Configuration Note

AudioCodes Mediant™ Family of Media Gateways & Session Border Controllers

Connecting AudioCodes' SBC to Microsoft Teams Direct Routing

Enterprise Model

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 SBC User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
Gateway and SBC CLI Reference Guide
SIP Message Manipulation Reference Guide

Document Revision Record

LTRT	Description
LTRT-TAP	Added Chapter "Direct Routing Media Optimization" for Direct Routing Media Optimization Routing between Microsoft Phone System (Cloud PBX) and SBC devices.
LTRT-TAP	Updates in Section "Configuring SBC for Media Optimization Proxy SBC"; Site SBCs Re-configuration.
13320	Updates to IP Profile configuration in Chapter "Configuring SBC for Media Optimization Proxy SBC" and Chapter "Site SBCs Re-configuration"
13320	Updates to Table "Configuration Example: Teams IP Profile" (updated parameters Remote REFER Mode and Remote 3xx Mode), Added Table "Configuration Example: SIP Trunk IP Profile (toward Remote SBC)", Changed title for Table "Configuration Example: Teams IP Profile (through the Proxy SBC) and Table "Configuration Example: SIP Trunk IP Profile (toward SIP Provider/ Media Gateway)".
13321	Updates to the names of the IP Group Media optimization parameters to "Local Media Optimization and "Teams Local Media Optimization Initial Behavior", Added Appendix "IP Profile – Quick Guidelines"
13322	Added Sections "Adopt Gateway Application to Work with Local Media Optimization" and Appendix C "Local Media Optimization – Quick Guidelines".
13323	Update to the "Related Documentation" table to include the Mediant 1000B Gateway & E-SBC product.
13324	All information related to Local Media Optimization was removed to a separate document. "Connecting AudioCodes' SBC to Microsoft Teams Direct Routing Local Media Optimization".
13325	Update for Message Manipulation rule towards Microsoft Teams.
13326	"SipSignallingPort" replaced by "SipSignalingPort".
13327	Update to the Firewall Table Rules table with two additional IP addresses of the new infrastructure in Japan.

LTRT	Description
13328	Update to SIP Trunk IP Profile and validated firmware version.
13329	Added section for overcoming problem of not playing music on hold during conversational transfer.
13331	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.
13332	TLS Root Certificate Authority updated by Microsoft.
13334	Updated Classification Table with stricter rules to only allow for documented Microsoft SIP Proxies.
13336	Note added detailing deployment in Office 365 GCC DoD and GCC High environments.
13339	TLS Private Key size of 1024 was removed. Microsoft subnets were updated in the Classification and Firewall tables.
33525	Teams IP Profile updatedwith 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 Enterprise model and refers to the AudioCodes SBC configuration only.

For configuring the Office 365 side, go to https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure.

This document is intended for IT or telephony professionals.

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

1.1 About Microsoft 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 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.

2 Topology Example

Teams Direct Routing can be implemented in the *Enterprise* or *Hosting* Models.

2.1 Enterprise Model Implementation

The figures below show examples of the connection topology between AudioCodes SBC and Teams Direct Routing Enterprise Model SIP Trunk with Teams Direct Routing Enterprise Model assume the following topology setup:

- Enterprise deployed with the IP-PBX (optional) and administrator's management station, located on the LAN.
- Enterprise deployed with Teams Phone System Direct Routing Interface located on the WAN for enhanced communication within the Enterprise.
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using Teams Direct Routing Enterprise Model's SIP Trunking service.
- AudioCodes SBC is implemented to interconnect between the SIP Trunk and Teams Direct Routing located in the WAN.

The figure below illustrates this topology example:

Figure 1: Connection Topology with SIP Trunk on the LAN

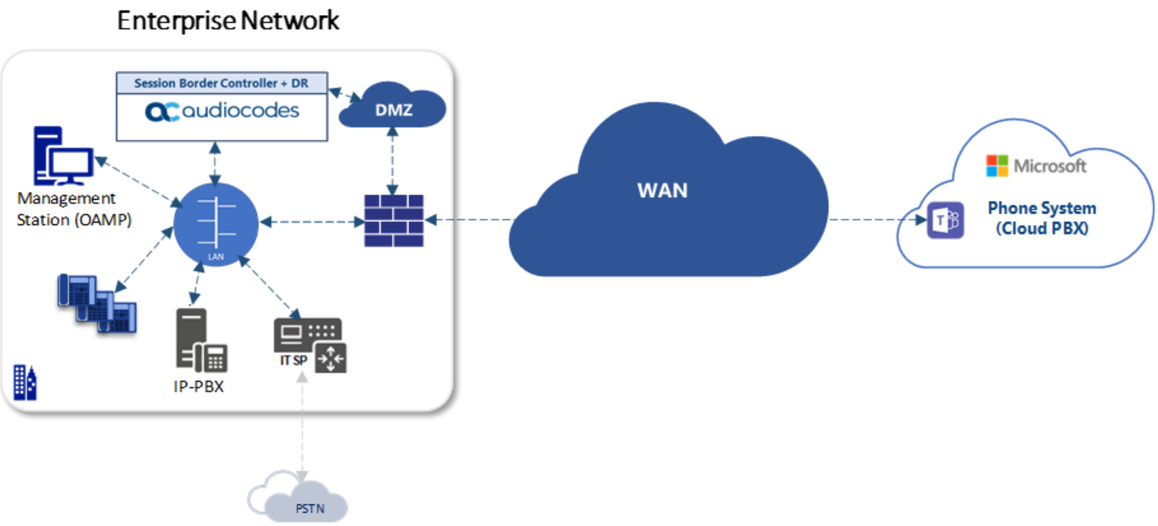
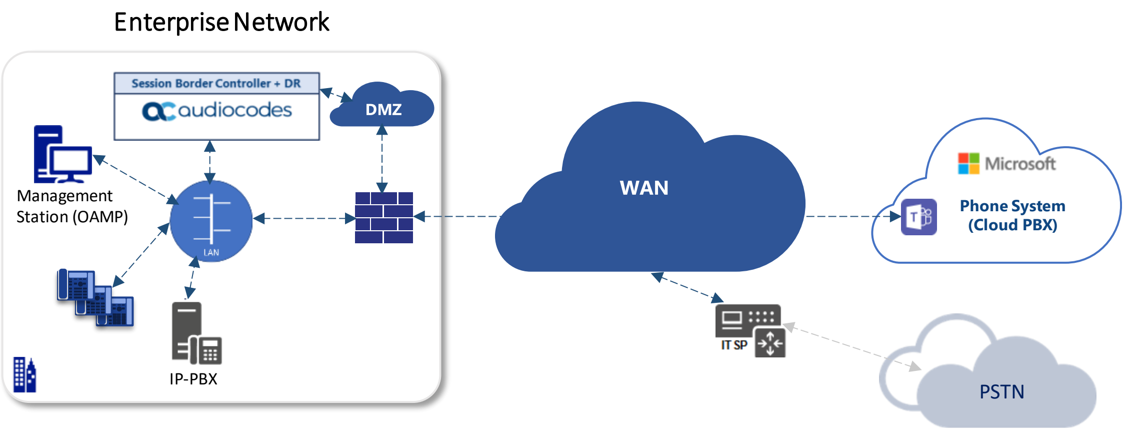


Figure 2: Connection Topology with SIP Trunk on the WAN



- 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, refer to AudioCodes' *SIP Trunk Configuration Notes* (in the interoperability suite of documents).
- This document only includes basic Teams Direct Routing configuration. Customers who would like to implement Direct Routing Local Media Optimization Routing between Microsoft Phone System (Cloud PBX) and SBC devices, refer to AudioCodes' Connecting AudioCodes' SBC to Microsoft Teams Direct Routing Local Media Optimization Configuration Notes document.

2.2 Environment Setup

The example topology includes the following environment setup:

Table 1: Environment Setup

Area	Setup
Network	■ Teams Direct Routing environment is located on the Enterprise's (or Service Provider's) WAN ■ Teams Direct Routing Enterprise Model SIP Trunk is located on the LAN
Signaling Transcoding	■ Teams Direct Routing operates with SIP-over-TLS transport type ■ Teams Direct Routing Enterprise Model SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	■ Teams Direct Routing supports G.711A-law, G.711U-law, G.729 and SILK (NB and WB) coders ■ Teams Direct Routing Enterprise Model SIP Trunk supports G.711A-law, G.711U-law, and G.729 coders
Media Transcoding	■ Teams Direct Routing operates with SRTP media type ■ Teams Direct Routing Enterprise Model SIP Trunk operates with RTP media type

2.3 Infrastructure Prerequisites

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

Table 2-2: Infrastructure Prerequisites

Infrastructure Prerequisite	Details
Certified Session Border Controller (SBC)	See Microsoft's document *Plan Direct Routing*.
SIP Trunks connected to the SBC	
Enterprise Office 365 Tenant	
Domains	
Public IP address for the SBC	
Fully Qualified Domain Name (FQDN) for the SBC	
Public DNS entry for the SBC	
Public trusted certificate for the SBC	
Firewall ports for Direct Routing Signaling	
Firewall IP addresses and ports for Direct Routing Media	
Media Transport Profile	
Firewall ports for Teams Clients Media	

3 Configuring Teams Direct Routing

This section describes an example of Teams Direct Routing configuration to operate with AudioCodes SBC.

3.1 Prerequisites

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

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

3.2 SBC Domain Name in the Teams Enterprise Model

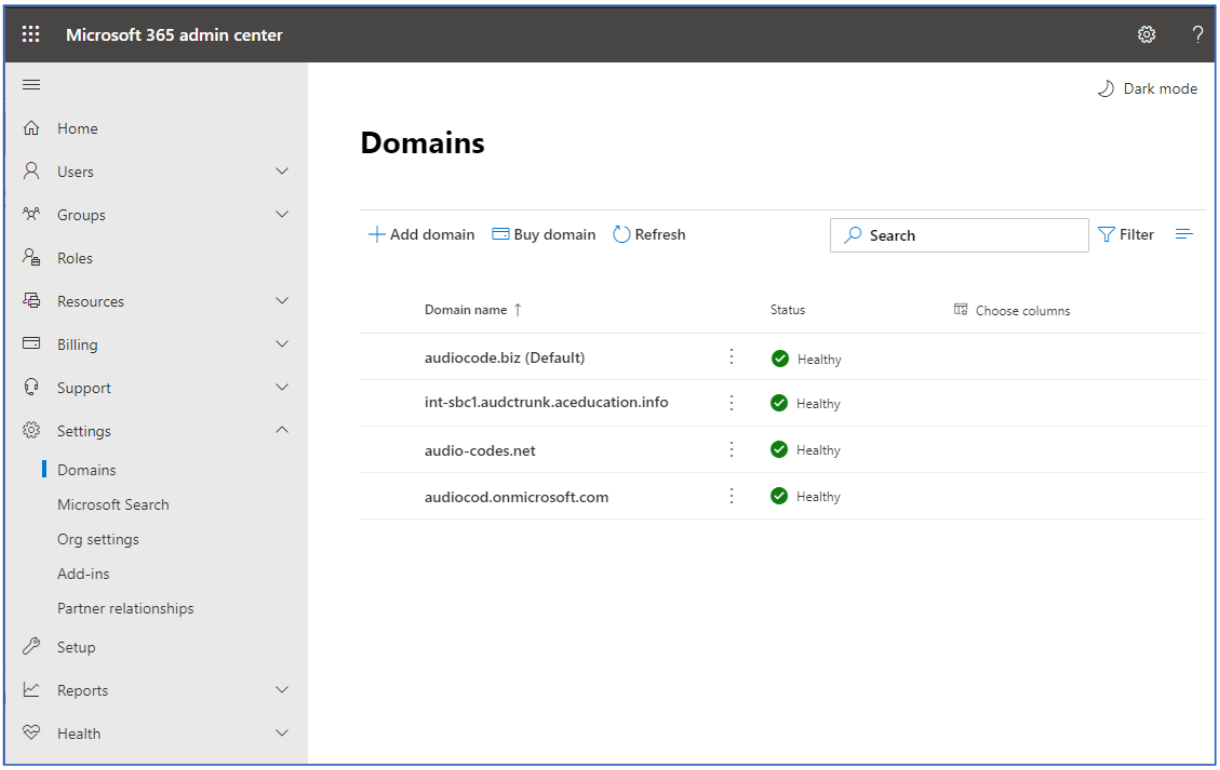
The SBC domain name must be from one of the names registered in 'Domains' of the Enterprise Office 365 tenant. You cannot use the ***.onmicrosoft.com** tenant for the domain name. For example, in Figure 3, the administrator registered the following DNS names for the Enterprise Office 365 tenant:

Table 3: DNS Names Registered by an Administrator for an Enterprise Office 365 Tenant

DNS name	Can be used for SBC FQDN	Examples of FQDN names
ACeducation.info	Yes	**Valid names**: ■ sbc.ACeducation.info ■ ussbcs15.ACeducation.info ■ europe.ACeducation.info **Invalid name:** sbc1.europe.ACeducation.info (requires registering domain name europe.atatum.biz in 'Domains' first)
adatumbiz.onmicrosoft.com	No	Using ***.onmicrosoft.com** domains is not supported for SBC names
hybridvoice.org	Yes	**Valid names**: ■ sbc1.hybridvoice.org ■ ussbcs15.hybridvoice.org ■ europe.hybridvoice.org **Invalid name:** sbc1.europe.hybridvoice.org (requires registering domain name europe.hybridvoice.org in 'Domains' first).

Users can be from any SIP domain registered for the Enterprise Office 365 tenant. For example, you can provide users user@ACeducation.info with the SBC FQDN **int-sbc1.audctrunk.aceducation.info** so long as both names are registered for this tenant.

Figure 3: Example of Registered DNS Names

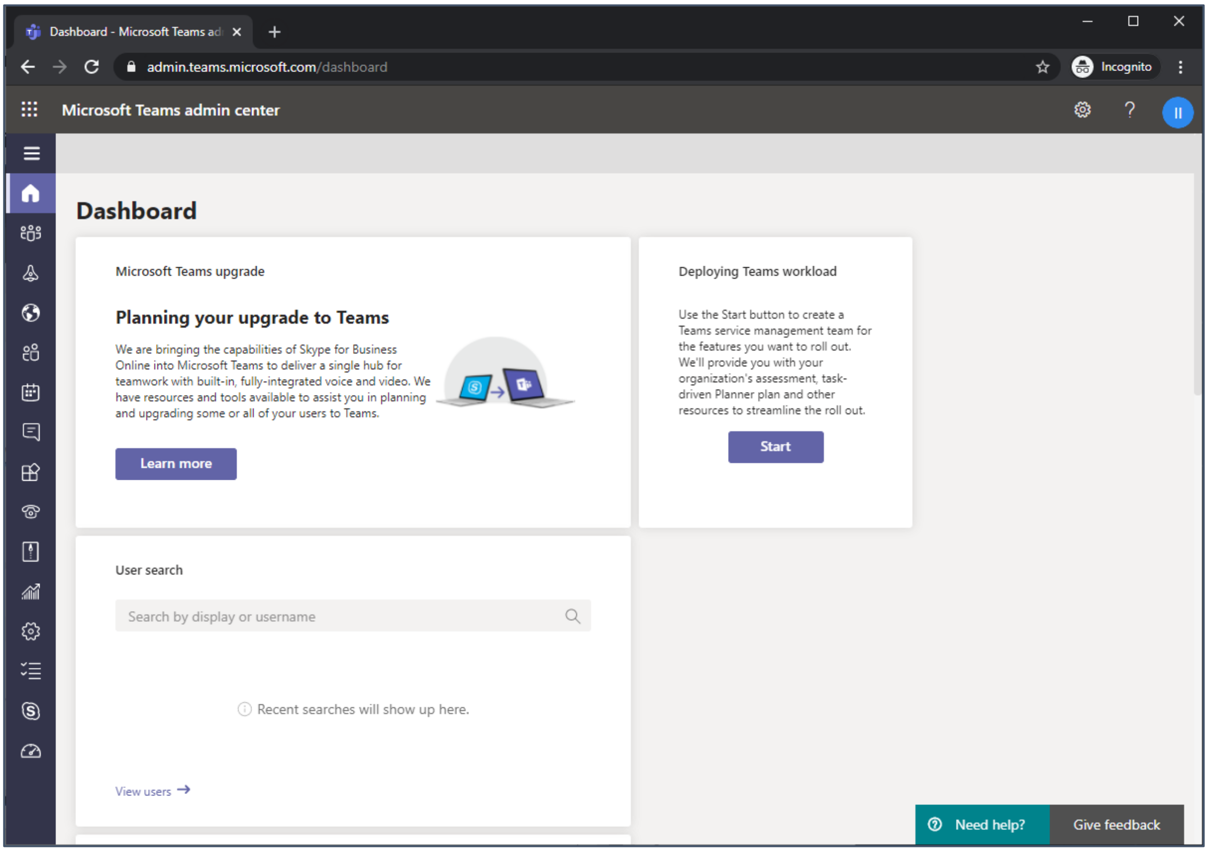


During creation of the Domain you will be forced to create public DNS record (**int-sbc1.audctrunk.aceducation.info** in our example.)

3.3 Example of the Enterprise Office 365 Tenant Direct Routing Configuration

Configuration can be done using the web or with PowerShell. For the web, login to the Teams Admin Center (https://admin.teams.microsoft.com) with Tenant Administrator credentials.

Figure 4: Teams Admin Center



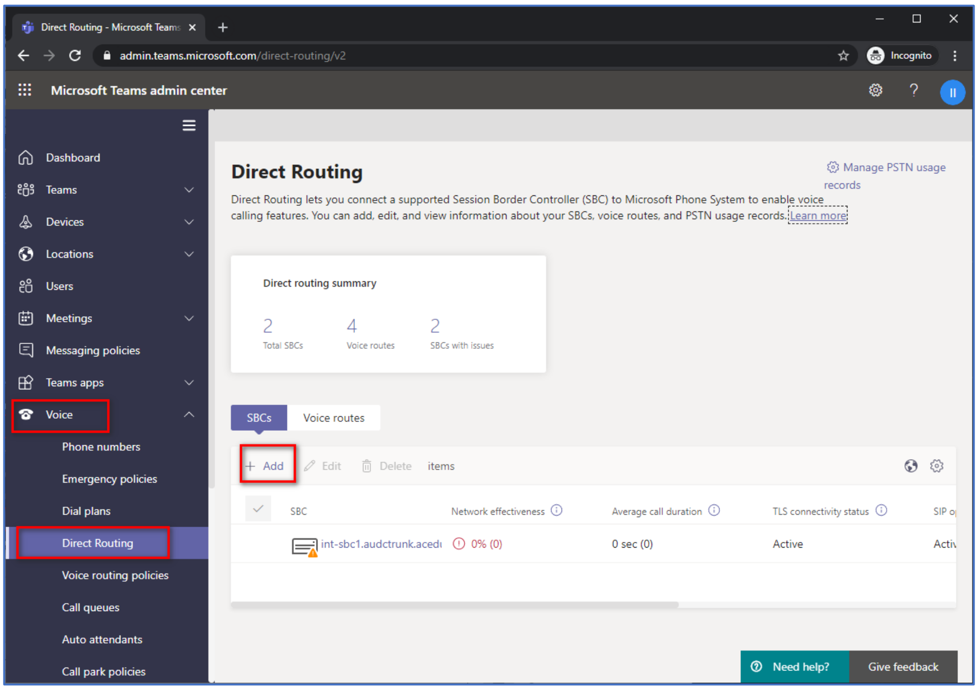
3.3.1 Adding New SBC to Direct Routing

The procedure below describes how add a new SBC to Direct Routing.

To add New SBC to Direct Routing:

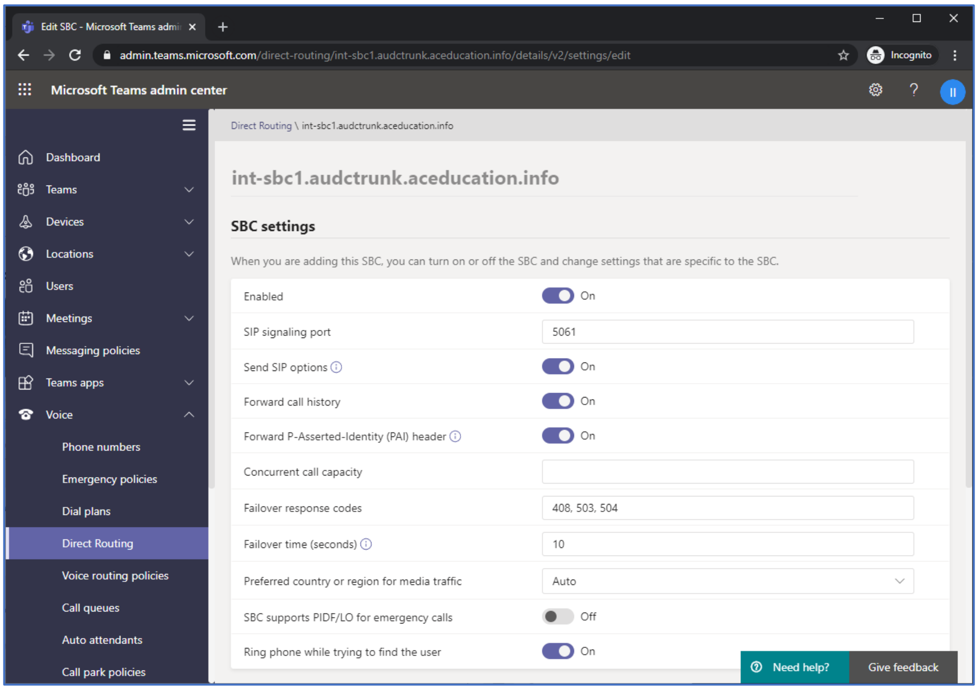
1. In the web interface, select **Voice**, and then click **Direct Routing**.
2. Under SBCs click **Add.**

Figure 5: Add new SBC to Direct Routing



3. Configure SBC.

Figure 6: Configure new SBC



You can use the following PowerShell command for creating a new Online PSTN Gateway:

```
New-CsOnlinePSTNGateway -Identity int-
sbc1.audctrunk.aceducation.info -SipSignalingPort 5061 -
ForwardCallHistory $True -ForwardPai $True -MediaBypass $True -
Enabled $True
```

Currently, enabling MediaBypass is available only through PowerShell.

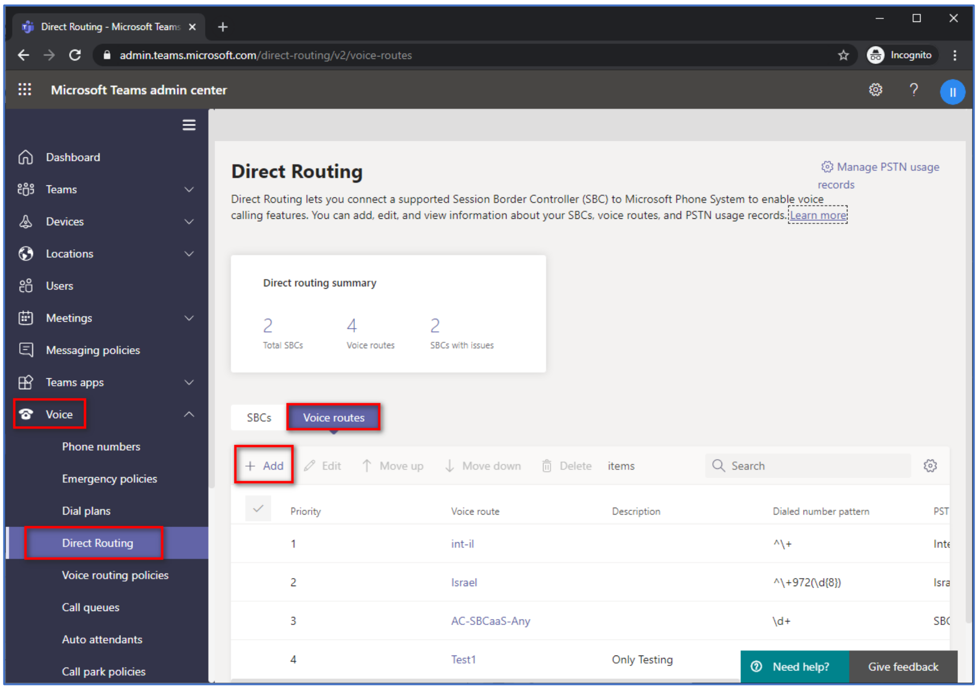
3.3.2 Adding Voice Route and PSTN Usage

The procedure below describes how add a voice route and PSTN usage.

To add voice route and PSTN usage:

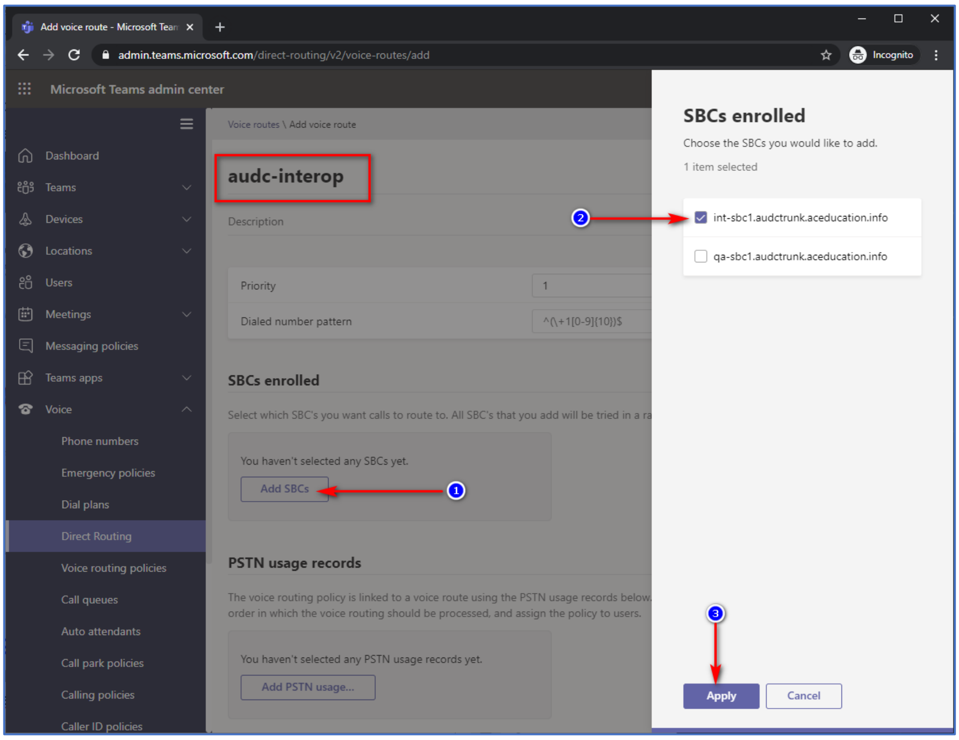
1. In the web interface, under **Direct Routing**, select **Voice routes**, and then click **Add**.

Figure 7: Add New Voice Route



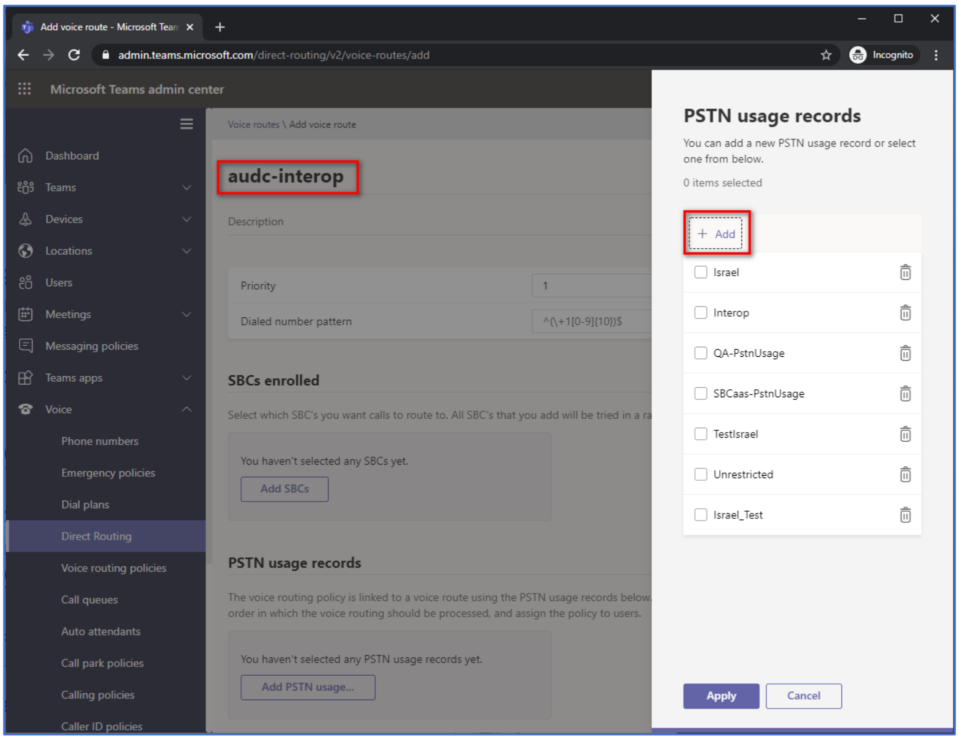
2. Create a new Voice Route and associate it with the SBC, configured in the previous step.

Figure 8: Associate SBC with new Voice Route



3. Add new (or associate existing) PSTN usage.

Figure 9: Associate PSTN Usage with New Voice Route



The same operations can be done using following PowerShell commands:

1. Creating PSTN Usage:

```
Set-CsOnlinePstnUsage -Identity Global -Usage @{Add="Interop"}
```

2. Creating new Online Voice Route and associating it with PSTN Usage:

```
New-CsOnlineVoiceRoute -Identity "audc-interop" -NumberPattern
"^\+" -OnlinePstnGatewayList int-sbc1.audctrunk.aceducation.info
-Priority 1 -OnlinePstnUsages "Interop"
```

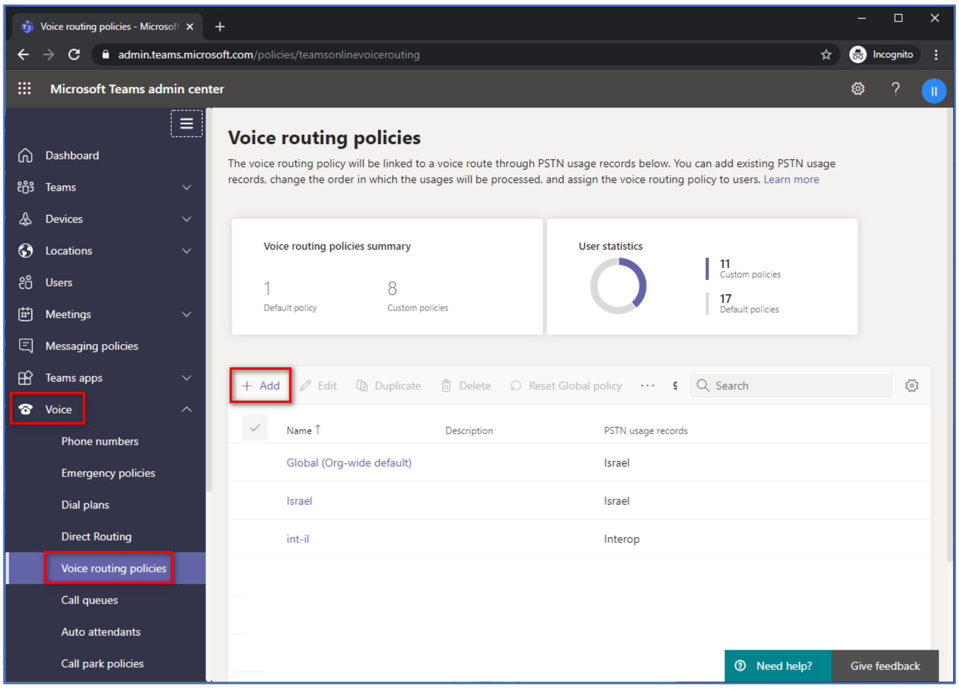
3.3.3 Adding Voice Routing Policy

The procedure below describes how add a voice routing policy

To add voice routing policy:

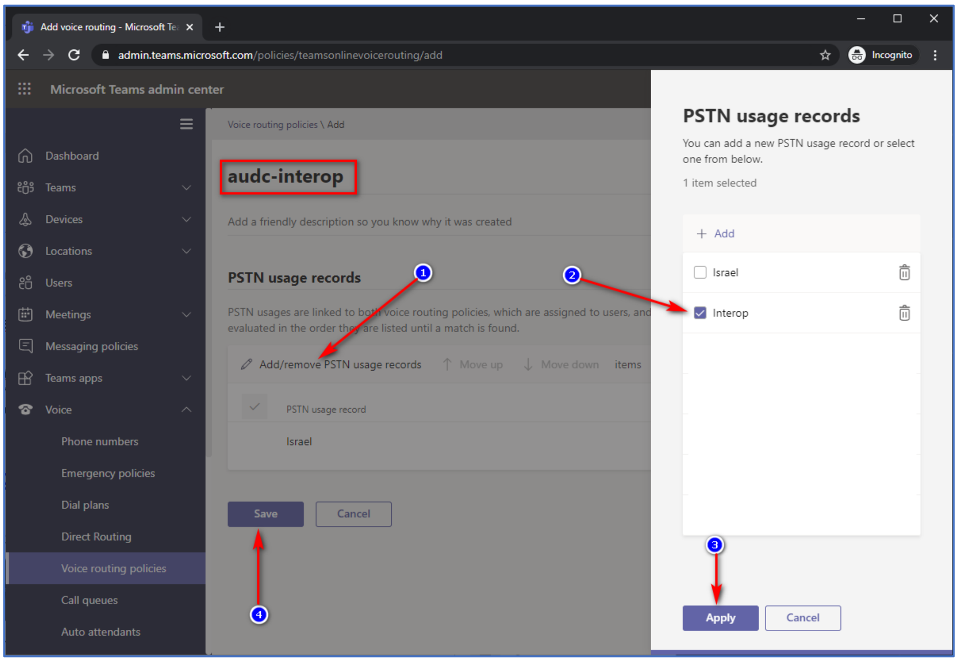
1. In the web interface, under **Voice**, select **Voice routing policies** and click **Add**.

Figure 10: Add New Voice Routing Policy



2. Create a new Voice Routing Policy and associate it with PSTN Usage, configured in the previous step.

Figure 11: Associate PSTN Usage with New Voice Routing Policy



The same operations can be done using following PowerShell command:

```
New-CsOnlineVoiceRoutingPolicy "audc-interop" -OnlinePstnUsages
"Interop"
```

> The commands specified in Sections 3.3.4 and 3.3.5, should be run **for each** Teams user in the Enterprise Office 365 tenant. They are currently available through PowerShell **only**.

3.3.4 Enabling Online User

Use following PowerShell command for enabling online user:

```
Set-CsPhoneNumberAssignment -Identity user1@company.com -
EnterpriseVoiceEnabled $true
```

```
Set-CsPhoneNumberAssignment -Identity user1@company.com -PhoneNumber
+12345678901 -PhoneNumberType DirectRouting
```

3.3.5 Assigning Online User to the Voice Routing Policy

Use following PowerShell command for assigning online user to the Voice Route:

Grant-CsOnlineVoiceRoutingPolicy** -PolicyName "**audc-interop**" -Identity **user1@company.com

3.3.6 Configuring with User Management Pack 365 (Optional)

As an alternative to PowerShell commands, AudioCodes recommend using User Management Pack 365 (UMP365). UMP365 provides a simple web-portal user interface for configuring and managing the Online Voice Route and associating it with PSTN Usage and PSTN Gateway. See examples below:

Figure 12: Example of Adding new Voice Route

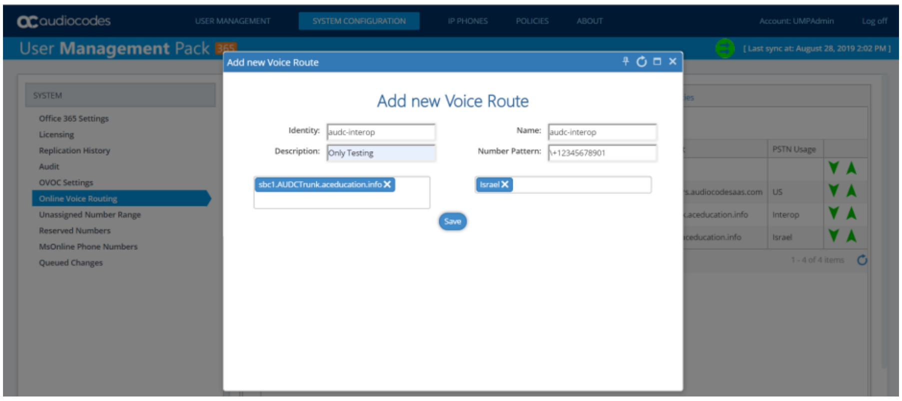
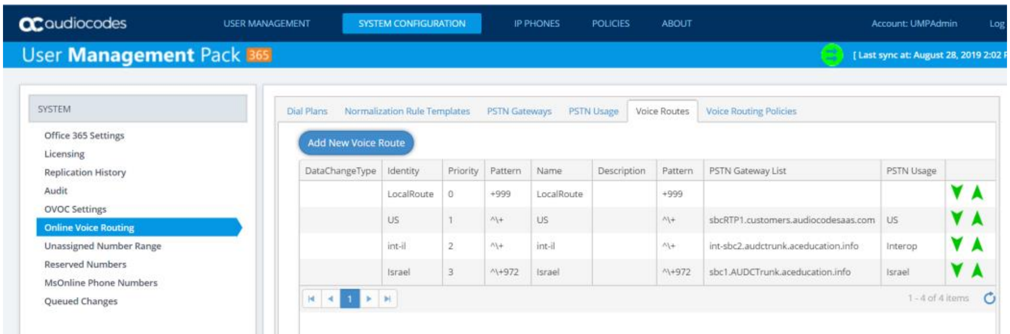


Figure 13: Example of Voice Routes Table



4 Configuring AudioCodes' SBC

This section provides example of step-by-step procedures on how to configure AudioCodes SBC for interworking between Teams Direct Routing and the Teams Direct Routing Enterprise Model SIP Trunk. These configuration procedures are based on the topology example described in Section 2.1 on page 3, and includes the following main areas:

- SBC LAN interface – administrator's management station and Teams Direct Routing Enterprise Model SIP Trunking (depend on topology) environment.
- SBC WAN interface - Teams Direct Routing Enterprise Model SIP Trunking (depend on topology) and Teams Direct Routing environment.

This configuration is done using the SBC's embedded Web server (hereafter, referred to as *Web interface*).

- For implementing Teams Direct Routing based on the configuration described in this section, AudioCodes SBC must be installed with a License Key. For more information, see Section 1.3 on page 2.
- The scope of this document does **not** cover all security aspects for configuring this topology. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document, which can be found at AudioCodes web site.

4.1 SBC Configuration Concept in Teams Direct Routing

The diagram below represents AudioCodes' device configuration concept.

Figure 14: SBC Configuration Concept

4.2 IP Network Interfaces Configuration

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

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

Figure 15: Network Interfaces in the Topology with SIP Trunk on the LAN

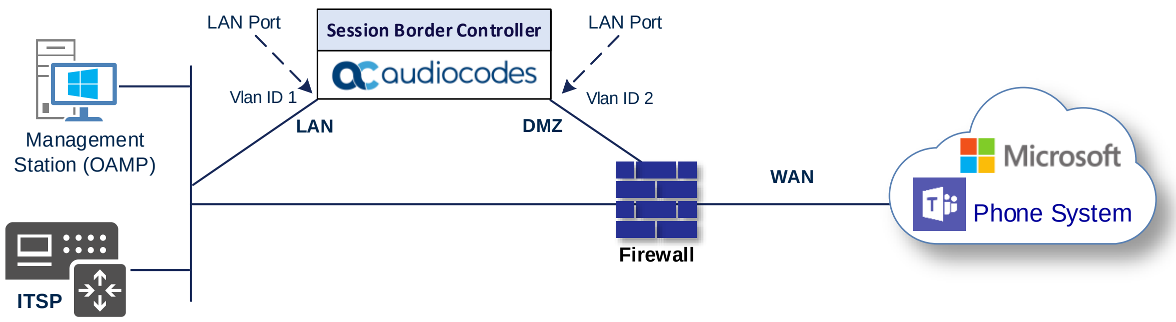
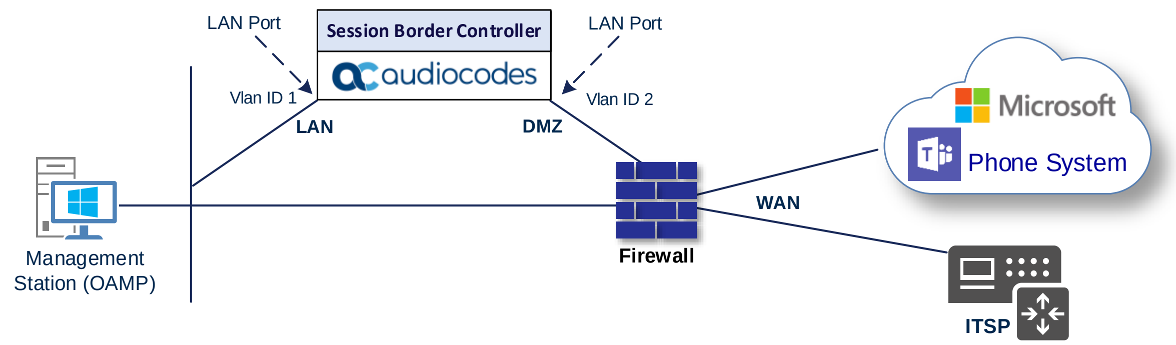


Figure 16: Network Interfaces in the Topology with SIP Trunk on the WAN



This Configuration Notes document provides an example topology with a SIP Trunk on the LAN.

4.2.1 Configuring VLANs

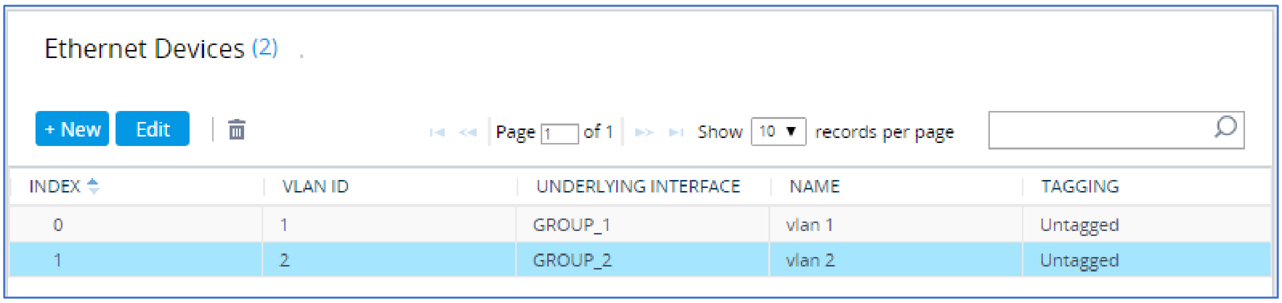
This section describes how to define VLANs for each of the following interfaces:

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

To configure the VLANs:

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

Figure 17: Configured VLAN IDs in Ethernet Device



4.2.2 Configuring 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:

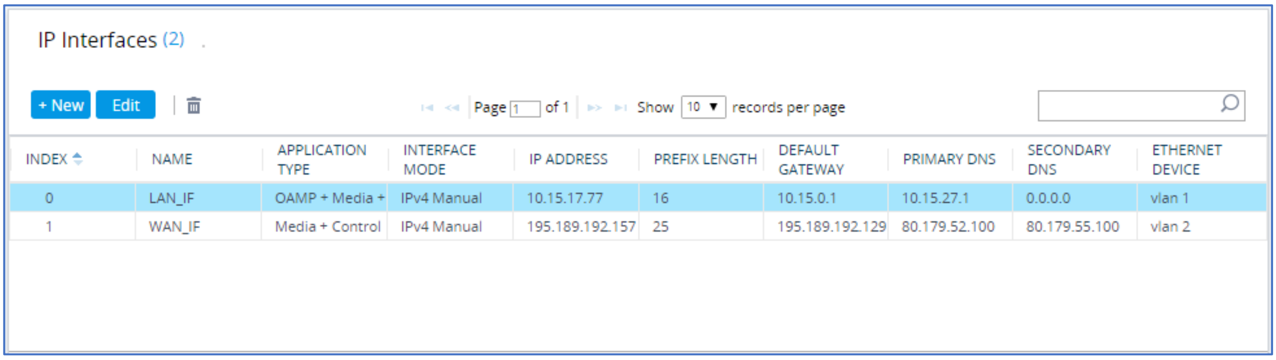
1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Configure the IP interfaces as follows (your network parameters might be different):

Table 4: 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 18: Configuration Example of the Network Interface Table


IP Interfaces (2)

+ New Edit Page 1 of 1 Show 10 records per page

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

4.3 SIP TLS Connection Configuration

This section describes how to configure the SBC for using a TLS connection with the Teams Direct Routing Phone System. This configuration is essential for a secure SIP TLS connection. The configuration instructions example 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: int-sbc1.audctrunk.aceducation.info
- SAN: int-sbc1.audctrunk.aceducation.info

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

The Phone System Direct Routing Interface allows ***only*** TLS connections from SBCs for SIP traffic with a certificate signed by one of the Trusted Certification Authorities.

Currently, supported Certification Authorities can be found in the following link:

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

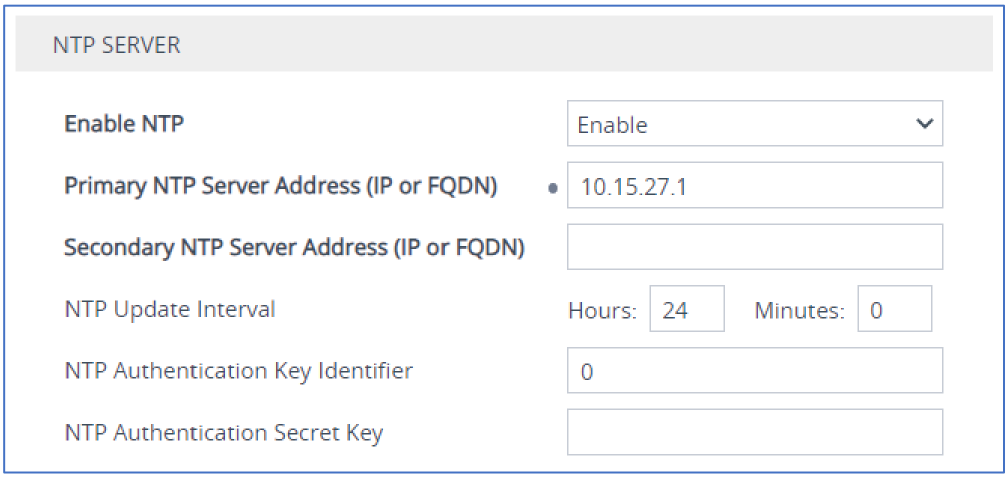
4.3.1 Configuring the NTP Server Address

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 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., **10.15.27.1**).

Figure 19: Configuring NTP Server Address



3. Click **Apply**.

4.3.2 Creating a TLS Context for Teams Direct Routing

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

The procedure involves the following main steps:

a. 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:

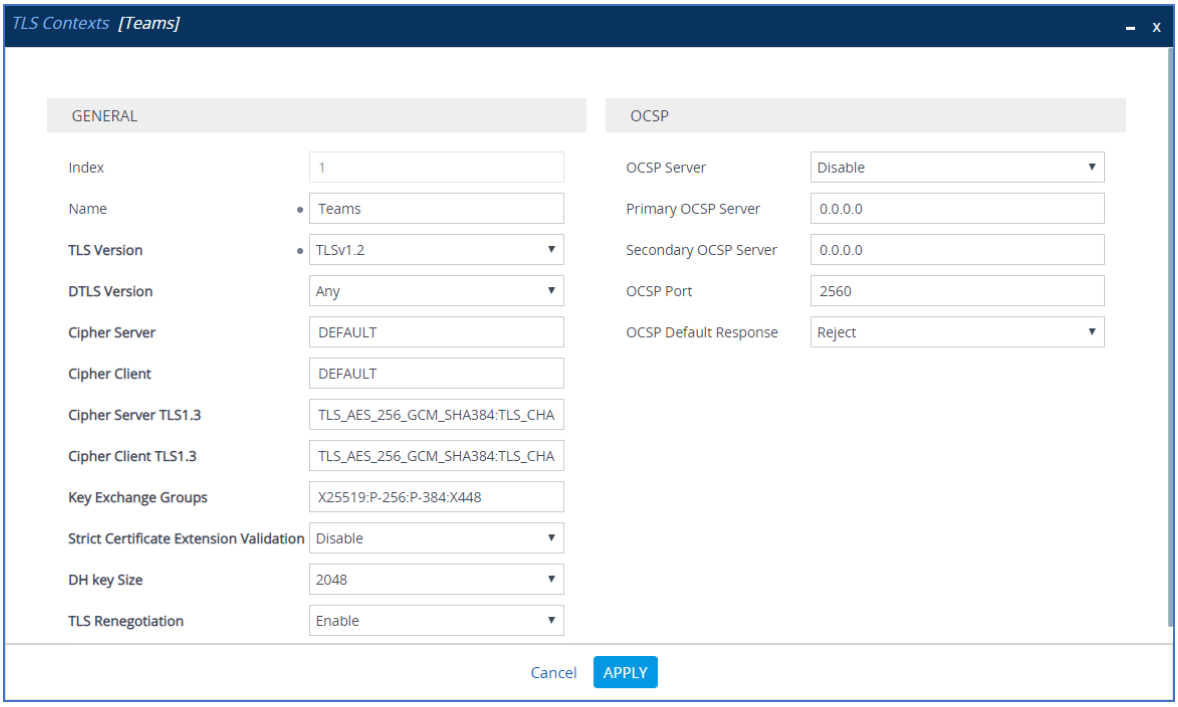
1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. Create a new TLS Context by clicking **+New** at the top of the interface, and then configure the parameters using the table below as reference.

Table 5: 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.		

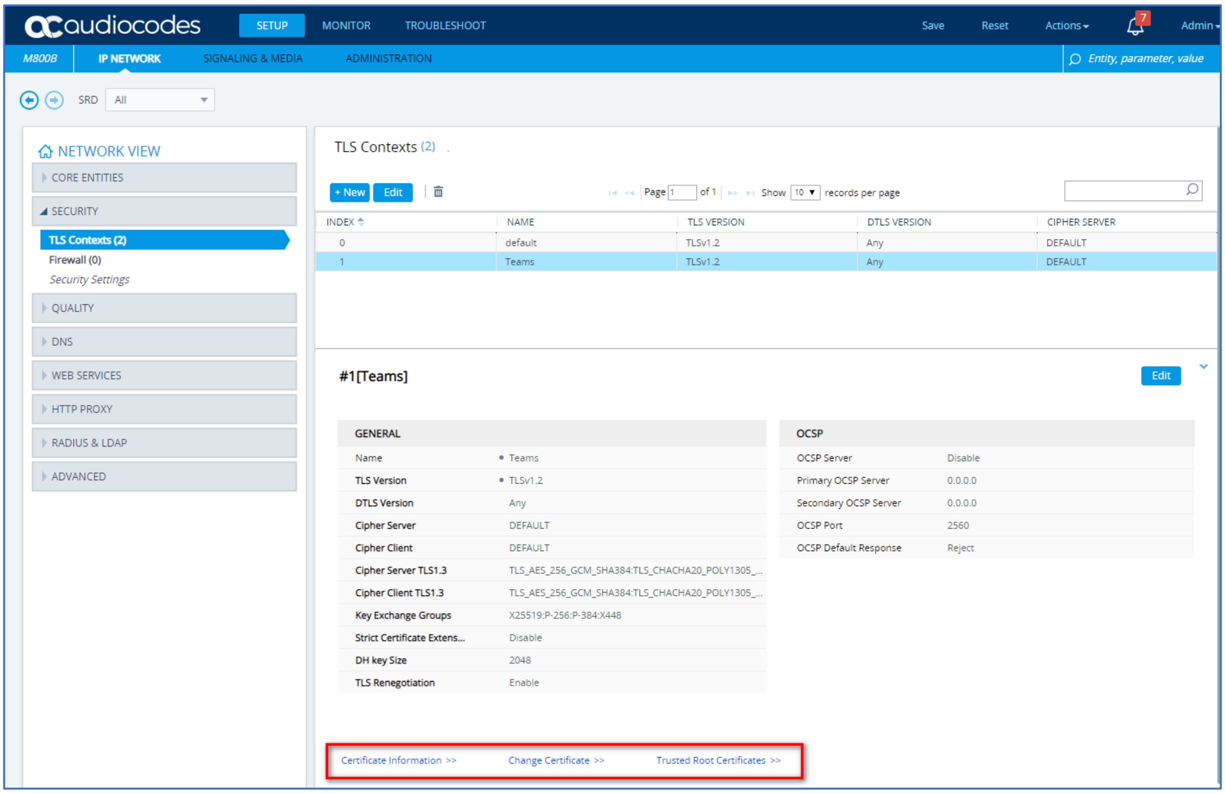
The table above exemplifies configuration focusing on interconnecting SIP and media. You might want to configure additional parameters according to your company's policies. For example, you might want to configure Online Certificate Status Protocol (OCSP) to check if SBC certificates presented in the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

Figure 20: Configuration of TLS Context for Direct Routing



3. Click **Apply**; you should see the new TLS Context and option to manage the certificates at the bottom of 'TLS Context' table.

Figure 21: Configured TLS Context for Direct Routing and Interface to Manage the Certificates



4.3.3 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.

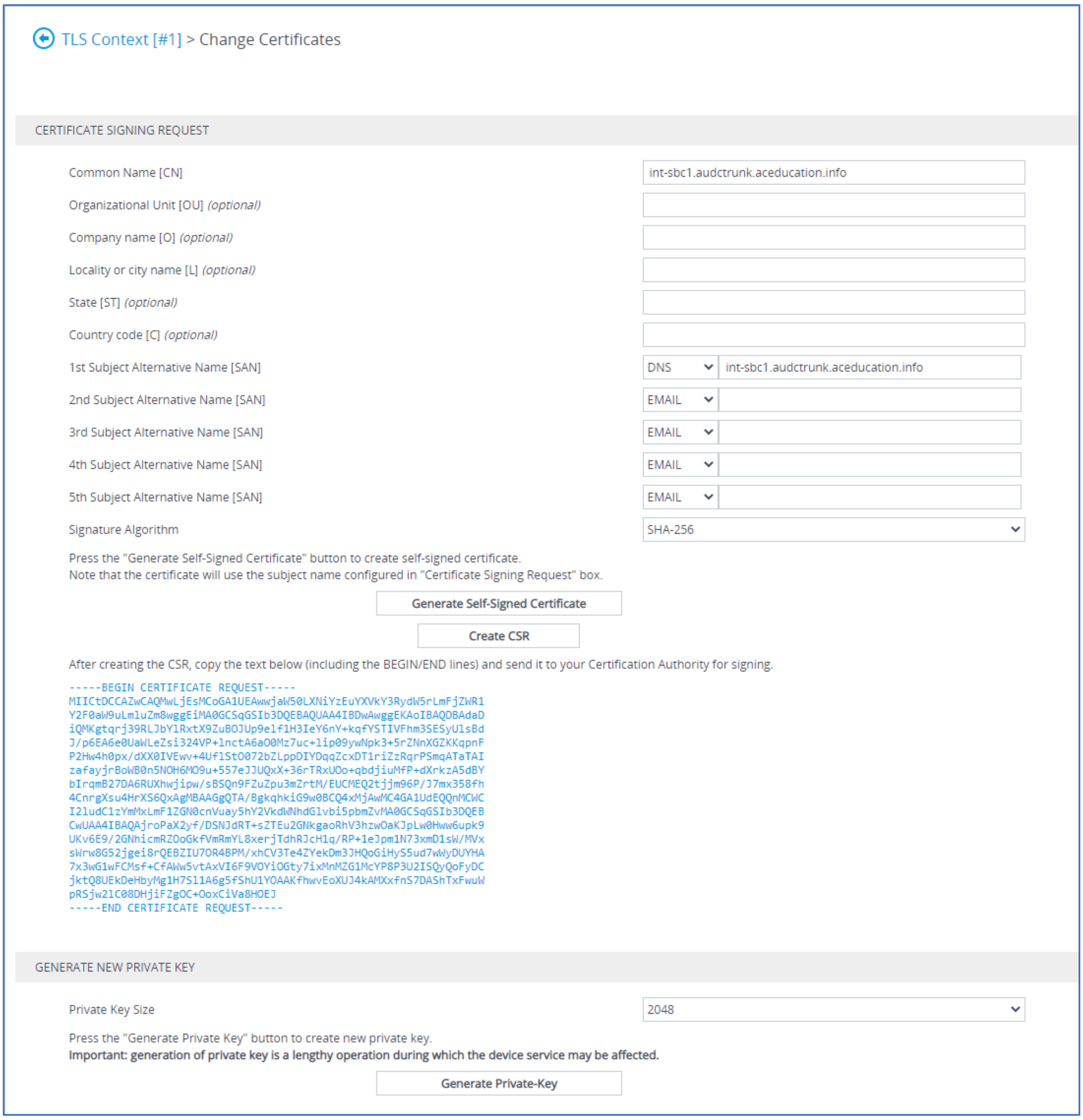
To generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority:

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 SBC FQDN name (based on example above, **int-sbc1.audctrunk.aceducation.info**).
   b. In the '1st Subject Alternative Name [SAN]' field, change the type to ‘DNS’, and then enter the SBC FQDN name (based on the example above, **int-sbc1.audctrunk.aceducation.info**).

> The domain portion of the Common Name [CN] and 1st Subject Alternative Name [SAN] must match the SIP suffix configured for Office 365 users.

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

Figure 22: Example of Certificate Signing Request – Creating CSR



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

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

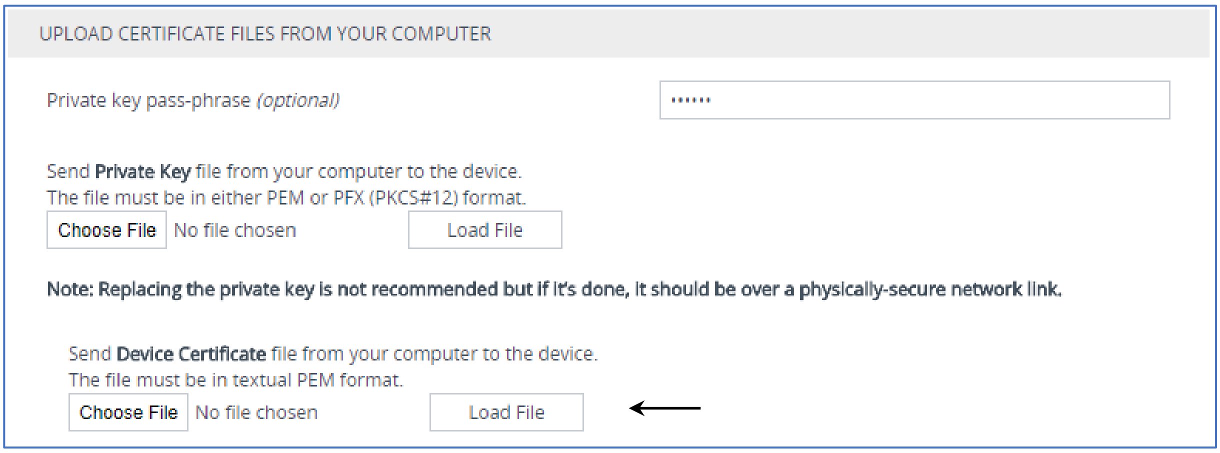
After obtaining the SBC signed and Trusted Root/Intermediate Certificate from the CA, install the following:

- SBC certificate
- Root / Intermediate certificates

To install the SBC certificate:

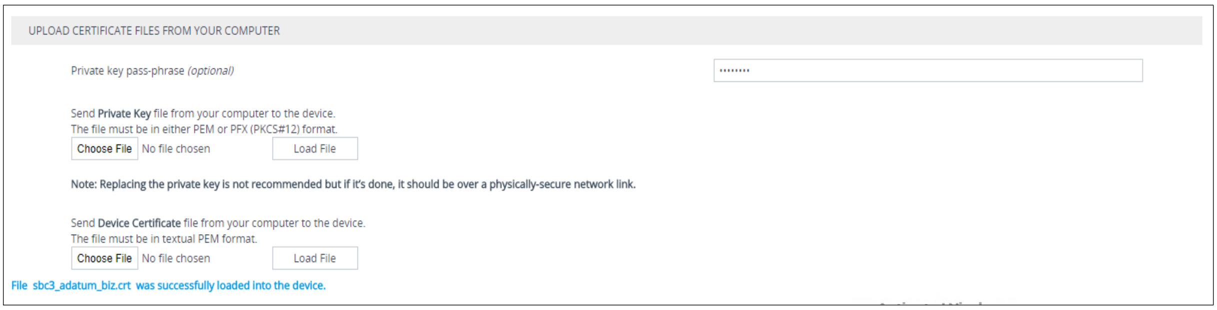
1. In the SBC's Web interface, return to the **TLS Contexts** page and do the following:
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
   b. Scroll down to the Upload 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 23: Uploading the Certificate Obtained from the Certification Authority



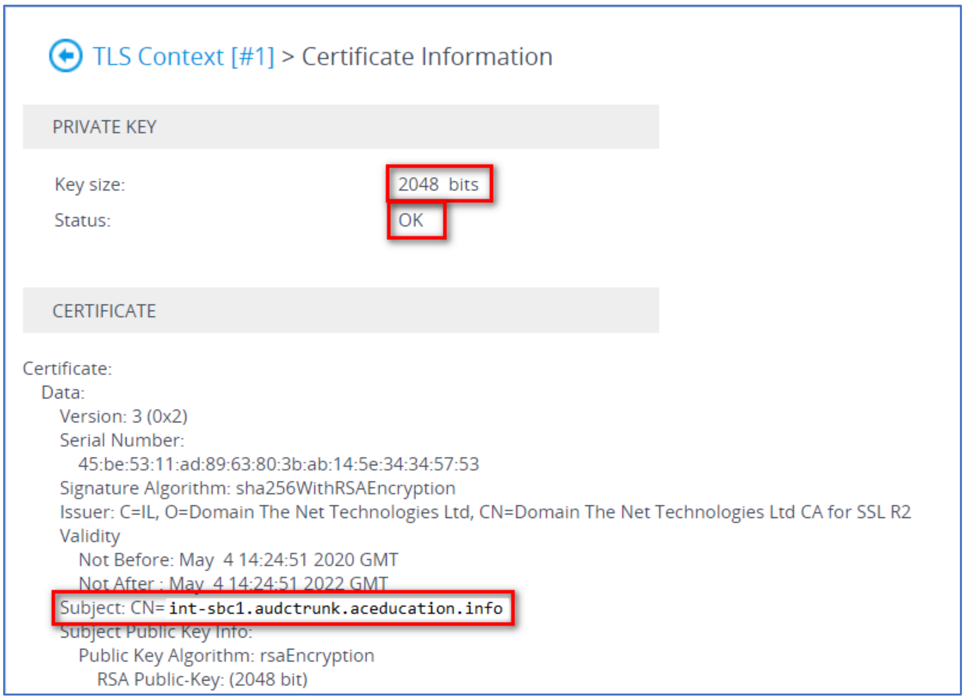
2. Validate that the certificate was uploaded correctly: A message indicating that the certificate was uploaded successfully is displayed in blue on the lower part of the page:

Figure 24: Message Indicating Successful Upload of the Certificate



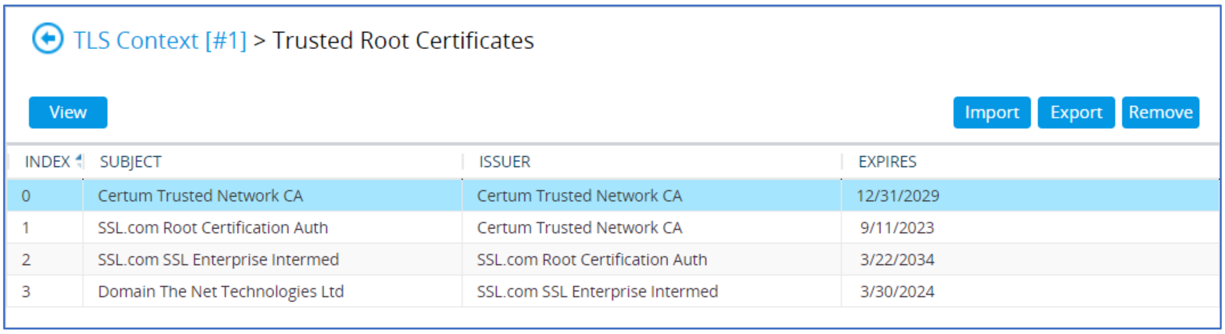
3. In the SBC's Web interface, return to the **TLS Contexts** page, select the required TLS Context index row, and then click the **Certificate Information** link, located at the bottom of the TLS. Then validate the Key size, certificate status and Subject Name:

Figure 25: Certificate Information Example



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 26: Example of Configured Trusted Root Certificates



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

4.4 Method for 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.

4.5 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.

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'.

4.6 Configuring Media Realm

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

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

To configure Media Realms:

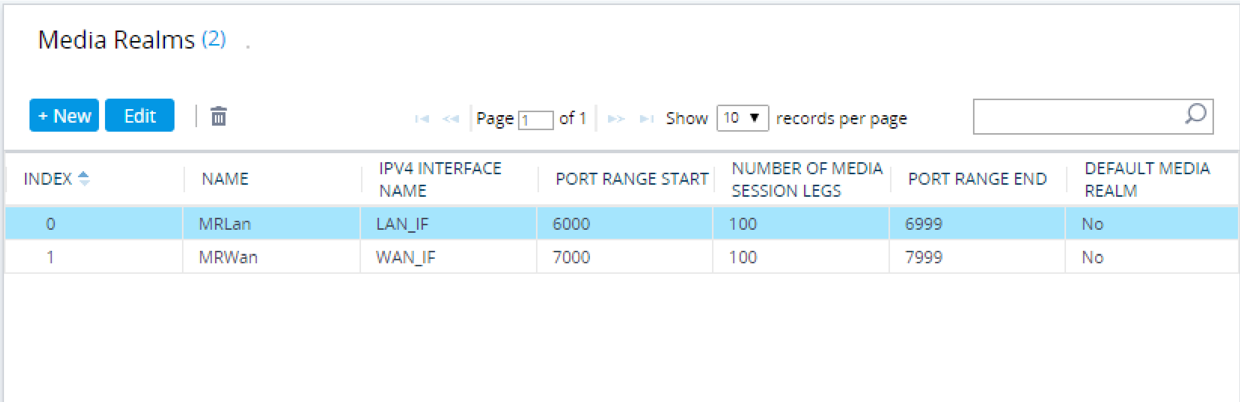
1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Configure Media Realms as follows (you can use the default Media Realm (Index 0), but modify it):

Table 6: 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 27: 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

4.7 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 SIP interfaces:

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

> 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 7: Configuration Example of SIP Signaling Interfaces

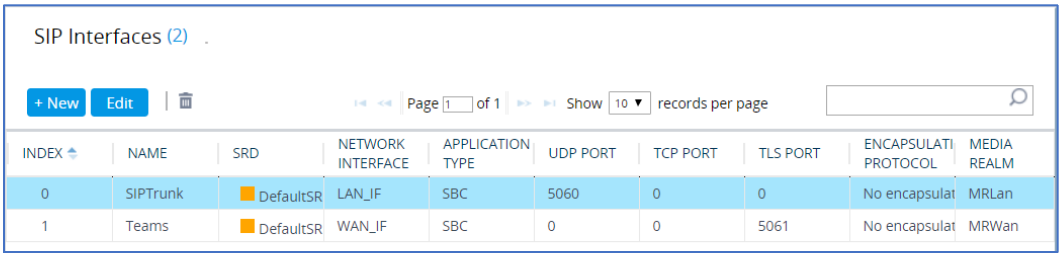
Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepalive	Classification Failure Response Type	Media Realm	TLS Context Name
0	SIPTrunk (arbitrary name)	LAN_IF	SBC	5060 (according to Service Provider requirement)	0	0	Disable (leave default value)	500 (leave default 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 4.5 on page 25.

The configured SIP Interfaces are shown in the figure below:

Figure 28: Configuration Example of SIP Signaling Interfaces



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

4.8 Configuring Proxy Sets and Proxy Address

4.8.1 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 Trunk. Note that the configuration of a Proxy Set for the SIP Trunk shows as an example and your configuration might be different. For specific configuration of interfaces pointing to SIP trunks and/or the third-party PSTN environment connected to the SBC, see the trunk/environment vendor's documentation. AudioCodes also offers a comprehensive suite of documents covering the interconnection between different trunks and the equipment. The Proxy Sets will later be applied to the VoIP network by assigning them to IP Groups.

To configure a Proxy Sets:

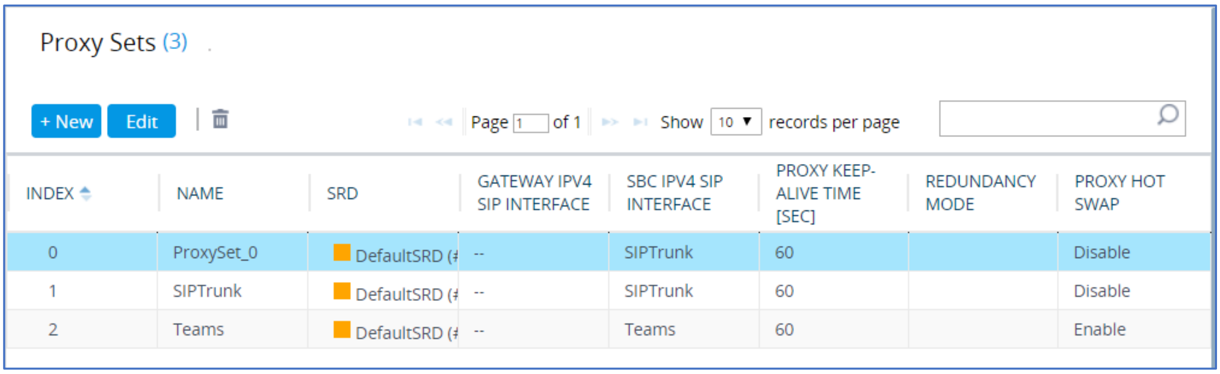
1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Configure Proxy Sets as shown in the table below:

Table 8: 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	SIPTrunk (arbitrary name)	SIPTrunk	Default	Using Options	-	-
2	Teams (arbitrary name)	Teams	Teams	Using Options	Enable	Random Weights

The configured Proxy Sets are shown in the figure below:

Figure 29: Configuration Example Proxy Sets in Proxy Sets Table



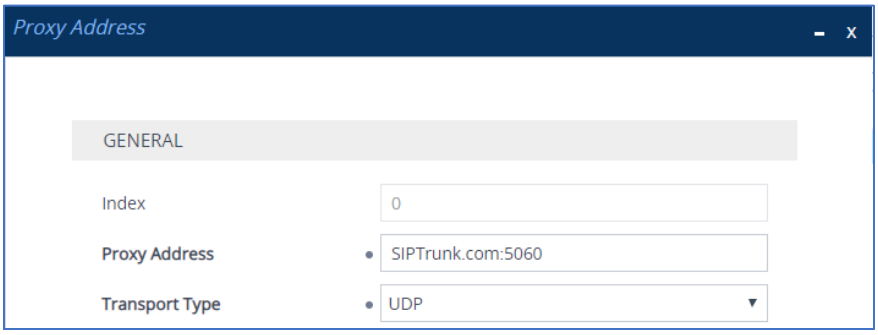
4.8.2 Configuring Proxy Addresses

This section shows how to configure a Proxy Address.

To configure a Proxy Address for SIP Trunk:

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

Figure 30: Configuring Proxy Address for SIP Trunk



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

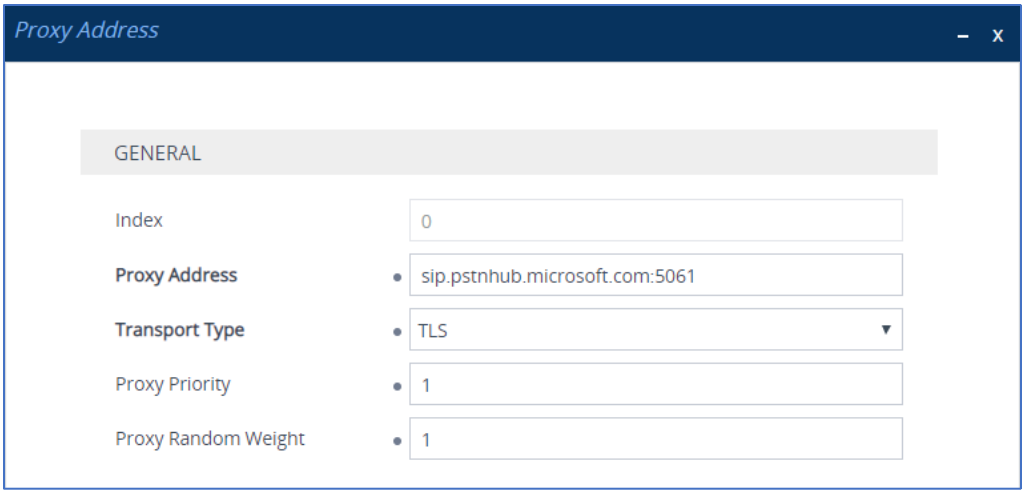
Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	SIPTrunk.com:5060 (SIP Trunk IP / FQDN and port)	UDP	0	0

4. Click **Apply**.

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 31: Configuring Proxy Address for Teams Direct Routing Interface



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

Table 10: 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** and then save your settings to flash memory.

> 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.

4.9 Configuring Coder Groups

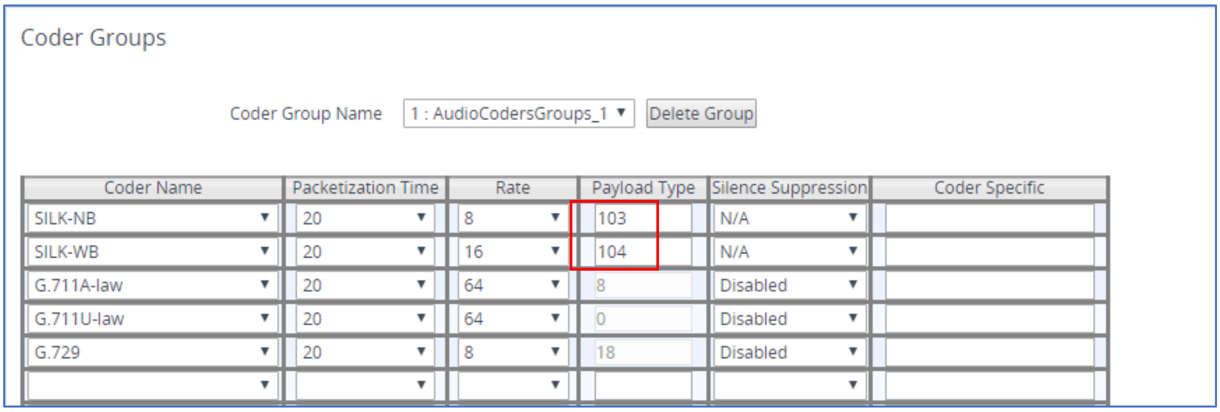
This section describes how to configure coders (known as *Coder Groups*). Teams Direct Routing supports the SILK and OPUS coders while the network connection to the SIP Trunk may restrict operation with a dedicated coders list. You need to add a Coder Group with the supported coders for each of the following leg, the Teams Direct Routing and the SIP Trunk.

> The Coder Group ID for this entity will be assigned to its corresponding IP Profile in Section 4.10.

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 32: Configuring Coder Group for Teams Direct Routing



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

4.10 Configuring IP Profiles

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

To configure an IP Profile:

1. Open the 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 11: 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 during Hold, but Microsoft expects them)
ICE Mode	**Lite** (required only when Media Bypass 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 at their default values.	

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

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

Table 12: Configuration Example: SIP Trunk IP Profile

Parameter	Value
General	
Name	**SIPTrunk**
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 4.18.

4.11 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. Click **+New** to add the IP Group for the SIP Trunk:

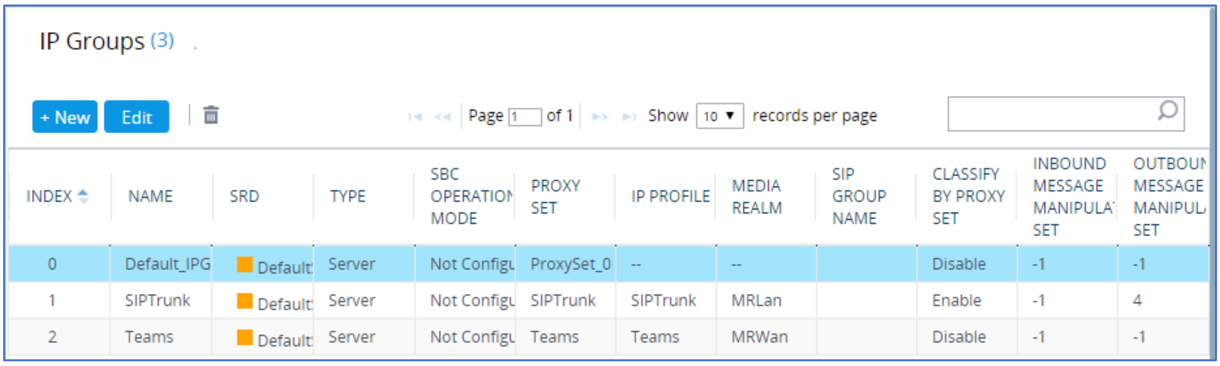
Parameter	Value
Name	**SIPTrunk**
Type	**Server**
Proxy Set	**SIPTrunk**
IP Profile	**SIPTrunk**
Media Realm	**MRLan** or **MRWan** (according to your network environment)
SIP Group Name	(according to ITSP requirement)
All other parameters can be left unchanged with their default values.	

3. Click **+New** to add the IP Group for the Teams Direct Routing:

Parameter	Value
Name	**Teams**
Topology Location	**Up**
Type	**Server**
Proxy Set	**Teams**
IP Profile	**Teams**
Media Realm	**MRWan**
Classify by Proxy Set	**Disable**
Local Host Name	**<FQDN name of the SBC in the Enterprise Office 365 tenant>** (based on our example, *int-sbc1.audctrunk.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**
Outbound Message Manipulation Set	**1**
Proxy Keep-Alive using IP Group settings	**Enable**
All other parameters can be left unchanged with their default values.	

The configured IP Groups are shown in the figure below:

Figure 33: Configured IP Groups in IP Group Table



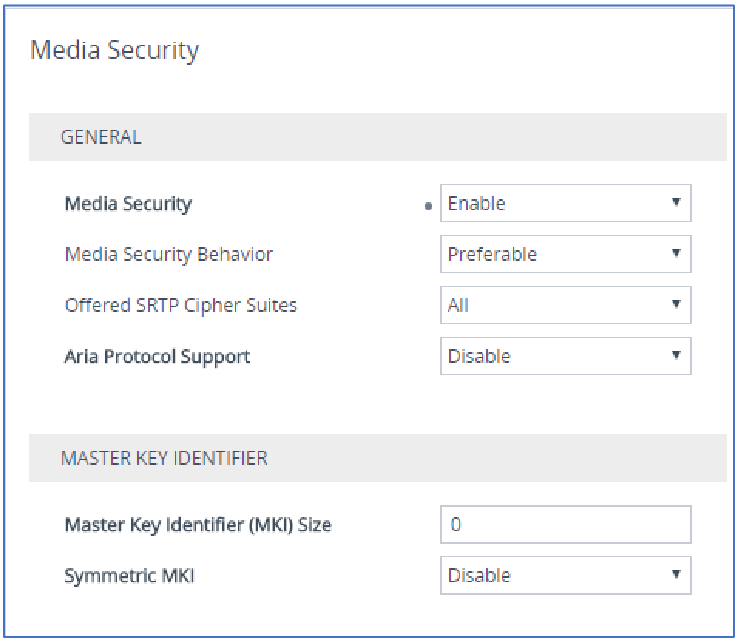
4.12 Configuring SRTP

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

To configure media security:

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

Figure 34: Configuring Media Security Parameter



3. Click **Apply**.

4.13 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.

> Implementation of the Message Manipulation rule with Microsoft Teams (shown below) is optional according to site deployment requirements.

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 1) for Teams IP Group. This rule applies to messages sent towards the Teams IP Group. This rule adds a routing policy rule towards Microsoft for handling different call forwarding scenarios (according to the action values shown below).

Parameter	Value
Index	**0**
Name	**Teams Routing Policy** (arbitrary name)
Manipulation Set ID	**1**
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**

4.14 Configuring Message Condition Rules

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

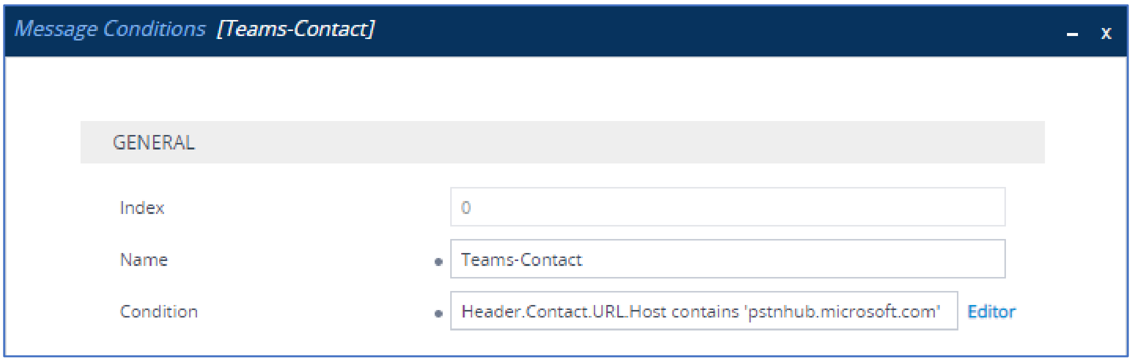
The following condition verifies that the Contact header contains Teams FQDN.

To configure a Message Condition rule:

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

Parameter	Value
Index	**0**
Name	**Teams-Contact** (arbitrary descriptive name)
Condition	**header.contact.url.host contains 'pstnhub.microsoft.com'**

Figure 35: Configuring Condition Table



3. Click **Apply**.

4.15 Configuring Classification Rules

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

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

To configure a Classification rule:

1. Open the Classification table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Classification Table**).
2. Configure Classification rules as shown in the table below:

Table 13: Classification Rules

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

3. Click **Apply**.

4.16 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 Trunk to Teams and vice versa. See AudioCodes' SBC documentation for more information on how to route in other scenarios.

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

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

To configure IP-to-IP routing rules:

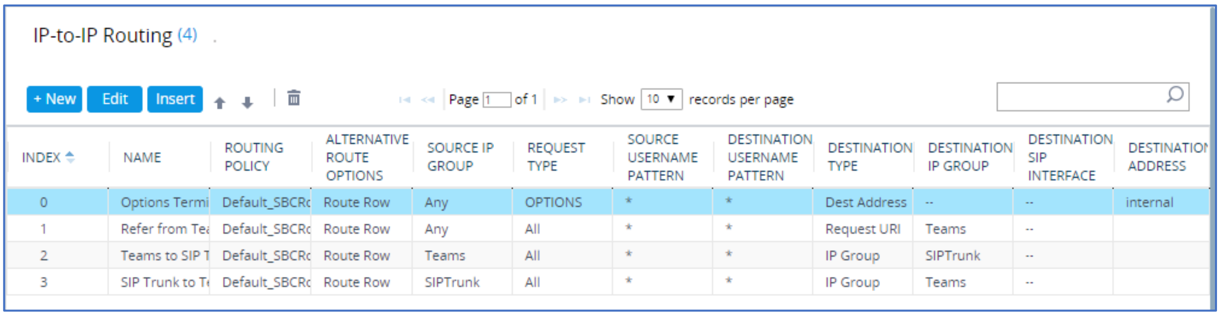
1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure routing rules as shown in the table below:

Table 14: IP-to-IP Call Routing Rules

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 from Teams (arbitrary name)	Any		REFER	Teams	Request URI	Teams	
2	Teams to SIP Trunk (arbitrary name)	Teams				IP Group	SIPTrunk	
3	SIP Trunk to Teams (arbitrary name)	SIPTrunk				IP Group	Teams	

The configured routing rules are shown in the figure below:

Figure 36: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table


IP-to-IP Routing (4)

+ New Edit Insert Page 1 of 1 Show 10 records per page

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	Options Termi	Default_SBCRc	Route Row	Any	OPTIONS	*	*	Dest Address	--	--	internal
1	Refer from Tea	Default_SBCRc	Route Row	Any	All	*	*	Request URI	Teams	--	
2	Teams to SIP T	Default_SBCRc	Route Row	Teams	All	*	*	IP Group	SIPTrunk	--	
3	SIP Trunk to Te	Default_SBCRc	Route Row	SIPTrunk	All	*	*	IP Group	Teams	--	

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

4.17 Configuring Firewall Settings

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

To configure a firewall rule:

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

Table 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.

4.18 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 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** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Choose SIP Trunk IP Profile, created in the Section 4.10 on the page 31. Configure the parameters using the table below as reference.

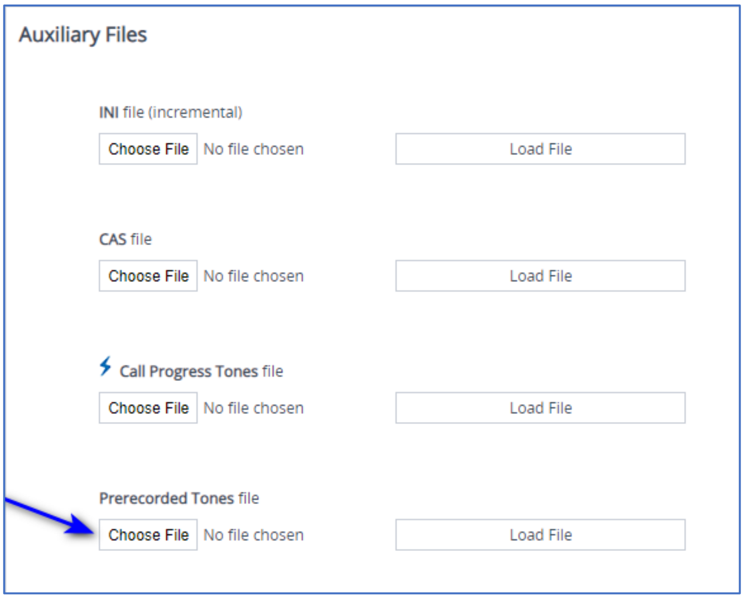
Table 16: Update Configuration of the SIP Trunk IP Profile

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.

5 Verifying the Pairing Between the SBC and Direct Routing

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

Figure 37: 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

6 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 a detailed description, refer to the AudioCodes User Manual documents.

To start, stop and restart a test call:

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

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

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

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

A.1 Terminology

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

A.2 Syntax Requirements for 'INVITE' Messages

Figure 38: Example of an 'INVITE' Message

```
INVITE sip:+16132606017@vendor4.lab.internetvoice.ca SIP/2.0
Via: SIP/2.0/TLS int-sbc1.audctrunk.aceducation.info:5061;alias;branch=z9hG4bKac659089971
Max-Forwards: 18
From: <sip:+97239764347@siptrunking.bell.ca;user=phone>;tag=1c132512889
To: "USER 6132606017" <sip:+16132606017@vendor4.lab.internetvoice.ca>
Call-ID: 2065125711112020102926@int-sbc1.audctrunk.aceducation.info
CSeq: 1 INVITE
Contact: <sip:+97239764347@int-sbc1.audctrunk.aceducation.info:5061;transport=tls>
Supported: 100rel,sdp-anat
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
User-Agent: M800B/v.7.20A.258.271
P-Asserted-Identity: <sip:+97239764347@siptrunking.bell.ca;user=phone>
Accept: application/media_control+xml,application/sdp,multipart/mixed
Recv-Info: x-broadworks-client-session-info
Content-Type: application/sdp
Content-Length: 1131
```

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

A.3 Requirements for 'OPTIONS' Messages Syntax

Figure 39: Example of 'OPTIONS' message

```
OPTIONS sip:vendor4.lab.internetvoice.ca SIP/2.0
Via: SIP/2.0/TLS int-sbc1.audctrunk.aceducation.info:5061;alias;branch=z9hG4bKac886439183
Max-Forwards: 70
From: <sip:195.189.192.160>;tag=1c1860024667
To: <sip:195.189.192.160>
Call-ID: 638931230111120201029946@int-sbc1.audctrunk.aceducation.info
CSeq: 1 OPTIONS
Contact: <sip:int-sbc1.audctrunk.aceducation.info:5061;transport=tls>
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: M800B/v.7.20A.258.271
Accept: application/sdp, application/simple-message-summary, message/sipfrag
Content-Length: 0
```

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

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

Table 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, *int-sbc1.audctrunk.aceducation.info*. The name changes the host name in the call received from the IP Group.	See Section 4.11.

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-33525**