Configuration Note

AudioCodes Professional Services – Interoperability Lab

Microsoft® Teams Direct Routing Enterprise Model and htp Business FleX SIP-Trunk Smart using AudioCodes Mediant™ SBC

Version 7.4

Table of Contents

Table of Contents ii

Notice iv

WEEE EU Directive iv
Customer Support iv
Stay in the Loop with AudioCodes iv
Abbreviations and Terminology iv
Document Revision Record iv
Documentation Feedback iv

1 Introduction 1

1.1 Intended Audience 1
1.2 About Microsoft Teams Direct Routing 1
1.3 About AudioCodes SBC Product Series 1

2 Component Information 2

2.1 AudioCodes SBC Version 2
2.2 htp Business FleX SIP-Trunk Smart Version 2
2.3 Microsoft Teams Direct Routing Version 2
2.4 Interoperability Test Topology 3
2.4.1 Enterprise Model Implementation 3
2.4.2 Environment Setup 4
2.4.3 Infrastructure Prerequisites 4
2.4.4 Known Limitations 4

3 Configuring Teams Direct Routing 5

3.1 Prerequisites 5
3.2 SBC Domain Name in Teams Enterprise Model 5
3.3 Example of Office 365 Tenant Direct Routing Configuration 6
3.3.1 Adding a New SBC to Direct Routing 7
3.3.2 Adding Voice Route and PSTN Usage 8
3.3.3 Adding Voice Routing Policy 10
3.3.4 Enabling an Online User 11
3.3.5 Assigning Online User to Voice Routing Policy 11

4 Configuring AudioCodes SBC 12

4.1 SBC Configuration Concept in Teams Direct Routing Enterprise Model 12
4.2 IP Network Interfaces Configuration 13
4.2.1 Configuring VLANs 13
4.2.2 Configuring Network Interfaces 13
4.3 SIP TLS Connection Configuration 14
4.3.1 Configuring NTP Server Address 14

4.3.2 Creating a TLS Context for Teams Direct Routing 15
4.3.3 Configuring a Certificate 15
4.3.4 Method of Generating and Installing Wildcard Certificate 17
4.3.5 Deploying Trusted Root Certificate for MTLS Connection 17
4.4 Configuring a Certificate for Operation with htp Business FleX SIP-Trunk Smart 18
4.5 Configuring Media Realms 19
4.6 Configuring SIP Signaling Interfaces 19
4.7 Configuring Proxy Sets and Proxy Address 20
4.7.1 Configuring a Proxy Address 20
4.8 Configuring Coders 21
4.9 Configuring IP Profiles 23
4.10 Configuring IP Groups 25
4.11 Configuring SRTP 26
4.12 Configuring Message Condition Rules 26
4.13 Configuring Classification Rules 27
4.14 Configuring IP-to-IP Call Routing Rules 28
4.15 Configuring Firewall Settings (Optional) 29
4.16 Configuring Message Manipulation Rules 30
4.17 Configuring Registration Accounts 32
4.18 Miscellaneous Configuration 33
4.18.1 Configuring Call Forking Mode 33
4.18.2 Optimizing CPU Cores Usage for a Specific Service (relevant for Mediant 9000 and Software SBC only) 33

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: July-10-2022

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
90585	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 website 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 htp Business FleX SIP-Trunk Smart 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 Web site at https://www.audiocodes.com/partners/sbc-interoperability-list.

1.1 Intended Audience

This document is intended for engineers, or AudioCodes and htp Business FleX SIP-Trunk Smart partners who are responsible for installing and configuring htp Business FleX SIP-Trunk Smart 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.250.363 or later
Protocol	For this interop, both htp Business FleX SIP-Trunk Smart and Microsoft Teams Direct Routing use SIP/TLS
Additional Notes	None

2.2 htp Business FleX SIP-Trunk Smart Version

Table 2: htp Business FleX SIP-Trunk Smart Access SBC Version

Vendor/Service Provider	AudioCodes/htp Business FleX SIP-Trunk Smart
SSW Model/Service	Mediant VE
Software Version	7.20A.258.367
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	Release v.2022.6.21.1
Protocol	SIP
Additional Notes	None

2.4 Interoperability Test Topology

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

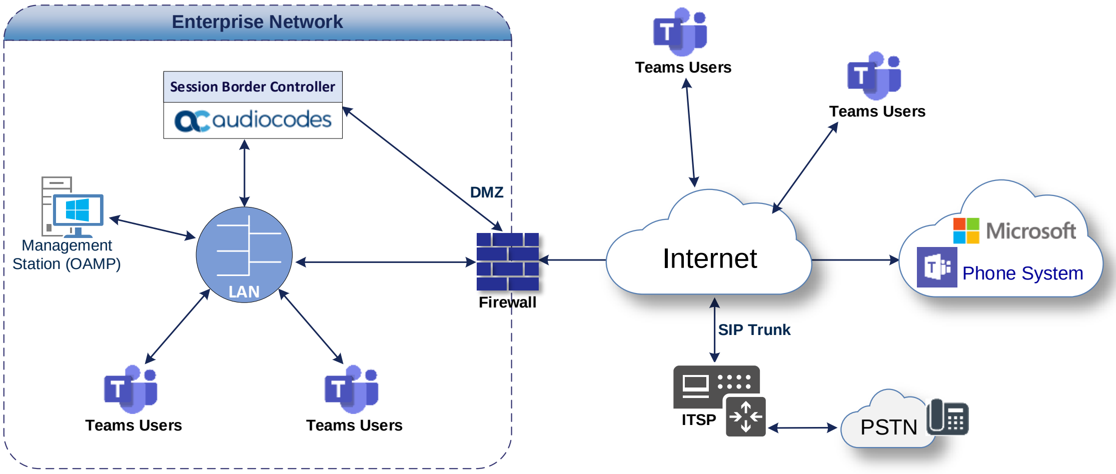
2.4.1 Enterprise Model Implementation

The interoperability testing between AudioCodes SBC and htp Business FleX SIP-Trunk Smart with Teams Direct Routing Enterprise Model was done using the following topology setup:

- Enterprise may be 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 htp Business FleX SIP-Trunk Smart service
- AudioCodes SBC is implemented to interconnect between the SIP Trunk and Microsoft Teams located on the WAN
    - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
    - **Border:** IP-to-IP network border – both the htp Business FleX SIP-Trunk Smart and the Microsoft Teams Phone System are located in the public network.

The figure below illustrates this interoperability test topology:

Figure 1: Interoperability Test Topology between SBC and Microsoft Teams Direct Routing Enterprise Model with htp Business FleX SIP-Trunk Smart



2.4.2 Environment Setup

The interoperability test topology includes the following environment setup:

Table 4: Environment Setup

Area	Setup
Network	Both Microsoft Teams Direct Routing environment and htp Business FleX SIP-Trunk Smart are located on the Enterprise's WAN
Signaling Transcoding	Both Microsoft Teams Direct Routing environment and htp Business FleX SIP-Trunk Smart are operates with SIP-over-TLS transport type
Codecs Transcoding	■ Microsoft Teams Direct Routing supports G.711A-law, G.711U-law, G.729, G.722 and SILK (NB and WB) coders ■ htp Business FleX SIP-Trunk Smart supports G.711A-law coder
Media Transcoding	Both Microsoft Teams Direct Routing environment and htp Business FleX SIP-Trunk Smart are 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

There were no limitations observed in the interoperability tests done for the AudioCodes SBC interworking between Microsoft Teams Direct Routing and htp Business FleX SIP-Trunk Smart.

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 Teams Enterprise Model

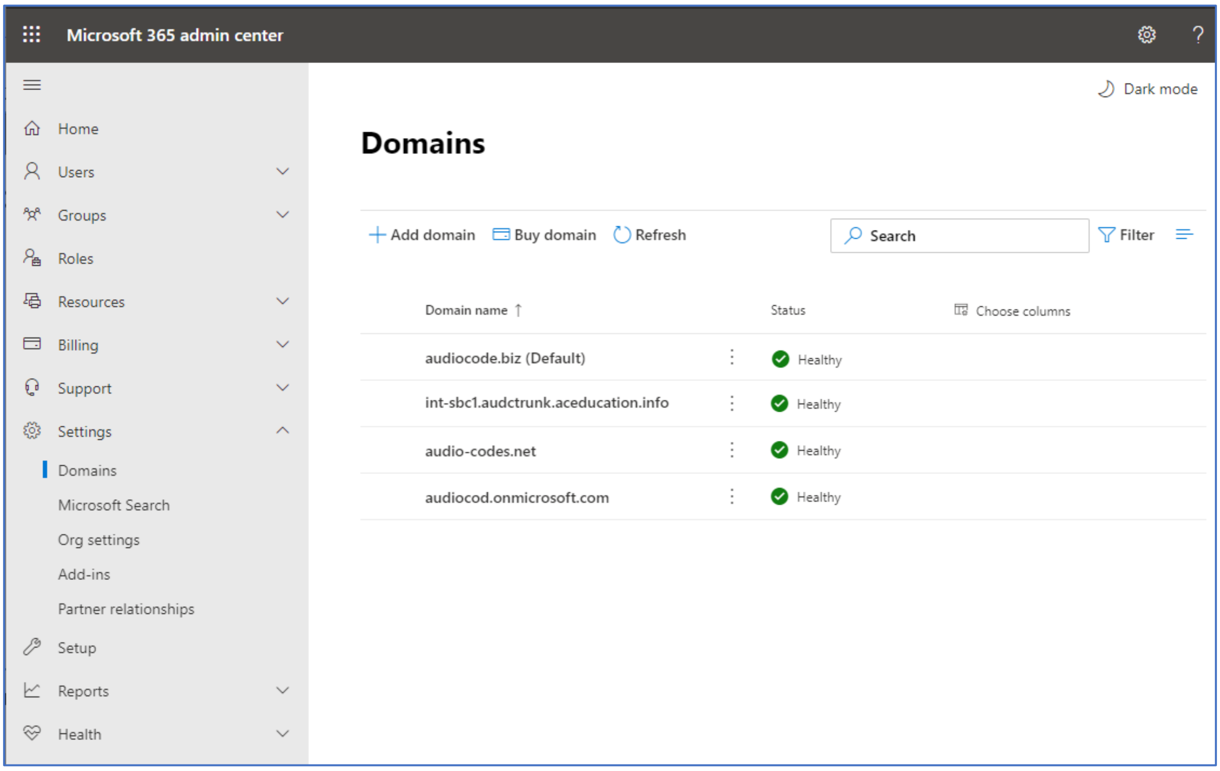
The SBC domain name must be from one of the names registered in 'Domains' of the tenant. You cannot use the ***.onmicrosoft.com** tenant for the domain name. For example, in Figure 3-1, the administrator registered the following DNS names for the tenant:

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 users user@ACeducation.info with the SBC FQDN **int-sbc1.audctrunk.aceducation.info** so long as both names are registered for this tenant.

Figure 2: Example of Registered DNS Names



Domains

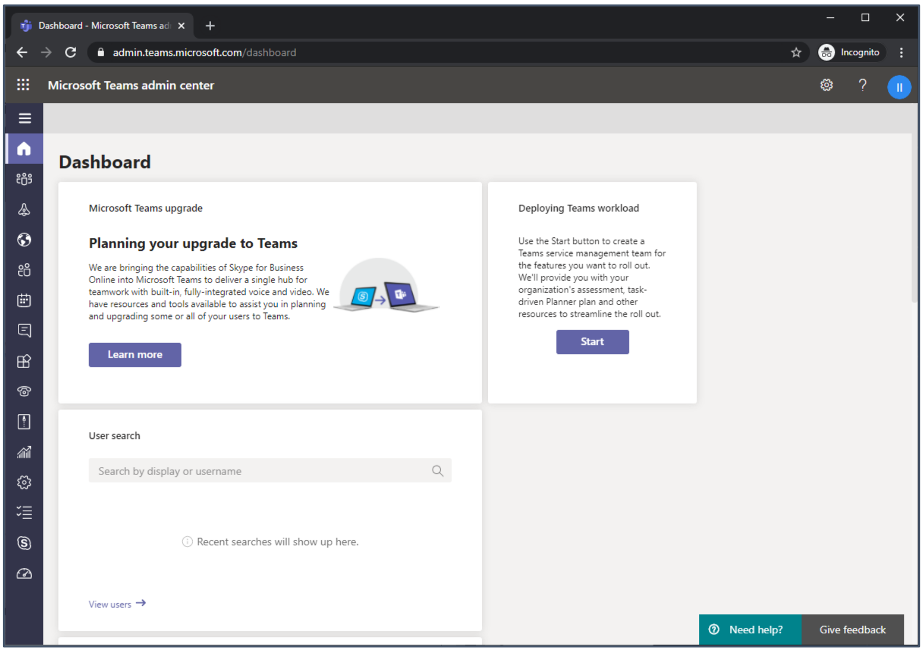
Domain name ↑	Status
audiocode.biz (Default)	Healthy
int-sbc1.audctrunk.aceducation.info	Healthy
audio-codes.net	Healthy
audiocod.onmicrosoft.com	Healthy

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 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 3: Teams Admin Center



Dashboard - Microsoft Teams ad
admin.teams.microsoft.com/dashboard
Incognito
Microsoft Teams admin center
Learn more
Start
Search by display or username
View users
Need help?
Give feedback

Dashboard

Microsoft Teams upgrade

Planning your upgrade to Teams

We are bringing the capabilities of Skype for Business Online into Microsoft Teams to deliver a single hub for teamwork with built-in, fully-integrated voice and video. We have resources and tools available to assist you in planning and upgrading some or all of your users to Teams.

Deploying Teams workload

Use the Start button to create a Teams service management team for the features you want to roll out. We'll provide you with your organization's assessment, task-driven Planner plan and other resources to streamline the roll out.

User search

Recent searches will show up here.

3.3.1 Adding a New SBC to Direct Routing

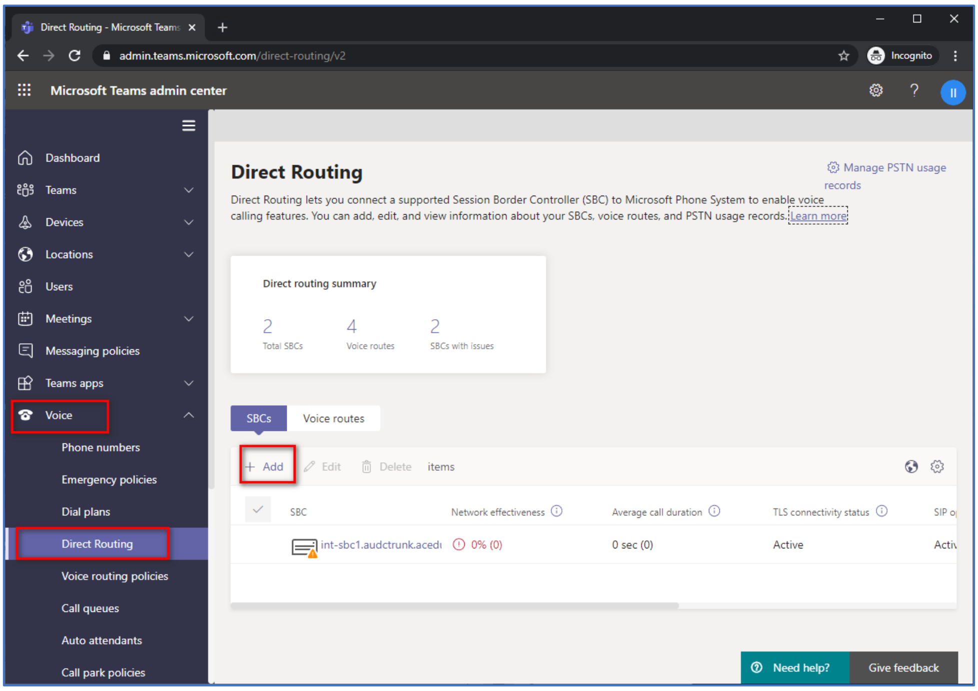
The procedure below describes how add a new SBC to Direct Routing.

To add New SBC to Direct Routing:

In the web interface, select **Voice**, and then click **Direct Routing**.

2. Under SBCs click **Add.**

Figure 4: Add new SBC to Direct Routing



Direct Routing

Direct Routing lets you connect a supported Session Border Controller (SBC) to Microsoft Phone System to enable voice calling features. You can add, edit, and view information about your SBCs, voice routes, and PSTN usage records. Learn more

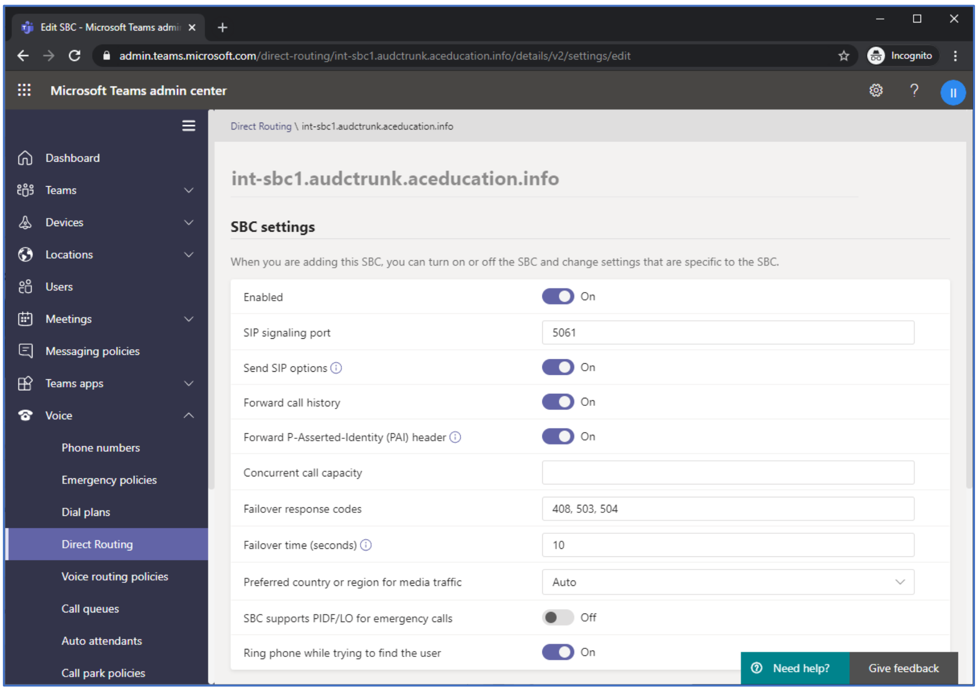
Direct routing summary

2	4	2
Total SBCs	Voice routes	SBCs with issues

SBC	Network effectiveness	Average call duration	TLS connectivity status	SIP o
int-sbc1.audctrunk.acedı	0% (0)	0 sec (0)	Active	Activ

3. Configure SBC.

Figure 5: Configure new SBC



int-sbc1.audctrunk.aceducation.info

SBC settings

When you are adding this SBC, you can turn on or off the SBC and change settings that are specific to the SBC.

Enabled	On
SIP signaling port	5061
Send SIP options	On
Forward call history	On
Forward P-Asserted-Identity (PAI) header	On
Concurrent call capacity	
Failover response codes	408, 503, 504
Failover time (seconds)	10
Preferred country or region for media traffic	Auto
SBC supports PIDF/LO for emergency calls	Off
Ring phone while trying to find the user	On

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
```

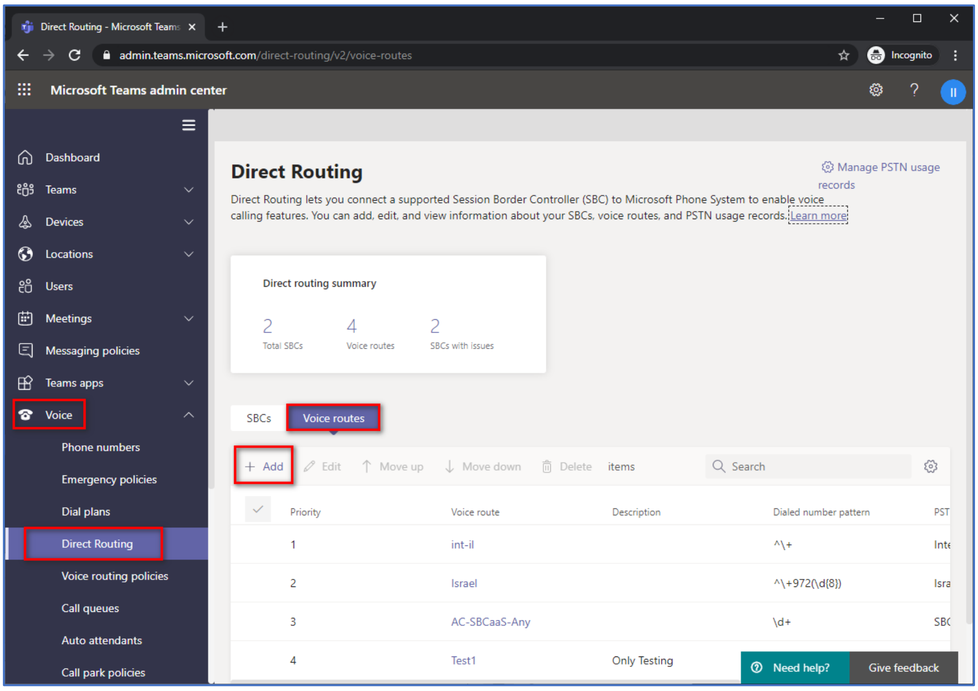
3.3.2 Adding Voice Route and PSTN Usage

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

To add voice route and PSTN usage:

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

Figure 6: Add New Voice Route



Direct Routing

Direct Routing lets you connect a supported Session Border Controller (SBC) to Microsoft Phone System to enable voice calling features. You can add, edit, and view information about your SBCs, voice routes, and PSTN usage records. Learn more

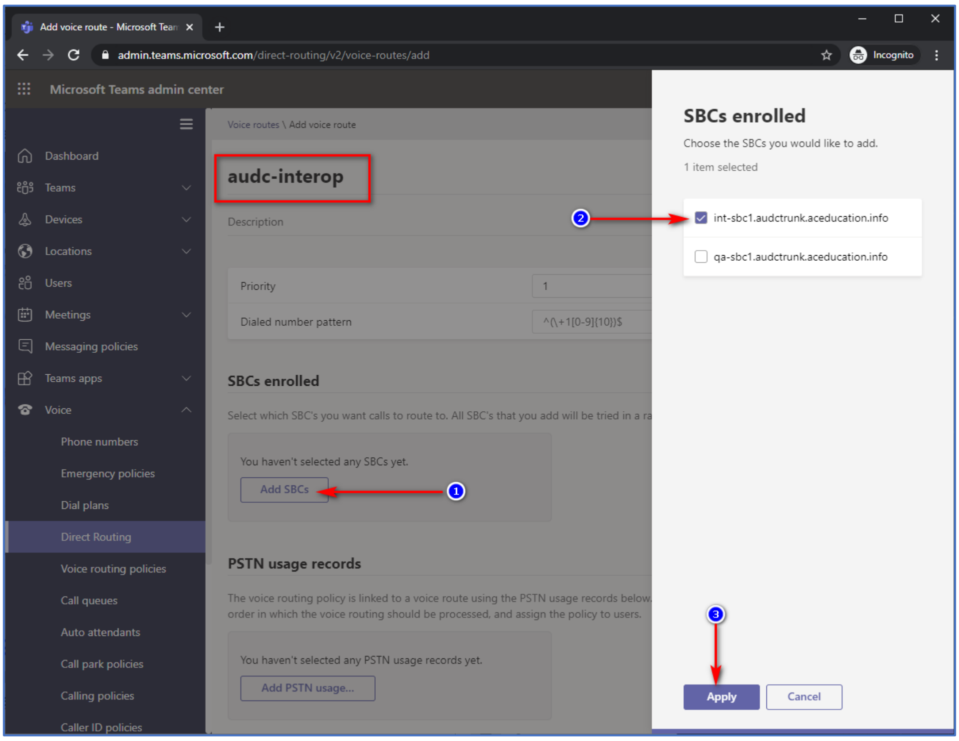
Direct routing summary

2 Total SBCs 4 Voice routes 2 SBCs with issues

Priority	Voice route	Description	Dialed number pattern	PST
1	int-il		^\+	Inte
2	Israel		^\+972(\d{8})	Isra
3	AC-SBCaaS-Any		\d+	SBC
4	Test1	Only Testing		

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

Figure 7: Associate SBC with new Voice Route



audc-interop

Description

Priority 1

Dialed number pattern ^(\+1[0-9]{10})$

SBCs enrolled

Select which SBC's you want calls to route to. All SBC's that you add will be tried in a ra

You haven't selected any SBCs yet.

PSTN usage records

The voice routing policy is linked to a voice route using the PSTN usage records below. order in which the voice routing should be processed, and assign the policy to users.

You haven't selected any PSTN usage records yet.

SBCs enrolled

Choose the SBCs you would like to add.

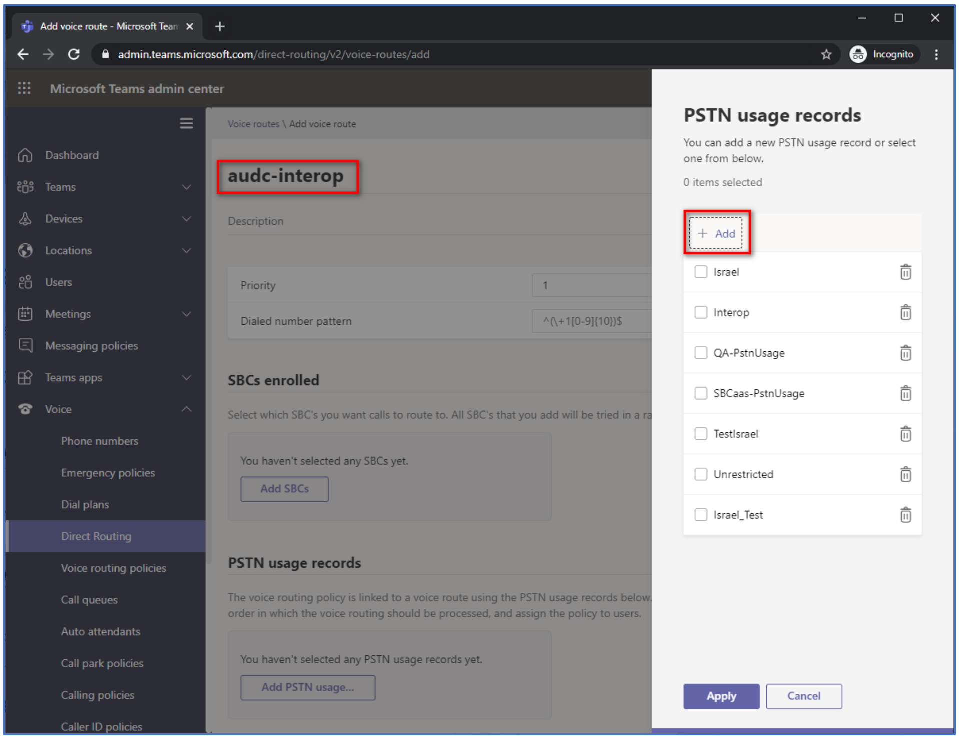
1 item selected

☑ int-sbc1.audctrunk.aceducation.info

□ qa-sbc1.audctrunk.aceducation.info

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

Figure 8: Associate PSTN Usage with New Voice Route



audc-interop

Description

Priority 1

Dialed number pattern ^(\+1[0-9]{10})$

SBCs enrolled

Select which SBC's you want calls to route to. All SBC's that you add will be tried in a ra

You haven't selected any SBCs yet.

PSTN usage records

The voice routing policy is linked to a voice route using the PSTN usage records below. order in which the voice routing should be processed, and assign the policy to users.

You haven't selected any PSTN usage records yet.

PSTN usage records

You can add a new PSTN usage record or select one from below.

0 items selected

□ Israel

□ Interop

□ QA-PstnUsage

□ SBCaas-PstnUsage

□ TestIsrael

□ Unrestricted

□ Israel_Test

The same operations can be done using following PowerShell commands:

6. Creating an empty PSTN Usage:

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

7. 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"
```

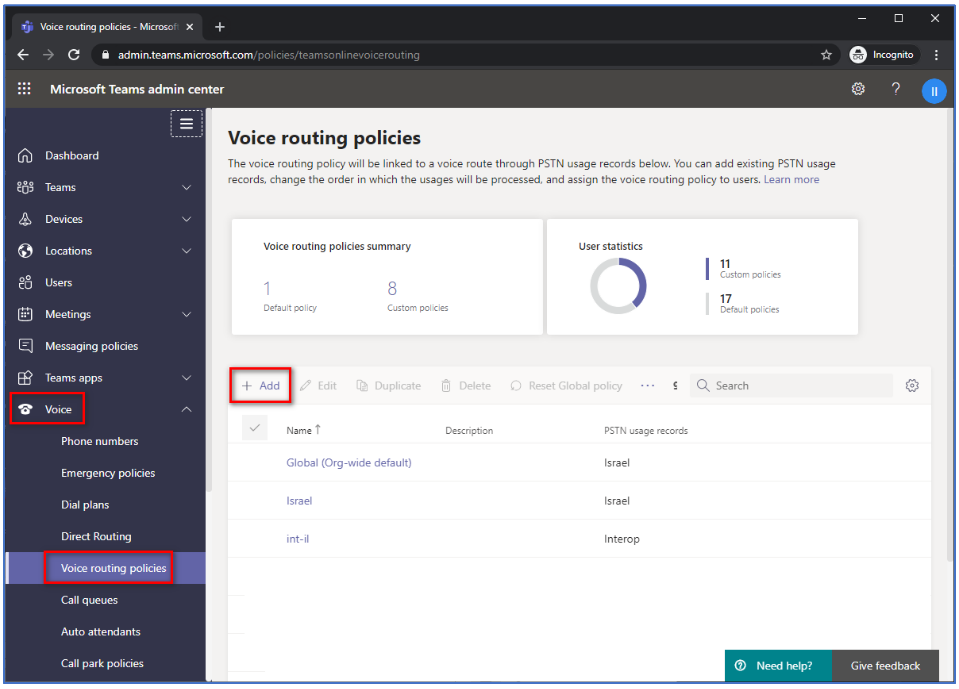
3.3.3 Adding Voice Routing Policy

The procedure below describes how add a voice routing policy

To add voice routing policy:

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

Figure 9: Add New Voice Routing Policy



Voice routing policies

The voice routing policy will be linked to a voice route through PSTN usage records below. You can add existing PSTN usage records, change the order in which the usages will be processed, and assign the voice routing policy to users. Learn more

Voice routing policies summary

1 Default policy

8 Custom policies

User statistics

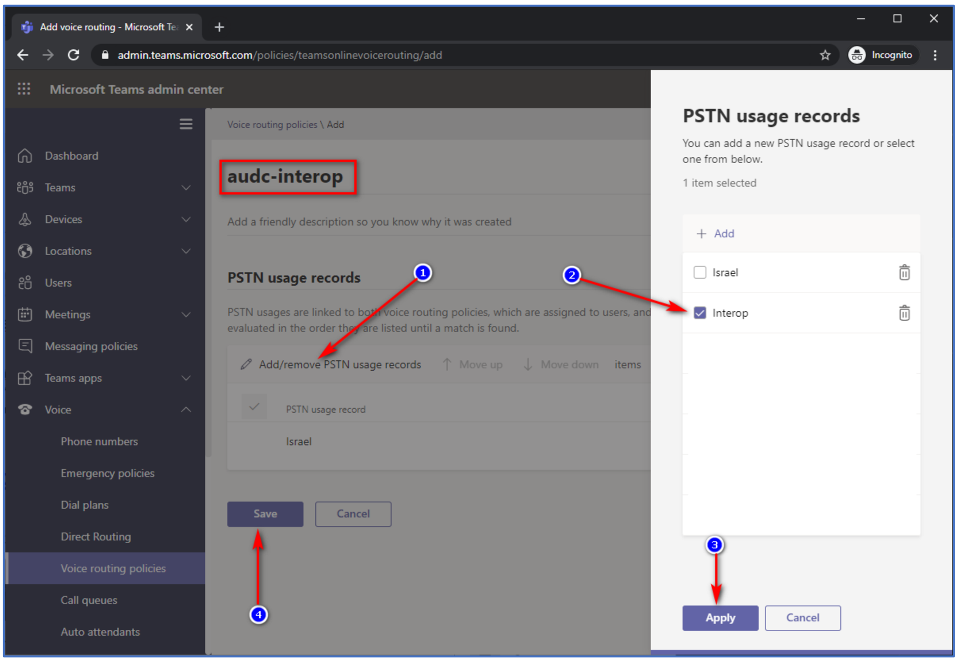
11 Custom policies

17 Default policies

Name ↑	Description	PSTN usage records
Global (Org-wide default)		Israel
Israel		Israel
int-il		Interop

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

Figure 10: Associate PSTN Usage with New Voice Routing Policy


Add voice routing - Microsoft Te
admin.teams.microsoft.com/policies/teamsonlinevoicerouting/add
Incognito
Microsoft Teams admin center
Dashboard
Teams
Devices
Locations
Users
Meetings
Messaging policies
Teams apps
Voice
Phone numbers
Emergency policies
Dial plans
Direct Routing
Voice routing policies
Call queues
Auto attendants
Voice routing policies \ Add
audc-interop
Add a friendly description so you know why it was created
PSTN usage records
PSTN usages are linked to both voice routing policies, which are assigned to users, and evaluated in the order they are listed until a match is found.
Add/remove PSTN usage records
Move up
Move down
items
PSTN usage record
Israel
Save
Cancel
PSTN usage records
You can add a new PSTN usage record or select one from below.
1 item selected
+ Add
□ Israel
☑ Interop
Apply
Cancel
1
2
3
4

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 Enabling an 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 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 htp Business FleX SIP-Trunk Smart. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 3, and includes the following main areas:

- SBC LAN interface – Management Station
- SBC WAN interface - htp Business FleX SIP-Trunk Smart and Teams Direct Routing environment

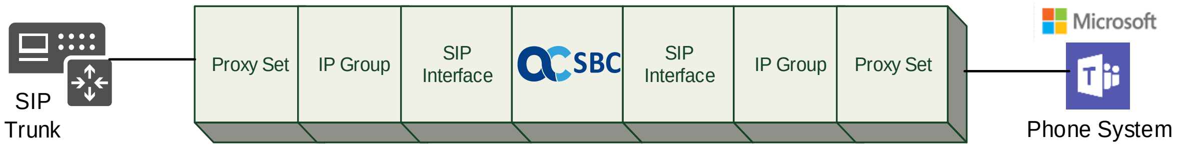
This configuration is done using the SBC's embedded Web server (hereafter, referred to as *Web interface*).

- For implementing Microsoft Teams Direct Routing and htp Business FleX SIP-Trunk Smart 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 11: SBC Configuration Concept

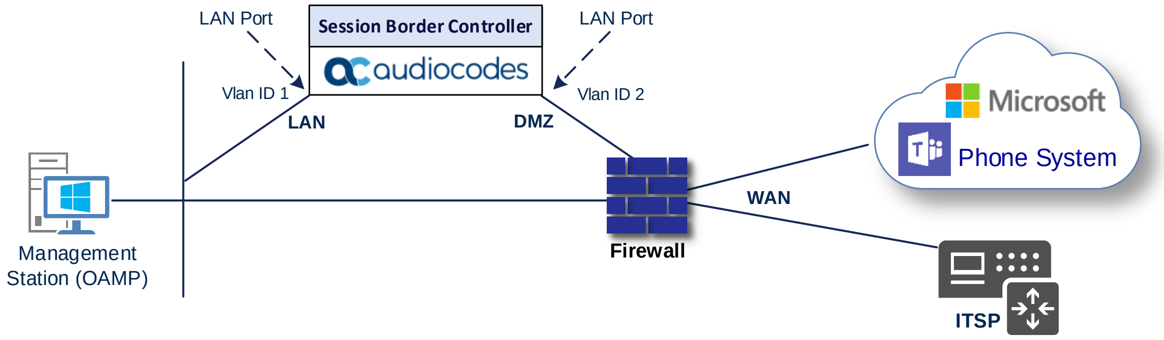


4.2 IP Network Interfaces Configuration

This section describes how to configure the SBC's IP network interfaces. There are several ways to deploy the SBC; 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 htp Business FleX SIP-Trunk Smart, 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 12: Network Interfaces in Interoperability Test Topology



4.2.1 Configuring 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:

Open the Ethernet Device table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Devices**).

9. There is one existing row for VLAN ID 1 and underlying interface GROUP_1.
10. Add another VLAN ID 2 for the WAN side

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 the IP network interfaces:

Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).

11. 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	195.189.192.158 (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 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 htp Business FleX SIP-Trunk Smart. This configuration is essential for a secure SIP TLS connection. The configuration instructions for Microsoft Teams Direct Routing 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 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

4.3.1 Configuring 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 the NTP Server is located on the OAMP IP Interface (LAN_IF in our case) or is accessible through it.

To configure the NTP server address:

Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**).

12. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., **10.15.27.1**).
13. Click **Apply**.

4.3.2 Creating 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:

Open the TLS Contexts table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).

14. 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
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.

15. Click **Apply**.

4.3.3 Configuring 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:

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:

Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).

16. 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.

17. Under the **Certificate Signing Request** group, do the following:

    In the 'Subject Name [CN]' field, enter the SBC FQDN name
    (based on example above, **int-sbc1.audctrunk.aceducation.info**).

    e. In the '1st Subject Alternative Name [SAN]' field, change the type to 'DNS' and enter the SBC FQDN name (based on our example, **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.

f. Change the 'Private Key Size' based on the requirements of your Certification Authority. Many CAs do not support private key of size 1024.

g. 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.

h. Fill in the rest of the request fields according to your security provider's instructions.

i. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button.

18. 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*.

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

20. 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:

    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.

    j. 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.

21. 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.

22. 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.

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

    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.

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

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

4.3.4 Method of Generating and Installing 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:

Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).

25. 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.
26. Scroll down to the **Upload certificates files from your computer** group and do the following:

    Enter the password assigned during export with the DigiCert utility in the '**Private key pass-phrase**' field.

    I. Click the **Choose File** button corresponding to the 'Send **Private Key**...' field and then select the SBC certificate file exported from the DigiCert utility.

4.3.5 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, 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 Configuring a Certificate for Operation with htp Business FleX SIP-Trunk Smart

> This section is relevant only if the connection to htp Business FleX SIP-Trunk Smart is implemented over TLS. For connection over UDP or TCP, skip this section.

This section describes how to exchange a certificate with the Certificate Authority (CA), trusted by htp GmbH SIP Trunk. The certificate is used by the SBC to authenticate the connection with the htp Business FleX SIP-Trunk Smart. To trust the certificate of the htp server, at least the following DigiCert root certificate "**DigiCert Global Root G2**" must be installed in the SBC.

The procedure involves the following main steps:

Generating a Private Key and Self-Signed Certificate.

27. Obtaining Trusted Root/Intermediate Certificate from CA (DigiCert).
28. Deploying Trusted Root/Intermediate Certificates on SBC.

To configure a certificate:

Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).

29. In the TLS Contexts page, select the default Context index (0) row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
30. Under the **Certificate Signing Request** group click the **Generate Self-Signed Certificate** button.
31. Under the **Generate New Private Key** group, click the **Generate Private Key** button to create new private key.
32. In the SBC's Web interface, return to the **TLS Contexts** page.

    In the TLS Contexts page, select the required TLS Context index 0 row, and then click the **Trusted Root Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.

    m. Click the **Import** button, and then select the **DigiCert Global Root G2** Certificates to load.
33. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.

4.5 Configuring 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:

Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).

34. Configure Media Realms as follows (you can use the default Media Realm (Index 0), but modify it):

Table 9: Configuration Example Media Realms in Media Realm Table

Index	Name	IPv4 Interface Name	UDP Port Range Start	Number of Media Session Legs
0	MR-htp	WAN_IF	30,000	100 (media sessions assigned with port range)
1	MR-Teams	WAN_IF	6000	100 (media sessions assigned with port range)
All other parameters can be left unchanged with their default values.				

4.6 Configuring SIP Signaling Interfaces

This section describes how to configure SIP Interfaces. Due to fact that both Microsoft Teams and htp Business FleX SIP-Trunk Smart are located at the WAN side of the SBC, only one SIP Interface can be used. For specific interworking tests, the default SIP Interface (Index 0) configuration was used.

To configure SIP Interfaces:

Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).

35. Configure SIP Interfaces. Modify the default SIP Interface (Index 0) 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 10: 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	SIPInterface_0 (arbitrary name)	WAN_IF	SBC	0	0	5061[1] (as configured in the Office 365)	Enable	0 (Recommended to prevent DoS attacks)	-	-

[1] Depend on connection with htp Business FleX. This is example of the connectivity over TLS.

4.7 Configuring 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:

- htp Business FleX SIP-Trunk Smart
- Teams Direct Routing

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

To configure Proxy Sets:

Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).

36. Configure Proxy Sets as shown in the table below:

Table 11: 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	DNS Resolve Method
1	htp (arbitrary name)	SIPInterface_0	default	Using Options	Enable	Random Weights	SRV
2	Teams (arbitrary name)	SIPInterface_0	Teams	Using Options	Enable	Random Weights	

4.7.1 Configuring a Proxy Address

This section shows how to configure a Proxy Address.

To configure a Proxy Address for SIP Trunk:

Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets) and then click the Proxy Set **htp**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.

37. Click **+New**; and configure the address of the Proxy Set according to the parameters described in the table below:

Table 12: Configuration Proxy Address for SIP Trunk

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	siptrunk.htp.net	TLS	0	0

38. Click **Apply**.

To configure a Proxy Address for Teams:

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.

39. 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 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

40. Click Apply.

4.8 Configuring 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 htp Business FleX SIP-Trunk Smart 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 htp Business FleX SIP-Trunk Smart.

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

To configure coders:

Open the Coder Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Coder Groups**).

41. Configure a Coder Group 0 for htp Business FleX SIP-Trunk Smart:

Table 14: Coder Group AudioCodersGroups_0 for htp Business FleX SIP-Trunk Smart

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711 A-law	20	64	8	Disabled

2. Click **Apply**.

3. Configure a Coder Group 1 for Microsoft Teams Direct Routing:

Table 15: Coder Group AudioCodersGroups_1 for Microsoft Teams Direct Routing

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

2. Click **Apply**.

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the htp Business FleX SIP-Trunk Smart uses the dedicated coders list whenever possible. Note that this Allowed Coders Group ID is assigned to the IP Profile belonging to the htp Business FleX SIP-Trunk Smart in the next step.

To set a preferred coder for the htp Business FleX SIP-Trunk Smart SIP Trunk:

Open the Allowed Audio Coders Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Audio Coders Groups**).

3. Click **New** and configure a name for the Allowed Audio Coders Group for htp Business FleX SIP-Trunk Smart (*e.g., htp-allowed*).
4. Click **Apply.**
5. 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.
6. Click **New** and configure an Allowed Coders as follows:

Index	Coder
0	G.711 A-law

7. Click **New** and configure a name for the Allowed Audio Coders Group for Microsoft Teams Direct Routing (*e.g., Teams-allowed*).
8. Click **Apply.**
9. 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.
10. Click **New** and configure an Allowed Coders as follows:

Index	Coder
0	SILK-NB
1	SILK-WB
2	G.729
3	G.711 A-law
4	G.711 U-law
5	Opus
6	G.722

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

4.9 Configuring 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:

- htp Business FleX SIP-Trunk Smart – to operate in secure mode using SRTP and SIP over TLS
- Microsoft Teams Direct Routing – to operate in secure mode using SRTP and SIP over TLS

To configure an IP Profile for the htp Business FleX SIP-Trunk Smart:

Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).

14. Click **New**, and then configure the parameters as follows:

Parameter	Value
General	
Index	**1**
Name	**htp** (arbitrary name)
Media Security	
SBC Media Security Mode	**Secured**
SBC Early Media	
Remote Early Media RTP Detection Mode	**By Media**
SBC Media	
Extension Coders Group	**AudioCodersGroups_0**
Allowed Audio Coders	**htp-allowed**
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**

15. Click **Apply**.

To configure IP Profile for the Microsoft Teams Direct Routing:

Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).

16. 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)
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**
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 replaces 0.0.0.0 with its IP address)

17. Click **Apply**.

4.10 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 ITSP) 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.

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

- htp Business FleX SIP-Trunk Smart
- Teams Direct Routing

To configure IP Groups:

Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).

18. Configure an IP Group for the htp Business FleX SIP-Trunk Smart:

Parameter	Value
Index	**1**
Name	**htp** (arbitrary descriptive name)
Type	**Server**
Proxy Set	**htp**
IP Profile	**htp**
Media Realm	**MR-htp**
SIP Group Name	**siptrunk.htp.net** (according to ITSP requirement)

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

Parameter	Value
Index	**2**
Name	**Teams** (arbitrary descriptive name)
Type	**Server**
Proxy Set	**Teams**
IP Profile	**Teams**
Media Realm	**MR-Teams**
SIP Group Name	**siptrunk.htp.net** (according to ITSP requirement)
Classify By Proxy Set	**Disable**
Local Host Name	**< FQDN name of your SBC in the Microsoft Teams tenant >** (For example, int-sbc1.audctrunk.aceducation.info)
Always Use Src Address	**Yes**
Teams Direct Routing Mode	**Enable**
Proxy Keep-Alive using IP Group settings	**Enable**

4.11 Configuring SRTP

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

To configure media security:

Open the Media Security page (**Setup** menu **> Signaling & Media** tab **> Media** folder **> Media Security**).

20. From the '**Media Security**' drop-down list, select **Enable** to enable SRTP.
21. 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:

Open the Message Conditions table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Conditions**).

22. 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'**

23. 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:

Open the Classification table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Classification Table**).

24. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	**0**
Name	**Teams**
Source SIP Interface	**SIPInterface_0**
Source IP Address	**52.*.*.***
Destination Host	**< FQDN name of your SBC in the Microsoft Teams tenant >** (e.g., int-sbc1.audctrunk.aceducation.info)
Message Condition	**Teams-Contact**
Action Type	**Allow**
Source IP Group	**Teams**

25. Click **Apply**.

4.14 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.

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

- 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 htp Business FleX SIP-Trunk Smart
- Calls from htp Business FleX SIP-Trunk Smart to Teams Direct Routing

To configure IP-to-IP routing rules:

Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).

26. 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 SIP Trunk (arbitrary name)	Teams				IP Group	htp	
3	SIP Trunk to Teams (arbitrary name)	htp				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 apply to all incoming packets, including UDP or TCP responses.

To configure a firewall rule:

Open the Firewall table (**Setup** menu > **IP Network** tab > **Security** folder> **Firewall**).

27. 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	TCP	Enable	WAN_IF	Allow
4	yyy.yyy.yyy.yyy	32	0	65535	TCP	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 rows of index 3 and 4.

4.16 Configuring Message Manipulation Rules

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

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

To configure SIP message manipulation rule:

Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).

28. Configure a new manipulation rule (Manipulation Set 1) for Teams. This rule applies to messages received from the Teams IP Group. This copies the user part of the index 0 of SIP P-Asserted-Identity header to the user part of index 1 of the same header.

Parameter	Value
Index	**0**
Name	**Build 1 PAI from 2** (arbitrary name)
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**

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

Parameter	Value
Index	**1**
Name	**Remove PAI tel** (arbitrary name)
Manipulation Set ID	**1**
Action Subject	**Header.P-Asserted-Identity.0**
Action Type	**Remove**

30. 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** (arbitrary name)
Manipulation Set ID	**1**
Condition	**Header.Privacy exists And Header.From.URL !contains 'anonymous'**

Parameter	Value
Action Subject	**Header.Privacy**
Action Type	**Remove**

31. Configure another manipulation rule (Manipulation Set 4) for htp Business FleX SIP-Trunk Smart. This rule applies to messages sent to the htp Business FleX SIP-Trunk Smart IP Group in a call transfer scenario. This replaces the host part of the SIP Referred-By header with the value from the SIP From header.

Parameter	Value
Index	**3**
Name	**Change Host of Referred-By**
Manipulation Set ID	**4**
Message Type	**Invite**
Condition	**Header.Referred-By exists**
Action Subject	**Header.Referred-By.URL.Host**
Action Type	**Modify**
Action Value	**Header.From.URL.Host**

The table 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 htp Business FleX SIP-Trunk Smart IP Group as well as the Teams Direct Routing IP Group. These rules are specifically required to enable proper interworking between htp Business FleX SIP-Trunk Smart 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 copies the user part of the index 0 of SIP P-Asserted-Identity header to the user part of index 1 of the same header.	If Teams is configured to send a P-Asserted-Identity header: It sends it in a format where the first index is presented as SIP TEL URI (tel:) and the second as SIP URI (sip:), when the DID presented in the TEL URI. Most SIP Trunks don't support TEL URI and prefer to receive DID as user part in SIP URI. This change is achieved by these two manipulations.
1	This rule applies to messages received from the Teams IP Group. This removes the SIP P-Asserted-Identity header.	
2	This removes the SIP Privacy header in all messages, except for call with presentation restriction.	
3	This rule applies to messages sent to the htp Business FleX SIP Trunk IP Group in a call transfer scenario. This replaces the host part of the SIP Referred-By header with the value from the SIP From header.	Mainly required for topology hiding.

32. Assign Manipulation Set IDs 1 to the Teams Direct Routing IP Group:

    Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).

    n. Select the row of the Teams Direct Routing IP Group, and then click **Edit**.

    o. Set the 'Inbound Message Manipulation Set' field to **1**.

    p. Click **Apply**.

33. Assign Manipulation Set ID 4 to the htp Business FleX SIP-Trunk Smart IP Group:

    Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).

    q. Select the row of the htp Business FleX SIP-Trunk Smart IP Group, and then click **Edit**.

    r. Set the 'Outbound Message Manipulation Set' field to **4**.

    s. Click **Apply**.

4.17 Configuring Registration Accounts

This section describes how to configure SIP registration accounts. This is required so that the SBC can register with the htp Business FleX SIP-Trunk Smart on behalf of Teams Direct Routing. The htp Business FleX SIP-Trunk Smart 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 htp Business FleX SIP-Trunk Smart IP Group.

To configure a registration account:

Open the Accounts table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**).

34. Click **New**.

35. Configure the account according to the provided information from , for example:

Parameter	Value
Served IP Group	**Teams**
Application Type	**SBC**
Serving IP Group	**htp**
Host Name	**siptrunk.htp.net**
Register	**Regular**
Contact User	As provided by the htp SIP Trunk
Username	As provided by the htp SIP Trunk
Password	As provided by the htp SIP Trunk

36. Click **Apply**.

4.18 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

4.18.1 Configuring 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:

Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).

37. From the 'SBC Forking Handling Mode' drop-down list, select **Sequential**.
38. Click **Apply**.

4.18.2 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:

Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).

39. From the 'SBC Performance Profile' drop-down list, select the required profile:

SBC Performance Profile • Optimized for transcoding ▼

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

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
200 Cottontail Lane
Suite A101E
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com

Document #: LTRT-90585