Configuration Note

AudioCodes Professional Services – Interoperability Lab

Microsoft® Teams Direct Routing Enterprise Model and Swisscom SIP Trunk "Smart Business Connect Internet" using AudioCodes Mediant™ SBC

Version 7.4

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: September-21-2025

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.

Document Revision Record

LTRT	Description
14417	Initial document release.

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 Web site at https://online.audiocodes.com/documentation-feedback.

1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (hereafter, referred to as *SBC*) for interworking between Swisscom's SIP Trunk and Microsoft's Teams Direct Routing environment.

You can also use AudioCodes' SBC Wizard tool to automatically configure the SBC based on this interoperability setup. However, it is recommended to read through this document to better understand the various configuration options. For more information on AudioCodes' SBC Wizard including the download option, visit AudioCodes Website at https://www.audiocodes.com/partners/sbc-interoperability-list.

1.1 Intended Audience

This document is intended for engineers, or AudioCodes and Swisscom partners who are responsible for installing and configuring Swisscom's SIP Trunk and Microsoft's Teams Direct Routing Service in Enterprise Model for enabling VoIP calls using AudioCodes SBC.

1.2 About Microsoft Teams Direct Routing

Microsoft Teams Direct Routing allows connecting a customer-provided SBC to the 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

1.3 About AudioCodes SBC Product Series

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

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.

2 Component Information

2.1 AudioCodes SBC Version

Table 1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500/L Gateway & E-SBC ▪ Mediant 800B/C Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000/B SBC ▪ Mediant 9000/9030/9080 SBC ▪ Mediant Software SBC (VE/SE/CE)
Software Version	7.40A.501.661 or later
Protocol	▪ SIP/TLS (to the Swisscom SIP Trunk) ▪ SIP/TLS (to the Teams Direct Routing)
Additional Notes	None

2.2 Swisscom SIP Trunking Version

Table 2: Swisscom Version

Vendor/Service Provider	Swisscom
SSW Model/Service	Smart Business Connect Internet Trunk
Software Version	
Protocol	SIP
Additional Notes	None

2.3 Microsoft Teams Direct Routing Version

Table 3: Microsoft Teams Direct Routing Version

Vendor	Microsoft
Model	Teams Phone System Direct Routing
Software Version	
Protocol	SIP
Additional Notes	None

2.4 Interoperability Test Topology

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

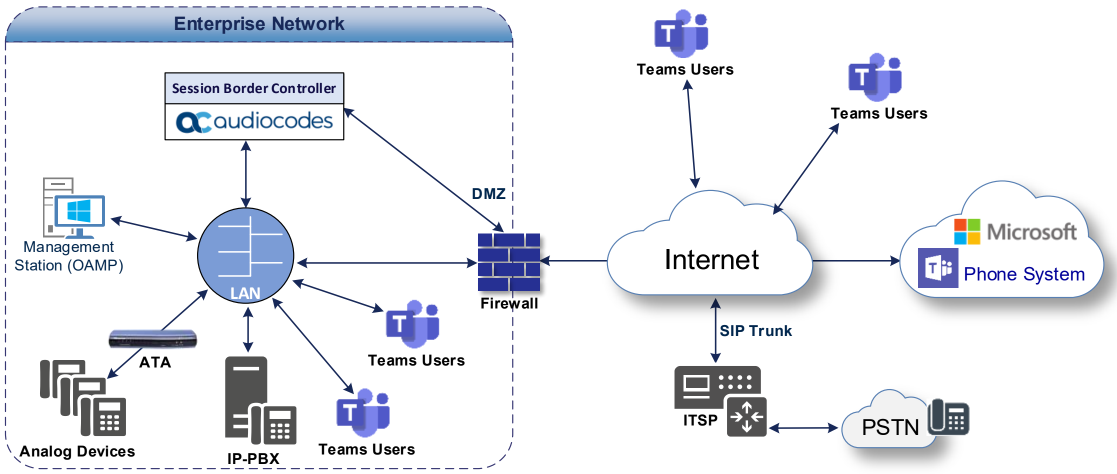
2.4.1 Enterprise Model Implementation

The interoperability testing between AudioCodes SBC and Swisscom SIP Trunk with Teams Direct Routing Enterprise Model was done using the following topology setup:

- Enterprise deployed with third-party IP-PBX, analog devices and the administrator's management station, located on the LAN
- Enterprise deployed with Microsoft 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 Swisscom's SIP Trunking service
- AudioCodes SBC is implemented to interconnect between the SIP Trunk in the Enterprise LAN and Microsoft Teams on the WAN
    - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
    - **Border:** IP-to-IP network border. Swisscom's SIP Trunk is located in the Enterprise LAN (or WAN) and the Microsoft Teams Phone Systems is located in the public network.

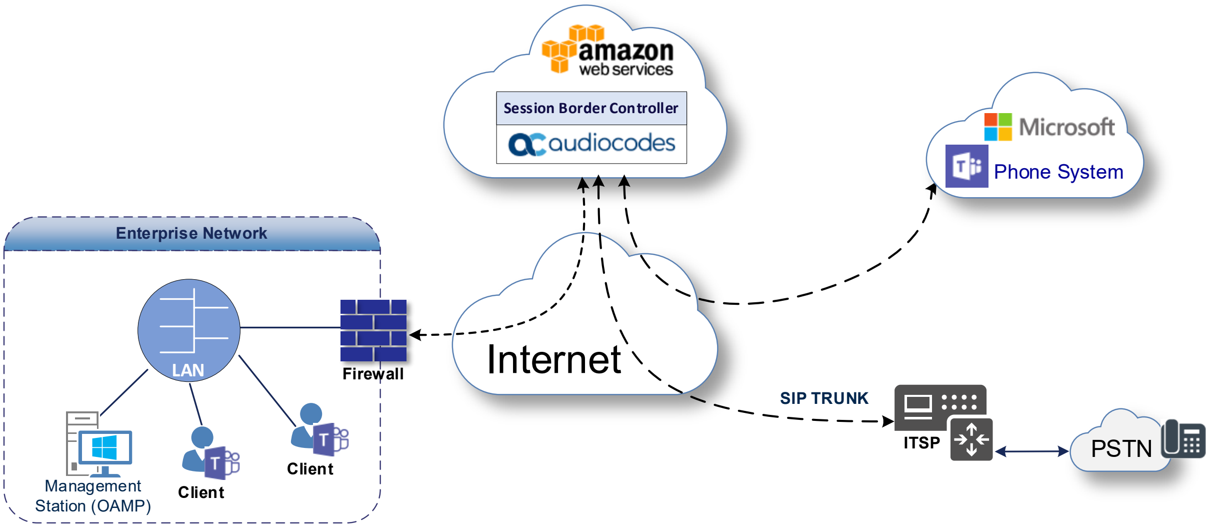
The figure below illustrates interoperability test topology when the SBC is deployed on the customer's premises:

Figure 1: On-prem Deployed SBC Topology between Swisscom SIP Trunk and Microsoft Teams Direct Routing Enterprise Model



The figure below illustrates interoperability test topology when the SBC is deployed in the AWS cloud:

Figure 2: AWS Deployed SBC Topology between Swisscom SIP Trunk and Microsoft Teams Direct Routing Enterprise Model



2.4.2 Environment Setup

The interoperability test topology includes the following environment setup:

Table 4: Environment Setup

Area	Setup
Network	▪ Microsoft Teams Direct Routing environment is located on the Enterprise's (or Service Provider's) WAN ▪ Swisscom SIP Trunk is located on the WAN
Signaling Transcoding	Both Microsoft Teams Direct Routing and Swisscom SIP Trunk operates with SIP-over-TLS transport type
Codecs Transcoding	▪ Microsoft Teams Direct Routing supports G.711A-law, G.711U-law, G.729, G.722, SILK (NB and WB) and OPUS coders ▪ Swisscom SIP Trunk supports G.711A-law, G.711U-law, G.722 and G.729 coders
Media Transcoding	Both Microsoft Teams Direct Routing and Swisscom SIP Trunk operates with SRTP media type

2.4.3 Infrastructure Prerequisites

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

Table 2-5: Infrastructure Prerequisites

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

2.4.4 Known Limitations

The following limitations were observed in the interoperability tests done for the AudioCodes SBC interworking between Microsoft Teams Direct Routing and Swisscom's SIP Trunk:

- Calls with special arrangements will be billed on the trunk main number instead of the user number. This is because the SIP P-Asserted Identity header contains the same number as the SIP ‘From’ header. This limitation does not affect the completion of such calls.

3 Configuring Teams Direct Routing

This section describes how to configure Microsoft Teams Direct Routing 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 users
- Public certificate, issued by one of the supported CAs

3.2 SBC Domain Name in the Teams Enterprise Model

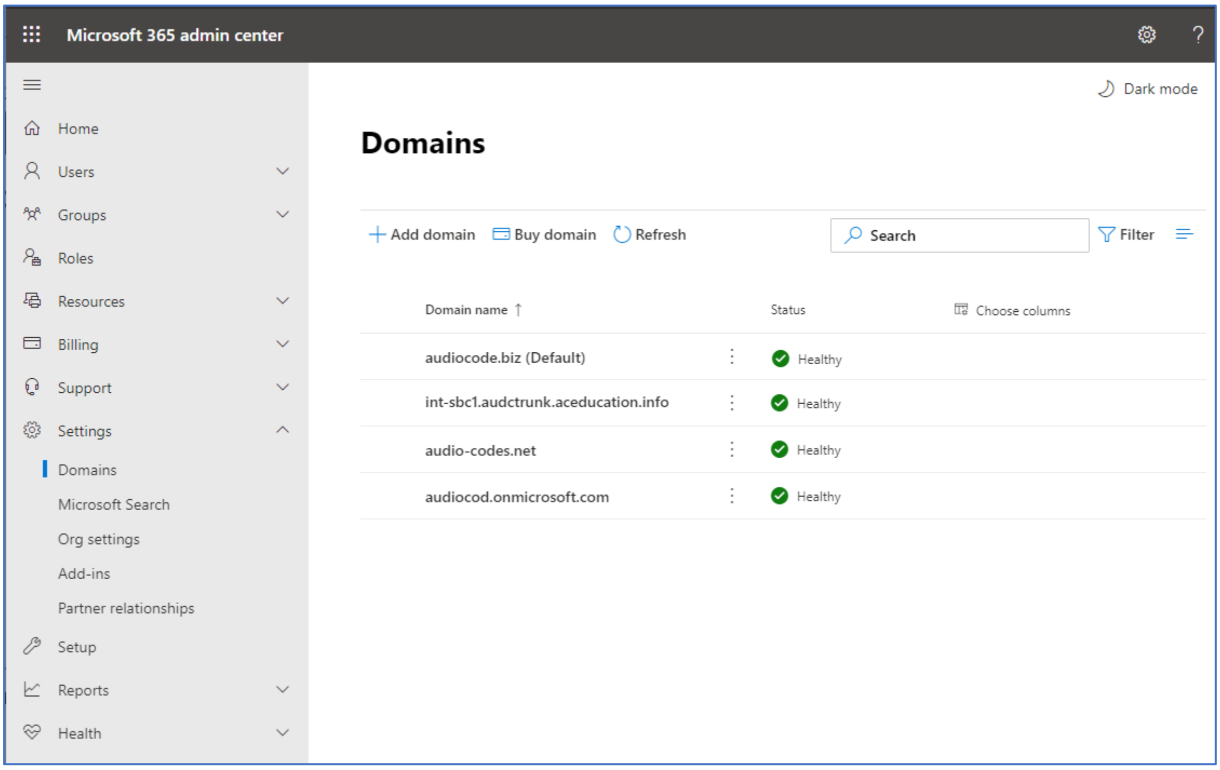
The SBC domain name must be from one of the names registered in 'Domains' of the tenant. You cannot use the ***.onmicrosoft.com** tenant for the domain name. For example, the administrator registered the following DNS names for the tenant:

Table 6: DNS Names Registered by an Administrator for a 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 tenant. For example, you can provide user 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

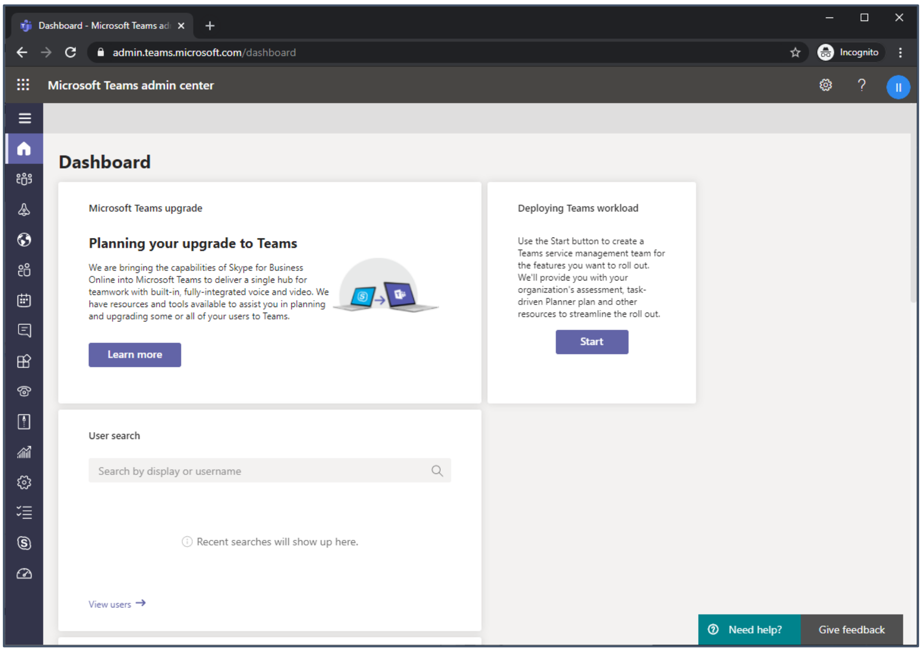


During the creation of the Domain, you will be forced to create public DNS record (**int-sbc1.audctrunk.aceducation.info** in our example.)

3.3 Example of the 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



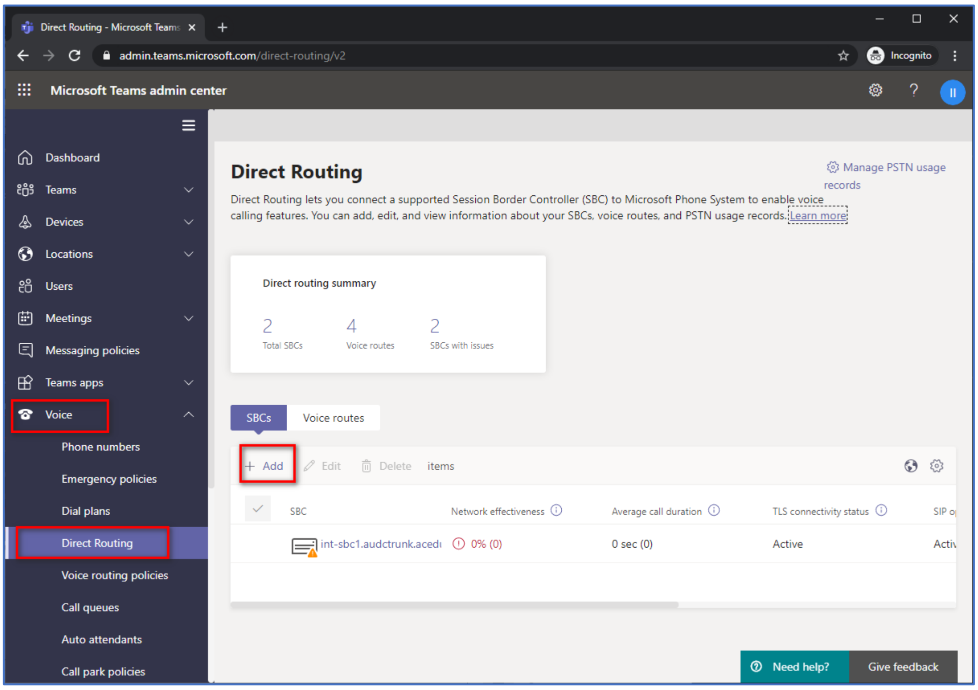
3.3.1 Add New SBC to Direct Routing

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

To add New SBC to Direct Routing:

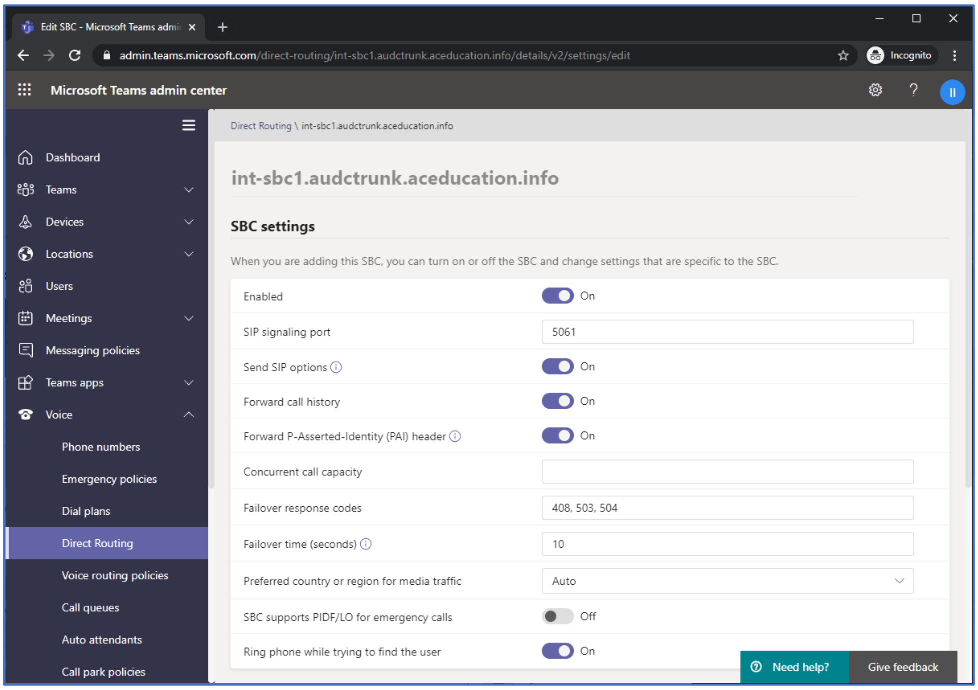
1. In the web interface, select **Voice**, and then click **Direct Routing**.
2. Under SBCs click **Add.**

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
```

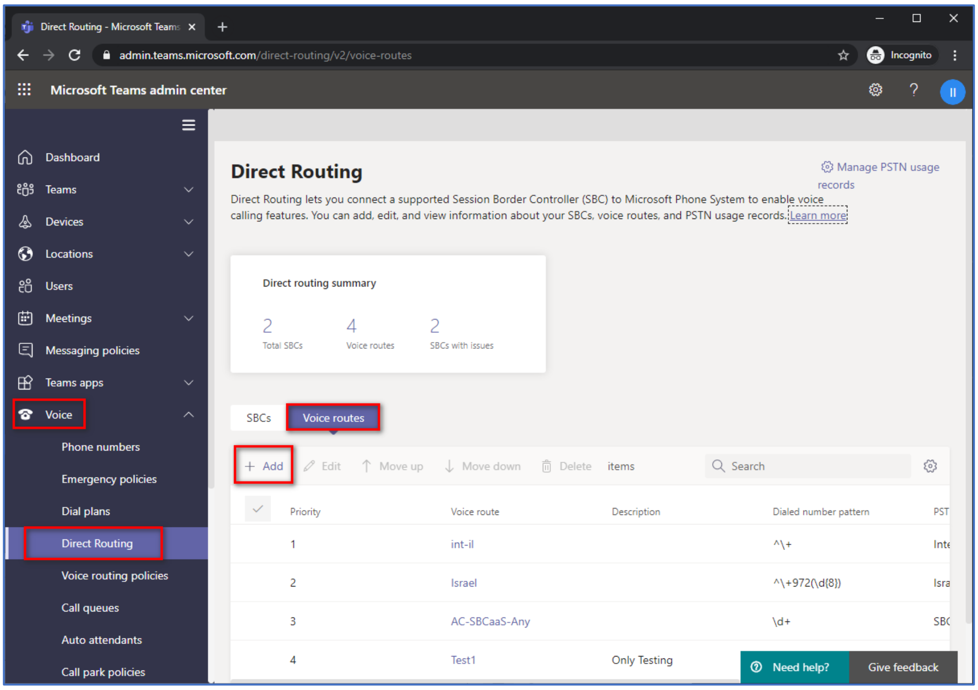
3.3.2 Add Voice Route and PSTN Usage

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

To add voice route and PSTN usage:

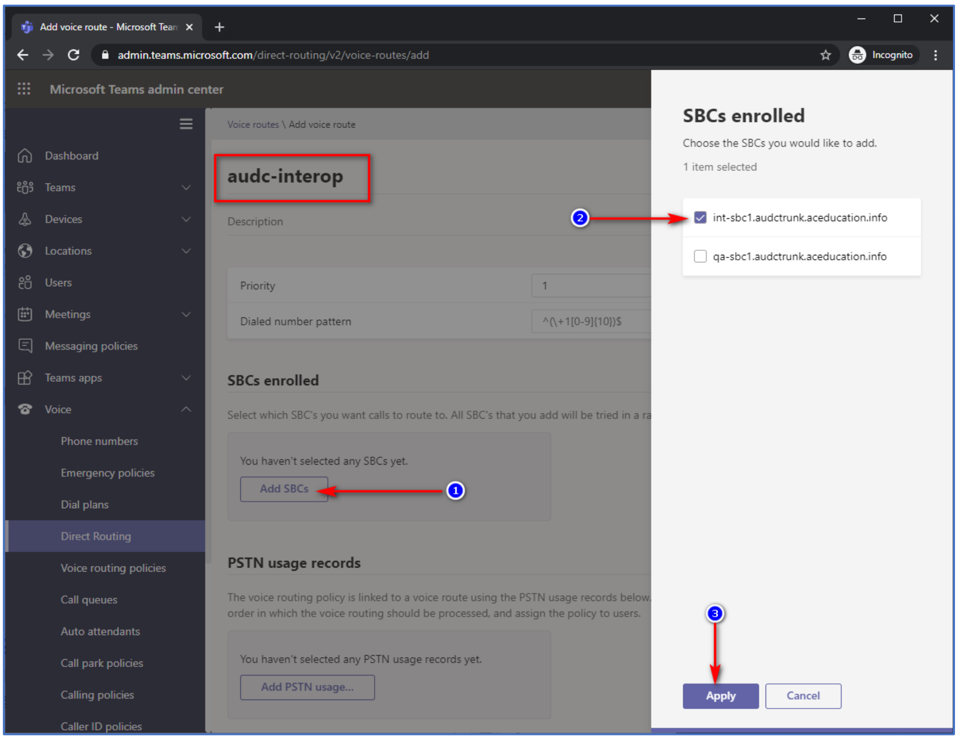
1. In the web interface, under **Direct Routing**, select **Voice routes**, and then click **Add**.

Figure 7: Add New Voice Route



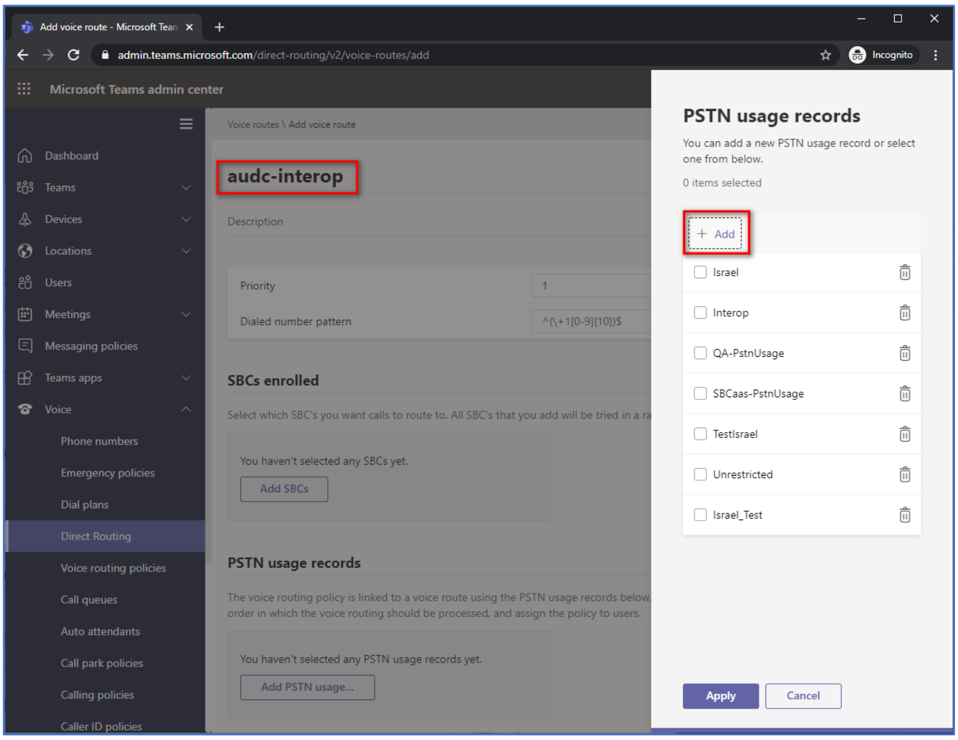
2. Create a new Voice Route and associate it with the SBC, configured in the previous step.

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:

4. Creating an empty PSTN Usage:

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

5. 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"
```

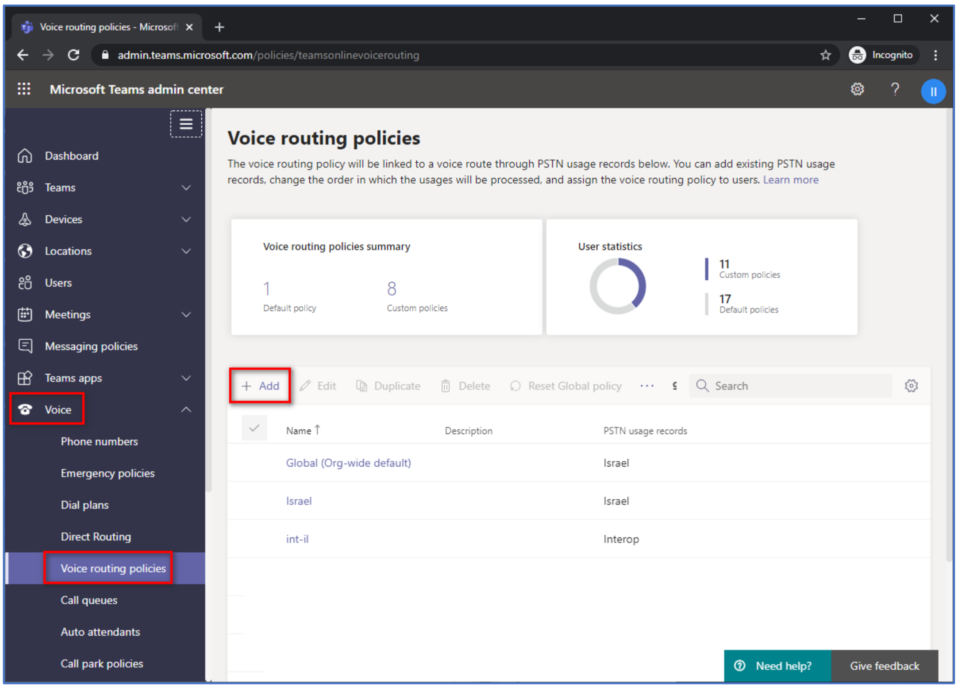
3.3.3 Add Voice Routing Policy

The procedure below describes how to add a voice routing policy

To add voice routing policy:

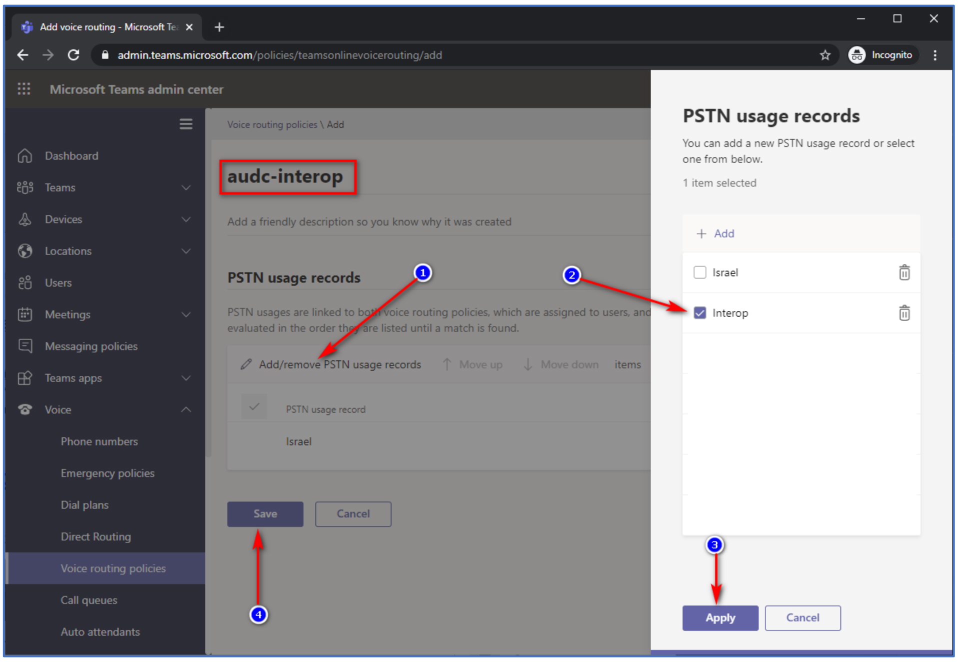
1. In the web interface, under **Voice**, select **Voice routing policies** and click **Add**.

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 company tenant. They are currently available through PowerShell **only**.

3.3.4 Enable Online User

Use the 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
```

4 Configuring AudioCodes SBC

This section provides step-by-step procedures on how to configure AudioCodes SBC for interworking between Microsoft Teams Direct Routing and the Swisscom SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 6, and includes the following main areas:

- SBC LAN interface – Management Station
- SBC WAN interface - Swisscom SIP Trunking and Teams Direct Routing environment

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

- For implementing Microsoft Teams Direct Routing and Swisscom SIP Trunk based on the configuration described in this section, AudioCodes SBC must be installed with a License Key that includes the following software 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.
- If your SBC is deployed in a virtual environment and transcoding is required, your virtual machine must have a minimum of two vCPUs. For more information, please refer to the appropriate *Installation Manual,* which can be found on AudioCodes website.
- 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 Enterprise Model

The diagram below represents AudioCodes' device configuration concept in the Enterprise Model.

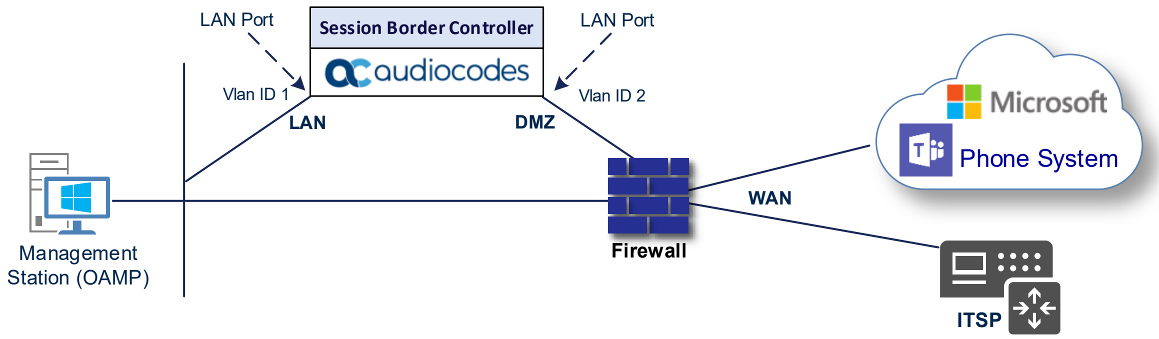
Figure 12: SBC Configuration Concept

4.2 IP Network Interfaces Configuration for On-Prem Deployment

This section describes how to configure the SBC's IP network interfaces. There are several ways to deploy the SBC; however, this interoperability test topology employs the following deployment method:

- SBC interfaces with the following IP entities:
  - Management Servers, located on the LAN
  - Microsoft Teams Direct Routing and Swisscom SIP Trunk, located on the 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 13: Network Interfaces in Interoperability Test Topology



4.2.1 Configure VLANs

This section describes how to configure 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

4.2.2 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 the IP network 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 7: 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

4.3 IP Network Interfaces Configuration for Deployment in AWS

This section describes how to configure the SBC deployed in the AWS.

4.3.1 Configure Network Interface

The Network Interface is configured automatically in the Amazon implementation. To configure the Amazon image (AMI), refer to the relevant document:

- *Mediant Virtual Edition SBC for Amazon AWS Installation Manual*
- *Mediant Cloud Edition SBC Installation Manual*.

4.3.2 Configure NAT Translation

The SBC, located in the Amazon Cloud, implements private IP addresses. The NAT Translation table lets you configure network address translation (NAT) rules for translating source IP addresses into NAT IP addresses (*global - public*) used in front of the Amazon firewall facing the Swisscom, Vonage SIP Trunk and Pindrop Fraud Detection and Authentication Solution.

To configure NAT translation rules:

1. Open the NAT Translation table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **NAT Translation**).
2. Click **New**; use the following table as reference when configuring a NAT translation rule:

Parameter	Value
Index	**0**
Source Interface	**eth0** (IP Network Interface, configured in the previous section)
Source Start Port	**1**
Source End Port	**65535**
Target IP Mode	**Automatic** (this mode is required if your AWS environment has been configured with an Elastic IP address and you want the device to automatically associate it with the selected source interface as the global (public) IP address).
Target IP Address	Configured only if the previous parameter is configured with 'Manual' value.
Automatic Target IP Address	Read-only-field

3. Click **Apply**.

Configure additional rules for each IP Interface.

4.4 SIP TLS Connection Configuration

This section describes how to configure the SBC for using a TLS connection with the Microsoft Teams Direct Routing Phone System and Swisscom Smart Business Connect Internet Trunk. This configuration is essential for a secure SIP TLS connection. 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: int-sbc.audctrunk.aceducation.info
- SAN: int-sbc.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 Microsoft 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

4.4.1 Configure the NTP Server Address

This section describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (any public NTP server) to ensure that the SBC receives the current date and time. This is necessary for validating certificates of remote parties.

To configure the NTP server address:

1. Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**).
2. From the 'NTP Interface' drop-down list, select an appropriated interface (e.g., **WAN_IF**).
3. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., **pool.ntp.org**).
4. Click **Apply**.

4.4.2 Create a TLS Context for Teams Direct Routing

This section describes how to configure TLS Context in the SBC. AudioCodes recommends implementing only TLS to avoid flaws in SSL.

To configure the TLS version:

1. Open the TLS Contexts table (**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 8: New TLS Context

Index	Name	TLS Version
1	Teams (arbitrary descriptive name)	TLSv1.2 and TLSv1.3
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.

3. Click **Apply**.

4.4.3 Configure a Certificate

This section describes how to request a certificate for the SBC 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 Microsoft Teams Direct Routing.

The procedure involves the following main steps:

a. Generating a Certificate Signing Request (CSR).
b. Requesting Device Certificate from CA.
c. Obtaining Trusted Root/Intermediate Certificate from CA.
d. Deploying Device and Trusted Root/Intermediate Certificates on SBC.

To configure a 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. Under the **Certificate Signing Request** group, do the following:
   a. In the 'Subject Name [CN]' field, enter the SBC FQDN name (based on example above, **int-sbc.audctrunk.aceducation.info**).
   b. In the '1st Subject Alternative Name [SAN]' field, change the type to 'DNS' and enter the SBC FQDN name (based on our example, **int-sbc.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. Change the 'Private Key Size' based on the requirements of your Certification Authority or leave the default value (2048).
   d. To change the key size on TLS Context, go to: **Generate New Private Key**, change the 'Private Key Size' to the value required by your CA and then click **Generate Private-Key**. To use **2048** as a Private Key Size value, you can click **Generate Private-Key** without changing the default key size value.
   e. Fill in the rest of the request fields according to your security provider's instructions.
   f. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button.
4. Copy the CSR from the line **"----BEGIN CERTIFICATE REQUEST" to "END CERTIFICATE REQUEST----"** to a text file (such as Notepad) and then save it to a folder on your computer with the file name, for example *certreq.txt*.
5. Send *certreq.txt* file to the Certified Authority Administrator for signing.
6. After obtaining an SBC signed and Trusted Root/Intermediate Certificate from the CA, in the SBC's Web interface, return to the **TLS Contexts** page and do the following:

a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.

b. Scroll down to the **Upload certificates files from your computer** group, click the **Choose File** button corresponding to the '**Send Device Certificate**...' field, navigate to the certificate file obtained from the CA, and then click **Load File** to upload the certificate to the SBC.

7. Confirm that the certificate was uploaded correctly. A message indicating that the certificate was uploaded successfully is displayed in blue in the lower part of the page.

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

9. 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.

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

4.4.4 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.

4.4.5 Deploy 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.

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, you will receive a 'Failed to load new certificate' error message. To convert to PEM format, use the Windows local store on any Windows OS and then export it as 'Base-64 encoded X.509 (.CER) certificate'.

4.4.6 Create a TLS Context for Swisscom SIP Trunk

Swisscom Smart Business Connect Internet Trunk uses SIP over TLS and therefore, requires a dedicated TLS Context. It’s not necessary to upload the Swisscom Trusted Root CA as it’s already part of the default CA Bundle.

To configure the TLS version:

1. Open the TLS Contexts table (**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 9: New TLS Context

Index	Name	TLS Version	Use default CA Bundle
2	SBCon (arbitrary descriptive name)	TLSv1.2 and TLSv1.3	Enable
All other parameters can be left unchanged with their default values.			

3. Click **Apply**.

4.5 Configure Media Realms

This section describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for the SIP Trunk traffic and one for the Teams traffic.

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 10: Configuration Example Media Realms in Media Realm Table

Index	Name	Topology Location	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
0	SBCon (arbitrary name)		WAN_IF (or eth0 for AWS)	6000	100 (media sessions assigned with port range)
1	Teams (arbitrary name)	Up	WAN_IF (or eth0 for AWS)	7000	100 (media sessions assigned with port range)

4.6 Configure SIP Signaling Interfaces

This section describes how to configure SIP Interfaces. For the interoperability test topology, towards the SIP Trunk and towards the Teams Direct Routing SIP Interfaces must be configured for the SBC.

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 11: Configured SIP Interfaces in SIP Interface Table

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	**SBCon** (arbitrary name)	**WAN_IF (or eth0 for AWS)**	**SBC**	**0**	**0**	**5061**	**Enable**	**0** (Recommended to prevent DoS attacks)	**SBCon**	**SBCon**
1	**Teams** (arbitrary name)	**WAN_IF (or eth0 for AWS)**	**SBC**	**0**	**0**	**5067** (as configured in the Office 365)	**Enable**	**0** (Recommended to prevent DoS attacks)	**Teams**	**Teams**

4.7 Configure Proxy Sets and Proxy Address

This section describes how to configure Proxy Sets. The Proxy Set defines the destination address (IP address or FQDN) of the IP entity server. Proxy Sets can also be used to configure load balancing between multiple servers.

For the interoperability test topology, two Proxy Sets need to be configured for the following IP entities:

- Swisscom SIP Trunk
- Teams Direct Routing

The Proxy Sets will later be applied to the VoIP network by assigning them to IP Groups.

To configure 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 12: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Proxy Keep-Alive Time [sec]	Proxy Hot Swap	Proxy Load Balancing Method
1	SBCon (arbitrary name)	SBCon	SBCon	Using Options	10	-	-
2	Teams (arbitrary name)	Teams	Teams	Using Options	30 (default)	Enable	Random Weights

4.7.1 Configure a Proxy Address

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**; and configure the address of the Proxy Set according to the parameters described in the table below:

Table 13: Configuration Proxy Address for SIP Trunk

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	strunkpub.join.swisscom.ch:5061 (FQDN and destination port)	TLS	0	0

3. 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**; and configure the address of the Proxy Set according to the parameters described in the table below:

Table 14: 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

3. Click Appl**y**.

4.8 Configure Coders

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

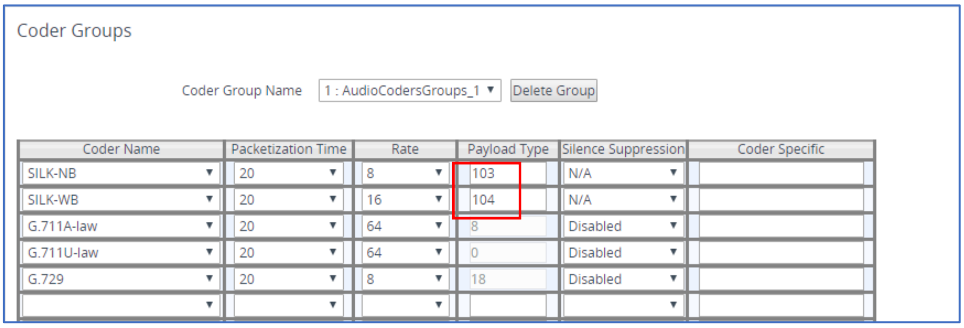
Note that the Coder Group ID for this entity will be assigned to its corresponding IP Profile in the next step.

To configure coders:

1. Open the Coder Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Coder Groups**).
2. Configure a Coder Group for Microsoft Teams Direct Routing:

Parameter	Value
Coder Group Name	**AudioCodersGroups_1**
Coder Name	■ SILK-NB ■ SILK-WB ■ G.711 A-law ■ G.711 U-law ■ G.729

Figure 14: Configuring Coder Group for Microsoft Teams Direct Routing



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

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Swisscom SIP Trunk uses the dedicated coders list whenever possible. Note that this Allowed Coders Group ID will be assigned to the IP Profile belonging to the Swisscom SIP Trunk in the next step.

To set a preferred coder for the Swisscom SIP Trunk:

1. Open the Allowed Audio Coders Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Audio Coders Groups**).
2. Click **New** and configure a name for the Allowed Audio Coders Group for Swisscom SIP Trunk (*e.g., Swisscom-AllowedAudioCoders*).
3. Click **Apply.**
4. Select the new row that you configured, and then click the **Allowed Audio Coders** link located below the table; the Allowed Audio Coders table opens.
5. Click **New** and configure an Allowed Coders as follows:

Parameter	Value
Index	**0**
Coder	**G.711 A-law**
Index	**1**
Coder	**G.729**
Index	**2**
Coder	**G.722**

6. Open the Media Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Settings**).
7. From the '**Extended Coders Behavior**' drop-down list, select **Include Extensions**.
8. Click **Apply**.

4.9 Configure IP Profiles

This section describes how to configure IP Profiles. The IP Profile defines a set of call capabilities relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder and transcoding method).

In this interoperability test topology, IP Profiles need to be configured for the following IP entities:

- Swisscom SIP trunk – to operate in non-secure mode using RTP and SIP over UDP
- Microsoft Teams Direct Routing – to operate in secure mode using SRTP and SIP over TLS

To configure an IP Profile for the Swisscom SIP Trunk:

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

Parameter	Value
General	
Index	**1**
Name	**SBCon**
Media Security	
SBC Media Security Mode	**Secured**
SBC Media	
Allowed Audio Coders	**Swisscom-AllowedAudioCoders**
Allowed Coders Mode	**Restriction and Preference** (reorganize coders according to Allowed Coders list and restrict all other)
SBC Signaling	
PRACK Mode	**Optional**
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**
Remote 3xx Mode	**Handle Locally**
SBC Hold	
Remote Hold Format	**Send Only**
Media	
Broken Connection Mode	**Disconnect**

3. Click **Apply**.

To configure IP Profile for the Microsoft Teams Direct Routing:

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

Parameter	Value
General	
Index	**2**
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 Microsoft Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18x response)
Generate RTP	**Until RTP Detected**
SBC Media	
Extension Coders Group	**AudioCodersGroups_1**
RTCP Mode	**Generate Always** (required, as some ITSPs do not send RTCP packets during while in Hold mode, but Microsoft expected to them)
ICE Mode	**Lite** (required only when Media Bypass enabled on Microsoft 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 3xx Mode	**Handle Locally**

3. Click **Apply**.

4.10 Configure IP Groups

This section describes how to configure IP Groups. The IP Group represents an IP entity on the network with which SBC communicates. This can be a server or it can be a group of users. 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.

In this interoperability test topology, IP Groups must be configured for the following IP entities:

- Swisscom SIP Trunk located on WAN
- Teams Direct Routing located on WAN

To configure IP Groups:

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Configure an IP Group for the Swisscom SIP Trunk:

Parameter	Value
Index	**1**
Name	**SBCon**
Type	**Server**
Proxy Set	**SBCon**
IP Profile	**SBCon**
Media Realm	**SBCon**
SIP Group Name	**XXXXXX.join.swisscom.ch** (customer domain, where XXXXXX is a 6-digit number unique to each customer)
Local Host Name	**XXXXXX.join.swisscom.ch** (customer domain, where XXXXXX is a 6-digit number unique to each customer)
Proxy Keep-Alive using IP Group settings	**Enable**

3. Configure an IP Group for the Microsoft Teams Direct Routing:

Parameter	Value
Index	**2**
Name	**Teams**
Topology Location	**Up**
Type	**Server**
Proxy Set	**Teams**
IP Profile	**Teams**
Media Realm	**Teams**
Classify By Proxy Set	**Disable**
SIP Group Name	**teams-sbc.your.domain.com** (SBC FQDN in the Microsoft Teams tenant)

Parameter	Value
Local Host Name	**teams-sbc.your.domain.com** (SBC FQDN in the Microsoft Teams tenant)
Always Use Src Address	**Yes**
Teams Direct Routing Mode	**Enable**
Proxy Keep-Alive using IP Group settings	**Enable**

4.11 Configure SRTP

This section describes how to configure media security. The Direct Routing Interface needs to use 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.
3. Click **Apply**.

4.12 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.

The following condition verifies that the Contact header contains Microsoft 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'**

3. Click **Apply**.

4.13 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 15: 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 FQDN in the Microsoft Teams tenant> (e.g., mediant.join.swisscom.ch)	Teams-Contact	Allow	Teams
1	Teams_52_113 (arbitrary name)	Teams	52.113.*.*	< SBC FQDN in the Microsoft Teams tenant> (e.g., mediant.join.swisscom.ch)	Teams-Contact	Allow	Teams
2	Teams_52_114 (arbitrary name)	Teams	52.114.*.*	< SBC FQDN in the Microsoft Teams tenant> (e.g., mediant.join.swisscom.ch)	Teams-Contact	Allow	Teams
3	Teams_52_115 (arbitrary name)	Teams	52.115.*.*	< SBC FQDN in the Microsoft Teams tenant> (e.g., mediant.join.swisscom.ch)	Teams-Contact	Allow	Teams
4	Teams_52_120 (arbitrary name)	Teams	52.120.*.*	< SBC FQDN in the Microsoft Teams tenant> (e.g., mediant.join.swisscom.ch)	Teams-Contact	Allow	Teams
5	Teams_52_121 (arbitrary name)	Teams	52.121.*.*	< SBC FQDN in the Microsoft Teams tenant> (e.g., mediant.join.swisscom.ch)	Teams-Contact	Allow	Teams
6	Teams_52_122 (arbitrary name)	Teams	52.122.*.*	< SBC FQDN in the Microsoft Teams tenant> (e.g., mediant.join.swisscom.ch)	Teams-Contact	Allow	Teams
7	Teams_52_123 (arbitrary name)	Teams	52.123.*.*	< SBC FQDN in the Microsoft Teams tenant> (e.g., mediant.join.swisscom.ch)	Teams-Contact	Allow	Teams

3. Click **Apply**.

4.14 Configure IP-to-IP Call Routing Rules

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

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Teams Direct Routing and Swisscom SIP Trunk:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity
- Terminate REFER messages to Teams Direct Routing
- Calls from Teams Direct Routing to Swisscom SIP Trunk
- Calls from Swisscom 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 16: Configuration IP-to-IP Routing Rules

Index	Name	Source IP Group	Request Type	Call Triger	ReRoute IP Group	Dest Type	Dest IP Group	Internal Action
0	Terminate OPTIONS	Any	OPTIONS			Internal		Reply (Response=' 200')
1	Refer from Teams (arbitrary name)	Any		REFER	Teams	Request URI	Teams	
2	Teams to SBCon (arbitrary name)	Teams				IP Group	SBCon	
3	SBCon to Teams (arbitrary name)	SBCon				IP Group	Teams	

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

4.15 Configuring Firewall Settings (Optional)

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 17: 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	52.120.0.0	14	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

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.

4.16 Configure Number Manipulation Rules

This section describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 4.10 on page 30) to denote the source and destination of the call.

> Adapt the manipulation table according to your environment dial plan.

For example, for this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number (if it not exists) for calls from the Swisscom SIP Trunk IP Group to the Teams Direct Routing IP Group for any destination username pattern.

To configure a number manipulation rule:

1. Open the Outbound Manipulations table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Outbound Manipulations**).
2. Configure the following rules.

Parameter	Value
Index	0
Name	Anonymous
Source IP Group	Any
Destination IP Group	SBCon
Destination Username Pattern	+41*31
Manipulated Item	Source URI
Privacy Restriction Mode	Restrict

Parameter	Value
Index	1
Name	Anonymous
Source IP Group	Any
Destination IP Group	SBCon
Destination Username Pattern	+41*31
Manipulated Item	Destination URI
Remove From Left	6

Parameter	Value
Index	2
Name	4 digits
Source IP Group	Any
Destination IP Group	SBCon
Destination Username Pattern	+411xxx
Manipulated Item	Destination URI
Remove From Left	3

The table below shows an example of configured IP-to-IP outbound manipulation rules for calls between Teams Direct Routing IP Group and Swisscom SIP Trunk IP Group:

Rule Index	Description
0	Calls from Any IP Group to SBCon IP Group with the prefix destination number "+41*31", apply restriction policy on the source number.
1	Calls from Any IP Group to SBCon IP Group with the prefix destination number "+41*31", remove 6 digits (+41*31) from this prefix.
2	Calls from Teams IP Group to SBCon IP Group with the prefix destination number “+411xxx”, remove 3 digits (+41) from this prefix.

4.17 Configure Message Manipulation Rules

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

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

To configure SIP message manipulation rule:

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. This rule applies to messages received from the Teams IP Group. This replaces the user part of ‘sip:’ index with the value from ‘tel:’ index in the SIP P-Asserted-Identity Header.

Parameter	Value
Index	**0**
Name	**Build 1 PAI from 2**
Manipulation Set ID	**1**
Action Subject	**Header.P-Asserted-Identity.1.URL.User**
Action Type	**Modify**
Action Value	**Header.P-Asserted-Identity.0.URL.User**

3. Configure another manipulation rule (Manipulation Set 1) for Teams. This rule applies to messages received from the Teams IP Group. This removes the ‘tel:’ index of the SIP P-Asserted-Identity Header.

Parameter	Value
Index	**1**
Name	**Remove PAI tel**
Manipulation Set ID	**1**
Action Subject	**Header.P-Asserted-Identity.0.URL.User**
Action Type	**Remove**

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

Parameter	Value
Index	**2**
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**

5. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule applies to messages sent to the Swisscom SIP Trunk IP Group in a call transfer scenario. This replaces the host part of the SIP Referred-By header with the value taken from the 'Group Name' field of the Swisscom SIP Trunk IP Group.

Parameter	Value
Index	**3**
Name	**Call Transfer**
Manipulation Set ID	**4**
Message Type	**Invite.Request**
Condition	**Header.Referred-By exists**
Action Subject	**Header.Referred-By.URL.Host**
Action Type	**Modify**
Action Value	**Param.IPG.Dst.Host**

6. If the manipulation rule index above is executed, then the following rule is also executed. It adds the SIP Diversion header with values from the SIP Referred-by header.

Parameter	Value
Index	**4**
Name	**Call Transfer**
Manipulation Set ID	**4**
Row Role	**Use Previous Condition**
Action Subject	**Header.Diversion**
Action Type	**Add**
Action Value	**Header.Referred-By**

7. If the manipulation rule index above is executed, then the following rule is also executed. It removes the SIP Referred-by header.

Parameter	Value
Index	**5**
Name	**Call Transfer**
Manipulation Set ID	**4**
Row Role	**Use Previous Condition**
Action Subject	**Header.Referred-By**
Action Type	**Remove**

8. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule applies to messages sent to the Swisscom SIP Trunk IP Group in a call forward scenario. This rule adds the SIP Diversion header with the value from the SIP History-Info header.

Parameter	Value
Index	**6**
Name	**Call Forward**
Manipulation Set ID	**4**
Message Type	**any**
Condition	**Header.History-Info exists**
Action Subject	**Header.Diversion**
Action Type	**Add**
Action Value	**Header.History-Info.HistoryInfo**

9. If the manipulation rule index 6 (above) is executed, then the following rule is also executed. It normalizes the SIP Diversion header.

Parameter	Value
Index	**7**
Name	**Call Forward**
Manipulation Set ID	**4**
Row Role	**Use Previous Condition**
Action Subject	**Header.Diversion**
Action Type	**Normalize**

10. If the manipulation rule Index 6 (above) is executed, then the following rule is also executed. It removes the SIP History-Info header.

Parameter	Value
Index	**8**
Name	**Call Forward**
Manipulation Set ID	**4**
Row Role	**Use Previous Condition**
Action Subject	**Header.History-Info**
Action Type	**Remove**

11. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule applies to messages sent to the Swisscom SIP Trunk IP Group. This rule replaces the host part of the SIP Diversion header with the value that was configured in the Swisscom SIP Trunk IP Group as Group Name.

Parameter	Value
Index	**9**
Name	**Change Diversion Host**
Manipulation Set ID	**4**
Message Type	**Invite.Request**
Condition	**Header.Diversion exists**
Action Subject	**Header.Diversion.URL.Host**
Action Type	**Modify**
Action Value	**Param.IPG.Dst.Host**

12. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to response messages sent to the Swisscom SIP Trunk IP Group. Sometimes Swisscom SIP Trunk sends two media streams in the SIP INVITE message – m=audio (for audio stream) and m=image (for T.38 fax stream). In the response message, when only the audio call is answered, AudioCodes SBC sends ‘m=image 0’ and ‘a=inactive’ to clarify that T.38 fax will not be used. But the Swisscom SIP Trunk requests to remove ‘a=inactive’ and leave only ‘m=image 0’.

Parameter	Value
Index	**10**
Name	**Remove ‘a=inactive’**
Manipulation Set ID	**4**
Message Type	**Any.Response**
Condition	**Body.Sdp regex (.*)(m=image 0)(.*)(a=inactive)(.*)**
Action Subject	**Body.Sdp**
Action Type	**Modify**
Action Value	**$1+$2+$3+$5**

13. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to response messages sent to the Swisscom SIP Trunk IP Group for Call Forward of Anonymous Call initiated by the Microsoft Teams IP Group. This removes the user=phone variable from the SIP 'From' header.

Parameter	Value
Index	**11**
Name	**For Forward Anonymous**
Manipulation Set ID	**4**
Message Type	**Any.Request**
Condition	**Header.From.URL contains 'anonymous'**
Action Subject	**Header.From.URL.Userphone**
Action Type	**Remove**

14. If the manipulation rule Index 11 (above) is executed, then the following rule is also executed. This adds the SIP Privacy header with a value of 'id'.

Parameter	Value
Index	**12**
Name	**For Forward Anonymous**
Manipulation Set ID	**4**
Row Role	**Use Previous Condition**
Action Subject	**Header.Privacy**
Action Type	**Add**
Action Value	**'id'**

15. If the manipulation rule Index 11 (above) is executed, then the following rule is also executed. This rule replaces the user part of the SIP P-Asserted-Identity header with the value from the SIP Diversion header.

Parameter	Value
Index	**13**
Name	**For Forward Anonymous**
Manipulation Set ID	**4**
Row Role	**Use Previous Condition**
Action Subject	**Header.P-Asserted-Identity.URL.User**
Action Type	**Modify**
Action Value	**Header.Diversion.URL.User**

16. If the manipulation rule Index 11 (above) is executed, then the following rule is also executed. This rule replaces the user part of the SIP P-Asserted-Identity header with the value from the SIP Diversion header.

Parameter	Value
Index	**14**
Name	**For Forward Anonymous**
Manipulation Set ID	**4**
Row Role	**Use Previous Condition**
Action Subject	**Header.From.URL.Host**
Action Type	**Modify**
Action Value	**'anonymous.invalid'**

17. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to 200 OK response messages sent to the Swisscom SIP Trunk IP Group. This adds a SIP Require header with a value of 'timer', if the SIP Session Expire header exists.

Parameter	Value
Index	**15**
Name	**Add Require=timer**
Manipulation Set ID	**4**
Message Type	**Any.Response.200**
Condition	**Header.Session-Expires exists**
Action Subject	**Header.Require**
Action Type	**Add**
Action Value	**'timer'**

18. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule removes the Display Name.

Parameter	Value
Index	**16**
Name	**Remove DisplayName**
Manipulation Set ID	**4**
Message Type	**Invite**
Action Subject	**Header.From.QuoteDisplayName**
Action Type	**Remove**

19. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule normalizes the SDP body of each message.

Parameter	Value
Index	**17**
Name	**Normalize SDP**
Manipulation Set ID	**4**
Message Type	**Any**
Action Subject	**Body.sdp**
Action Type	**Normalize**

20. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This replaces the host part of the SIP Request-URI header with the destination host.

Parameter	Value
Index	**18**
Name	**To ITSP change R-URI Host to Cust Domain**
Manipulation Set ID	**4**
Message Type	**Any**
Action Subject	**Header.Request-Uri.URL.Host**
Action Type	**Modify**
Action Value	**Param.Message.Address.Dst.Host**

21. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This replaces the host part of the SIP To header with the destination host.

Parameter	Value
Index	**19**
Name	**To ITSP change To Host to Cust Domain**
Manipulation Set ID	**4**
Message Type	**Any**
Action Subject	**Header.To.URL.Host**
Action Type	**Modify**
Action Value	**Param.Message.Address.Dst.Host**

22. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This replaces the host part of the SIP From header with the destination host.

Parameter	Value
Index	**20**
Name	**To ITSP change From Host to Cust Domain**
Manipulation Set ID	**4**
Message Type	**Any**
Action Subject	**Header.From.URL.Host**
Action Type	**Modify**
Action Value	**Param.Message.Address.Dst.Host**

23. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This replaces the host part of the SIP P-Asserted-Identity header with the destination host.

Parameter	Value
Index	**21**
Name	**To ITSP change PAI Host to Cust Domain**
Manipulation Set ID	**4**
Message Type	**Any**
Action Subject	**Header.P-Asserted-Identity.URL.Host**
Action Type	**Modify**
Action Value	**Param.Message.Address.Dst.Host**

24. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This removes the 'ms-opaque' parameter from the SIP Contact header.

Parameter	Value
Index	**22**
Name	**Remove ms-opaque from Contact**
Manipulation Set ID	**4**
Message Type	**Invite**
Action Subject	**Header.Contact.URL.Param.ms-opaque**
Action Type	**Remove**

25. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule adds the SIP P-Preferred-Identity header with the value from the SIP P-Asserted-Identity header, if the SIP P-Asserted-Identity header exists.

Parameter	Value
Index	**23**
Name	**PPI**
Manipulation Set ID	**4**
Message Type	**Any**
Condition	**Header.P-Asserted-Identity exists**
Action Subject	**Header.P-Preferred-Identity**
Action Type	**Add**
Action Value	**Header.P-Asserted-Identity**

26. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule modifies the host part of the SIP P-Preferred-Identity header with the value of Customer Domain.

Parameter	Value
Index	**24**
Name	**PPI**
Manipulation Set ID	**4**
Message Type	**Any**
Action Subject	**Header.P-Preferred-Identity.URL.Host.Name**
Action Type	**Modify**
Action Value	**Param.IPG.Dst.Host**

27. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule removes the SIP P-Asserted-Identity header.

Parameter	Value
Index	**25**
Name	**PPI**
Manipulation Set ID	**4**
Action Subject	**Header.P-Asserted-Identity**
Action Type	**Remove**

The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set IDs (Manipulation Set IDs 1 and 4) and which are executed for messages sent to and from the Swisscom SIP Trunk IP Group as well as the Teams Direct Routing IP Group. These rules are specifically required to enable proper interworking between Swisscom SIP Trunk and Teams Direct Routing. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule applies to messages received from the Teams IP Group. This replaces the user part of 'sip:' index with the value from 'tel:' index in the SIP P-Asserted-Identity header.	Microsoft Teams send SIP P-Asserted-Identity header with two indexes: 'tel:' and 'sip:'. Swisscom SIP Trunk didn't support such a format and required DID in the 'sip:' index.
1	This rule applies to messages received from the Teams IP Group. This removes the 'tel:' index of the SIP P-Asserted-Identity header.	
2	This rule applies to messages received from the Teams IP Group. This removes the SIP Privacy header in all messages, except for calls with presentation restriction.	Enabling PAI on Teams side sets the Privacy header. All calls are therefore set to CLIR in the Swisscom network. The rule prevents this for non-anonymous calls.
3	This rule applies to messages sent to the Swisscom SIP Trunk IP Group in a call transfer scenario. This rule replaces the host part of the SIP Referred-By header with the value taken from the 'Group Name' field of the Swisscom SIP Trunk IP Group.	For call transfer scenarios, Swisscom SIP Trunk requires the SIP Diversion header instead of SIP Referred-By header, sent from the Microsoft Teams.
4	If manipulation rule index above is executed, then the following rule is also executed. It adds the SIP Diversion header with values from the SIP Referred-by header.	
5	If manipulation rule index above is executed, then the following rule is also executed. It removes the SIP Referred-by header.	
6	This rule applies to messages sent to the Swisscom SIP Trunk IP Group in a call forward scenario. This rule adds the SIP Diversion header with the value from the SIP History-Info header.	For call forward scenarios, Swisscom SIP Trunk requires that the user part in the SIP From header be a defined number. To do this, the user part of the From header is replaced with the value from the History-Info header.
7	If the manipulation rule index above is executed, then the following rule is also executed. It normalizes the SIP Diversion header.	
8	If the manipulation rule index above is executed, then the following rule is also executed. It removes the History-Info header.	
9	This rule applies to messages sent to the Swisscom SIP Trunk IP Group. This rule replaces the host part of the SIP Diversion header with the value that was configured in the Swisscom SIP Trunk IP Group as Group Name.	Swisscom SIP Trunk requires that the host part of the SIP Diversion header be pre-configured.

Rule Index	Rule Description	Reason for Introducing Rule
10	This rule is applied to response messages sent to the Swisscom SIP Trunk IP Group. It removes 'a=inactive' from responses sent to the Swisscom SIP Trunk.	Swisscom SIP Trunk sends two media streams in the SIP INVITE message – m=audio (for audio stream) and m=image (for T.38 fax stream). In the response message, when only the audio call is answered, the AudioCodes SBC sends 'm=image 0' and 'a=inactive' to clarify that T.38 fax will not be used. But the Swisscom SIP Trunk requests to remove 'a=inactive' and leave only 'm=image 0'.
11	This rule is applied to response messages sent to the Swisscom SIP Trunk IP Group for call forward of anonymous calls initiated by the Microsoft Teams IP Group. This removes the 'user=phone' variable from the SIP From header.	These rules are required to normalize messages for Call Forward of Anonymous Calls initiated by the Microsoft Teams.
12	If the manipulation rule index above is executed, then the following rule is also executed. This rule is applied to response messages sent to the Swisscom SIP Trunk IP Group for call forward of anonymous calls initiated by the Microsoft Teams IP Group. This adds the SIP Privacy header with value 'id'.	
13	If the manipulation rule index above is executed, then the following rule is also executed. This rule replaces the user part of the SIP P-Asserted-Identity header with the value from the SIP Diversion header.	
14	If the manipulation rule index above is executed, then the following rule is also executed. This rule replaces the host part of the SIP From header with the value 'anonymous.invalid'.	
15	This rule is applied to 200 OK response messages sent to the Swisscom SIP Trunk IP Group. This adds the SIP Require header with a value of 'timer' if the SIP Session Expire header exists.	According to Swisscom SIP Trunk requirements.
16	This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule removes the display name.	
17	This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule normalizes the SDP body of each message.	
18	This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule replaces the host part of the SIP Request-URI header with the Customer's domain.	According to Swisscom SIP Trunk requirements.
19	This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule replaces the host part of the SIP To header with the Customer's domain.	

Rule Index	Rule Description	Reason for Introducing Rule
20	This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule replaces the host part of the SIP From header with the Customer's domain.	
21	This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This replaces the host part of the SIP P-Asserted-Identity header with the Customer's domain.	
22	This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This removes the 'ms-opaque' parameter from the SIP Contact header.	
23	This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule adds the SIP P-Preferred-Identity header with the value from the SIP P-Asserted-Identity header, if the SIP P-Asserted-Identity header exists.	According to Swisscom requirements, SBCon Trunk supports SIP P-Preferred-Identity header and doesn't support SIP P-Asserted-Identity header.
24	This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule modifies the host part of the SIP P-Preferred-Identity header with the value of Customer Domain.	
25	This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule removes the SIP P-Asserted-Identity header.	

28. Assign Manipulation Set IDs 1 to the Teams Direct Routing IP Group:
    a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
    b. Select the row of the Teams Direct Routing IP Group, and then click **Edit**.
    c. Set the 'Inbound Message Manipulation Set' field to **1**.
    d. Click **Apply**.
29. Assign Manipulation Set ID 4 to the Swisscom SIP trunk IP Group:
    a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
    b. Select the row of the Swisscom SIP trunk IP Group, and then click **Edit**.
    c. Set the 'Outbound Message Manipulation Set' field to **4**.
    d. Click **Apply**.

4.18 Configure Registration Accounts

This section describes how to configure SIP registration accounts. This is required so that the SBC can register with the Swisscom SIP Trunk on behalf of Teams Direct Routing. The Swisscom SIP Trunk requires registration and authentication to provide service.

In the interoperability test topology, the Served IP Group is Teams Direct Routing IP Group and the Serving IP Group is Swisscom SIP Trunk IP Group.

To configure a registration account:

1. Open the Accounts table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**).
2. Click **New**.
3. Configure the account according to the provided information from , for example:

Parameter	Value
Served IP Group	**Teams**
Application Type	**SBC**
Serving IP Group	**SBCon**
Host Name	-
Register	**Regular**
Contact User	**+41xxxxxxxxx** (trunk main line)
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

4. Click **Apply**.

4.19 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

4.19.1 Configure Call Forking Mode

This section describes how to configure the SBC's handling of SIP 18x responses received for call forking of INVITE messages. For the interoperability test topology, if a SIP 18x response with SDP is received, the SBC opens a voice stream according to the received SDP. The SBC re-opens the stream according to subsequently received 18x responses with SDP or plays a ringback tone if a 180 response without SDP is received. It is mandatory to set this field for the Teams Direct Routing environment.

To configure call forking:

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).
2. From the 'SBC Forking Handling Mode' drop-down list, select **Sequential**.
3. Click **Apply**.

4.19.2 Optimizing CPU Cores Usage for a Specific Service (relevant for Mediant 9000 and Software SBC only)

This section describes how to optimize the SBC's CPU cores usage for a specified profile to achieve maximum capacity for that profile. The supported profiles include:

- SIP profile – improves SIP signaling performance, for example, SIP calls per second (CPS)
- SRTP profile – improves maximum number of SRTP sessions
- Transcoding profile – enables all DSP-required features, for example, transcoding and voice in-band detectors

To optimize core allocation for a profile:

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).
2. From the 'SBC Performance Profile' drop-down list, select the required profile:

3. Click **Apply** and then reset the device with a burn-to-flash for your settings to take effect.

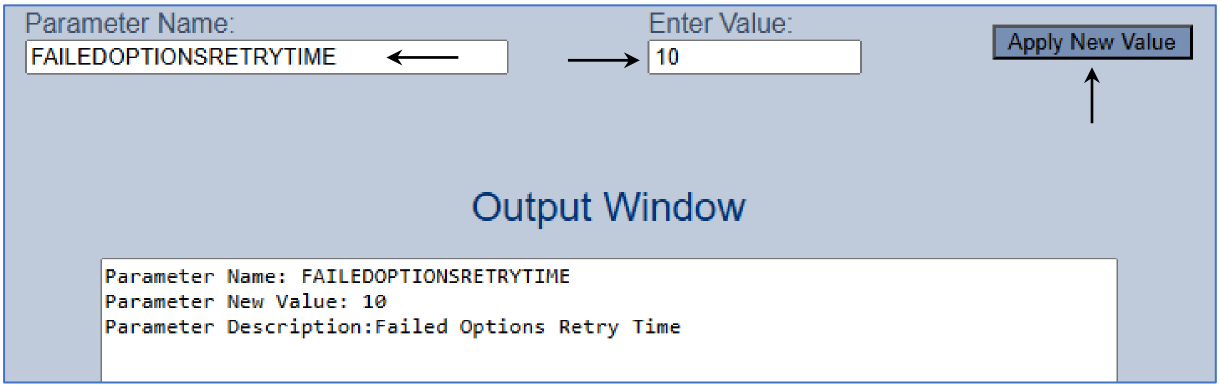
4.19.3 Configure Failed Options Retry Time

This section describes how to configure how long the SBC waits (in seconds) before re-sending a SIP OPTIONS keep-alive message to the proxy after the SBC considers the proxy as offline. By default, it is set to 1 sec which gives heavy traffic.

To configure Failed Options Retry Time:

1. Open the Admin page: Append the case-sensitive suffix 'AdminPage' to the device's IP address in your Web browser's URL field (e.g., http://10.15.17.10/AdminPage).
2. In the left pane of the page that opens, click ***ini* Parameters**.

Figure 4-15: Configure Failed Options Retry Time parameters in AdminPage



3. Enter these values in the 'Parameter Name' and 'Enter Value' fields:

Parameter	Value
FAILEDOPTIONSRETRYTIME	10

4. Click the **Apply New Value** button for each field.

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-14417