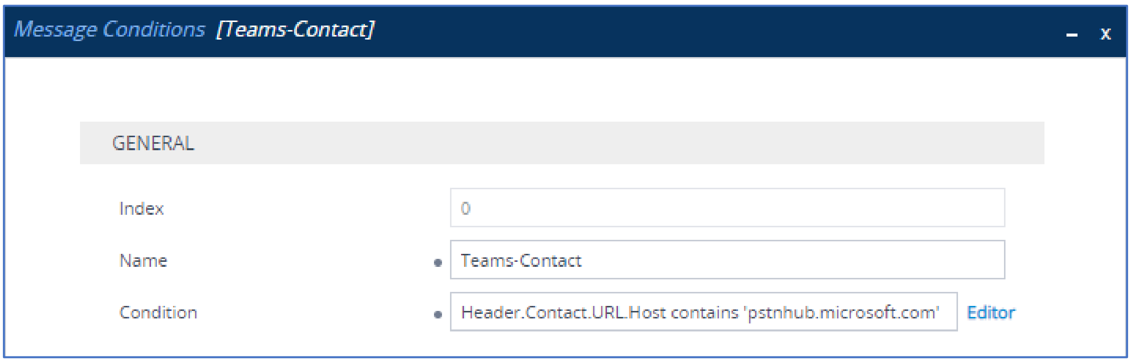
This section describes how to configure the Message Condition Rules. A Message Condition defines special conditions (pre-requisites) for incoming SIP messages. These rules can be used as additional matching criteria for the IP-to-IP routing rules in the IP-to-IP Routing table.

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 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**.

2.19 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. Configure Classification rules as shown in the table below:

Table 14: Classification Rules

Index	Name	Source SIP Interface	Source IP Address	Message Condition	Action Type	Source IP Group
0	Teams_52_112 (arbitrary name)	Teams	52.112.*.*	Teams-Contact	Allow	Teams
1	Teams_52_113 (arbitrary name)	Teams	52.113.*.*	Teams-Contact	Allow	Teams
2	Teams_52_114 (arbitrary name)	Teams	52.114.*.*	Teams-Contact	Allow	Teams
3	Teams_52_115 (arbitrary name)	Teams	52.115.*.*	Teams-Contact	Allow	Teams
4	Teams_52_122 (arbitrary name)	Teams	52.122.*.*	Teams-Contact	Allow	Teams
5	Teams_52_123 (arbitrary name)	Teams	52.123.*.*	Teams-Contact	Allow	Teams

3. Click **Apply**.

2.20 Configuring IP-to-IP Call Routing Rules

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

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

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

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

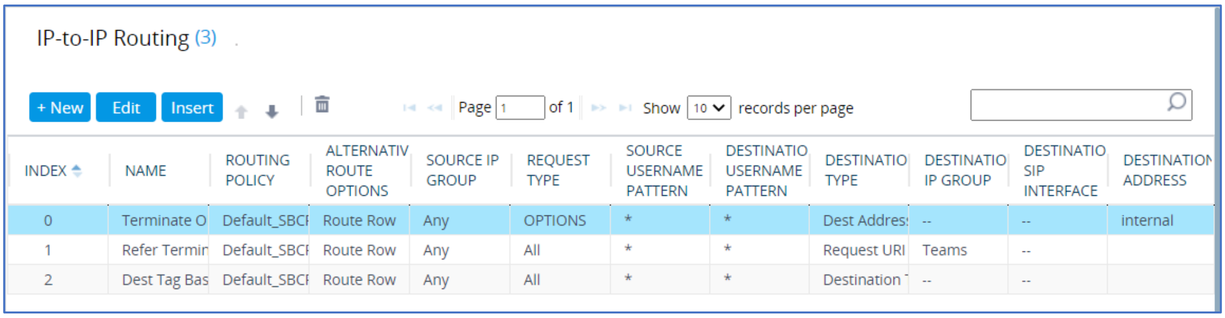
To configure IP-to-IP routing rules:

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

Index	Name	Source IP Group	Request Type	Call Triger	ReRoute IP Group	Dest Type	Dest IP Group	Dest Address
0	Terminate OPTIONS	Any	OPTIONS			Dest Address		internal
1	Refer Termination (arbitrary name)	Any		REFER	Teams	Request URI	Teams	
2	Dest Tag Based Routing (arbitrary name)	Any				Destination Tag	-	-

The configured routing rules are shown in the figure below:

Figure 37: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



IP-to-IP Routing (3)

INDEX	NAME	ROUTING POLICY	ALTERNATIV ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATIO USERNAME PATTERN	DESTINATIO TYPE	DESTINATIO IP GROUP	DESTINATIO SIP INTERFACE	DESTINATION ADDRESS
0	Terminate O	Default_SBCI	Route Row	Any	OPTIONS	*	*	Dest Addres:	--	--	internal
1	Refer Termir	Default_SBCI	Route Row	Any	All	*	*	Request URI	Teams	--	
2	Dest Tag Bas	Default_SBCI	Route Row	Any	All	*	*	Destination ˈ	--	--	

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

2.21 Configuring Firewall Settings

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

To configure a firewall rule:

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

Table 15: Firewall Table Rules

Index	Source IP	Subnet Prefix	Start Port	End Port	Protocol	Use Specific Interface	Interface ID	Allow Type
0	<Public DNS Server IP> (e.g., 8.8.8.8)	32	0	65535	Any	Enable	WAN_IF	Allow
1	52.112.0.0	14	0	65535	TCP	Enable	WAN_IF	Allow
2	52.122.0.0	15	0	65535	TCP	Enable	WAN_IF	Allow
3	xxx.xxx.xxx.xxx	32	0	65535	UDP	Enable	WAN_IF	Allow
49	0.0.0.0	0	0	65535	Any	Enable	WAN_IF	Block

For information about prerequisites and planning your deployment, refer to Plan Direct Routing.

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. See an example in the row of index 3.

2.22 Configuring SBC To Play Music On Hold (Optional)

Teams Hold music is not supported by Microsoft in consultative transfer of a PSTN call. The transferee will hear silence during the transfer. To overcome this issue, it is possible to configure SBC to play music during a consultative transfer. To do this, a Prerecorded Tones (PRT) file needs to be prepared and loaded to the SBC. This section shows how to load a PRT file to the SBC. For a detailed procedure how to create a Prerecorded Tones (PRT) file, refer to appropriated AudioCodes' device *User Manual* document.

Update configuration of the SIP Trunk IP Profile:

1. Open the Proxy Sets table (Setup > Signaling and Media > Coders and Profiles > IP Profiles).
2. Choose SIP Trunk IP Profile, created in the Section 2.15 on the page 33. Configure the parameters using the table below as reference.

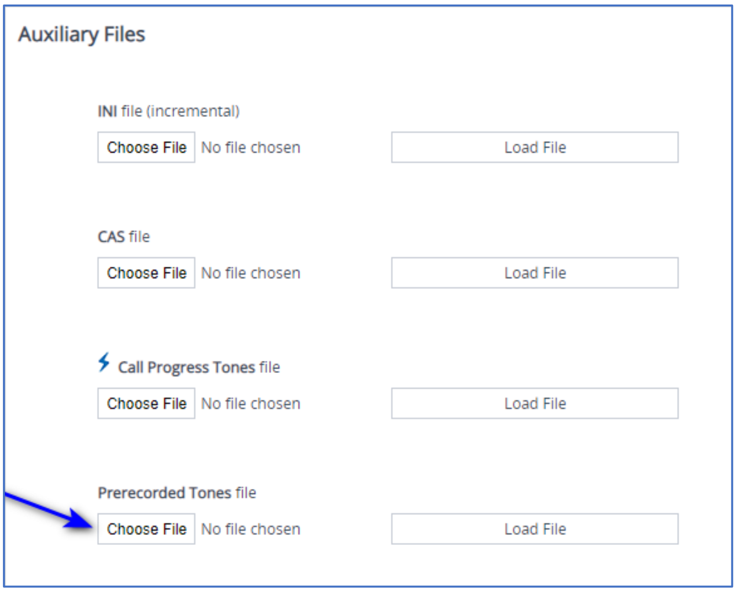
Table 16: Update Configuration of the SIP Trunk IP Profile

Parameter	Value
SBC Hold	
Remote Hold Format	**Send Only**
Reliable Held Tone Source	**No**
Play Held Tone	**Internal**

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

To load PRT file to the device using the Web interface:

1. Open the Auxiliary Files page:
   - Toolbar: From the **Actions** drop-down menu, choose **Auxiliary Files**.
   - Navigation tree: **Setup** menu > **Administration** tab > **Maintenance** folder > **Auxiliary Files**.



2. Click the **Browse** button corresponding to the **Prerecorded Tones** file type that you want to load, navigate to the folder in which the file is located, and then click **Open**; the name and path of the file appear in the field next to the **Browse** button.
3. Click the **Load File** button corresponding to the file you want to load.
4. Save the loaded auxiliary files to flash memory.

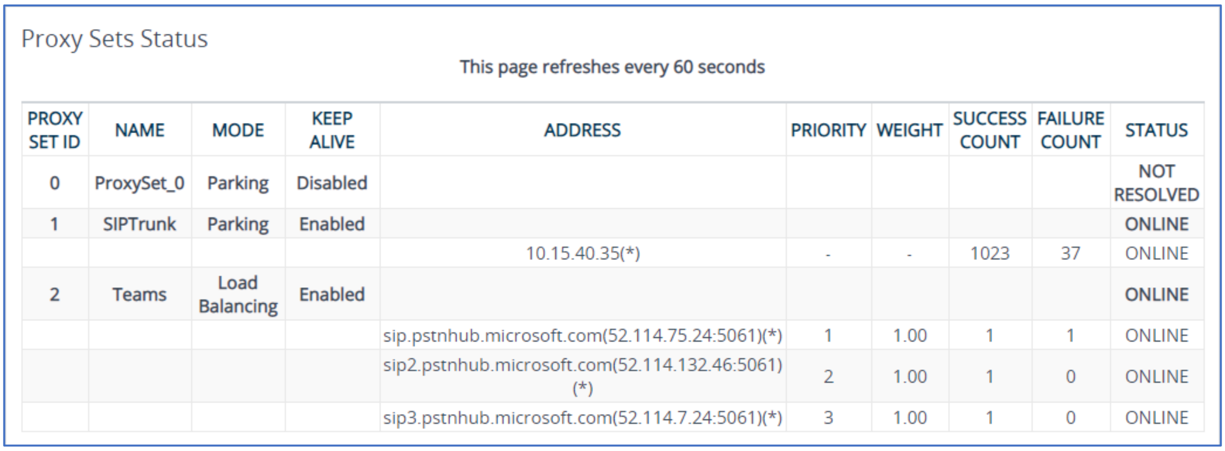
3 Verifying the Pairing between the SBC and Direct Routing

After you've paired the SBC with Direct Routing, validate that the SBC can successfully exchange OPTIONs with Direct Routing.

To validate the pairing using SIP OPTIONS:

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

Figure 38: Proxy Set Status



Proxy Sets Status

This page refreshes every 60 seconds

PROXY SET ID	NAME	MODE	KEEP ALIVE	ADDRESS	PRIORITY	WEIGHT	SUCCESS COUNT	FAILURE COUNT	STATUS
0	ProxySet_0	Parking	Disabled						NOT RESOLVED
1	SIPTrunk	Parking	Enabled						ONLINE
				10.15.40.35(*)	-	-	1023	37	ONLINE
2	Teams	Load Balancing	Enabled						ONLINE
				sip.pstnhub.microsoft.com(52.114.75.24:5061)(*)	1	1.00	1	1	ONLINE
				sip2.pstnhub.microsoft.com(52.114.132.46:5061)(*)	2	1.00	1	0	ONLINE
				sip3.pstnhub.microsoft.com(52.114.7.24:5061)(*)	3	1.00	1	0	ONLINE

4 Making a Test Call

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

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

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

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

To configure the Test Agent:

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

To start, stop and restart a test call:

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

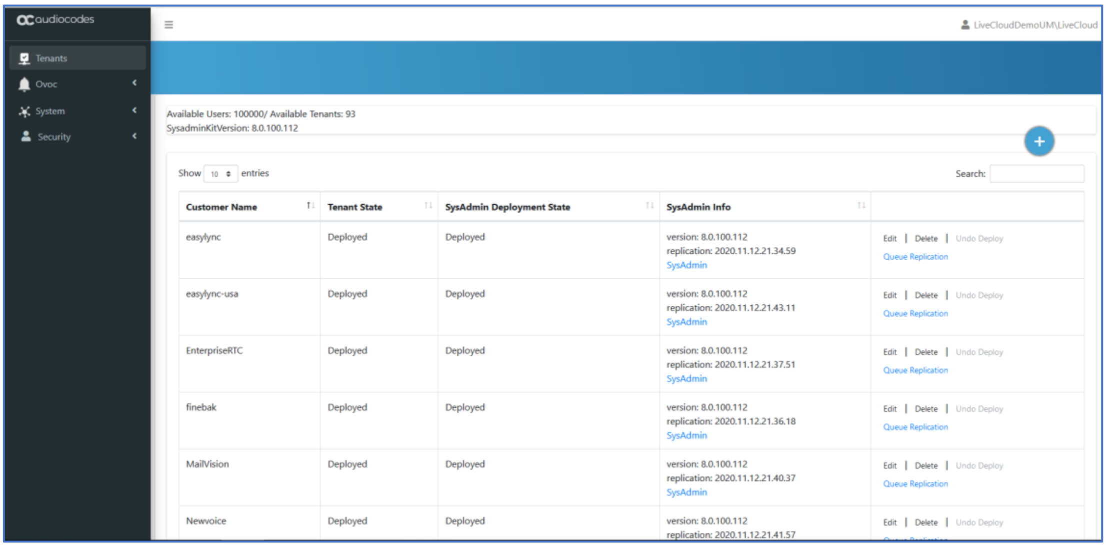
5 Configuring via UMP 365 (Optional)

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

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

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

Figure 39: Provider Main Screen View



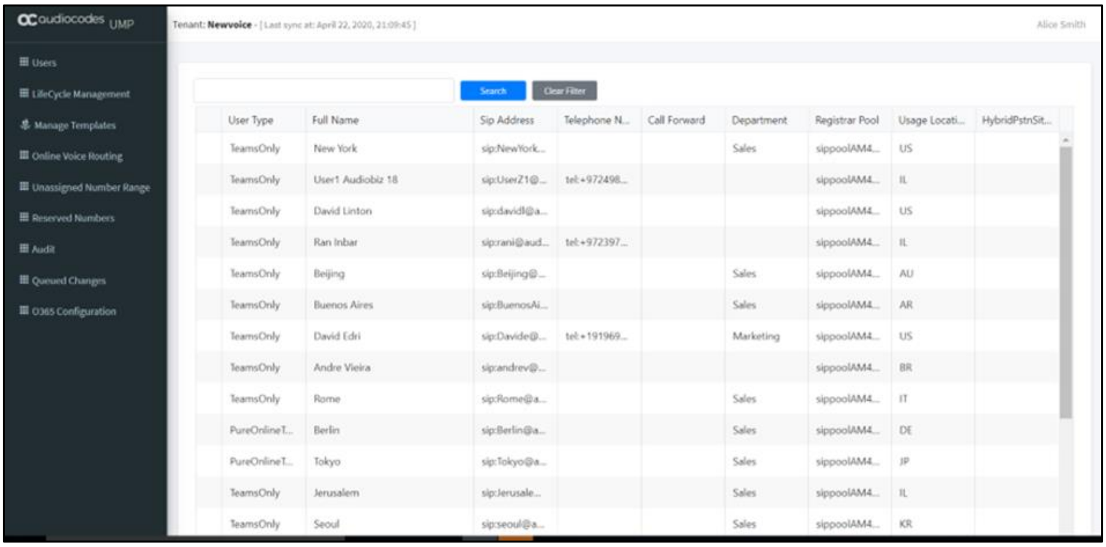
Available Users: 100000/ Available Tenants: 93
SysadminKitVersion: 8.0.100.112

Show 10 entries Search:

Customer Name	Tenant State	SysAdmin Deployment State	SysAdmin Info	
easylync	Deployed	Deployed	version: 8.0.100.112 replication: 2020.11.12.21.34.59 SysAdmin	Edit | Delete | Undo Deploy Queue Replication
easylync-usa	Deployed	Deployed	version: 8.0.100.112 replication: 2020.11.12.21.43.11 SysAdmin	Edit | Delete | Undo Deploy Queue Replication
EnterpriseRTC	Deployed	Deployed	version: 8.0.100.112 replication: 2020.11.12.21.37.51 SysAdmin	Edit | Delete | Undo Deploy Queue Replication
finebak	Deployed	Deployed	version: 8.0.100.112 replication: 2020.11.12.21.36.18 SysAdmin	Edit | Delete | Undo Deploy Queue Replication
MailVision	Deployed	Deployed	version: 8.0.100.112 replication: 2020.11.12.21.40.37 SysAdmin	Edit | Delete | Undo Deploy Queue Replication
Newvoice	Deployed	Deployed	version: 8.0.100.112 replication: 2020.11.12.21.41.57	Edit | Delete | Undo Deploy

- View typical Microsoft 365 Tenant Phone Numbers
- Audit activities
- View queue for tasks status and results
- Update the Microsoft 365 Setting

Figure 40: Customer Tenant view – User List



Tenant: **Newvoice** - [Last sync at: April 22, 2020, 21:09:45]

User Type	Full Name	Sip Address	Telephone N...	Call Forward	Department	Registrar Pool	Usage Locati...	HybridPstnSit...
TeamsOnly	New York	sip:NewYork...			Sales	sippoolAM4...	US	
TeamsOnly	User1 Audiobiz 18	sip:UserZ1@...	tel:+972498...			sippoolAM4...	IL	
TeamsOnly	David Linton	sip:davidl@a...				sippoolAM4...	US	
TeamsOnly	Ran Inbar	sip:rani@aud...	tel:+972397...			sippoolAM4...	IL	
TeamsOnly	Beijing	sip:Beijing@...			Sales	sippoolAM4...	AU	
TeamsOnly	Buenos Aires	sip:BuenosAi...			Sales	sippoolAM4...	AR	
TeamsOnly	David Edri	sip:Davide@...	tel:+191969...		Marketing	sippoolAM4...	US	
TeamsOnly	Andre Vieira	sip:andrev@...				sippoolAM4...	BR	
TeamsOnly	Rome	sip:Rome@a...			Sales	sippoolAM4...	IT	
PureOnlineT...	Berlin	sip:Berlin@a...			Sales	sippoolAM4...	DE	
PureOnlineT...	Tokyo	sip:Tokyo@a...			Sales	sippoolAM4...	JP	
TeamsOnly	Jerusalem	sip:Jerusale...			Sales	sippoolAM4...	IL	
TeamsOnly	Seoul	sip:seoul@a...			Sales	sippoolAM4...	KR	

For a detailed description, refer to *AudioCodes User Management Pack 365 SP Edition Installation and Administration Guide.*

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

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

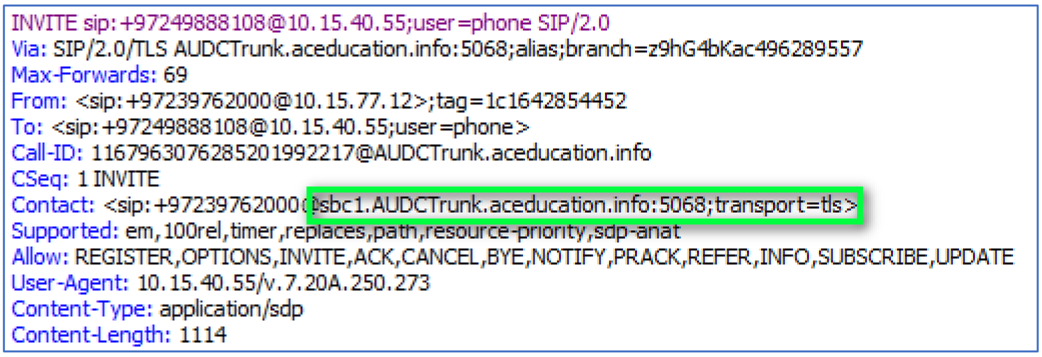
This section covers the high-level requirements for the SIP syntax used in 'INVITE' and 'OPTIONS' messages. You can use the information presented here as a first step when troubleshooting unsuccessful calls. AudioCodes has found that most issues are related to incorrect syntax in SIP messages.

A.1 Terminology

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

A.2 Syntax Requirements for 'INVITE' Messages

Figure 41: Example of an 'INVITE' Message

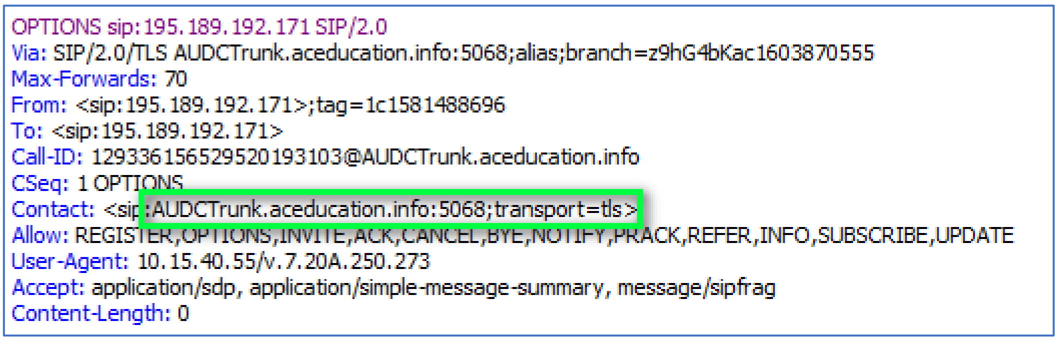


```
INVITE sip:+97249888108@10.15.40.55;user=phone SIP/2.0
Via: SIP/2.0/TLS AUDCTrunk.aceducation.info:5068;alias;branch=z9hG4bKac496289557
Max-Forwards: 69
From: <sip:+97239762000@10.15.77.12>;tag=1c1642854452
To: <sip:+97249888108@10.15.40.55;user=phone>
Call-ID: 1167963076285201992217@AUDCTrunk.aceducation.info
CSeq: 1 INVITE
Contact: <sip:+97239762000@sbc1.AUDCTrunk.aceducation.info:5068;transport=tls>
Supported: em,100rel,timer,replaces,path,resource-priority,sdp-anat
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: 10.15.40.55/v.7.20A.250.273
Content-Type: application/sdp
Content-Length: 1114
```

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

A.3 Requirements for 'OPTIONS' Messages Syntax

Figure 42: Example of 'OPTIONS' message



```
OPTIONS sip:195.189.192.171 SIP/2.0
Via: SIP/2.0/TLS AUDCTrunk.aceducation.info:5068;alias;branch=z9hG4bKac1603870555
Max-Forwards: 70
From: <sip:195.189.192.171>;tag=1c1581488696
To: <sip:195.189.192.171>
Call-ID: 129336156529520193103@AUDCTrunk.aceducation.info
CSeq: 1 OPTIONS
Contact: <sip:AUDCTrunk.aceducation.info:5068;transport=tls>
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: 10.15.40.55/v.7.20A.250.273
Accept: application/sdp, application/simple-message-summary, message/sipfrag
Content-Length: 0
```

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

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

Table 17: Syntax Requirements for an 'OPTIONS' Message

Parameter	Where configured	How to configure
Contact	**Setup** > **Signaling and Media** > **Core Entities** > **IP Groups**> <Group Name> > **Local Host Name** In IP Group, 'Contact' must be configured. In this field ('Local Host Name'), define the local host name of the SBC as a string, for example, *sbc1.AUDCTrunk.ACeducation.info*. The name changes the host name in the call received from the IP Group.	See Section 2.16.

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 18: 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	-
	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 (RFC5245) – recommended ■ Client also has Transport Relays	-
	Audio codecs	■ G711 ■ Silk (Teams clients) ■ Opus (WebRTC clients) - only if Media Bypass is used ■ G729	-
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

Teams Direct Routing has three FQDNs:

- **sip.pstnhub.microsoft.com** [Global FQDN. The SBC attempts to use it as the first priority region. When the SBC sends a request to resolve this name, the Microsoft Azure DNS server returns an IP address pointing to the primary Azure datacenter assigned to the SBC. The assignment is based on performance metrics of the datacenters and geographical proximity to the SBC. The IP address returned corresponds to the primary FQDN.]
- **sip2.pstnhub.microsoft.com** [Secondary FQDN. Geographically maps to the second priority region.]
- **sip3.pstnhub.microsoft.com** [Tertiary FQDN. Geographically maps to the third priority region.]

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

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

B.1 Failover Mechanism

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

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

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

International Headquarters
Naimi Park
6 Ofra Haza Street
Or Yehuda, 6032303, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
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-33524**