

Connecting AudioCodes' SBC to Microsoft® Teams Direct Routing Enterprise Model

Version 7.2



Microsoft Teams

Microsoft Partner

Gold Communications



Table of Contents

1	Introduction	9
1.1	About Microsoft Teams Direct Routing	9
1.2	Validated AudioCodes Version	9
1.3	About AudioCodes SBC Product Series	9
1.4	Infrastructure Prerequisites	10
2	Configuring AudioCodes' SBC	11
2.1	Prerequisites	12
2.1.1	About the SBC Domain Name	13
2.2	Validate AudioCodes' License	14
2.3	Configure LAN and WAN IP Interfaces	15
2.3.1	Validate Configuration of Physical Ports and Ethernet Groups	16
2.3.2	Configure LAN and WAN VLANs	17
2.3.3	Configure Network Interfaces	17
2.4	Configure TLS Context	19
2.4.1	Generate a CSR and Obtain the Certificate from a Supported CA	21
2.4.2	Deploy the SBC and Root / Intermediate Certificates on the SBC	23
2.5	Alternative Method of Generating and Installing the Certificate	25
2.6	Deploy Baltimore Trusted Root Certificate	25
2.7	Configure Media Realm	26
2.8	Configure a SIP Signaling Interface	28
2.9	Configure Proxy Set and Proxy Address	30
2.10	Configure a Coder Group	31
2.11	Configure an IP Profile	32
2.12	Configure an IP Group	34
2.13	Configure SRTP	36
2.14	Configuring Message Condition Rules	37
2.15	Configuring Classification Rules	38
2.16	Configure IP-to-IP Call Routing Rules	39
2.17	Configuring an SBC to Suppress Call Line ID	45
3	Verify the Pairing Between the SBC and Direct Routing	47
4	Make a Test Call	49
A	Syntax Requirements for SIP Messages 'INVITE' and 'OPTIONS'	51
A.1	Terminology	51
A.2	Syntax Requirements for 'INVITE' Messages	51
A.3	Requirements for 'OPTIONS' Messages Syntax	52
A.4	Connectivity Interface Characteristics	53
B	SIP Proxy Direct Routing Requirements	55
B.1	Failover Mechanism	55

List of Figures

Figure 2-1: Connection Topology with SIP Trunk on the LAN	11
Figure 2-2: Example of Registered DNS Names.....	13
Figure 2-3: Network Interfaces in the Topology with SIP Trunk on the LAN.....	15
Figure 2-4: Network Interfaces in the Topology with SIP Trunk on the WAN	15
Figure 2-5: Physical Ports Configuration Interface.....	16
Figure 2-6: Ethernet Groups Configuration Interface	16
Figure 2-7: Configured VLAN IDs in Ethernet Device	17
Figure 2-8: Configured Network Interfaces in IP Interfaces Table	18
Figure 2-9: Configuration of TLS Context for Direct Routing	20
Figure 2-10: Configured TLS Context for Direct Routing and Interface to Manage the Certificates.....	20
Figure 2-11: Example of Certificate Signing Request – Creating CSR.....	22
Figure 2-12: Uploading the Certificate Obtained from the Certification Authority	23
Figure 2-13: Message Indicating Successful Upload of the Certificate.....	23
Figure 2-14: Certificate Information Example.....	24
Figure 2-15: Example of Configured Trusted Root Certificates	24
Figure 2-16: Configuring Media Realm for LAN	26
Figure 2-17: Configuring Media Realm for WAN.....	27
Figure 2-18: Configured Media Realms in Media Realm Table	27
Figure 2-19: Configured SIP Interface.....	29
Figure 2-20: Configuring Proxy Set for Microsoft Teams Direct Routing	30
Figure 2-21: Configuring Proxy Address for Microsoft Teams Direct Routing Interface	31
Figure 2-22: Configured Coder Group.....	32
Figure 2-23: Configured IP Group for Teams.....	35
Figure 2-24: Configuring SRTP	36
Figure 2-25: Configuring Condition Table	37
Figure 2-26: Configuring Classification Rule.....	38
Figure 2-27: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS	40
Figure 2-28: Configuring IP-to-IP Routing Rule for REFER from Teams.....	41
Figure 2-29: Configuring IP-to-IP Routing Rule for Teams to SIP Trunk	42
Figure 2-30: Configuring IP-to-IP Routing Rule for SIP Trunk to Teams	43
Figure 2-31: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table.....	44
Figure 2-32: Privacy Restriction Mode	45
Figure 2-33: P-Asserted-Identity Header Mode.....	45
Figure 3-1: Proxy Set Status	47
Figure A-1: Example of an 'INVITE' Message	51
Figure A-2: Example of 'OPTIONS' message	52

List of Tables

Table 1-1: Infrastructure Prerequisites	10
Table 2-1: DNS Names Registered by an Administrator for a Tenant	13
Table 2-2: New TLS Context	19
Table 2-3: Configuration Example: SIP Interface	28
Table 2-4: Configuration Example: Proxy Set for Teams	30
Table 2-5: Configuration Example: Teams IP Profile	33
Table 2-6: Configuration Example: SIP Trunk IP Profile	33
Table 2-7: Configuration Example: IP Group for Teams	34
Table A-1: Syntax Requirements for an 'INVITE' Message	52
Table A-2: Teams Direct Routing Interface - Technical Characteristics	53

This page is intentionally left blank.

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: May-07-2019

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at <https://www.audiocodes.com/services-support/maintenance-and-support>.

Stay in the Loop with AudioCodes



Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Related Documentation

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

Document Revision Record

LTRT	Description
12770	Initial document release for Version 7.2. Teams Enterprise Model.
12771	Baltimore certificate import requirement: pem/pfx format
12772	Corrected the .pem certificate path
12773	MSFT and customer feedback
12774	Fixes from customer feedback
12775	Fixes from customer feedback. Title change: Enterprise Model
12776	Fixes
12777	Configuration Example: IP Profile; new IP-to-IP routing rules; Configuration Example: Refer Terminate; removed figure 'Configured IP-to-IP Routing'. Appendix B.
12778	Fixes
12779	SIP I/F parameter deleted. IP Profile modified description. Message Manipulations. OPTIONS Terminate.
12785	From Firmware Version 7.20A.204.015 and later: The new 'Proxy Keep-Alive using IP Group settings' parameter was added in the IP Group Table. Due to this, Message Manipulation Set for OPTIONS was removed.
12786	Updates to the Proxy Sets configuration
12787	Fix mismatch in the Proxy Sets configuration

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 connect AudioCodes' SBC to Microsoft Teams Direct Routing. The document is intended for IT or telephony professionals.



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

1.1 About Microsoft Teams Direct Routing

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

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

1.2 Validated AudioCodes Version

Microsoft has successfully conducted validation tests with AudioCodes' Mediant SBC Ver. 7.20A.204.222. Previous firmware versions may run successfully; however, Microsoft did not test such versions. Note the following:

- Validate that you have the correct License key. Refer to AudioCodes' device's *User's Manual* for more information on how to view the device's License Key including licensed features and capacity. If you don't have the correct License key, contact your AudioCodes representative to obtain one.
- The main AudioCodes licenses required by the SBC are as follows:
 - SW/TEAMS
 - Number of SBC sessions *[Based on requirements]*
 - Transcoding sessions *[If media transcoding is needed]*

1.3 About AudioCodes SBC Product Series

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

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

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

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

1.4 Infrastructure Prerequisites

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

Table 1-1: Infrastructure Prerequisites

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

2 Configuring AudioCodes' SBC

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

The figures below show examples of the connection topology. Multiple connection entities are shown in the figure:

- Third-party IP-PBX, analog devices and the administrator's management station, located on the LAN
- Microsoft Teams Phone Systems Direct Routing Interface on the WAN
- SIP trunk from a third-party provider, which can be located on the LAN or on the WAN

This guide covers how to configure the connection between AudioCodes' SBC and the Microsoft Phone Systems Direct Routing Interface. The interconnection of other entities, such as the connection of the SIP trunk, third-party IP-PBX and/or analog devices, is outside the scope of this guide. Information about how to configure connections like these is available in other guides produced by AudioCodes.

Figure 2-1: Connection Topology with SIP Trunk on the LAN

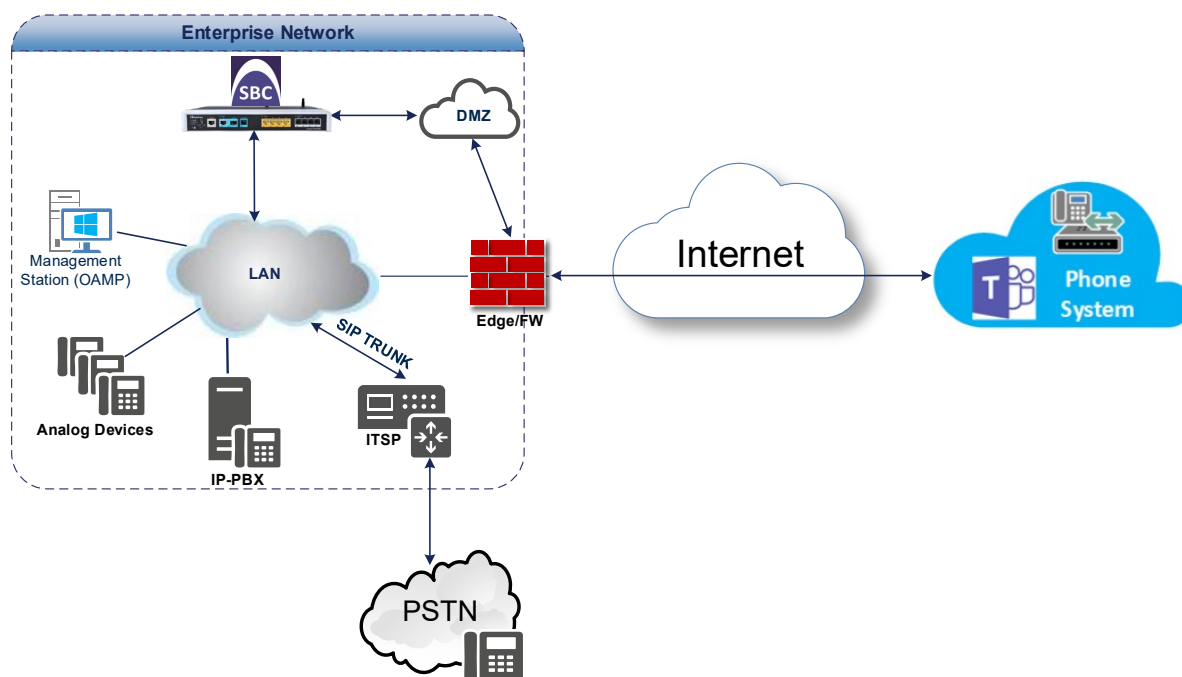
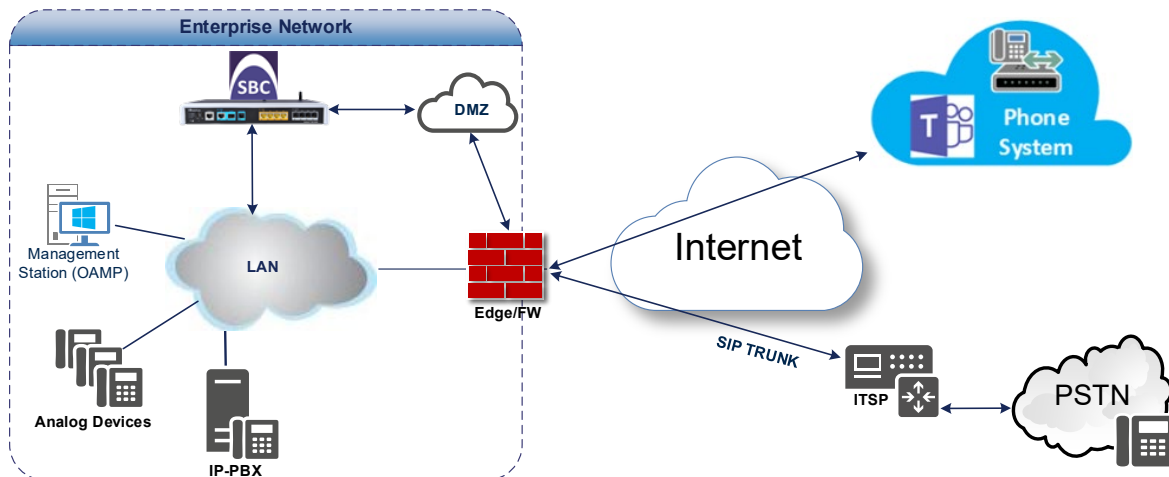


Figure 2-2: Connection Topology with SIP Trunk on the WAN



Note: This document shows how to configure the Microsoft Teams side. To configure other entities in the deployment such as the SIP Trunk Provider and the local IP-PBX, see *AudioCodes' SIP Trunk Configuration Notes* (in the interoperability suite of documents).

2.1 Prerequisites

Before you begin the 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 (see Table A-3 for more details about supported Certification Authorities).

2.1.1 About the SBC Domain Name

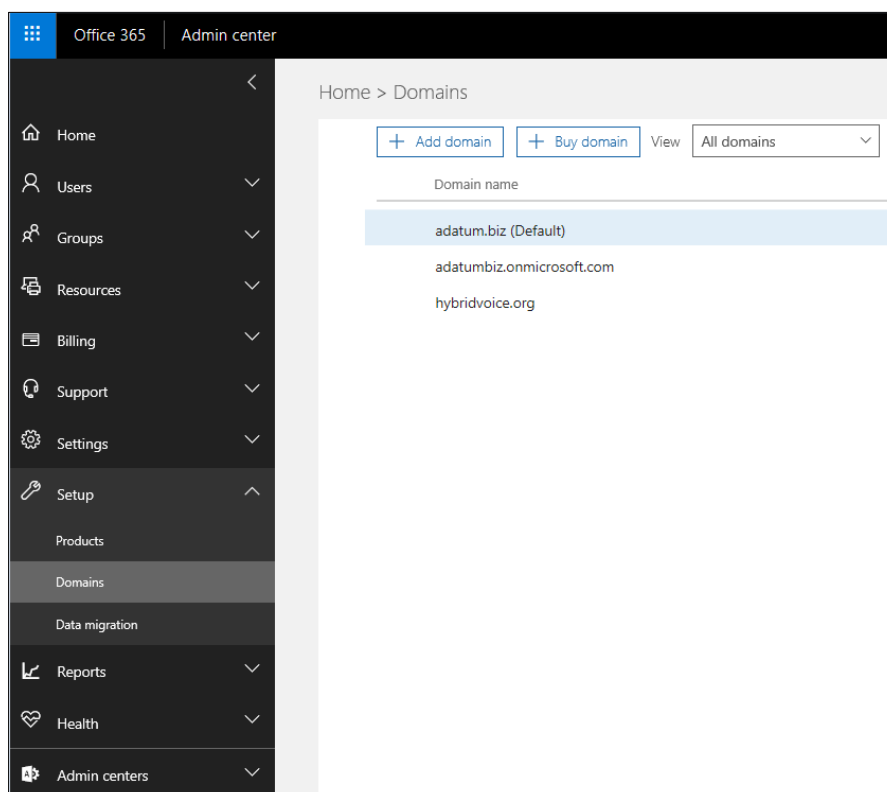
The SBC domain name must be from one of the names registered in 'Domains' of the tenant. You cannot use the ***.onmicrosoft.com** tenant for the domain name. For example, in Figure 2-2, the administrator registered the following DNS names for the tenant:

Table 2-1: 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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 **sbc1.hybridvoice.org** so long as both names are registered for this tenant.

Figure 2-2: Example of Registered DNS Names



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

Public IP	FQDN Name
96.66.240.132	sbc.ACeducation.info

The certificate in the example is from DigiCert. Figure 2-2 shows the high-level configuration flow. Detailed steps are covered later in the document.

2.2 Validate AudioCodes' License

The following licenses are required on AudioCodes' device:

1. **Enable Microsoft** (licensing MSFT) [All AudioCodes media gateways and SBCs are by default shipped with this license. Exceptions: MSBR products and Mediant 500 SBC or Media Gateways].
2. **Enable TEAMS** (licensing SW/TEAMS) [The feature is required in order to support Teams. All AudioCodes media gateways and SBCs are require the license. Current version will not present the TEAMS License Key, this will be supported on the next version].
3. **Number of SBC sessions** [based on requirements].
4. **Transcoding sessions** [If media transcoding is needed].

2.3 Configure LAN and WAN IP Interfaces

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

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

Figure 2-3: Network Interfaces in the Topology with SIP Trunk on the LAN

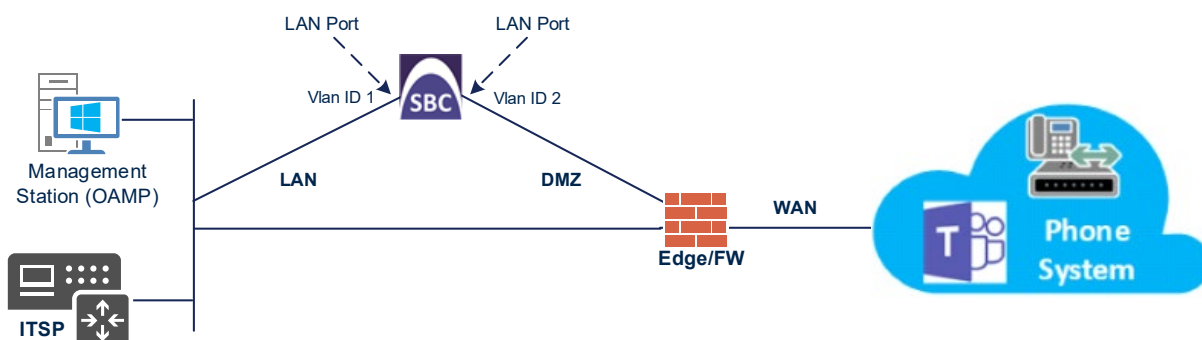
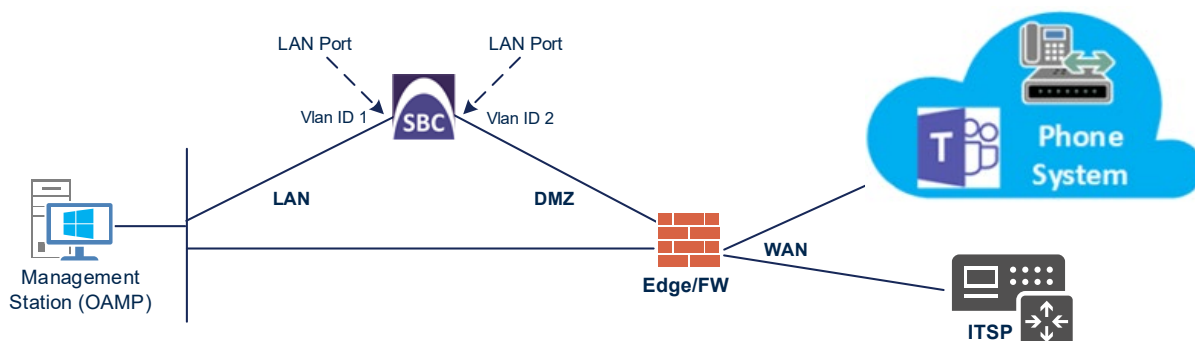


Figure 2-4: Network Interfaces in the Topology with SIP Trunk on the WAN



2.3.1 Validate Configuration of Physical Ports and Ethernet Groups

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

➤ To validate physical ports:

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



Note: Based on your configuration, you might have more than two ports.

Figure 2-5: Physical Ports Configuration Interface

The screenshot shows the 'Physical Ports' configuration page. The left sidebar lists 'CORE ENTITIES' with 'Physical Ports (4)' selected. The main area displays a table of 4 physical ports. The table has columns: INDEX, NAME, MODE, SPEED AND DUPLEX, DESCRIPTION, MEMBER OF ETHERNET GROUP, and GROUP STATUS. The data shows two active ports (GE_4_1 and GE_4_2) and two redundant ports (GE_4_3 and GE_4_4).

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

➤ To validate Ethernet Groups:

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

Figure 2-6: Ethernet Groups Configuration Interface

The screenshot shows the 'Ethernet Groups' configuration page. The left sidebar lists 'CORE ENTITIES' with 'Ethernet Groups (4)' selected. The main area displays a table of 4 Ethernet groups. The table has columns: INDEX, NAME, MODE, MEMBER 1, and MEMBER 2. The data shows two groups with members (GROUP_1 and GROUP_2) and two groups without members (GROUP_3 and GROUP_4).

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

2.3.2 Configure LAN and WAN VLANs

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

- LAN VoIP (assigned the name "LAN_IF")
- WAN VoIP (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 as follows:

Parameter	Value
Index	1
VLAN ID	2
Underlying Interface	GROUP_2 (Ethernet port group)
Name	vlan 2
Tagging	Untagged

Figure 2-7: Configured VLAN IDs in Ethernet Device

Ethernet Devices (2)				
<div> + New Edit 🗑️ </div> <div> Page 1 of 1 Show 10 records per page </div>				
INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING
0	1	GROUP_1	vlan 1	Untagged
1	2	GROUP_2	vlan 2	Untagged

2.3.3 Configure Network Interfaces

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

- LAN VoIP (assigned the name "LAN_IF")
- WAN VoIP (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. Modify the existing LAN network interface:
 - a. Select the 'Index' radio button of the **OAMP + Media + Control** table row, and then click **Edit**.
 - b. Configure the interface as follows:

Parameter	Value
Name	LAN_IF (arbitrary descriptive name)
Application Type	OAMP + Media + Control (This interface points to the internal network where the network administrator's station is located; so enabling OAMP is necessary)
Ethernet Device	vlan 1
IP Address	10.15.17.77 (LAN IP address of SBC)
Prefix Length	16 (subnet mask in bits for 255.255.0.0)
Default Gateway	10.15.0.1
Primary DNS	10.15.27.1

3. Add a network interface for the WAN side:

- a. Click **New**.
- b. Configure the interface as follows:

Parameter	Value
Name	WAN_IF
Application Type	Media + Control (as this interface points to the internet, enabling OAMP is not recommended)
Ethernet Device	vlan 2
IP Address	195.189.192.157 (DMZ IP address of SBC)
Prefix Length	25 (subnet mask in bits for 255.255.255.128)
Default Gateway	195.189.192.129 (router's IP address)
Primary DNS	According to your internet provider's instructions
Secondary DNS	According to your internet provider's instructions

4. Click **Apply**.

The configured IP network interfaces are shown below:

Figure 2-8: Configured Network Interfaces in IP Interfaces Table

IP Interfaces (2)									
+ New Edit				Page 1 of 1		Show 10 records per page			
INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	LAN_IF	OAMP + Media +	IPv4 Manual	10.15.17.77	16	10.15.0.1	10.15.27.1	0.0.0.0	vlan 1
1	WAN_IF	Media + Control	IPv4 Manual	195.189.192.157	25	195.189.192.129	80.179.52.100	80.179.55.100	vlan 2

2.4 Configure TLS Context

The Microsoft Phone System Direct Routing Interface only allows 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>

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

The procedure involves the following main steps:

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

➤ **To create a TLS Context for Microsoft Phone System Direct Routing:**

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

Table 2-2: New TLS Context

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



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

Figure 2-9: Configuration of TLS Context for Direct Routing

TLS Contexts [Teams]

GENERAL

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

OCSP

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

Cancel APPLY

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

Figure 2-10: Configured TLS Context for Direct Routing and Interface to Manage the Certificates

audiocodes

SETUP

MONITOR

TROUBLESHOOT

MEDIANET VE-H SBC

IP NETWORK

SIGNALING & MEDIA

ADMINISTRATION

Save

Reset

Actions

Admin

SRD All

NETWORK VIEW

CORE ENTITIES

SECURITY

TLS Contexts (2)

Firewall (1)

Security Settings

QUALITY

DNS

WEB SERVICES

HTTP PROXY

RADIUS & LDAP

MEDIA CLUSTER

ADVANCED

TLS Contexts (2)

+ New

Edit

Page 1 of 1

Show 10 records per page

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

#1[Teams]

GENERAL

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

OCSP

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

Certificate Information >>

Change Certificate >>

Trusted Root Certificates >>

2.4.1 Generate a CSR and Obtain the Certificate from a Supported CA

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

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

1. In the TLS Contexts page, select the Teams TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
2. 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, **ACeducation.info**).
 - b. In the '1st Subject Alternative Name [SAN]' field, enter the SBC FQDN name (based on example above, **ACeducation.info**).



Note: The domain portion of the CN must match the SIP suffix configured for Office 365 users.

- a. Change the 'Private Key Size' based on the requirements of your Certification Authority. Many CAs do not support private key of size **1024**. In this case, you must change the key size to **2048**.
- b. To change the key size on TLS Context, go to: **Generate New Private Key and Self-Signed Certificate**, change the 'Private Key Size' to **2048** and then click **Generate Private-Key**. To use **1024** as a Private Key Size value, you can click **Generate Private-Key** without changing the default key size value.
- c. Fill in the rest of the request fields according to your security provider's instructions.
- d. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

TLS Context [#1] > Change Certificates

CERTIFICATE SIGNING REQUEST

Common Name [CN]

1st Subject Alternative Name [SAN]

2nd Subject Alternative Name [SAN]

3rd Subject Alternative Name [SAN]

4th Subject Alternative Name [SAN]

5th Subject Alternative Name [SAN]

Organizational Unit [OU] (optional)

Company name [O] (optional)

Locality or city name [L] (optional)

State [ST] (optional)

Country code [C] (optional)

Signature Algorithm

AEducation.info

EMAIL ▼ AEducation.info

EMAIL ▼

EMAIL ▼

EMAIL ▼

EMAIL ▼

Ad

SHA-256 ▼

Create CSR

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIICmzCCAYMAQAwKDE2MBcGA1UEAwQUNlZHVjYXRpb24uYW5mb2ZELMAkGA1UE
BhMCQWQwggEiMA0GCsgqSB3DQEBAAQAAIIBDwAwggEKAoIBAQCdOMIA99/vHHoX
2/6s4agonEHXNBpK1HkQr5f9g90j1SzmVBO3wZ+fo4Yntg7HwJ5YdmJ5Wmkf64CI
NcZ1gW57yfuamIucQj1g1vdSeKouYHBU5pcg3yK0ShAdRY0xkxmxPgPTt1m1sw
B5w5v7AIE3sZKETIy204VKPVtKS5Nlr/c6L8Nr3jocdkur18Kky1tdnEspNwE3
6Y15v+xE/LHxN37/dkaBQhLdden01GcZkeTQBPoLnTFNEzqcFVZ4NZuC/SovJXE
M5CxrQXY7sncMuZ8Wg7zVamZvF3ugSudnTymzvA/1iRwOf5dNqu25ftLP7kAqfH1
wKcJ35g9AgMBAAGLjAsBgqhkiG9w0BQC4xH+AdMBsGA1UdEQQUMBKBEEDZWR1
Y2F0aw9uLm1uZm8wDQYJKoZIhvcNAQELBQADggEBAAtkoGHSVn1ooCXghQWizXg1
dquy71unbivncgUhrzLCB9JAixX0ghqKjw0KQPrUahcs2iAC1VQywmf6CsNU7BZ
QWxtIbpEWjTSQHHT8bya8mVzLKI2/06CyySt39t+bK9I20wHY0211Mpf/Yndwq9
6k07mt7532ZHp/71oucRf40S0uIySh/VhHba8mh1GU09EKWfIvxp+kagHRdfrf3
6zCK81abPM9c2uRbCxtS2NO/qduCwdVwLAgcL/fj775HYy5CaNow5FWCXR196DjW
Bm5Qkx701VfQm8NS5jeJLCS44eJESKD619xdpd/j0Rv95TX1TRJjYEmyKE+JoQ=
-----END CERTIFICATE REQUEST-----
```

GENERATE NEW PRIVATE KEY AND SELF-SIGNED CERTIFICATE

Private Key Size

Private key pass-phrase (optional)

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

2048 ▼

Generate Private-Key

Generate Self-Signed Certificate

3. Copy the CSR from the line **"---BEGIN 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*.
4. Send *certreq.txt* file to the Certified Authority Administrator for signing.

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

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

- SBC certificate
- Root / Intermediate certificates

➤ **To install the SBC certificate:**

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

Figure 2-12: Uploading the Certificate Obtained from the Certification Authority

UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase (optional)

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

No file chosen

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

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

No file chosen ←

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

Figure 2-13: Message Indicating Successful Upload of the Certificate

UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase (optional)

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

No file chosen

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

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

No file chosen

File sbc3_adatum_biz.crt was successfully loaded into the device.

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

Figure 2-14: Certificate Information Example

⊕ TLS Context [#2] > Certificate Information

PRIVATE KEY

Key size: 2048 bits

Status: OK

CERTIFICATE

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

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

Figure 2-15: Example of Configured Trusted Root Certificates

⊕ TLS Context [#2] > Trusted Root Certificates

View Import Export Remove

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

6. Reset the SBC by clicking **Save To Flash** for your settings to take effect.

2.5 Alternative Method of Generating and Installing the Certificate

To use the same certificate on multiple devices, you may prefer using [DigiCert Certificate Utility for Windows](#) to process the certificate request from your Certificate Authority on another machine, with this utility installed.

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

➤ **To install the certificate:**

1. Open 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.

2.6 Deploy Baltimore Trusted Root Certificate

The DNS name of the Microsoft Teams Direct Routing interface is **sip.pstnhub.microsoft.com**. In this interface, a certificate is presented which is signed by Baltimore Cyber Baltimore CyberTrust Root with Serial Number: 02 00 00 b9 and SHA fingerprint: d4:de:20:d0:5e:66:fc: 53:fe:1a:50:88:2c:78:db:28:52:ca:e4:74.

To trust this certificate, your SBC *must* have the certificate in Trusted Certificates storage. Download the certificate from <https://cacert.omniroot.com/bc2025.pem> and follow the steps above to import the certificate to the Trusted Root storage.



Note: Before importing the Baltimore root certificate into AudioCodes' SBC, make sure it's in .pem or .pfx format. If it isn't, you need to convert it to .pem or .pfx format else you'll receive the error message 'Failed to load new certificate'. To convert to PEM format, use Windows local store on any Windows OS and then export it as 'Base-64 encoded X.509 (.CER) certificate'.

2.7 Configure Media Realm

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

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

➤ **To configure Media Realms:**

1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Add a Media Realm for the LAN interface. You can use the default Media Realm (Index 0), but modify it as shown below:

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

Figure 2-16: Configuring Media Realm for LAN

Media Realms [MRLan]

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

Cancel APPLY

3. Configure a Media Realm for WAN traffic:

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

Figure 2-17: Configuring Media Realm for WAN

Media Realms [MRWan]

GENERAL

Index: 1

Name: MRWan

Topology Location: Up

IPv4 Interface Name: #1 [WAN_IF]

Port Range Start: 7000

Number Of Media Session Legs: 100

Port Range End: 7999

Default Media Realm: No

QUALITY OF EXPERIENCE

QoE Profile: -- View

Bandwidth Profile: -- View

Cancel APPLY

The configured Media Realms are shown in the figure below:

Figure 2-18: Configured Media Realms in Media Realm Table

Media Realms (2)

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

INDEX	NAME	IPv4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	MRlan	LAN_IF	6000	100	6999	No
1	MRWan	WAN_IF	7000	100	7999	No

2.8 Configure a SIP Signaling Interface

This section shows how to configure a SIP signaling interface pointing to the Direct Routing interface.

Note that the configuration of a SIP Interface for the SIP trunk and/or a third-party IP-PBX is also required but not covered in this guide. For specific configuration of interfaces pointing to SIP trunks and/or a third-party environment connected to the SBC, see the trunk / environment vendor documentation.

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

➤ **To configure a SIP interface:**

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Click **+New** to add a SIP Interface for the WAN interface pointing to the Direct Routing service. The table below shows an example of the configuration. You can change some parameters according to your requirements.



Note: The Direct Routing interface can only use TLS for a SIP port. It does not support using TCP due to security reasons. The SIP port might be any port of your choice. When pairing the SBC with Office 365, the chosen port is specified in the pairing command.

Table 2-3: Configuration Example: SIP Interface

Parameter	Value
Index	1
Name	Teams (arbitrary descriptive name)
Network Interface	WAN_IF
Application Type	SBC
UDP and TCP Port	0 (Microsoft Phone System does not use UDP or TCP for SIP signaling)
TLS Port	5061 (as configured in the Office 365)
Enable TCP Keepalive	Enable
Classification Failure Response Type	0 (Recommended to prevent DoS attacks)
Media Realm	MRWan

3. Click **Apply**.



Notes:

- All other parameters can be left unchanged at their default values.
- Remember to configure SIP Interfaces for the SIP trunks and other equipment you may have.

Figure 2-19: Configured SIP Interface

#1[Teams]
[DefaultSRD]
Edit

GENERAL	
Name	Teams
Topology Location	Up
Network Interface	# [WAN_IF] View
Application Type	SBC
UDP Port	0
TCP Port	0
TLS Port	5061
Additional UDP Ports	
Encapsulating Protocol	No encapsulation
Enable TCP Keepalive	Enable
Used By Routing Server	Not Used
Pre-Parsing Manipulati...	# [-] View
CAC Profile	# [-] View

MEDIA	
Media Realm	# [MRWan] View
Direct Media	Disable

SECURITY	
TLS Context Name	# [default] View
TLS Mutual Authentica...	Disable
Message Policy	# [-] View
User Security Mode	Not Configured
Enable Un-Authenticat...	Not configured
Max. Number of Regis...	-1

CLASSIFICATION	
Classification Failure R...	0
Pre-classification Mani...	-1

2.9 Configure Proxy Set and Proxy Address

The Proxy Set and Proxy Address defines TLS parameters, IP Interfaces, FQDN and the remote entity's port. The example below covers configuration of a Proxy Set for Microsoft Direct Routing. Note that configuration of a Proxy Set for the SIP Trunk and/or the third-party IP-PBX is also necessary; however, is not covered in this guide. For specific configuration of interfaces pointing to SIP trunks and/or the third-party environment connected to the SBC, refer to the specific trunk/environment vendor's documentation. AudioCodes also offers a comprehensive suite of documents covering the interconnection between different trunk vendors and their equipment.

➤ To configure a Proxy Set:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Click **+New** to add the Proxy Set for the Direct Routing Service. The table below shows an example of the configuration. You can change parameters according to requirements.

Table 2-4: Configuration Example: Proxy Set for Teams

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

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

Figure 2-20: Configuring Proxy Set for Microsoft Teams Direct Routing

Proxy Sets [Teams]

SRD #0 [DefaultSRD]

GENERAL

Index: 1

Name: Teams

Gateway IPv4 SIP Interface: -- [View](#)

SBC IPv4 SIP Interface: #1 [Teams] [View](#)

TLS Context Name: #1 [Teams] [View](#)

KEEP ALIVE

Proxy Keep-Alive: Using OPTIONS

Proxy Keep-Alive Time [sec]: 60

Keep-Alive Failure Responses:

REDUNDANCY

Redundancy Mode:

Proxy Hot Swap: Enable

Proxy Load Balancing Method: Random Weights

Min. Active Servers for Load Balancing: 1

ADVANCED

Classification Input: IP Address only

DNS Resolve Method:

Cancel **APPLY**

3. Click **Apply**.

4. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
5. Click **New**; the following dialog box appears:

Figure 2-21: Configuring Proxy Address for Microsoft Teams Direct Routing Interface

The screenshot shows a 'Proxy Address' configuration window. It contains a 'GENERAL' tab with the following fields:

- Index:** 0
- Proxy Address:** sip.pstnhub.microsoft.com:5061
- Transport Type:** TLS
- Proxy Priority:** 1
- Proxy Random Weight:** 1

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

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

7. Click **Apply**.

2.10 Configure a Coder Group

The coder group defines which codecs to use during calls. The coder group is assigned to IP Profiles (see the next step).

➤ To configure a Coder Group:

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

Figure 2-22: Configured Coder Group

Coder Groups

Coder Group Name 1 : AudioCodersGroups_1 ▼ Delete Group

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

- Click **Apply**.

2.11 Configure an IP Profile

An IP Profile is a set of parameters with user-defined settings related to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder type).

An IP Profile can later be assigned to specific IP calls (inbound and/or outbound).

➤ To configure an IP Profile:

- Open the Proxy Sets table (**Setup > Signaling and Media > Coders and Profiles > IP Profiles**).
- Click **+New** to add the IP Profile for the Direct Routing interface. Configure the parameters using the table below as reference.

Table 2-5: Configuration Example: Teams IP Profile

Parameter	Value
General	
Name	Teams (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	SRTP
SBC Early Media	
Remote Early Media RTP Detection Mode	By Media (required, as Microsoft Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18x response)
SBC Media	
Extension Coders Group	AudioCodersGroups_1
ICE Mode	Lite (required only when Media Bypass enabled on Microsoft Teams)
SBC Signaling	
Remote Update Support	Not Supported
Remote re-INVITE Support	Supported Only With SDP
Remote Delayed Offer Support	Not Supported
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally
Remote 3xx Mode	Handle Locally
SBC Hold	
Remote Hold Format	Inactive (some SIP Trunk may answer with a=inactive and IP=0.0.0.0 in response to the Re-Invite with Hold request from Teams. Microsoft Media Stack doesn't support this format. So, SBC will replace 0.0.0.0 with its IP address)

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

3. Click **Apply**.

Table 2-6: Configuration Example: SIP Trunk IP Profile

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

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

2.12 Configure an IP Group

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

➤ **To configure an IP Group:**

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Click **+New** to add an IP Group for the Direct Routing interface. Configure the parameters using the table below as reference.

Table 2-7: Configuration Example: IP Group for Teams

Parameter	Value
Name	Teams
Topology Location	Up
Type	Server
Proxy Set	Teams
IP Profile	Teams
Media Realm	MRWan
Classify By Proxy Set	Disable
Local Host Name	<FQDN name of your tenant in the SBC> (For example, sbc1.customers.ACeducation.info defines the host name (string) that the device uses in the SIP message's Via and Contact headers. This is typically used to define an FQDN as the host name. The device uses this string for Via and Contact headers in outgoing INVITE messages sent to a specific IP Group, and the Contact header in SIP 18x and 200 OK responses for incoming INVITE messages received from a specific IP Group. More information about the requirements for the various parts of SIP messages can be found at Requirements for Invite and OPTIONS messages syntax appendix.)
Always Use Src Address	Yes
Proxy Keep-Alive using IP Group settings	Enable
All other parameters can be left unchanged at their default values.	

Figure 2-23: Configured IP Group for Teams

IP Groups [Teams] — x

SRD #0 [DefaultSRD]

GENERAL		QUALITY OF EXPERIENCE	
Index	<input type="text" value="2"/>	QoE Profile	-- View
Name	▪ <input type="text" value="Teams"/>	Bandwidth Profile	-- View
Topology Location	▪ Up		
Type	Server		
Proxy Set	▪ #2 [Teams] View		
IP Profile	▪ #2 [Teams] View		
Media Realm	▪ #0 [MRWan] View		
Contact User	<input type="text"/>		
SIP Group Name	▪ <input type="text" value="teams-sbc.your.domain.com"/>		
Created By Routing Server	<input type="text" value="No"/>		

MESSAGE MANIPULATION

Inbound Message Manipulation Set	<input type="text" value="-1"/>
Outbound Message Manipulation Set	<input type="text" value="-1"/>
Message Manipulation User-Defined String 1	<input type="text"/>
Message Manipulation User-Defined String 2	<input type="text"/>
Proxy Keep-Alive using IP Group settings	▪ Enable

[Cancel](#) [APPLY](#)

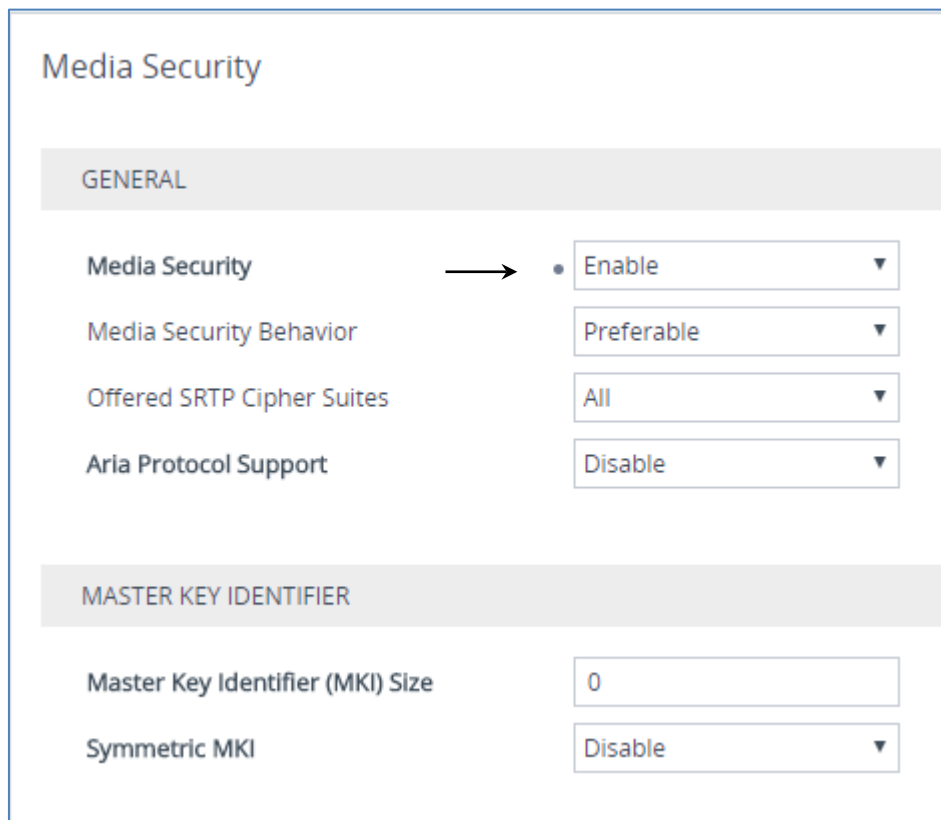
2.13 Configure SRTP

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

➤ **To configure media security:**

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

Figure 2-24: Configuring SRTP



The screenshot shows the 'Media Security' configuration page. It has a title 'Media Security' and two main sections: 'GENERAL' and 'MASTER KEY IDENTIFIER'. In the 'GENERAL' section, there are four settings: 'Media Security' (set to 'Enable'), 'Media Security Behavior' (set to 'Preferable'), 'Offered SRTP Cipher Suites' (set to 'All'), and 'Aria Protocol Support' (set to 'Disable'). An arrow points to the 'Media Security' dropdown menu. The 'MASTER KEY IDENTIFIER' section has two settings: 'Master Key Identifier (MKI) Size' (set to '0') and 'Symmetric MKI' (set to 'Disable').

Media Security	
GENERAL	
Media Security	• Enable ▼
Media Security Behavior	Preferable ▼
Offered SRTP Cipher Suites	All ▼
Aria Protocol Support	Disable ▼
MASTER KEY IDENTIFIER	
Master Key Identifier (MKI) Size	0
Symmetric MKI	Disable ▼

2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.
3. Click **Apply**.

2.14 Configuring Message Condition Rules

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

The following condition verifies that the Contact header contains 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'

Figure 2-25: Configuring Condition Table

The screenshot shows a web interface window titled "Message Conditions [Teams-Contact]". Inside, there is a "GENERAL" tab. Under this tab, there are three configuration fields: "Index" with the value "0", "Name" with the value "Teams-Contact", and "Condition" with the value "header.contact.url.host contains 'pstnhub.micro:". To the right of the condition field is a blue "Editor" button.

3. Click **Apply**.

2.15 Configuring Classification Rules

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

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

➤ **To configure a Classification rule:**

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

Parameter	Value
Index	0
Name	Teams
Source SIP Interface	Teams
Destination Host	sbc.ACeducation.info (example)
Message Condition	Teams-Contact
Action Type	Allow
Source IP Group	Teams

Figure 2-26: Configuring Classification Rule

Classification [Teams]

SRD: #0 [DefaultSRD]

MATCH	ACTION
Index: 0	Action Type: Allow
Name: Teams	Destination Routing Policy: -- View
Source SIP Interface: #2 [Teams] View	IP Group Selection: Source IP Group
Source IP Address:	Source IP Group: #2 [Teams] View
Source Transport Type: Any	IP Group Tag Name: default
Source Port: 0	IP Profile: -- View
Source Username Pattern: *	
Source Host: *	
Destination Username Pattern: *	
Destination Host: sbc.ACeducation.info	
Message Condition: #0 [Teams-Contact] View	

Cancel APPLY

3. Click **Apply**.

2.16 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.

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

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

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

➤ **To configure IP-to-IP routing rules:**

1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure a rule to terminate SIP OPTIONS messages received on the SBC:
 - a. Click **New**, and then configure the parameters as follows:

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

Figure 2-27: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS

The screenshot shows the 'IP-to-IP Routing [Terminate OPTIONS]' configuration window. At the top, the 'Routing Policy' is set to '#0 [Default_SBCRoutingPolicy]'. The window is divided into two main sections: 'GENERAL' and 'ACTION'.

GENERAL Section:

- Index:** 0
- Name:** Terminate OPTIONS
- Alternative Route Options:** Route Row

MATCH Section:

- Source IP Group:** Any
- Request Type:** OPTIONS
- Source Username Pattern:** *
- Source Host:** *
- Source Tag:** (empty)

ACTION Section:

- Destination Type:** Dest Address
- Destination IP Group:** ..
- Destination SIP Interface:** ..
- Destination Address:** internal
- Destination Port:** 0
- Destination Transport Type:** (empty)
- IP Group Set:** ..
- Call Setup Rules Set ID:** -1
- Group Policy:** Sequential
- Cost Group:** ..

At the bottom of the window, there are 'Cancel' and 'APPLY' buttons.

- b. Click **Apply**.

3. Configure a rule to terminate REFER messages to Teams Direct Routing:
 - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	1
Route Name	Refer from Teams (arbitrary descriptive name)
Source IP Group	Any
Call Trigger	REFER
ReRoute IP Group	Teams
Destination Type	Request URI
Destination IP Group	Teams

Figure 2-28: Configuring IP-to-IP Routing Rule for REFER from Teams

The screenshot shows the 'IP-to-IP Routing [Refer from Teams]' configuration window. At the top, the 'Routing Policy' is set to '#0 [Default_SBCRoutingPolicy]'. The window is divided into two main sections: 'GENERAL' and 'ACTION'.

GENERAL Section:

- Index:** 1
- Name:** Refer from Teams
- Alternative Route Options:** Route Row

MATCH Section:

- Source IP Group:** Any
- Request Type:** All
- Source Username Pattern:** *
- Source Host:** *
- Source Tag:** (empty)

ACTION Section:

- Destination Type:** Request URI
- Destination IP Group:** #2 [Teams]
- Destination SIP Interface:** ..
- Destination Address:** (empty)
- Destination Port:** 0
- Destination Transport Type:** (empty)
- IP Group Set:** ..
- Call Setup Rules Set ID:** -1
- Group Policy:** Sequential
- Cost Group:** ..

At the bottom of the window, there are 'Cancel' and 'APPLY' buttons.

- b. Click **Apply**.

4. Configure a rule to route calls from Teams Direct Routing to AudioCodes SBC SIP Trunk:
 - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	2
Route Name	Teams to SIP Trunk (arbitrary descriptive name)
Source IP Group	Teams
Destination Type	IP Group
Destination IP Group	SIPTrunk

Figure 2-29: Configuring IP-to-IP Routing Rule for Teams to SIP Trunk

The screenshot shows the 'IP-to-IP Routing [Teams to SIP Trunk]' configuration window. At the top, the 'Routing Policy' is set to '#0 [Default_SBCRoutingPolicy]'. The window is divided into two main sections: 'GENERAL' and 'ACTION'.

GENERAL Section:

- Index:** 2
- Name:** Teams to SIP Trunk
- Alternative Route Options:** Route Row

MATCH Section:

- Source IP Group:** #2 [Teams] (with a 'View' link)
- Request Type:** All
- Source Username Pattern:** *
- Source Host:** *
- Source Tag:** (empty field)

ACTION Section:

- Destination Type:** IP Group
- Destination IP Group:** #1 [SIPTrunk] (with a 'View' link)
- Destination SIP Interface:** .. (with a 'View' link)
- Destination Address:** (empty field)
- Destination Port:** 0
- Destination Transport Type:** (empty dropdown)
- IP Group Set:** .. (with a 'View' link)
- Call Setup Rules Set ID:** -1
- Group Policy:** Sequential
- Cost Group:** .. (with a 'View' link)

At the bottom of the window, there are 'Cancel' and 'APPLY' buttons.

- b. Click **Apply**.

5. Configure rule to route calls from AudioCodes SBC SIP Trunk to Teams Direct Routing:
 - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	3
Route Name	SIP Trunk to Teams (arbitrary descriptive name)
Source IP Group	SIPTrunk
Destination Type	IP Group
Destination IP Group	Teams

Figure 2-30: Configuring IP-to-IP Routing Rule for SIP Trunk to Teams

The screenshot shows the 'IP-to-IP Routing [SIP Trunk to Teams]' configuration window. At the top, the 'Routing Policy' is set to '#0 [Default_SBCRoutingPolicy]'. The window is divided into two main sections: 'GENERAL' and 'ACTION'.

GENERAL Section:

- Index:** 3
- Name:** SIP Trunk to Teams
- Alternative Route Options:** Route Row

MATCH Section:

- Source IP Group:** #1 [SIPTrunk] (with a 'View' link)
- Request Type:** All
- Source Username Pattern:** *
- Source Host:** *
- Source Tag:** (empty field)

ACTION Section:

- Destination Type:** IP Group
- Destination IP Group:** #2 [Teams] (with a 'View' link)
- Destination SIP Interface:** .. (with a 'View' link)
- Destination Address:** (empty field)
- Destination Port:** 0
- Destination Transport Type:** (empty dropdown)
- IP Group Set:** .. (with a 'View' link)
- Call Setup Rules Set ID:** -1
- Group Policy:** Sequential
- Cost Group:** .. (with a 'View' link)

At the bottom of the window, there are 'Cancel' and 'APPLY' buttons.

- b. Click **Apply**.

The configured routing rules are shown in the figure below:

Figure 2-31: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing (4)

+ New Edit Insert ↑ ↓ | 🗑️ | Page 1 of 1 | Show 10 records per page

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



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

2.17 Configuring an SBC to Suppress Call Line ID

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

- Suppressing all IDs
- Suppressing only the Forward P-Asserted-Identity header and allowing the From header

➤ **To override the Privacy:**

- Use Outbound Manipulations: Set their 'Privacy Restriction Mode' to **Remove Restriction**; the P-Asserted-Identity header will remain and no privacy will apply.

Figure 2-32: Privacy Restriction Mode

The screenshot shows a configuration page titled 'ACTION'. It contains several input fields and dropdown menus. The 'Privacy Restriction Mode' dropdown menu is highlighted with a yellow background and a green border. The other fields are: 'Manipulated Item' (Source URI), 'Remove From Left' (0), 'Remove From Right' (0), 'Leave From Right' (255), 'Prefix to Add' (empty), and 'Suffix to Add' (empty).

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

➤ **To suppress the Forward P-Asserted-Identity header if required by the customer:**

- (In addition to the previous step above) Use Teams' IP Profile to set the 'P-Asserted-Identity Header Mode' to **Remove**:

Figure 2-33: P-Asserted-Identity Header Mode

The screenshot shows a configuration page titled 'SBC SIGNALING'. It contains two dropdown menus. The 'P-Asserted-Identity Header Mode' dropdown menu is highlighted with a yellow background and a green border. The other field is: 'PRACK Mode' (Transparent).

SBC SIGNALING	
PRACK Mode	Transparent
P-Asserted-Identity Header Mode	Remove

This page is intentionally left blank.

3 Verify the Pairing Between the SBC and Direct Routing

After you have paired the SBC with Direct Routing using the *New-CsOnlinePSTNGateway* PowerShell command, validate that the SBC can successfully exchange OPTIONS with Direct Routing.

➤ To validate the pairing using SIP OPTIONS:

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

Figure 3-1: Proxy Set Status

Proxy Sets Status

This page refreshes every 60 seconds

PROXY SET ID	MODE	KEEP ALIVE	ADDRESS	PRIORITY	WEIGHT	SUCCESS COUNT	FAILURE COUNT	STATUS
0	Load Balancing	Enabled	192.168.1.125:5067(*)	-	-	3250	5	ONLINE
1	Parking	Disabled	206.80.250.100(*)	-	-	0	0	ONLINE
2	Parking	Enabled	adatum.pstn.bellio.com(54.172.60.28*)	-	-	1	1	ONLINE
			adatum.pstn.bellio.com(54.172.60.38*)	-	-	0	0	ONLINE
			adatum.pstn.bellio.com(54.172.60.18*)	-	-	0	0	ONLINE
			adatum.pstn.bellio.com(54.172.60.08*)	-	-	0	0	ONLINE
3	Parking	Enabled	teams.local(52.114.76.5061*)	1	1.00	40	2	ONLINE
			teams.local(52.114.132.46.5061*)	2	1.00	41	0	ONLINE
			teams.local(52.114.7.24.5061*)	3	0.00	41	1	ONLINE

This page is intentionally left blank.

4 Make a Test Call

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

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

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

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

➤ **To configure the Test Agent:**

- Open the Test Call Rules table (**Troubleshooting** menu > **Troubleshooting** tab > **Test Call** > **Test Call Rules**).

➤ **To start, stop and restart a test call:**

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

This page is intentionally left blank.

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

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

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

A.1 Terminology

Recommended	Not required, but to simplify troubleshooting it's recommended to configure as shown in the examples below.
Must	Strictly required. The deployment does not function correctly without the correct configuration of these parameters.

A.2 Syntax Requirements for 'INVITE' Messages

Figure A-1: Example of an 'INVITE' Message

```
INVITE sip:+97239764550@sbc.ACeducation.info;user=phone SIP/2.0
Via: SIP/2.0/TLS sbc.aceducation.info:5068;alias;branch=z9hG4bKac1922410385
Max-Forwards: 69
From: "Tal Shl" <sip:+97239764270@sbc.ACeducation.info;user=phone>;tag=1c133776823;epid=C418C3BA39
To: <sip:+97239764550@sbc.ACeducation.info;user=phone>
Call-ID: 5608046482692017151418@sbc.ACeducation.info
CSeq: 1 INVITE
Contact: <sip:sbc.ACeducation.info:5068;transport=tls;ms-opaque=253de93336fd81f9>
Supported: 100rel,sdp-anat
ALLOW: ACK
Allow: CANCEL,BYE,INVITE,PRACK,UPDATE
```

■ Request-URI

- **Recommended:** Configure the SBC FQDN in the URI hostname when sending calls to the Direct Routing interface
- **Syntax:** INVITE sip: <phone number>@<FQDN of the SBC> SIP/2.0

■ Contact header

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

- **To header**
 - **Recommended:** When placing calls to the Direct Routing interface, the 'To' header can have the SBC FQDN in the URI hostname
 - **Syntax:** *To: INVITE sip: <phone number>@<FQDN of the SBC>*

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

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

Parameter	Where Configured	How to Configure
Request-URI	Setup > Signaling and Media > Core Entities > IP Group> <Group Name> > SIP Group Name	See AudioCodes' <i>SIP Message Manipulation Reference Guide</i> .
To	Signaling and Media > Message Manipulations > Manipulation Set Note that the Manipulation Set must be applied to the Teams IP Group as an Outbound Message Manipulation Set.	See AudioCodes' <i>SIP Message Manipulation Reference Guide</i> .
Contact	Setup > Signaling and Media > Core Entities > IP Group> <Group Name> > Local Host Name In IP Groups, 'Contact' must also be configured. In this field, define the local host name of the SBC as a string, for example, sbc.ACeducation.info. The name changes the host name in the call received from the IP group. For outbound calls, configure 'Local Host Name' in the IP Group setting.	See Section 2.12.

A.3 Requirements for 'OPTIONS' Messages Syntax

Figure A-2: Example of 'OPTIONS' message

```

OPTIONS sip:sbc.ACeducation.info SIP/2.0
Via: SIP/2.0/TLS 195.189.192.159:5068;alias;branch=z9hG4bKac1404080305
Max-Forwards: 70
From: <sip:sbc.ACeducation.info>;tag=1c386006673
To: <sip:sbc.ACeducation.info>
Call-ID: 188403163931122017223248@195.189.192.159
CSeq: 1 OPTIONS
Contact: <sip:sbc.ACeducation.info:5068;transport=tls>
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
  
```

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

A.4 Connectivity Interface Characteristics

The table below shows the technical characteristics of the Direct Routing interface.

In most cases, Microsoft uses RFC standards as a guide during development, but does not guarantee interoperability with SBCs - even if they support all the parameters in the table below - due to the specifics of the implementation of the standards by SBC vendors.

Microsoft has a partnership with some SBC vendors and guarantees their devices' interoperability with the interface. All validated devices are listed on Microsoft's website. Microsoft only supports devices *that are validated* in order to connect to the Direct Routing interface.

AudioCodes is one of the vendors who are in partnership with Microsoft.

AudioCodes' SBCs are validated by Microsoft to connect to the Direct Routing interface.

Table A-2: Teams Direct Routing Interface - Technical Characteristics

Category	Parameter	Value	Comments
Ports and IP ranges	SIP Interface FQDN Name	See Microsoft's document <i>Deploying Direct Routing Guide</i> .	-
	IP Addresses range for SIP interfaces	See Microsoft's document <i>Deploying Direct Routing Guide</i> .	-
	SIP Port	5061	-
	IP Address range for Media	See Microsoft's document <i>Deploying Direct Routing Guide</i> .	-
	Media port range on Media Processors	See Microsoft's document <i>Deploying Direct Routing Guide</i> .	-
	Media Port range on the client	See Microsoft's document <i>Deploying Direct Routing Guide</i> .	-
Transport and Security	SIP transport	TLS	-
	Media Transport	SRTP	-
	SRTP Security Context	DTLS, SIPS Note: Support for DTLS is pending. Currently, SIPS must be configured. When support for DTLS will be announced, it will be the recommended context.	https://tools.ietf.org/html/rfc5763
	Crypto Suite	AES_CM_128_HMAC_SH A1_80, non-MKI	-
	Control protocol for media transport	SRTCP (SRTCP-Mux recommended)	Using RTCP MUX helps reduce the number of required ports
	Supported Certification Authorities	See the <i>Deployment Guide</i>	-
	Transport for Media Bypass (of configured)	<ul style="list-style-type: none"> ICE-lite (RFC5245) – recommended Client also has Transport Relays 	-
	Audio codecs	<ul style="list-style-type: none"> G711 	-

Category	Parameter	Value	Comments
		<ul style="list-style-type: none"> ▪ Silk (Teams clients) ▪ Opus (WebRTC clients) - only if Media Bypass is used ▪ G729 	
Codecs	Other codecs	<ul style="list-style-type: none"> ▪ CN ▪ Required narrowband and wideband ▪ RED - Not required ▪ DTMF - Required ▪ Events 0-16 ▪ Silence Suppression - Not required 	-

B SIP Proxy Direct Routing Requirements

Microsoft Teams Direct Routing has three FQDNs:

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

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

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

B.1 Failover Mechanism

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

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

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

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/>

©2019 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-12787

