Configuration Note

AudioCodes Mediant™ Family of Media Gateways & Session Border Controllers

Connecting AudioCodes' SBC to Microsoft Teams Direct Routing Enterprise Model

Version 7.2

audiocodes

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 12
2.2 Validate AudioCodes' License 13
2.3 Configure LAN and WAN IP Interfaces 14
2.3.1 Validate Configuration of Physical Ports and Ethernet Groups 14
2.3.2 Configure LAN and WAN VLANs 15
2.3.3 Configure Network Interfaces 15
2.4 Configure TLS Context 17
2.4.1 Create a TLS Context for Microsoft Phone System Direct Routing 17
2.4.2 Generate a CSR and Obtain the Certificate from a Supported CA 19
2.4.3 Deploy the SBC and Root / Intermediate Certificates on the SBC 20
2.5 Alternative Method of Generating and Installing the Certificate 22
2.6 Deploy Baltimore Trusted Root Certificate 22
2.7 Configure Media Realm 22
2.8 Configure a SIP Signaling Interface 24
2.9 Configure Proxy Sets and Proxy Address 26
2.9.1 Configure Proxy Sets 26
2.9.2 Configure a Proxy Address 27
2.10 Configure a Coder Group 27
2.11 Configure an IP Profile 28
2.12 Configure an IP Group 29
2.13 Configure the Internal SRV Table 31
2.14 Configure SRTP 33
2.15 Configure SIP Options 33
2.15.1 Configure FQDN in Contact Header of Options Message using Message Manipulations Sets 34
2.16 Configuring Message Condition Rules 36
2.17 Configuring Classification Rules 36
2.18 Configure IP to IP Routing 36
2.19 Configuring an SBC to Suppress Call Line ID 39
3 Verify the Pairing between the SBC and Direct Routing 41
4 Make a Test Call 43
A Syntax Requirements for SIP Messages 'INVITE' and 'Options' 45
A.1 Terminology 45
A.2 Syntax Requirements for 'INVITE' Messages 45
A.3 Requirements for 'OPTIONS' Messages Syntax 46
A.4 Connectivity Interface Characteristics 47
B SIP Proxy Direct Routing Requirements 49
B.1 Failover Mechanism 49

List of Figures

Figure 2-1: Connection Topology - Network Interfaces....11
Figure 2-2: Example of Registered DNS Names....13
Figure 2-3: Physical Ports Configuration Interface....14
Figure 2-4: Ethernet Groups Configuration Interface....14
Figure 2-5: Configured VLANs in the Ethernet Device Table....15
Figure 2-6: Configured IP Interfaces....16
Figure 2-7: Configuration of TLS Context for Direct Routing....18
Figure 2-8: Configured TLS Context for Direct Routing and Interface to Manage the Certificates....18
Figure 2-9: Example of Certificate Signing Request Page....19
Figure 2-10: Uploading the Certificate Obtained from the Certification Authority....20
Figure 2-11: Message Indicating Successful Upload of the Certificate....20
Figure 2-12: Certificate Information....21
Figure 2-13: Configured Trusted Certificates Page....21
Figure 2-14: Configured Media Realms....23
Figure 2-15: Configured SIP Interface....25
Figure 2-16: Configured Proxy Set....26
Figure 2-17: Configured Proxy Address....27
Figure 2-18: Configured Coder Group....28
Figure 2-19: Configured IP Group....30
Figure 2-20: Configured Internal SRV Table....32
Figure 2-21: Configured Media Security Parameter....33
Figure 2-22: Configured Manipulation Rules....35
Figure 2-23: Activating 'OPTIONS' Manipulation Set....35
Figure 2-24: Privacy Restriction Mode....39
Figure 2-25: P-Asserted-Identity Header Mode....39
Figure 3-1: Proxy Set Status....41
Figure A-1: Example of an 'INVITE' Message....45
Figure A-2: Example of 'OPTIONS' message....46

List of Tables

Table 1-1: Infrastructure Prerequisites 10
Table 2-1: DNS Names Registered by an Administrator for a Tenant 12
Table 2-2: Adding VLAN ID 2 for the WAN Side 15
Table 2-3: Configuration Example: Network Interfaces 16
Table 2-4: Adding a Network Interface for the WAN for Teams 16
Table 2-5: New TLS Context 17
Table 2-6: Configuration Example: Media Realm for the LAN 23
Table 2-7: Configuration Example: Media Realm for the WAN 23
Table 2-8: Configuration Example: SIP Interface 24
Table 2-9: Configuration Example: Proxy Set - Teams – Global FQDNs 26
Table 2-10: Configuration Example: Proxy Address 27
Table 2-11: Configuration Example: IP Profile 28
Table 2-12: Configuration Example: IP Group - Teams Global FQDNs 29
Table 2-13: Configuration Example: Internal SRV Table 31
Table 2-14: Configuration Example: Media Security 33
Table 2-15: Configuration Example 34
Table 2-16: Activating 'OPTIONS' Manipulation Set 35
Table 2-17: Condition Table 36
Table 2-18: Classification Rules 36
Table 2-19: Configuration Example: Options Terminate 37
Table 2-20: Configuration Example: Refer Terminate 37
Table 2-21: Configuration Example: Routing from the Direct Routing Service to the SIP Trunk 37
Table 2-22: Configuration Example: Routing from the SIP Trunk to Direct Routing 38
Table A-1: Syntax Requirements for an 'INVITE' Message 46
Table A-2: Syntax Requirements for an 'OPTIONS' Message 47
Table A-3: Teams Direct Routing Interface - Technical Characteristics 47

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: June-18-2018

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 Web site at https://www.audiocodes.com/services-support/maintenance-and-support.

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.
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.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at https://online.audiocodes.com/documentation-feedback.

1 Introduction

This *Configuration Note* describes how to 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 successfully conducted validation tests with AudioCodes' Mediant VE SBC/v.7.20A.158.035. Older firmware versions might work, but Microsoft did not test previous versions of the firmware.

- Validate that you have the correct License Key. See AudioCodes' device's *User's Manual* for more information on how to view the device's License Key with licensed features and capacity. If you don't have a key, contact your AudioCodes representative to obtain one.
- AudioCodes licenses required for the SBC are mainly:
  - SILK Narrow Band
  - SILK Wideband
  - OPUS

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 *Deploying Direct Routing Guide.*
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

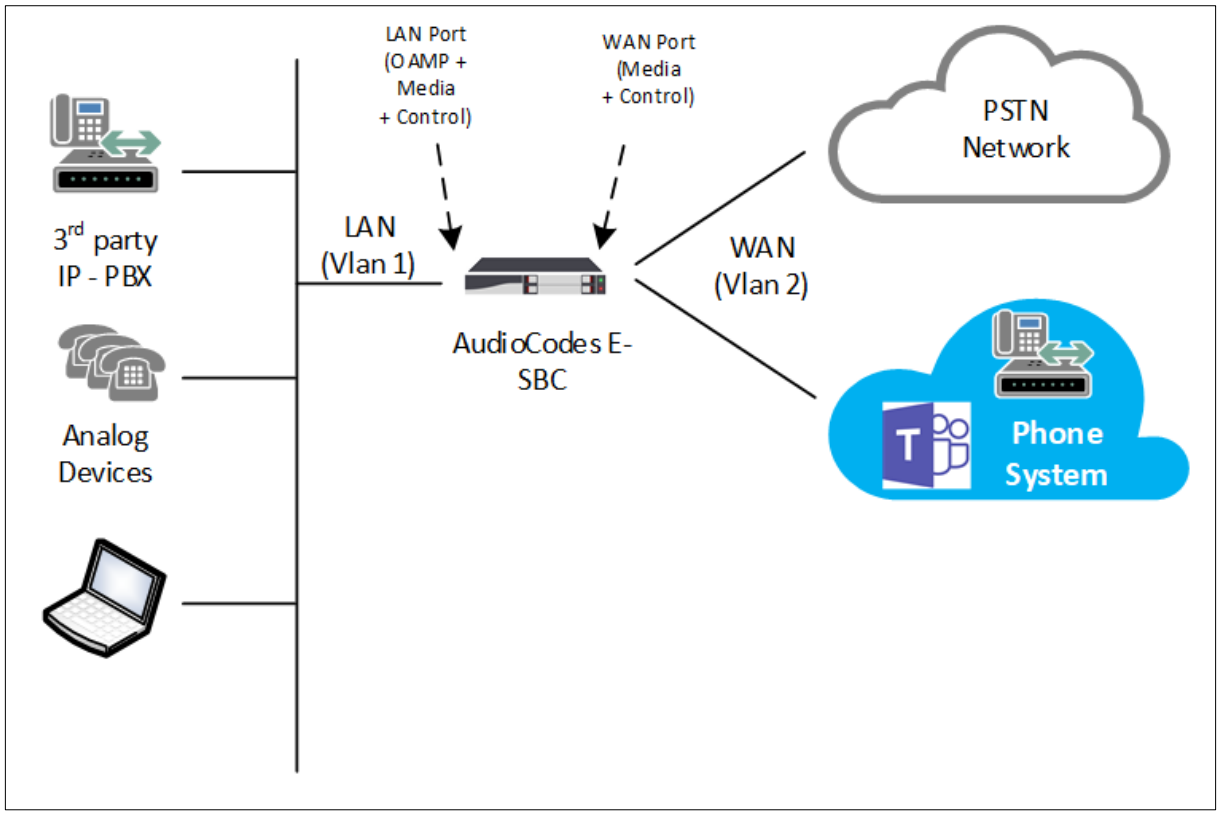
This section shows how to configure AudioCodes' SBC for internetworking with Microsoft Teams Direct Routing.

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

- Third-party 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 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 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 - Network Interfaces



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

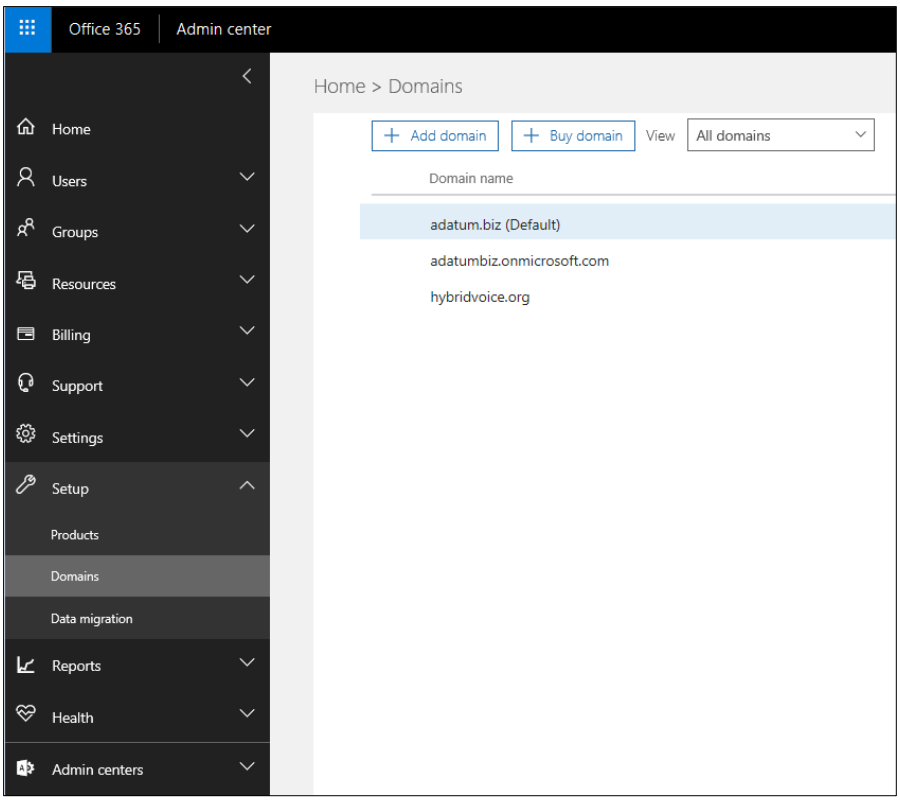
The SBC domain name must be from one of the names registered in 'Domains' of the tenant. You cannot use the ***.onmicrosoft.com** tenant for the domain name. For example, in Figure 2-2, the administrator registered the following DNS names for the tenant:

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**: ▪ 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 **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 gateway.]
2. **Number of SBC sessions** [Based on requirements]
3. **Transcoding sessions** [If media transcoding is needed]

2.3 Configure LAN and WAN IP Interfaces

2.3.1 Validate Configuration of Physical Ports and Ethernet Groups

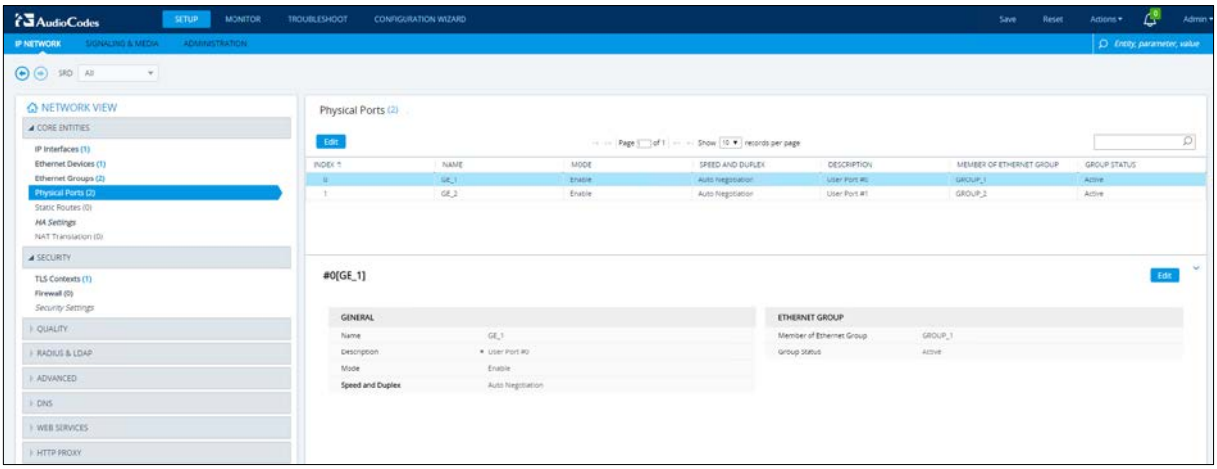
The physical ports are automatically detected by the SBC. The ethernet groups are also auto-assigned to the ports. In this step, only parameter validation is necessary.

➢ **To validate physical ports:**

1. Go to Setup > IP Network > Core Entities > 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.

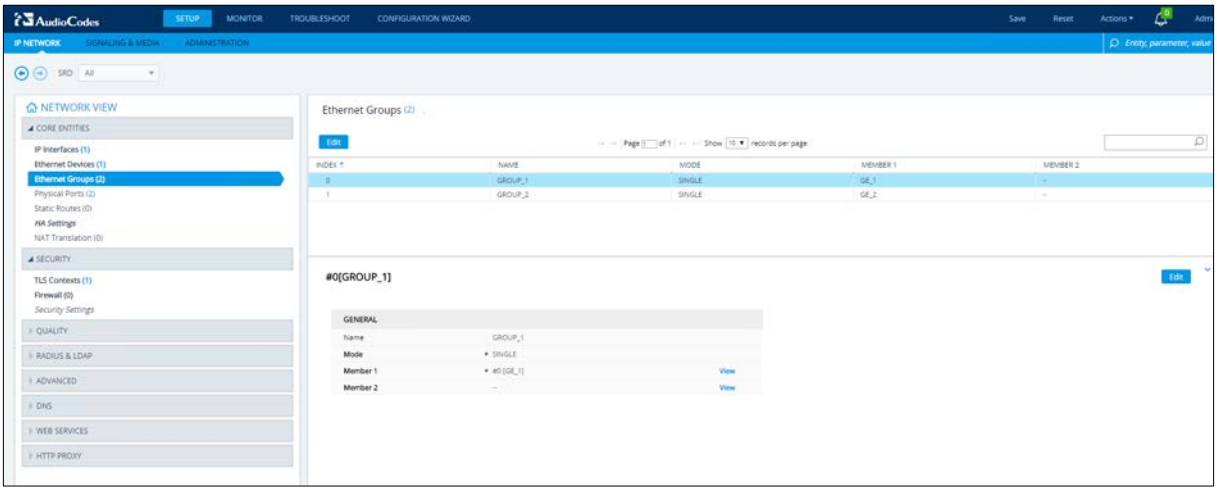
Figure 2-3: Physical Ports Configuration Interface



➢ **To validate Ethernet Groups:**

1. Go to Setup > IP Network > Core Entities > 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 2-4: Ethernet Groups Configuration Interface



2.3.2 Configure LAN and WAN VLANs

This step shows how to configure VLANs for LAN and WAN interfaces.

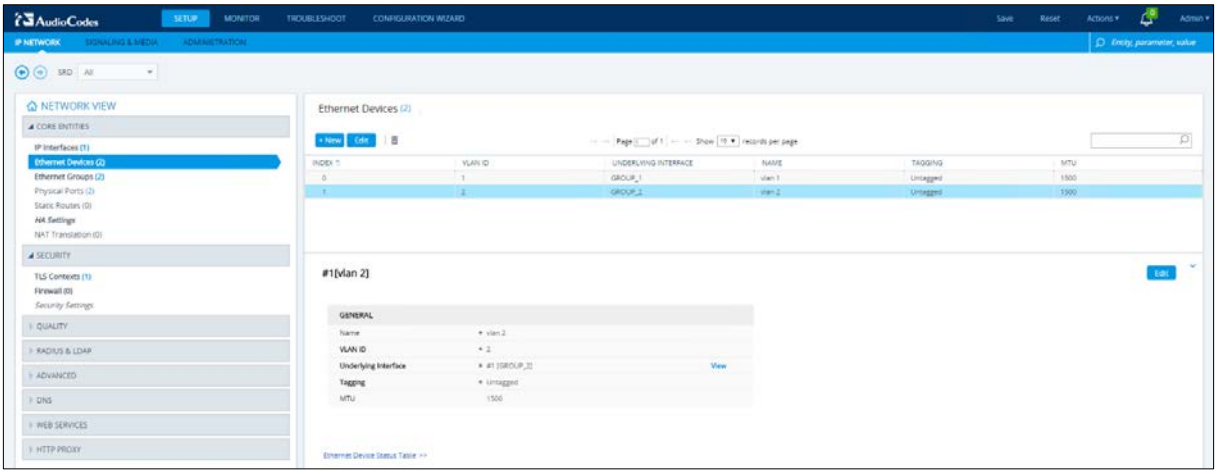
➢ **To configure VLANs:**

1. Open the Ethernet Device Page (Setup > IP Network > Core Entities > Ethernet Devices); there'll be a VLAN ID for the underlying interface Group 1 (Lan).
2. Add VLAN ID 2 for the WAN side as follows:

Table 2-2: Adding VLAN ID 2 for the WAN Side

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

Figure 2-5: Configured VLANs in the Ethernet Device Table



2.3.3 Configure Network Interfaces

This step shows how to configure network parameters for both LAN and WAN interfaces.

➢ **To configure network parameters for both LAN and WAN interfaces:**

1. Open the IP Interfaces Table (Setup > IP Network > Core Entities > IP Interfaces) – see Figure 2-6 below.
2. Configure network parameters for LAN interface.
   - Open O+M+C interface.
   - Configure the network parameters.

The table below shows a configuration example; your network parameters might be different.

Table 2-3: Configuration Example: Network Interfaces

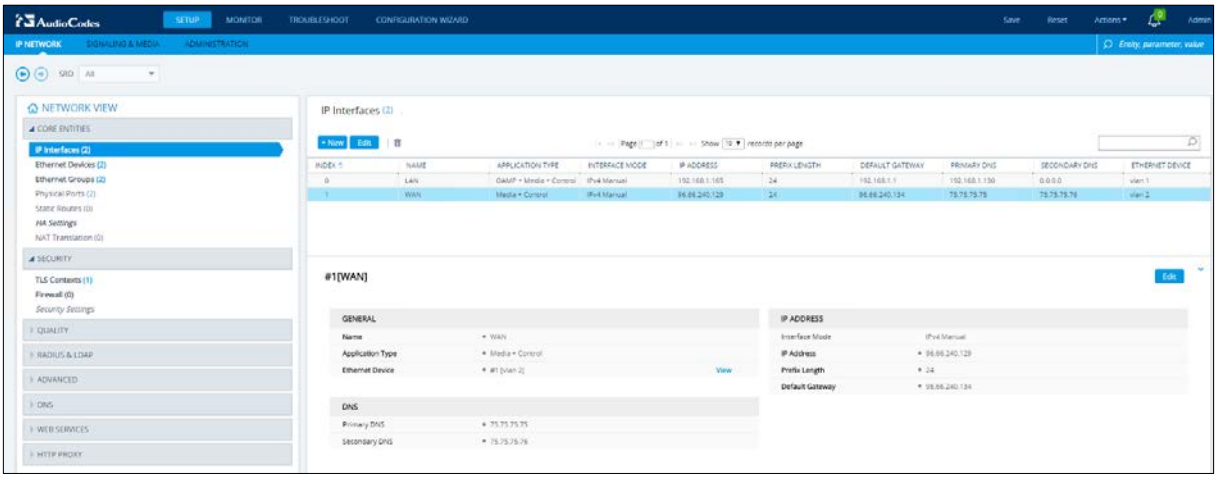
Parameter	Value
Name	LAN (arbitrary descriptive name)
Application type	OAMP + Media + Control (this interface points to the internal network where the network administrator's station is located, so enabling OAMP is necessary)
Ethernet Device	#0[vlan 1]
Interface Mode	IPv4 Manual (if you use IPv4)
IP address	192.168.1.165 (example)
Prefix length	24 (example)
Default Gateway	192.168.1.1 (example)
Primary DNS	192.168.1.130 (example)
Secondary DNS	192.168.1.131 (example)

3. Add a network interface for the WAN side for Teams. Use the table below as reference.

Table 2-4: Adding a Network Interface for the WAN for Teams

Parameter	Value
Name	WAN (arbitrary descriptive name)
Application type	Media + Control (as this interface points to the internet, enabling AMP is not recommended)
Ethernet Device	#1[vlan 2]
Interface Mode	IPv4 Manual (if you use IPv4)
IP address	96.66.240.129 (Public IP example)
Prefix length	24 (example)
Default Gateway	96.66.240.134 (example)
Primary DNS	According to your internet provider's instructions
Secondary DNS	According to your internet provider's instructions

Figure 2-6: Configured IP Interfaces



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 are:

- AddTrust External CA Root
- Baltimore CyberTrust Root (see Section 2.6)
- Class 3 Public Primary Certification Authority
- DigiCert Global Root CA
- Verisign, Inc.
- Symantec Enterprise Mobile Root for Microsoft
- Thawte Timestamping CA

The step below shows how to request a certificate for the SBC WAN interface and to configure it based on the example of DigiCert.

The step includes these stages:

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

2.4.1 Create a TLS Context for Microsoft Phone System Direct Routing

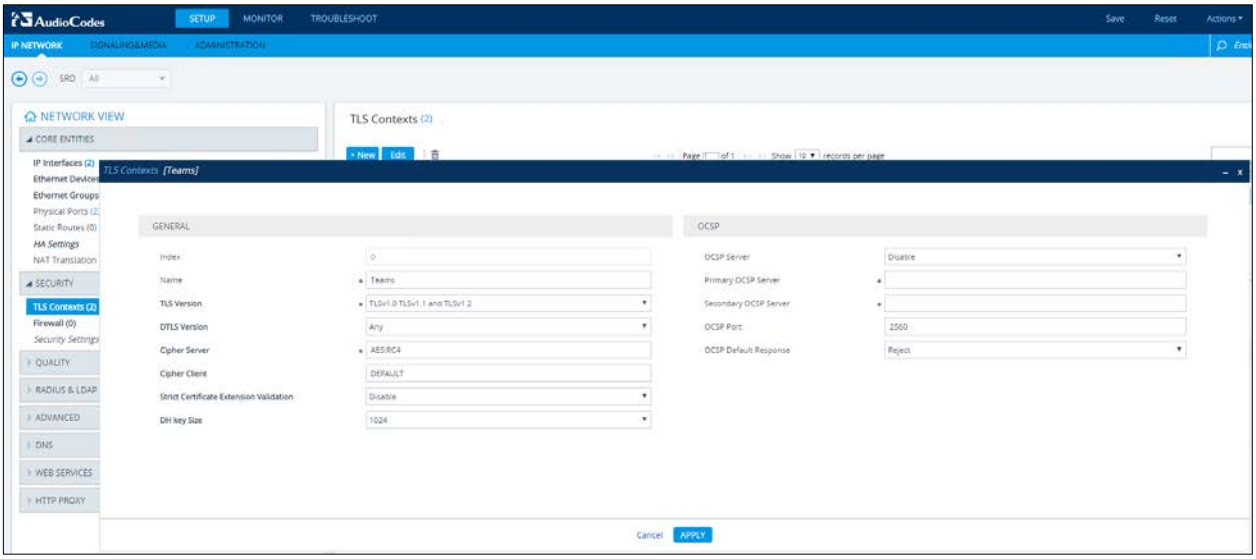
1. Open TLS Contexts (Setup > IP Network >Security>TLS Contexts).
2. Create a new TLS Context by clicking **+New** at the top of the interface, and then configure the parameters using the table below as reference.

Table 2-5: New TLS Context

Parameter	Value
Index	1 (default)
Name	Teams (arbitrary descriptive name)
TLS Version	TLSv1.0 TLSv1.1 and TLSv1.2
DTLS version	Any (default)
Cipher Server	RC4:AES128 (default)
Cipher Client	DEFAULT (default)
Strict Certificate Extension Validation	Disable (default)
DH Key Size	1024 (default)
OCSP	All parameters default

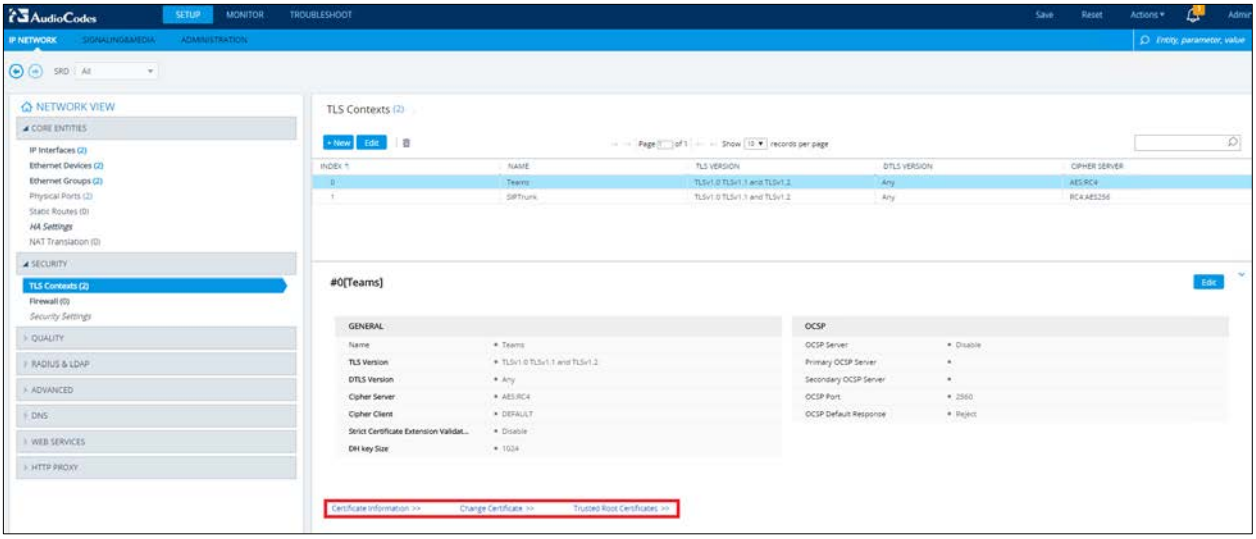
Note: The table above exemplifies configuration focusing on interconnecting SIP and media. You might want to configure additional parameters according to your company's policies. For example, you might want to configure Online Certificate Status Protocol (OCSP) to check if SBC certificates presented 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 2-7: Configuration of TLS Context for Direct Routing



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

Figure 2-8: Configured TLS Context for Direct Routing and Interface to Manage the Certificates



2.4.2 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.

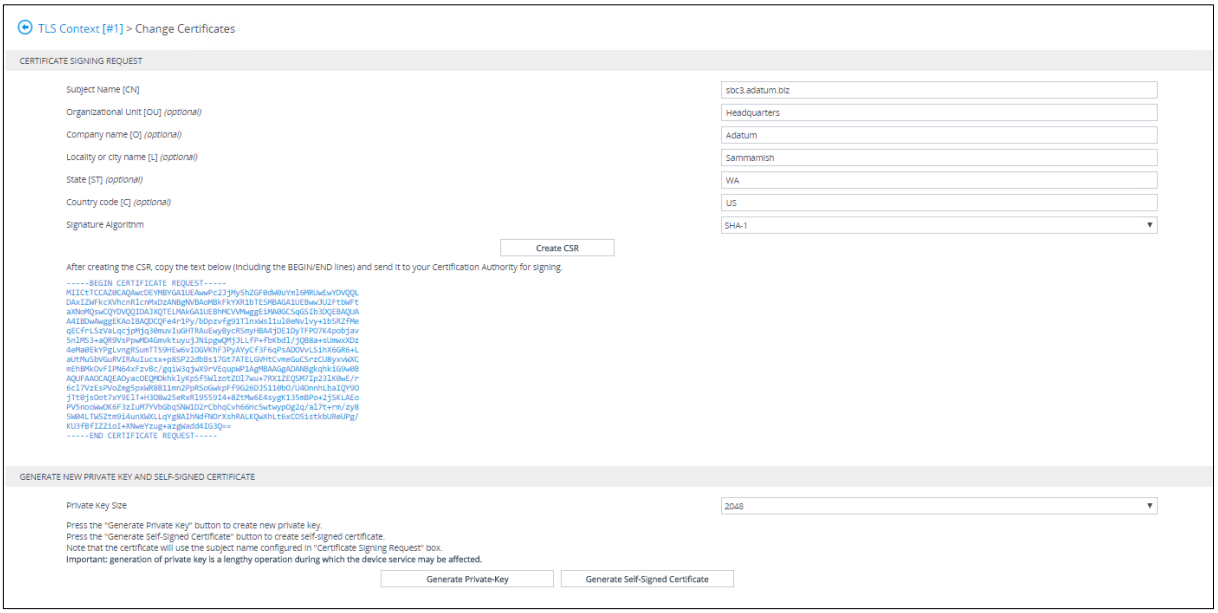
➢ **To generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority:**

1. Click **Change Certificate>>** in the TLS Contexts page. In the 'Certificate Signing Request', enter your company's data.

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

2. 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.
3. To change the key size on TLS Context, go to: Change Certificate > 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.
4. Under 'Certificate Signing Request' click **Generate CSR**, copy it and request a Standard SSL Certificate.
5. Obtain Trusted Root and Intermediary Signing Certificates from your Certification Authority.

Figure 2-9: Example of Certificate Signing Request Page



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

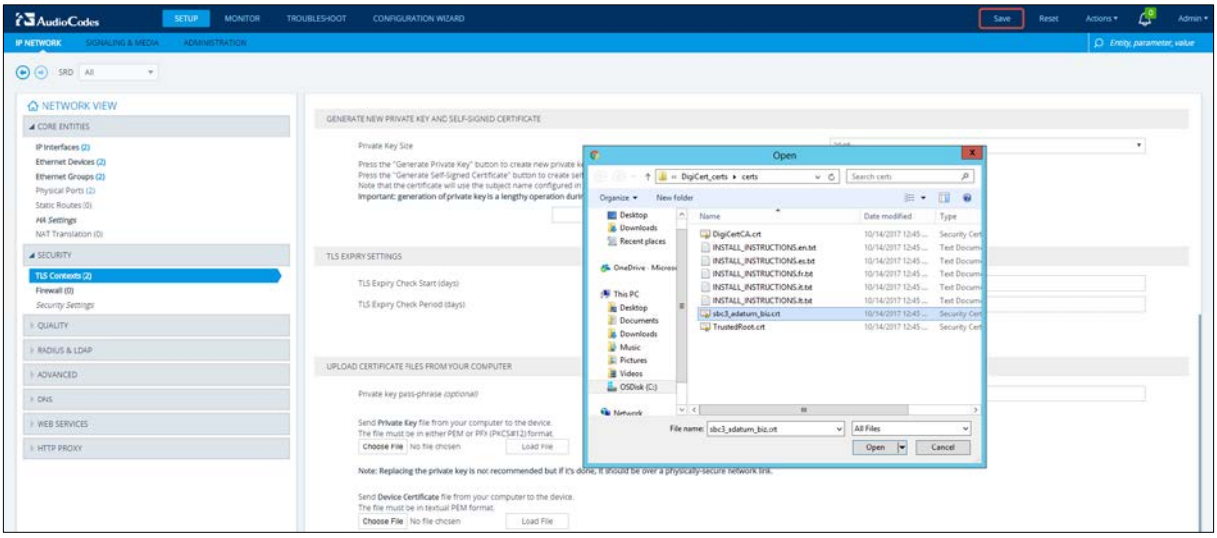
After receiving the certificates from the Certification Authority, install the

- SBC certificate
- Root / Intermediate certificates

➢ To install the SBC certificate:

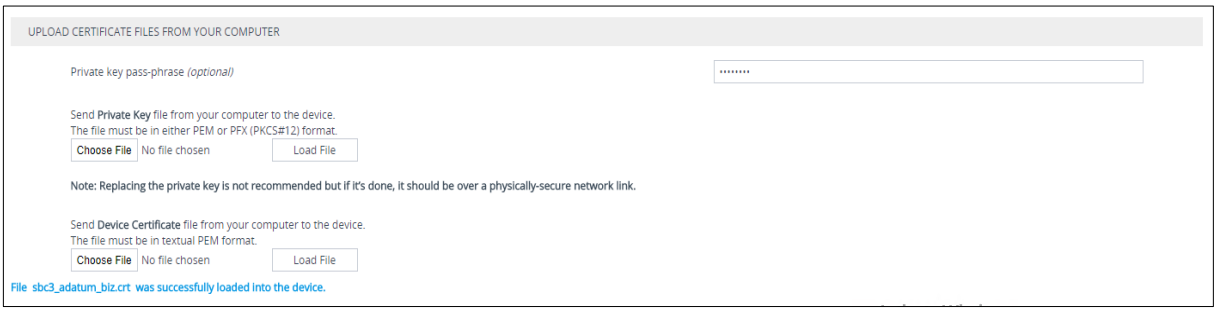
1. Open Setup > IP Network > Security > TLS Contexts > Direct Connect > Change Certificate.
2. Under 'Upload Certificate Files From Your Computer', click **Choose File** below 'Device Certificate' and then select the SBC certificate file obtained from your Certification Authority.

Figure 2-10: Uploading the Certificate Obtained from the Certification Authority



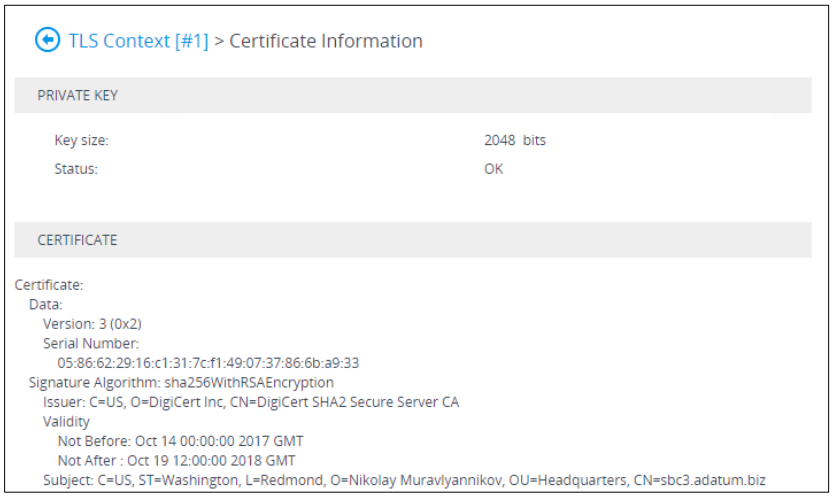
a. Validate that the certificate was uploaded correctly: A message indicating that the certificate was uploaded successfully is displayed lowermost in the page.

Figure 2-11: Message Indicating Successful Upload of the Certificate



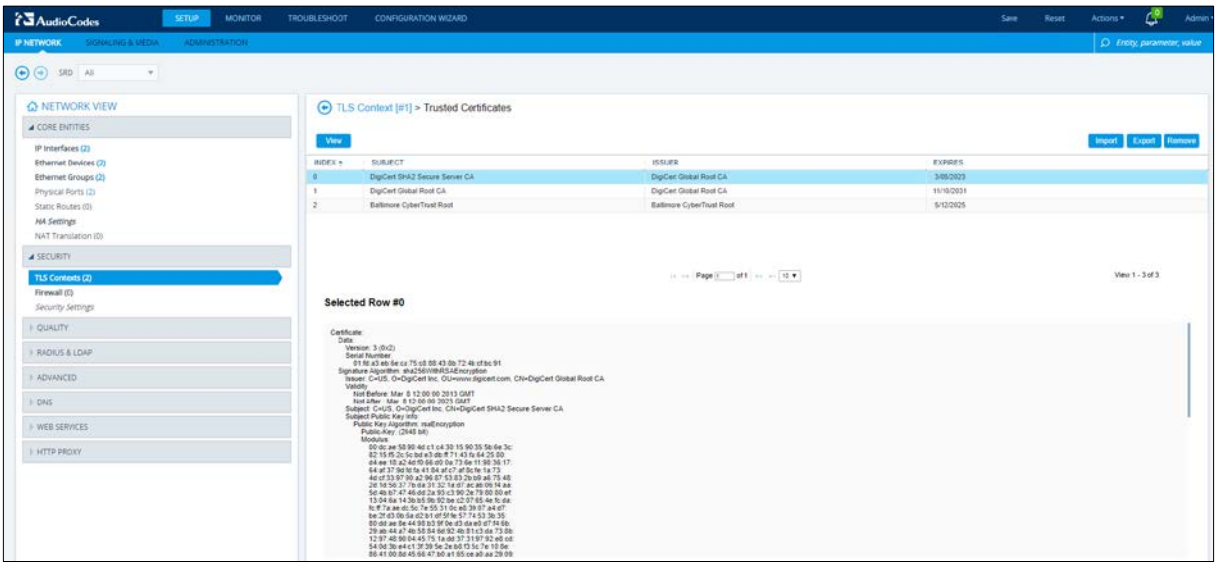
b. Go to Setup > IP Network > Security > TLS Contexts > Direct Connect > Certificate Information and then validate the certificate Subject Name.

Figure 2-12: Certificate Information



3. To install the root and the intermediate certificate, go to Setup > IP Network > Security > TLS Contexts > Direct Connect > Trusted Root Certificates and then click **Import** and upload all root and intermediate certificates obtained from your Certification Authority.

Figure 2-13: Configured Trusted Certificates Page



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 Setup > IP Network > Security > TLS Contexts > Direct Connect > Change Certificate.
2. Enter the password assigned during export with the DigiCert utility in the 'Private key pass-phrase' field.
3. Under 'Upload Certificate Files From Your Computer', click **Choose File** under 'Private Key' and then select the SBC certificate file exported from the DigiCert utility.

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 a Media Realm for the LAN:**

1. Open the Media Realm page (Setup > Signaling and Media > Core Entities > Media Realms).
2. Open the default Media Realm and change the parameters based on the requirements of your organization. The example below shows a Media Realm configuration with port ranges starting at 6000 and capable of handling 100 media legs.

Table 2-6: Configuration Example: Media Realm for the LAN

Parameter	Value
Index	0 (default)
Name	LAN (arbitrary descriptive name)
Topology Location	Down (default)
IPv4 Interface Name	#0 [LAN]
Port Range Start	6000
Number of media session legs	100 (example value)
Default Media Realm	Yes (default)

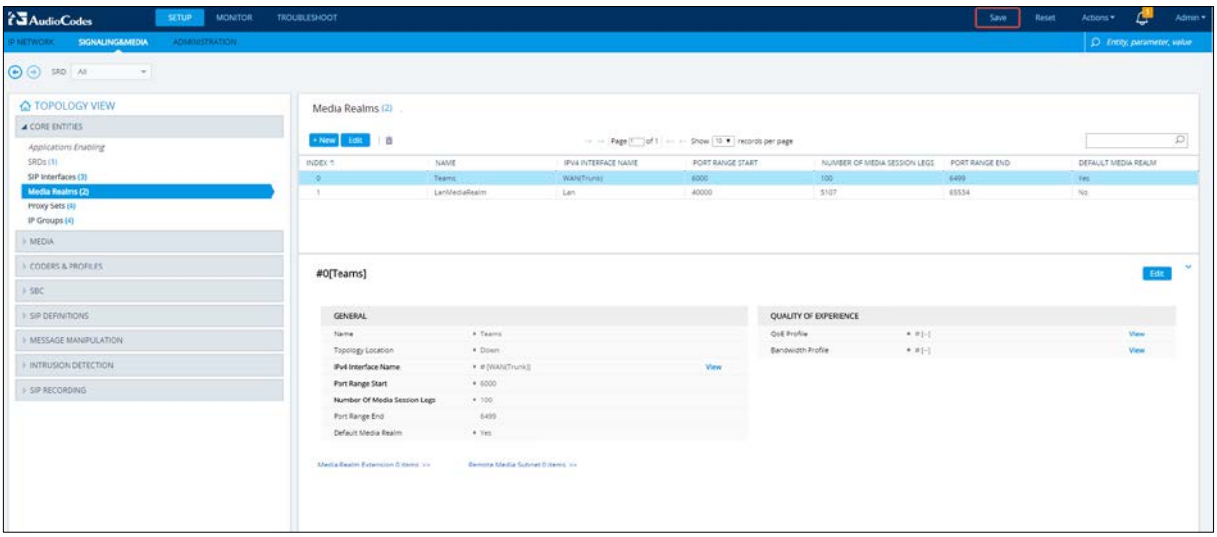
➢ **To configure a Media Realm for the WAN:**

1. Open the Media Realm page (Setup > Signaling and Media > Core Entities > Media Realms).
2. Click **+New** and then define the Media Realm for the WAN. The example below shows a Media Realm configuration with port ranges starting at 7000 and capable of handling 100 media legs.
3. Click **Save**.

Table 2-7: Configuration Example: Media Realm for the WAN

Parameter	Value
Index	1 (default)
Name	Teams (arbitrary descriptive name)
Topology Location	Down (default)
IPv4 Interface Name	#1 [WAN]
Port Range Start	7000
Number of media session legs	100 (example value)
Default Media Realm	No (default)

Figure 2-14: Configured Media Realms



2.8 Configure a SIP Signaling Interface

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

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

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

➢ **To configure a SIP interface:**

1. Open the SIP Interface table (Setup > Signaling and Media > Core Entities > 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.

3. Click **Save**.

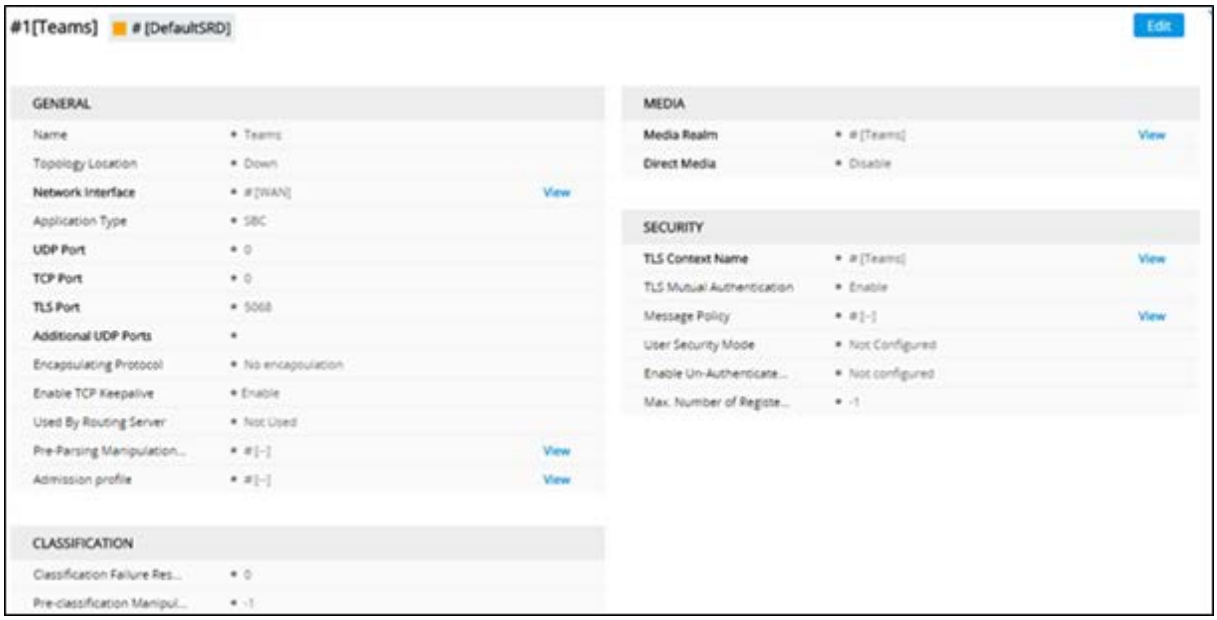
Table 2-8: Configuration Example: SIP Interface

Parameter	Value
Name	Teams (arbitrary descriptive name)
Network Interface	#1 [WAN]
UDP port	0 (Microsoft Phone System does not use UDP for SIP signaling)
TCP Port	0 (Microsoft Phone System does not use TCP for SIP signaling)
TLS Port	5068 (arbitrary port)
Enable TCP Keepalive	Enable
Media Realm	[Teams]
TLS Context Name	[Teams]
TLS Mutual Authentication	Enable
Classification Failure Response Type	0 (Recommended to prevent DoS attacks)

Note:

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

Figure 2-15: Configured SIP Interface



2.9 Configure Proxy Sets and Proxy Address

2.9.1 Configure Proxy Sets

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 PSTN trunk and the third-party PBX is also necessary, but isn't covered in this guide. For specific configuration of interfaces pointing to SIP trunks and/or the third-party PSTN environment connected to the SBC, see the trunk / environment vendor's documentation. AudioCodes also offers a comprehensive suite of documents covering the interconnection between different trunks and the equipment.

➢ **To configure a Proxy Set:**

1. Open the Proxy Sets table (Setup > Signaling and Media > Core Entities > 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.

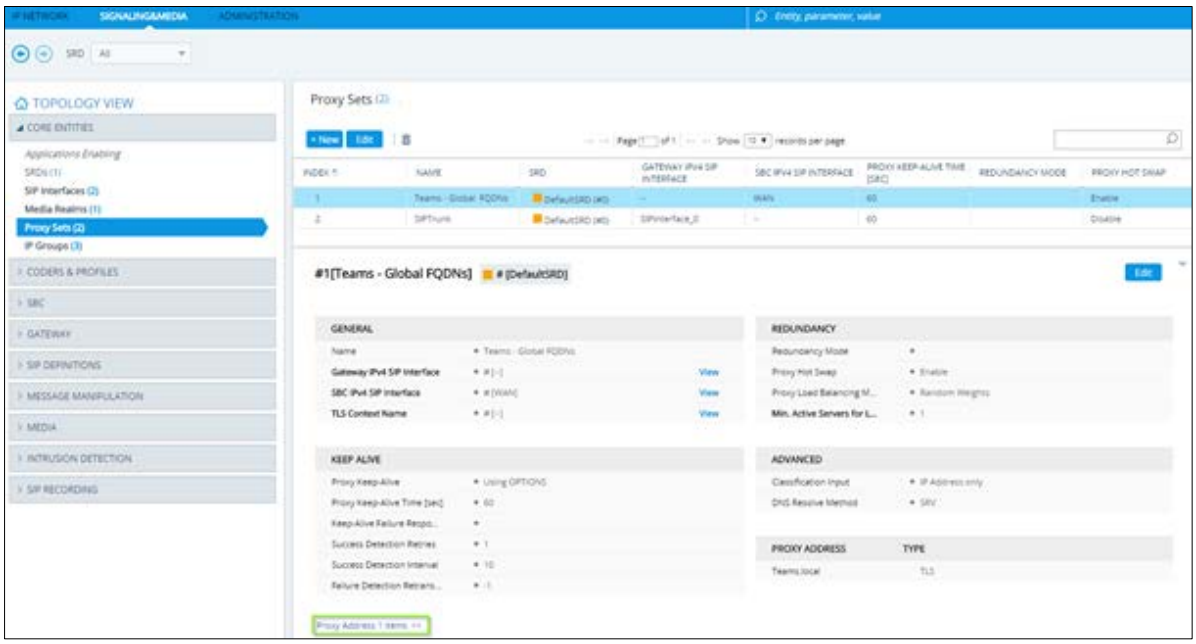
Table 2-9: Configuration Example: Proxy Set - Teams – Global FQDNs

Parameter	Value
Index	1
Name	Teams – Global FQDNs (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
DNS Resolve Method	SRV

3. Click **Save**.

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

Figure 2-16: Configured Proxy Set



2.9.2 Configure a Proxy Address

This step shows how to configure a Proxy Address.

➢ **To configure a Proxy Address:**

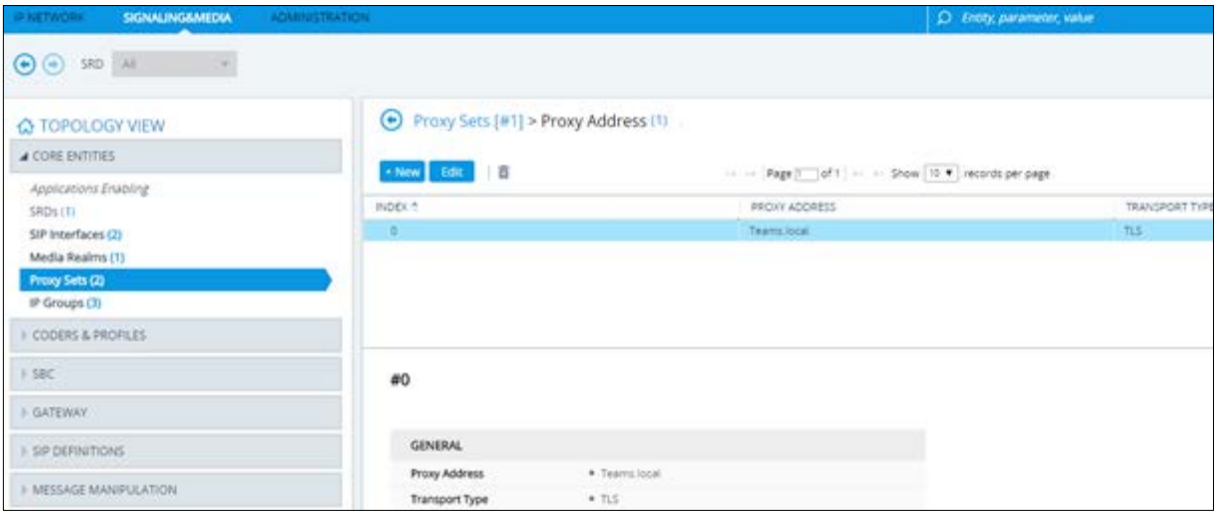
1. Open the Proxy Sets table (Setup > Signaling and Media > Core Entities > Proxy Sets) and then click the Proxy Set **Teams**.
2. Click **Proxy Address** (see this in Figure 2-16 above).
3. Click **+New** to add the DNS name of the Direct Routing interface (teams.local), select the **TLS** transport type and then click **Save**.

Table 2-10: Configuration Example: Proxy Address

Parameter	Value
Proxy Address	teams.local (See also Section 2.13, 'Configure the Internal SRV Table')
Transport Type	TLS

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

Figure 2-17: Configured Proxy Address



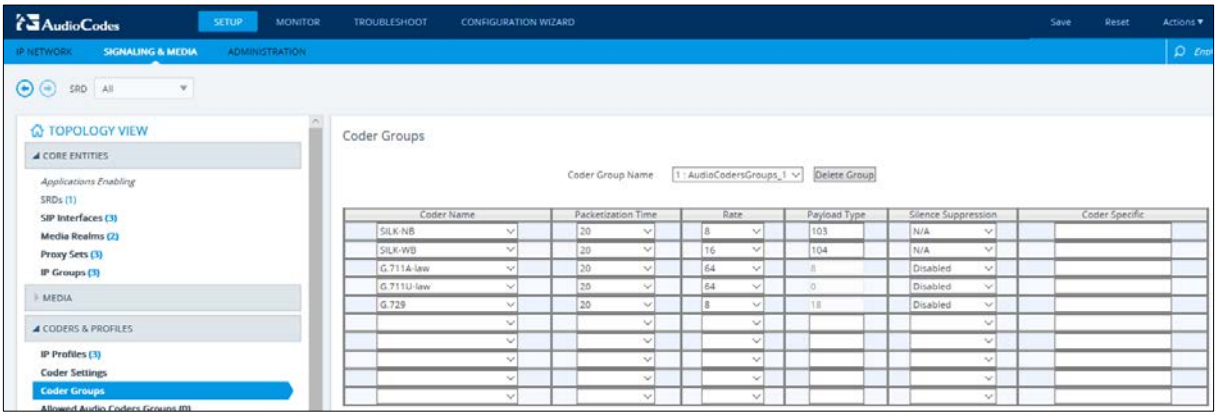
2.10 Configure a Coder Group

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 > Signaling and Media > Coders and Profiles> 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 2-18: Configured Coder Group



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

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:**

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

Table 2-11: Configuration Example: IP Profile

Parameter	Value
Name	Teams (arbitrary descriptive name)
Remote re-INVITE	Supported only with SDP
Remote Delayed Offer Support	Not supported
Remote REFER Mode	Handle locally
SBC Media Security Mode	SRTP
SBC Media Security Method	SDES (for TAP only as DTLS is unsupported at present. When the General Availability (GA) version of Teams will be announced, the recommended method will be DTLS)
Extension Coders Group	Audio_Coders_Groups_1 (from the previous step)
ICE Mode	Lite (Required only if Teams is configured with Media Bypass)

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

2.12 Configure an IP Group

An IP group represents a SIP entity. This section shows how to configure one.

➢ **To configure an IP Group:**

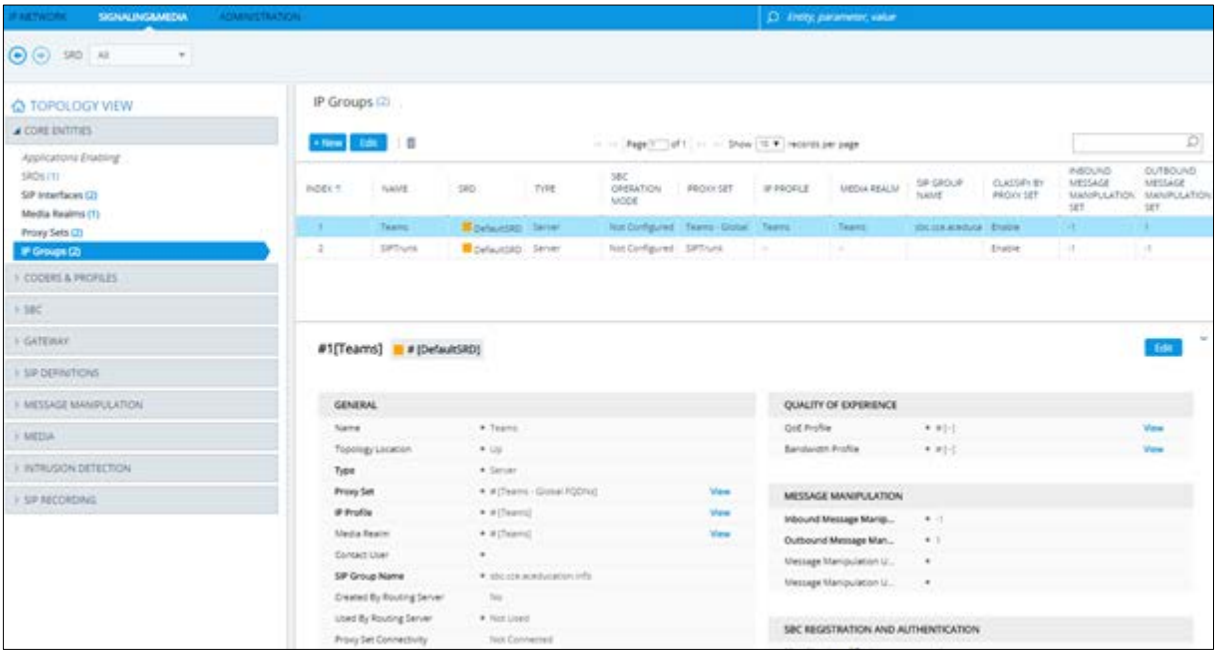
1. Open the IP Groups table (Setup > Signaling and Media > Core Entities > IP Group).
2. Click **+New** to add an IP Group for the Direct Routing interface. Configure the parameters using the table below as reference.

Table 2-12: Configuration Example: IP Group - Teams Global FQDNs

Parameter	Value
Name	Teams Global FQDNs (arbitrary descriptive name)
Proxy Set	[Teams Global FQDN]
IP Profile	[Teams]
Media Realm	[Teams]
SBC Operation Mode	B2BUA
Classify By Proxy Set	Disable
Local Host Name	<FQDN name of your SBC>. For example, sbc.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*
Always Use Src Address	Yes
DTLS Context	[Teams]

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

Figure 2-19: Configured IP Group



2.13 Configure the Internal SRV Table

The Internal SRV table resolves host names to DNS A-Records. Three different A-Records can be assigned to each host name, where each A-Record contains the host name, priority, weight, and port.

➢ **To configure the internal SRV Table:**

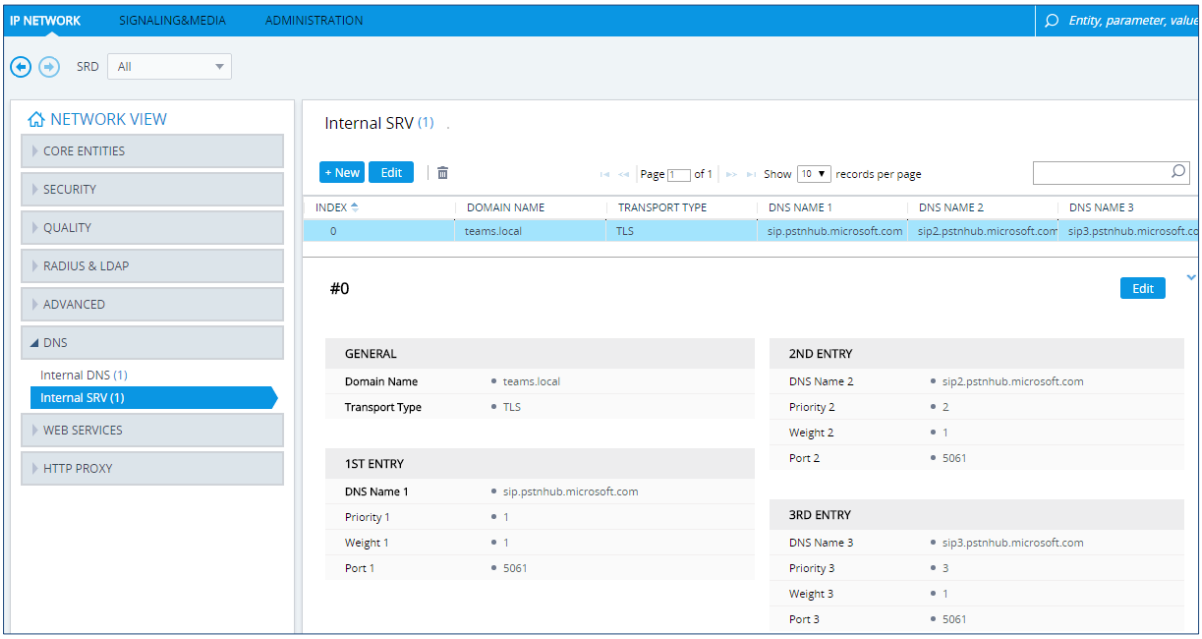
1. Open the Internal SRV table (Setup > IP Network > DNS > Internal SRV).
2. Click **+New** to add the SRV record for teams.local and use the table below as configuration reference.

Table 2-13: Configuration Example: Internal SRV Table

Parameter	Value
Domain Name	teams.local Note: FQDN is case-sensitive; configure in line with the configuration of the Teams Proxy Set (see under Section 2.9.2).
Transport Type	TLS
1ST ENTRY	
DNS Name 1	sip.pstnhub.microsoft.com
Priority 1	1
Weight 1	1
Port 1	5061
2ND ENTRY	
DNS Name 2	sip2.pstnhub.microsoft.com
Priority 2	2
Weight 2	1
Port 2	5061
3RD ENTRY	
DNS Name 3	sip3.pstnhub.microsoft.com
Priority 3	3
Weight 3	1
Port 3	5061

Use the figure below as reference.

Figure 2-20: Configured Internal SRV Table



2.14 Configure SRTP

By default, SRTP is disabled.

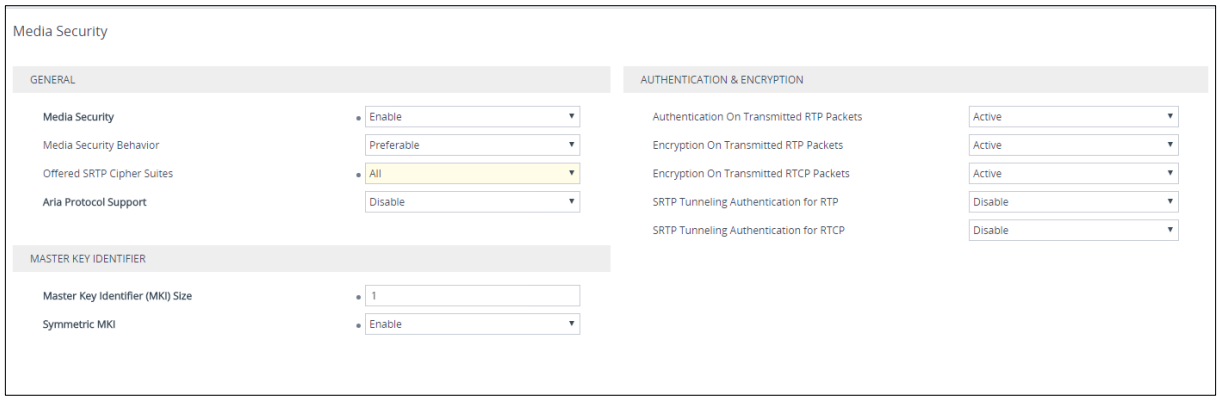
➢ **To enable SRTP:**

- Open the Media Security page (Setup > Signaling and Media > Media > Media Security).
- Set the parameter 'Media Security' to **Enable**; configure the other parameters using the table below as reference.

Table 2-14: Configuration Example: Media Security

Parameter	Value
Media Security	Enable
Media Security Behavior	Preferable - Single Media

Figure 2-21: Configured Media Security Parameter



- Click **Save**.
- Click **Reset** to reset the device.

2.15 Configure SIP Options

SIP Options is an important mechanism used to monitor the connection from the AudioCodes SBC to the Microsoft Phone System. Microsoft Phone System requires the FQDN of the trunk sent in the 'CONTACT' field of SIP Options. The FQDN of the trunk is the name that was specified during the pairing, for example:

New-CSOnlinePSTNGateway -FQDN sbc.ACeducation.info

The IP address of the SBC is by default sent in the 'CONTACT' field:

```
From: <sip:96.66.240.133>;tag=1c850914553
```

It's mandatory, however, that the 'CONTACT' field contains the FQDN of the SBC. More information about the requirements can be found at Requirements for 'OPTIONS' messages syntax.

Use the Message Manipulation Rules to configure sending the FQDN in the 'CONTACT' header of SIP Options.

2.15.1 Configure FQDN in Contact Header of Options Message using Message Manipulations Sets

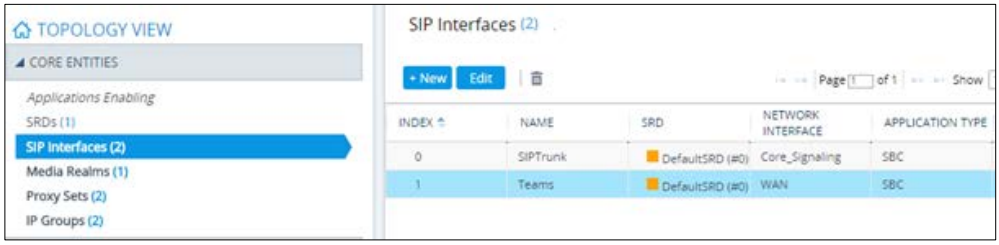
This method allows manipulation of the 'CONTACT' header based on the Destination address of the entity. For example,

- SIP Options going to sip.pstnhub.microsoft.com should be in the format:

  Contact:admin@sbc.ACeducation.info

The method will not function if you need to send a different FQDN in the 'Contact' header to multiple entities.

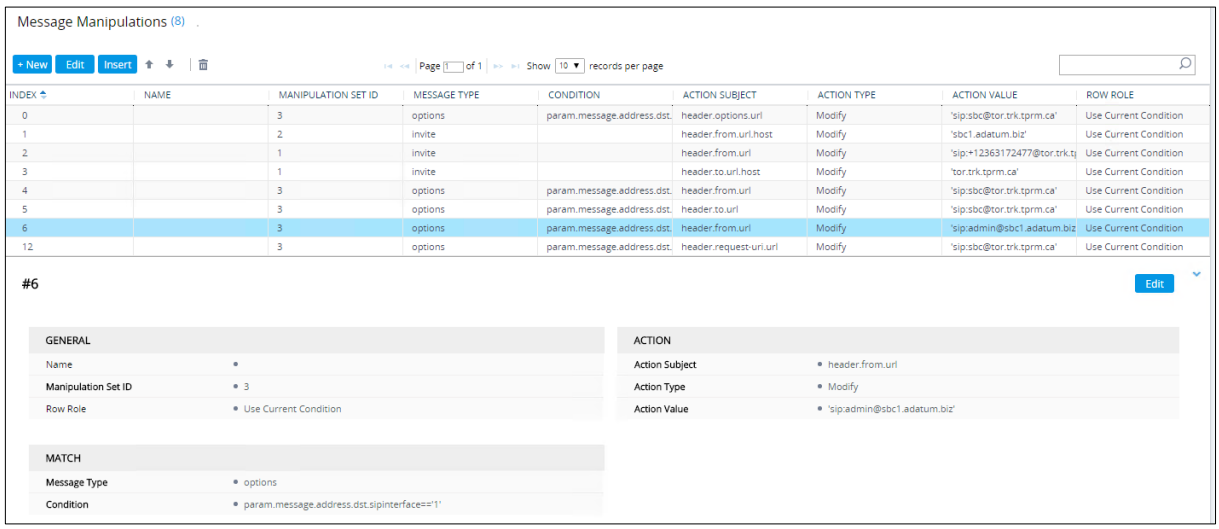
Table 2-15: Configuration Example

Parameter	Value
Manipulation Set ID	2 (arbitrary; you can use any number, but the same for both rules)
Message Type	Options
Condition	param.message.address.dst.sipinterface=='1' (The ID assigned to the SIP Interface by the system; view the SIP interfaces and identify the Index value assigned to Teams) 
Action Subject	header.contact.url.host
Action Type	Modify
Action Value	'sbc.ACeducation.info'

➢ **To configure as in the example above:**

1. Open the Message Manipulations page (Signalling and Media > Message Manipulation > Message Manipulations).
2. Configure a new Message Manipulation Set as shown in Figure 2-23.

Figure 2-22: Configured Manipulation Rules



Note: If modification of the Options request header itself is required, for example, instead of sending **OPTIONS 99.66.240.132 SIP/2.0** it's required to send **OPTIONS sip:sbc@sbc.ACeducation.info SIP/2.0**, you must specify the Action Subject **header.request-uri.url**

For a detailed description of the syntax used for configuring Message Manipulation rules, refer to the *SIP Message Manipulations Quick Reference Guide* on AudioCodes' website.

These rules will not apply automatically. For them to work, you must activate this set.

➢ **To activate this set:**

1. Open https://<SBCFQDN or IP > /AdminPage.
2. Go to 'ini Parameters'.

Table 2-16: Activating 'OPTIONS' Manipulation Set

Parameter	Value
Parameter Name	GWOutboundManipulationSet
Enter Value	2 (Message Manipulation Set ID configured in the previous step)

3. Click **Apply New Value**.

Figure 2-23: Activating 'OPTIONS' Manipulation Set

2.16 Configuring Message Condition Rules

The Message Condition table lets you configure up to 20 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.

Condition #0 verifies that the Contact header contains Teams FQDN.

Table 2-17: Condition Table

Index	Name	Condition
0	Teams-Contact	header.contact.url.host contains 'pstnhub.microsoft.com'

2.17 Configuring Classification Rules

The Classification table lets you configure up to 102 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.

Table 2-18: Classification Rules

Index	Name	Source SIP Interface	Message Condition	Destination Host	Action Type	Source IP Group
1	Teams	WAN	Teams-Contact	sbc.ACeducation.info	Allow	Teams

➢ **To configure a Classification rule:**

1. Open the Classification table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Classification Table**).
2. Click **New**.
3. Configure the Classification rule according to the parameters described in the table above.
4. Click **Apply**.

2.18 Configure IP to IP Routing

IP to IP routing defines the routes for forwarding SIP messages received from one entity, to another entity.

The SBC selects the rule based on input characteristics, for example, calls originating from an IP Group. If multiple rules are defined, they'll be evaluated in order, and the first matching rule will apply.

The example shown in the table below only covers IP to IP routing, though you can route the calls from TDM connections. See AudioCodes' SBC documentation for more information on how to route in other scenarios.

The following IP-to-IP routing rules will be defined:

- Options SBC Termination
- Refer SBC Termination

- Calls from Teams Service to SIP Trunk
- Calls from SIP Trunk to Teams

➢ To configure a route from the Direct Routing Service to the SIP trunk:

- Open the IP-to-IP Routing table (Setup > Signaling and Media > SBC > Routing > IP-to-IP Routing).
- Click **+New**.
- Configure the rule using the example in the table below as reference. Note that this example is only a *basic* routing example. For detailed information on configuring voice routing rules, see AudioCodes' manuals.

Table 2-19: Configuration Example: Options Terminate

Parameter	Value
Name	Options Terminate (arbitrary name)
Destination Type	Dest Address
Destination Address	internal

Table 2-20: Configuration Example: Refer Terminate

Parameter	Value
Name	Refer Terminate (arbitrary name)
Call Trigger	Refer
Destination Type	Request URI
Destination IP Group	#0 Teams Global FQDNs

Table 2-21: Configuration Example: Routing from the Direct Routing Service to the SIP Trunk

Parameter	Value
Name	Direct Routing to SIP Trunk (arbitrary name)
Source IP Group	Teams Global FQDNs
Destination Type	IP Group
Destination IP Group	#2 SIP Trunk

➢ To configure routing from the SIP Trunk to Direct Routing:

1. Click **+New**.
2. Configure the rule using the example in the table below as reference. Note that this example is only a *basic* routing example. For detailed information on configuring voice routing rules, see AudioCodes' manuals.
3. Click **Save**.

Table 2-22: Configuration Example: Routing from the SIP Trunk to Direct Routing

Parameter	Value
Name	SIP Trunk to Direct Routing (arbitrary name)
Source IP Group	#2 SIP Trunk
Destination Type	IP Group
Destination IP Group	#0 Teams Global FQDNs

2.19 Configuring an SBC to Suppress Call Line ID

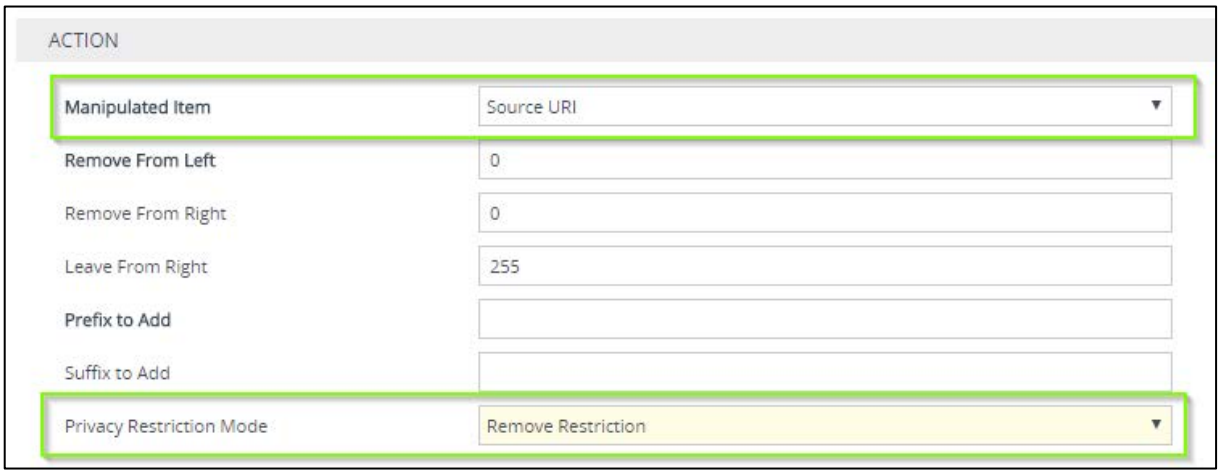
This section shows how to configure an SBC in two steps when Forward P-Asserted-Identity header is included with the Privacy ID header. This allows:

- 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.

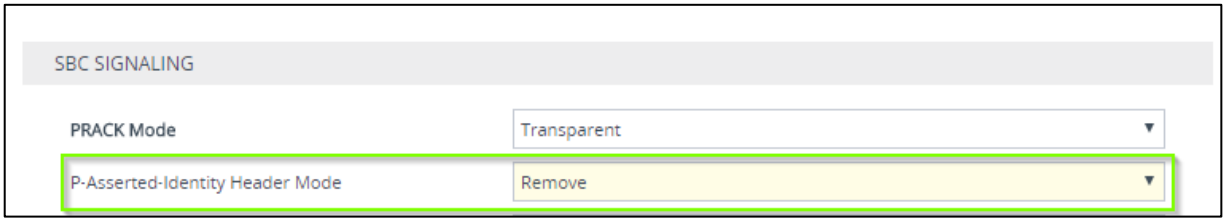
Figure 2-24: Privacy Restriction Mode



➢ **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 2-25: P-Asserted-Identity Header Mode



This page is intentionally left blank.

3 Verify the Pairing between the SBC and Direct Routing

After you've paired the SBC with Direct Routing using the New-CsOnlinePSTNGateway cmdlet, validate that the SBC can successfully exchange OPTIONs with Direct Routing.

➢ **To validate the pairing using SIP Options:**

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

Figure 3-1: Proxy Set Status

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 > Troubleshooting > 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 issues 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: 560804648269201715141 8@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' *SIP Message Manipulation Reference Guide*.
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' *SIP Message Manipulation Reference Guide*.
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

Table A-2: Syntax Requirements for an 'OPTIONS' Message

Parameter	Where configured	How to configure
Contact	Message Manipulation Set	See Section 2.15.

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-3: Teams Direct Routing Interface - Technical Characteristics

Category	Parameter	Value	Comments
Ports and IP ranges	SIP Interface FQDN Name	See Microsoft's document *Deploying Direct Routing Guide.*	
	IP Addresses range for SIP interfaces	See Microsoft's document *Deploying Direct Routing Guide.*	
	SIP Port	5061	
	IP Address range for Media	See Microsoft's document *Deploying Direct Routing Guide.*	
	Media port range on Media Processors	See Microsoft's document *Deploying Direct Routing Guide.*	
	Media Port range on the client	See Microsoft's document *Deploying Direct Routing Guide.*	
Transport and Security	SIP transport	TLS	
	Media Transport	SRTP	
	SRTP Security Context	DTLS, SIPS Note: Support for DTLS is pending. Currently, SIPS must be configured. When support for DTLS will be announced, it will be the recommended context.	https://tools.ietf.org/html/rfc5763
	Crypto Suite	AES_CM_128_HMAC_SHA1_80, non-MKI	
	Control protocol for media transport	SRTCP (SRTCP-Mux recommended)	Using RTCP MUX helps reduce the number of required ports

Category	Parameter	Value	Comments
	Supported Certification Authorities	See the *Deployment Guide*	
	Transport for Media Bypass (of configured)	▪ ICE-lite (RFC5245) – recommended ▪ Client also has Transport Relays	
	Audio codecs	▪ G711 ▪ Silk (Teams clients) ▪ Opus (WebRTC clients) - only if Media Bypass is used ▪ G729	
Codecs	Other codecs	▪ CN ▪ Required narrowband and wideband ▪ RED - Not required ▪ DTMF - Required ▪ Events 0-16 ▪ Silence Suppression - Not required	

B SIP Proxy Direct Routing Requirements

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.
27 World's Fair Drive,
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-12777