Configuration Note

AudioCodes Mediant™ Family of Media Gateways & Session Border Controllers

Connecting AudioCodes' SBC to Microsoft Teams Direct Routing with Local Media Optimization

Enterprise Model

Table of Contents

Notice

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

This document is subject to change without notice.

Date Published: June-12-2023

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes

Abbreviations and Terminology

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

Related Documentation

Document Name
Mediant 500 Gateway & E-SBC User's Manual
Mediant 500L Gateway & E-SBC User's Manual
Mediant 800 Gateway & E-SBC User's Manual
Mediant 1000B Gateway & E-SBC User's Manual
Mediant 2600 SBC User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
Gateway and SBC CLI Reference Guide
SIP Message Manipulation Reference Guide

Document Revision Record

LTRT	Description
33450	All information related to Local Media Optimization was removed from document 'Connecting AudioCodes' SBC to Microsoft Teams Direct Routing Enterprise Model' and included in this document. Added Appendix "AudioCodes ARM and SBCs with Teams Direct Local Media Optimization".
33451	Update for Message Manipulation rule towards Microsoft Teams.
33452	Updated parameter name.
33453	Update to SIP Trunk IP Profile and validated firmware version. Update to the Firewall Table Rules table with additional IP addresses for the new infrastructure DCs.
33454	Added section for overcoming problem of not playing music on hold during conversational transfer.
33455	Update to the Firewall Table Rules table due to new Microsoft requirements.
33456	Changed *Destination Type* in Table 2-31: SBC IP-to-IP Routing Rules.
33457	Updated parameters in Configuration Example: Teams IP Profile table.
33458	*Teams Direct Routing Mode* parameter added to the Teams IP Group in the Proxy SBC
33459	TLS Root Certificate Authority updated by Microsoft.
33520	Updated Classification Table with stricter rules to only allow for documented Microsoft SIP Proxies.
33521	Note added detailing deployment in Office 365 GCC DoD and GCC High environments.
33522	TLS Private Key size of 1024 was removed. Microsoft subnets were updated in the Classification and Firewall tables.

Documentation Feedback

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

1 Introduction

This document describes how to connect AudioCodes' SBC to Teams Direct Routing with Local Media Optimization and refers to the AudioCodes SBC configuration only.

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

This document is intended for IT or telephony professionals.

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

1.1 About Teams Direct Routing

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

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

1.2 Validated AudioCodes Version

Microsoft has successfully conducted validation tests with AudioCodes' Mediant SBC Ver. 7.40A.250. Previous certified firmware versions are 7.20A.258 and 7.40A.100. For an updated list, refer to *List of Session Border Controllers certified for Direct Routing*. 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: Infrastructure Prerequisites

Infrastructure Prerequisite	Details
Certified Session Border Controller (SBC)	See Microsoft's *Plan Direct Routing* document.
SIP Trunks connected to the SBC	
Office 365 Enterprise 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 Direct Routing Local Media Optimization

This chapter describes the Direct Routing Local Media Optimization Routing between Microsoft Phone System (Cloud PBX) and SBC devices.

- The implementation of this feature is **only relevant** for customers with site topology requiring **Local Media Optimization** solution
- SIP Signaling is always routed via the Microsoft Phone System Cloud PBX
- For Quick guidelines, see Appendix C "Configuration Quick Guidelines".

2.1 Introduction

The SBC supports the capability to optimize media flow between the Microsoft Phone System (Cloud PBX) and Direct Route SBC devices. It implements network policies for media traffic control flows paths between the Teams clients and the SBC devices for PSTN termination.

Enterprises consider PSTN voice as a business-critical application with high emphasis on voice quality. Media Path Optimization in Media Bypass mode for Direct Routing helps to better manage voice quality by enabling enterprises to do the following:

- Control how the media traffic flows between the Teams clients and customer SBCs;
- Allowing media streams between the Teams clients and SBCs even if SBCs are behind the corporate firewalls with private IPs and not directly visible to Microsoft.

By default, media bypass (referred to as Direct Media by the AudioCodes SBC application) is configured per SIP interface or per SBC device by the parameter Microsoft Teams PowerShell configured parameter MediaBypass (True or False). When enabled, media is routed directly between the Teams user and the SBC, bypassing the Microsoft Phone System Cloud PBX Media Relay or Media Proxy, on the condition that the client and the SBC media interface can establish a routed connection (verified during ICE negotiation).

Affectively this means that traffic does not need to route through an unnecessary loop. For example, the Teams user is in the same building and/or network as the SBC (the Teams client is inside the corporate network and has access to the Internal IP address of the SBC). Alternatively, if the Teams user is outside the corporate network and cannot reach the internal IP address of the SBC, then RTP media needs to pass via the Microsoft Phone System Cloud PBX.

The new functionality of Local Media Optimization uses an additional capability for the location of the Teams user device (for the inbound or the outgoing call). In other words, the SBC offers the correct interface for the media based on the user device location.

The handling is based on supplementary SIP headers supplied by Microsoft Teams HUB:

- **X-MS-UserLocation:** Indicates whether the Teams user is inside or outside the corporate network.
- **X-MS-MediaPath**: Indicates the FQDN of the SBC devices in the network that the call must traverse.
- **X-MS-UserSite:** Indicates the name of the network site

This case applies for the following topologies:

- A distributed mode (central SBC with remote branches with local breakouts)
- A single SBC in a corporate DMZ with two media interfaces (external and internal)

See detailed descriptions of these call scenarios below in Section 2.2.

2.2 Typical Call Scenarios

The following describes call scenarios that are implemented using this feature:

- When the destination SBC is the paired SBC (the call breaks out to the SIP Trunk which is connected to this SBC), determines whether the Teams user is calling from inside (internal) or outside the corporate network (external). If the Teams user is calling from inside the corporate network, RTP media flows via the SBC's internal media interface (internal media realm). If the Teams user is calling from outside the corporate network, media flows via the SBC's external media interface (regular media realm).
- When the destination SBC is not the paired SBC (in a distributed topology), determines whether RTP media should traverse it or directly terminate to the remote SBC. For example, when the Teams user is calling from inside the corporate network, located in the same branch as the remote SBC.

  The paired SBC serves as a proxy SBC for the downstream (remote) SBCs in the network, which are not directly connected to the Microsoft Phone System; however, are declared in Teams via a new PowerShell command (see below) to the Direct Routing interface. The downstream SBCs are configured on Microsoft Teams with Voice Routes.

2.2.1 Implemented Scenarios

This section describes the implemented scenarios.

2.2.1.1 Central SBC Scenario

In this scenario, all trunks are centralized with media flowing between the central SBC (Site HQ) and the users, based on the user's location. If user is internal, media flows between the internal IP of the central SBC (Site HQ) and the Teams client. If user is external, media flows between the external IP of the SBC and Teams client.

In this example, the administrator is paired to a single SBC (sbc4.contoso.com) to the service, the SBC has a centralized trunk connected to it. When the user is in the internal network, the SBC provides the internal IP of the SBC for media, when the user is outside the corporate network, the SBC provides the external (public) IP of the SBC.

Figure 1: Central SBC Traffic Flow - User at "Home" (Internal)

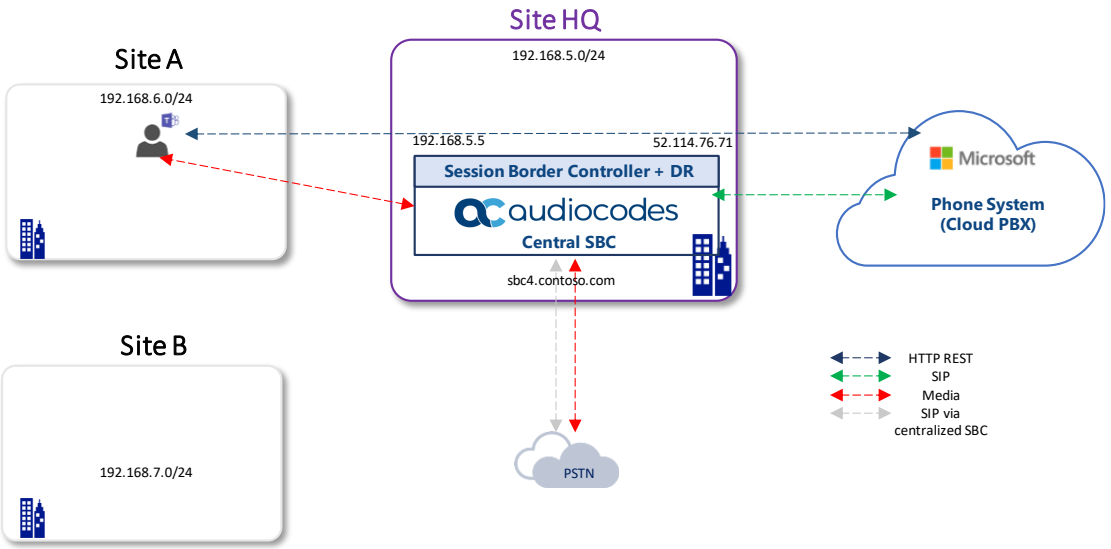
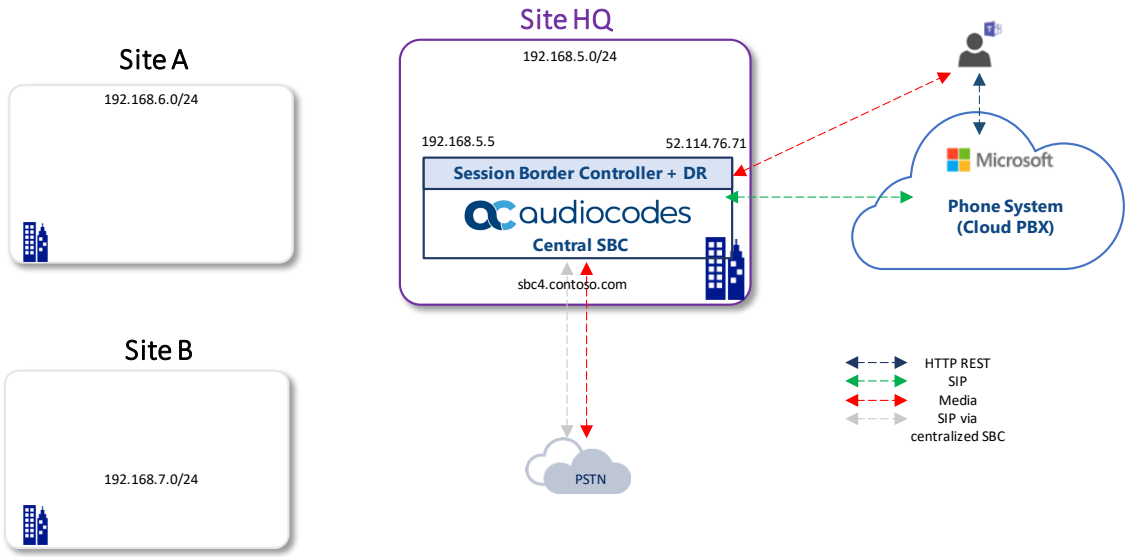


Figure 2: Central SBC Traffic Flow - User is External



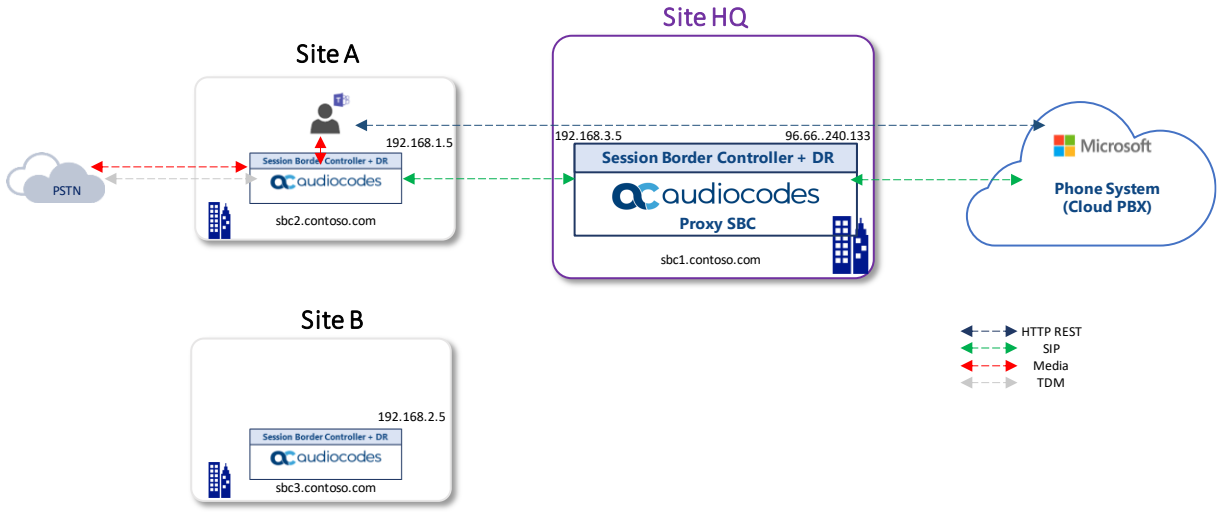
2.2.1.2 Proxy SBC Scenario

For this scenario, the administrator is paired only to a single SBC (sbc1.contoso.com) also referred to as the **Proxy SBC** to the Direct Routing service.

The administrator adds the downstream SBCs using PowerShell command *New-CsOnlinePSTNGateway* (or Via the UMP365 Online Voice Routing), indicating that they can be reached via the proxy SBC. The downstream SBC does not have a WAN interface (it is not configured with a public IP address), however can be assigned to voice routes.

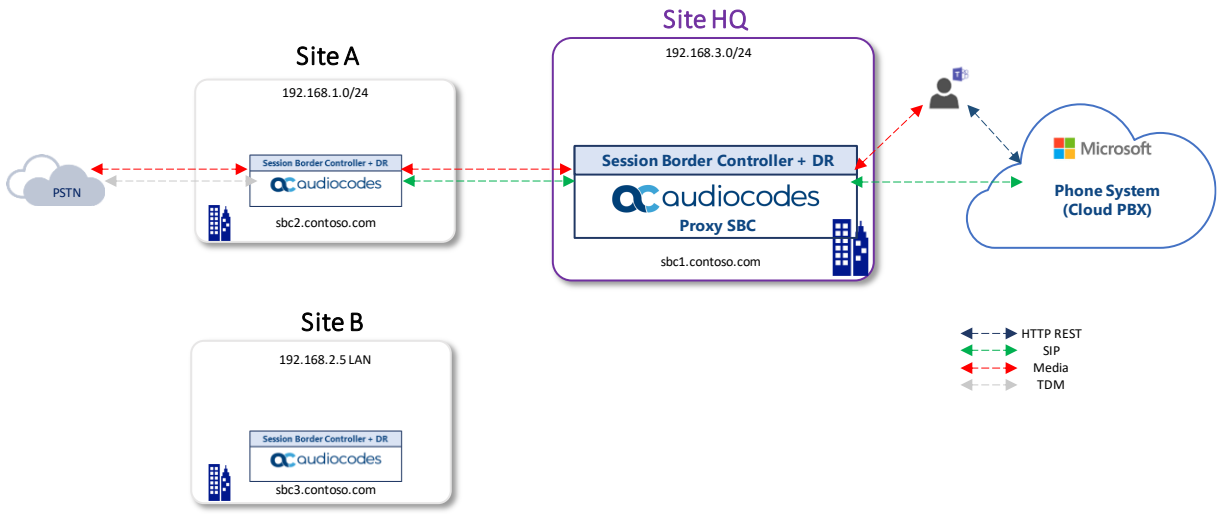
When a user is in an office where the downstream SBC is, the media traffic flows between the user and the SBC directly.

Figure 3: Proxy SBC Traffic Flow - user at "home" (Internal)



When a user is outside of the office (on a public internet or in a different office) the media flows from the user to the public IP of the Proxy SBC, which proxies it to the downstream SBC(s).

Figure 4: Proxy SBC Traffic Flow - user is external



2.2.1.3 Local Media Optimization Modes

Media Path Optimization technology in the Microsoft Teams network consists of two modes:

- **Always Bypass**: In the case where the Teams client is internal, the local media candidates of the target SBC will always be offered to the clients.
- **OnlyForLocalUsers**: The local media candidates of the target SBC is offered only if a user is in the same location as the SBC. For all other cases, either the local or external IP of the proxy SBC is offered.

2.3 Online PSTN Gateway Configuration

This section describes the Online PSTN Gateway configuration.

2.3.1 Online PSTN Gateway Configuration (Office 365) - Proxy SBC Scenario

- Run the following PowerShell commands on the Office 365, to configure the Proxy SBC PSTN Gateway on Teams Direct Routing:

New-CsOnlinePSTNGateway *-Identity* ***sbc1.contoso.com*** *-SipSignalingPort* ***5068*** *-ForwardCallHistory $True -ForwardPai $True -MediaBypass $True -Enabled $True*

Set-CsOnlinePSTNGateway *-BypassMode* ***alwaysbypass*** *(or* ***OnlyForLocalUsers****) -ProxySbc $null*

New-CsTenantTrustedIPAddress *-IPAddress {Public IP (After NAT)} -MaskBits {Subnet Mask Prefix} -Description "Description Text"*

- Run the following PowerShell commands (O365) for each remote SBC device:

New-CsOnlinePSTNGateway *-Identity* ***sbc2.contoso.com*** *-SipSignalingPort* ***5068*** *-ForwardCallHistory $True -ForwardPai $True -MediaBypass $True -Enabled $True*

Set-CsOnlinePSTNGateway *-BypassMode* ***alwaysbypass*** *(or* ***OnlyForLocalUsers****) -ProxySbc {ProxySBCFQDN} -GatewaySiteId {Location-based routing site-"site address"}*

New-CsTenantTrustedIPAddress *-IPAddress {Public IP (After NAT)} -MaskBits {Subnet Mask Prefix} -Description " Description Text "*

> Enabling Location-based routing policies is not Mandatory for LMO, instead only the assigning of the SBC devices to the sites is required, as shown in the above PowerShell command sets. If you would like to enable Location-based routing, refer to the configuration reference: https://docs.microsoft.com/en-us/microsoftteams/location-based-routing-enable

Based on the information above the Direct Routing will include three proprietary SIP Headers to SIP Invites and Re-invites.

2.3.2 Configuring Online PSTN Gateway Configuration via UMP 365 (Optional)

User Management Pack 365 (UMP) is a powerful software application that simplifies user lifecycle and identity management across Skype for Business Server, hosted, cloud, hybrid and Microsoft Teams deployments.

UMP offer Simple to use web-portal user interface, Under System Configuration, the following voice routing components can be configured for use with Microsoft Teams in a direct routing environment:

- Online Dial Plans
- Normalization rule templates for use within Dial Plans
- PSTN Gateways
- PSTN Usage records for use within Voice Routes and Voice Routing Policies
- Voice Routes
- Voice Routing Policies

> This Chapter is optional, UMP offer simple and easy to use WEB portal user interface that Alleviates need for PowerShell expertise (Chapter 4.3.1)

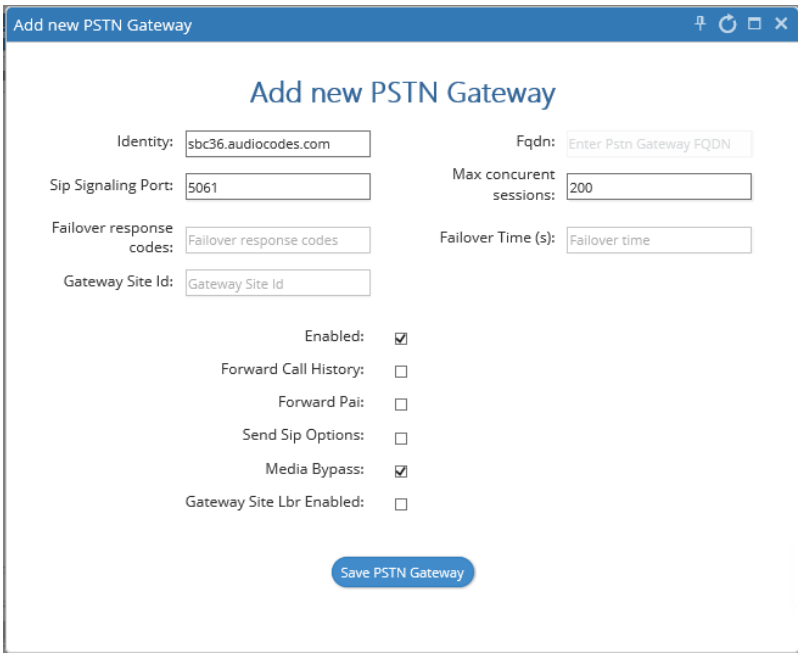
2.3.2.1 Creating PSTN Gateway

This section provides an example of how to create a new PSTN Gateway using the AudioCodes User Management Pack 365 install wizard:

To create a PSTN Gateway:

- Click Add new PSTN Gateway.

Figure 5: Add New PSTN Gateway



> For detailed description on Adding a PSTN Gateway, refer to LTRT-26685 AudioCodes User Management Pack 365 Release Notes Ver. 7.8.100.382.

2.4 Call Scenario Example Topologies

The following call scenario example topologies are shown in this section:

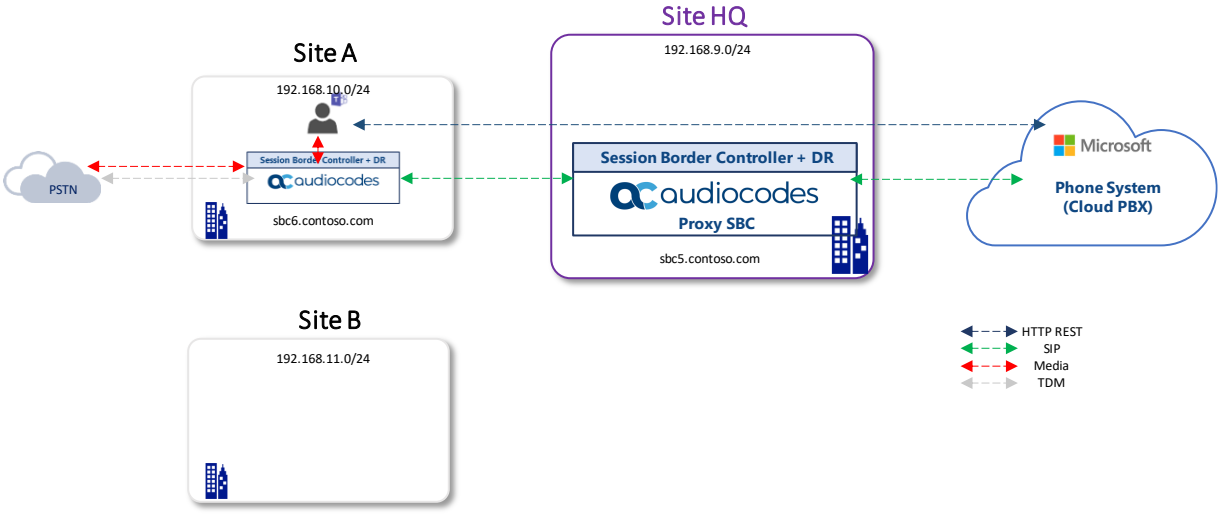
- Always Bypass with Internal Teams User (see Section 2.4.1)
- Always Bypass with External Teams User (see Section 2.4.2)
- Always Bypass with Teams User and SBC in Different Sites (see Section 2.4.3)
- Only for Local Users with Internal Teams User (see Section 2.4.4)
- Only for Local Users with External Teams User (see Section 2.4.5)
- Only for Local Users with Internal Teams User in Different Sites (see Section 2.4.6)

2.4.1 Always Bypass with Internal Teams User

This topology reflects when the Teams user is in the same location as the SBC inside the corporate network and *BypassMode* is configured to ***alwaysbypass***:

- The Teams user is located inside the corporate network "Internal" and places an Outbound call from the same location as the SBC – *BypassMode* is set to ***alwaysbypass***.
- The Teams user is located inside the corporate network "Internal" and places an Inbound call from the same location as the SBC.

Figure 6: Always Bypass with Internal Teams User

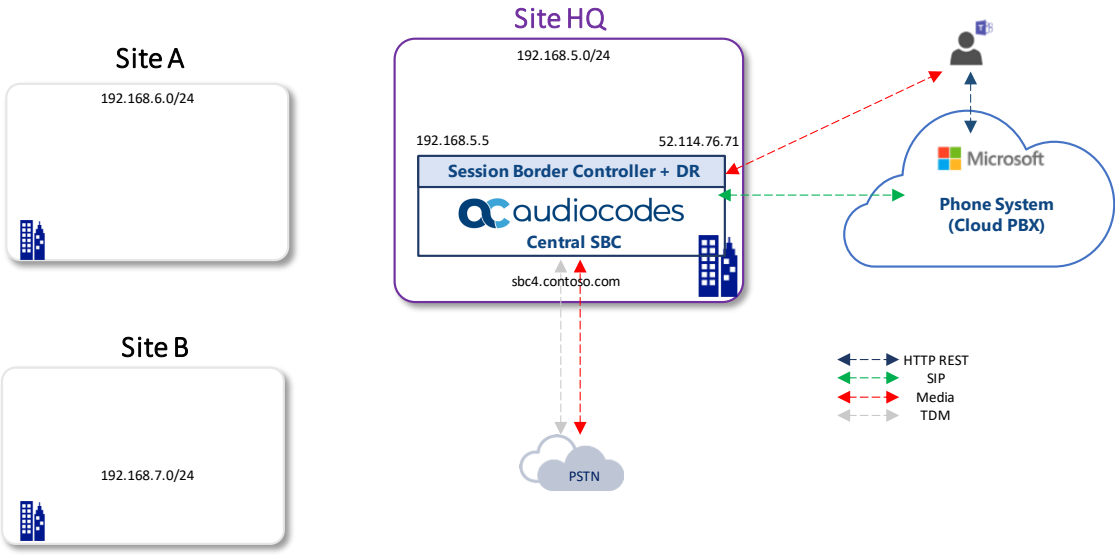


2.4.2 Always Bypass with External Teams User

This topology reflects when the Teams user is located outside the corporate network and *BypassMode is configured to **alwaysbypass**:*

- The Teams user is located outside the corporate network "External" and places an Outbound call – *BypassMode* is set to ***alwaysbypass***.
- The Teams user is located outside the corporate network "External" and places an Inbound call – *BypassMode* is set to ***alwaysbypass***.

Figure 7: Always Bypass with External Teams User

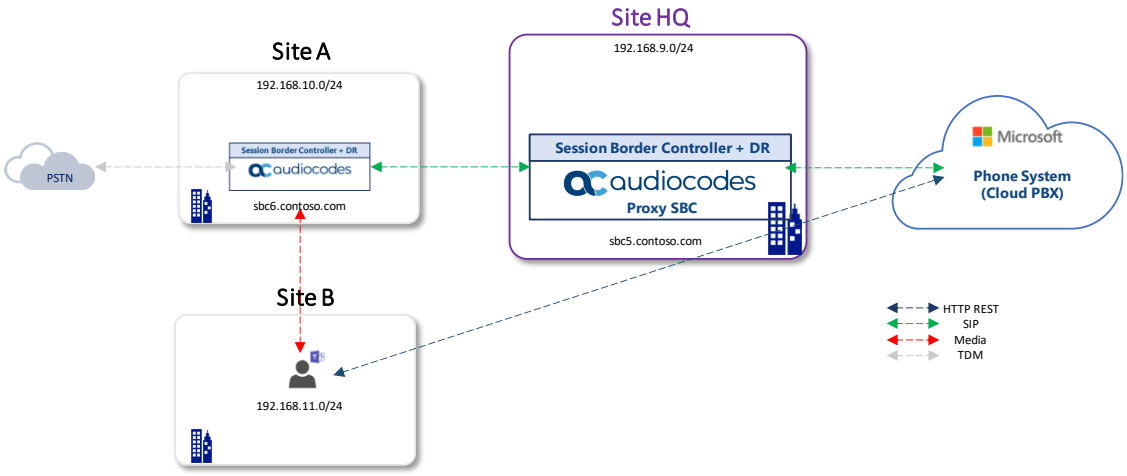


2.4.3 Always Bypass with Teams User and SBC in Different Sites

This topology reflects when the Teams user is in a different location to the branch SBC; however, located inside the corporate network and *BypassMode* is configured to ***alwaysbypass***:

- The Teams user device is inside the corporate network "Internal" and is in a different location to the branch SBC and places an Outbound call – *BypassMode* is set to ***alwaysbypass***.
- The Teams user device is inside the corporate network "Internal" and is in a different location to the branch SBC, receiving an Inbound call – *BypassMode* is set to ***alwaysbypass***.

Figure 8: Always Bypass with Teams User and SBC in Different Sites

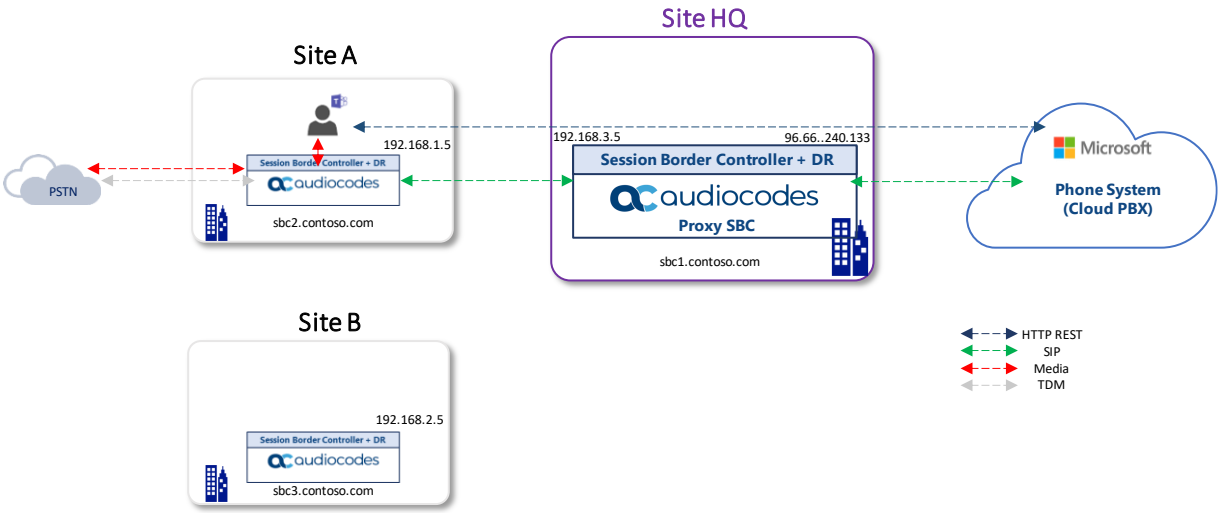


2.4.4 Only for Local Users with Internal Teams User

This topology reflects when the Teams user is in the same location as the SBC inside the corporate network and *BypassMode is configured to* ***OnlyForLocalUsers****:*

- The Teams user is "Internal" and in the same location as the target SBC, placing an Outbound call (handled the same as above as in Section 2.4.1) - *BypassMode* is set to ***OnlyForLocalUsers***.
- The Teams user is "Internal" and in the same location as the SBC (as above) making an Inbound call (handled the same as above as in Section 2.4.1) - *BypassMode* is set to ***OnlyForLocalUsers***.

Figure 9: Always Bypass with Internal Teams User



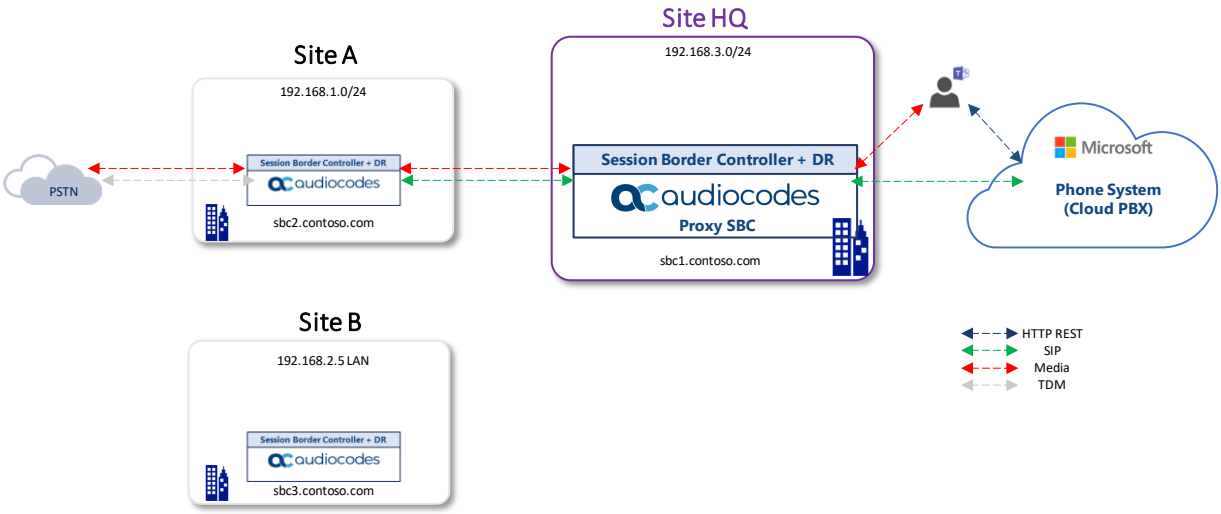
2.4.5 Only for Local Users with External Teams User

This topology reflects when the Teams user is located outside the corporate network and *BypassMode is configured to **OnlyForLocalUsers**:*

- (Outbound call) The Teams user is located outside the corporate network "External" and places an Outbound call – *BypassMode* is set to ***OnlyForLocalUsers***.

  In this case, the central SBC (Proxy SBC) always offers an external interface since the use is outside of the corporate network.
- The Teams user is located outside the corporate network "External" and receives an Inbound call – *BypassMode* is set to ***OnlyForLocalUsers***.

Figure 10: Only for Local Users with External Teams User

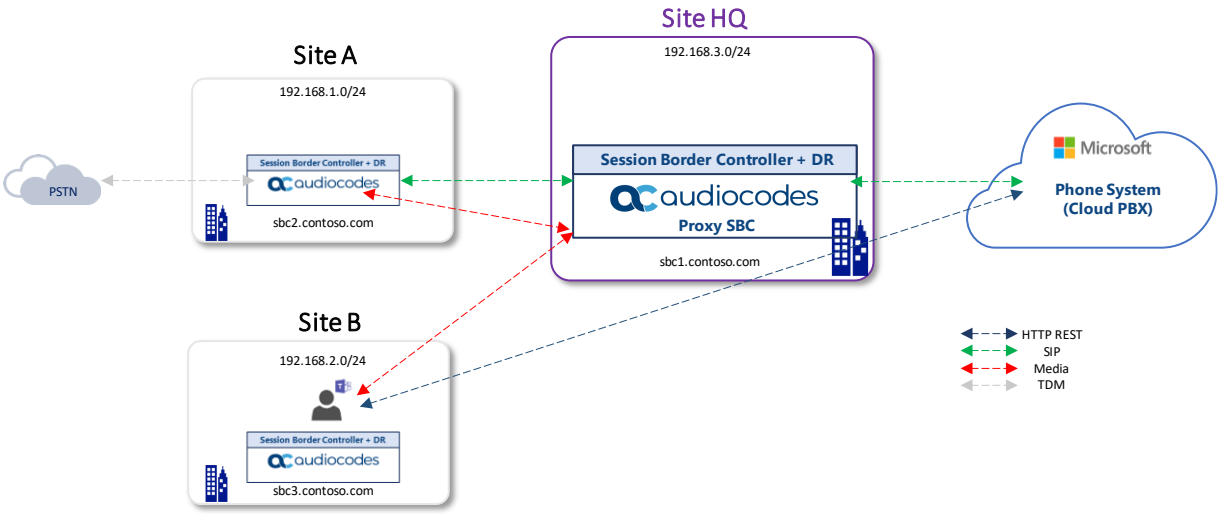


2.4.6 Only for Local Users with Internal Teams User in Different Sites

This topology reflects when the Teams User is in a different location to the branch SBC; however, located inside the corporate network and *BypassMode* is configured to ***OnlyForLocalUsers****:*

- The Teams user is inside the corporate network "Internal" and is in a different location to the branch SBC and places an Outbound call – *BypassMode* is set to ***OnlyForLocalUsers***.
- The Teams user is inside the corporate network "Internal" and is in a different location to the branch SBC, receiving an Inbound call – *BypassMode* is set to ***OnlyForLocalUsers***.

Figure 11: Only for Local Users with Internal Teams User in Different Sites



2.5 Configuring SBC for Local Media Optimization (LMO) Proxy SBC

This section describes the configuration required for supporting Local Media Optimization handling on the **Proxy SBC**.

> This document shows how to configure the connection between AudioCodes' SBC and the Teams Direct Routing with a generic SIP Trunk. For detailed configuration of other entities in the deployment such as the SIP Trunk Provider and the local IP-PBX, refer to AudioCodes' *SIP Trunk Configuration Notes* (in the interoperability suite of documents).

2.5.1 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 Office 365 tenants
- Public certificate issued by one of the supported CAs

2.5.2 About the SBC Domain Name

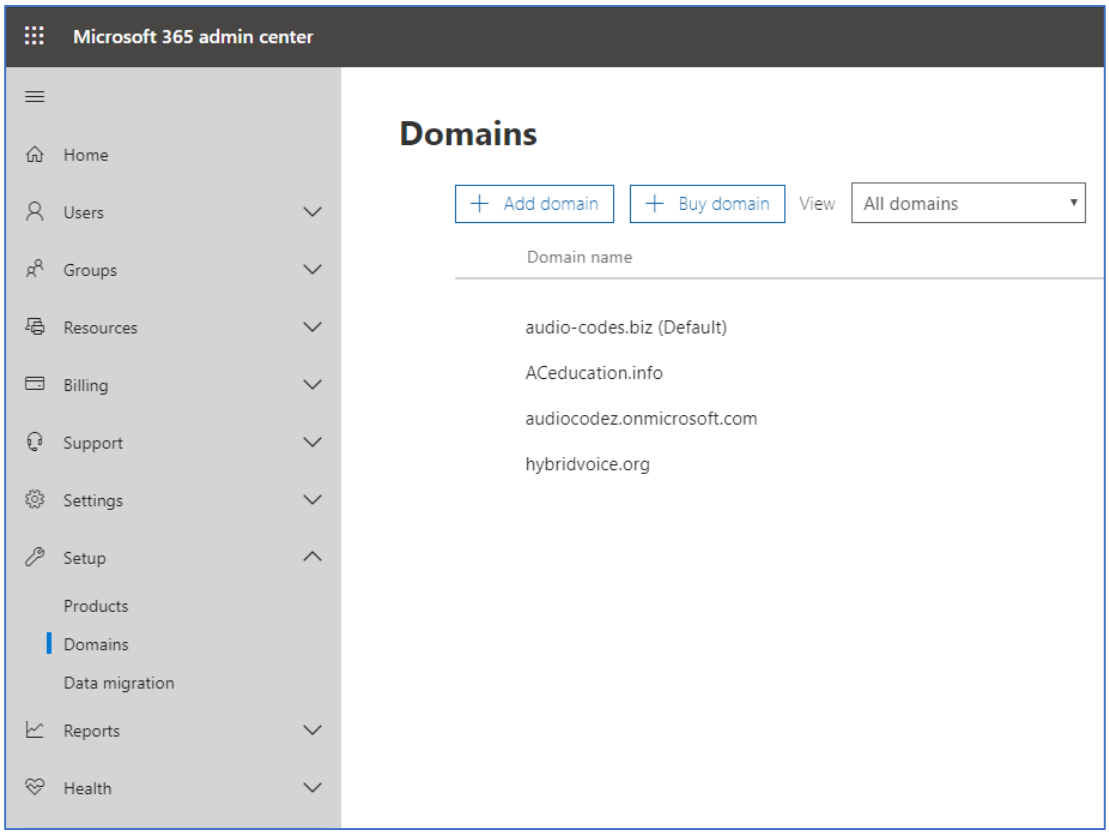
The SBC domain name must be from one of the names registered in 'Domains' of the tenant. You cannot use the ***.onmicrosoft.com** tenant for the domain name. For example, in Figure 2, the administrator registered the following DNS names for the tenant:

Table 2: DNS Names Registered by an Administrator for an Enterprise Office 365 Tenant

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

Users can be from any SIP domain registered for the 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 12: Example of Registered DNS Names



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

Public IP	FQDN Name
195.189.192.157	sbc.ACeducation.info

The certificate in the example is from DigiCert.

2.5.3 Validating AudioCodes' License

The following licenses are required on AudioCodes' device:

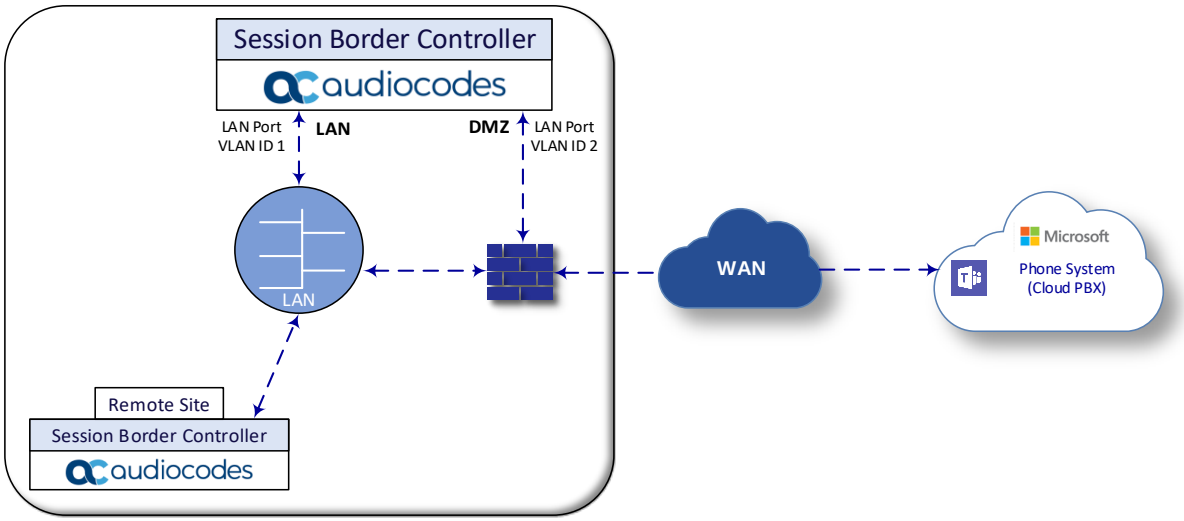
- **Enable Microsoft** (licensing MSFT) [All AudioCodes media gateways and SBCs are by default shipped with this license. Exceptions: MSBR products and Mediant 500 SBC or Media Gateways]
- **Enable TEAMS** (licensing SW/TEAMS)
- **Number of SBC sessions** [based on requirements]
- **Transcoding sessions** [if media transcoding is needed]
- **Coders** [based on requirements]

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

Figure 13: Network Interfaces in the Topology of the Proxy SBC



2.5.4.1 Validating Configuration of Physical Ports and Ethernet Groups

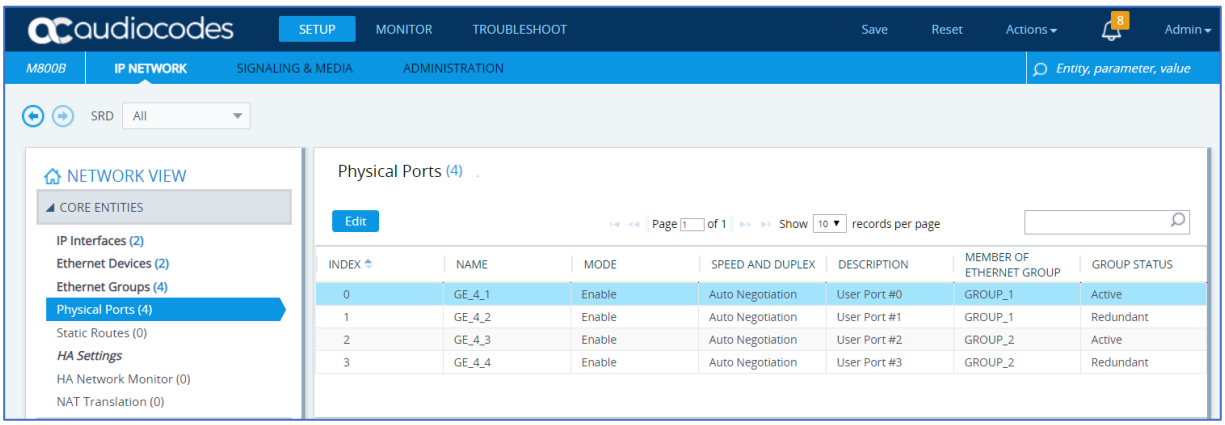
The physical ports are automatically detected by the SBC. The Ethernet groups are also auto-assigned to the ports. In this step, only parameter validation is necessary.

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.

> Based on your hardware configuration, you might have more than two ports.

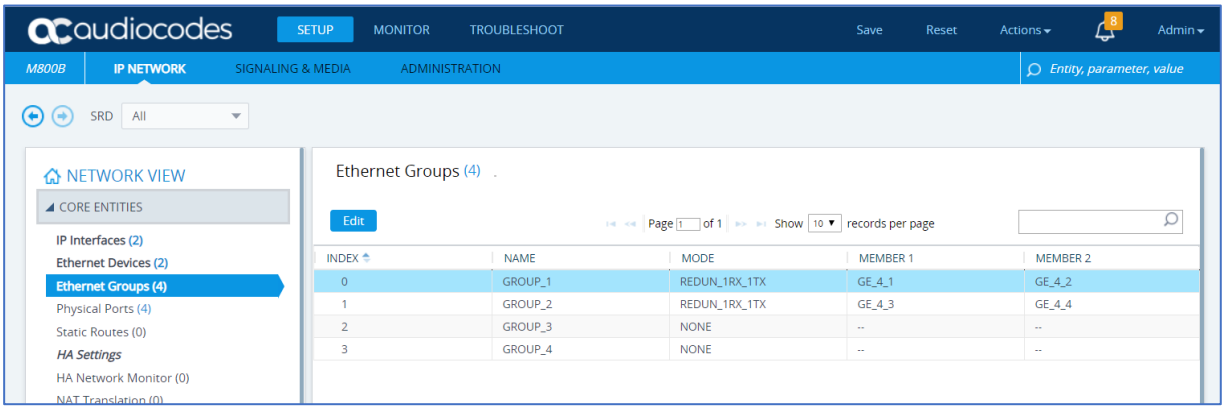
Figure 14: Physical Ports Configuration Interface



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 15: Ethernet Groups Configuration Interface



2.5.4.2 Configuring LAN and WAN VLANs

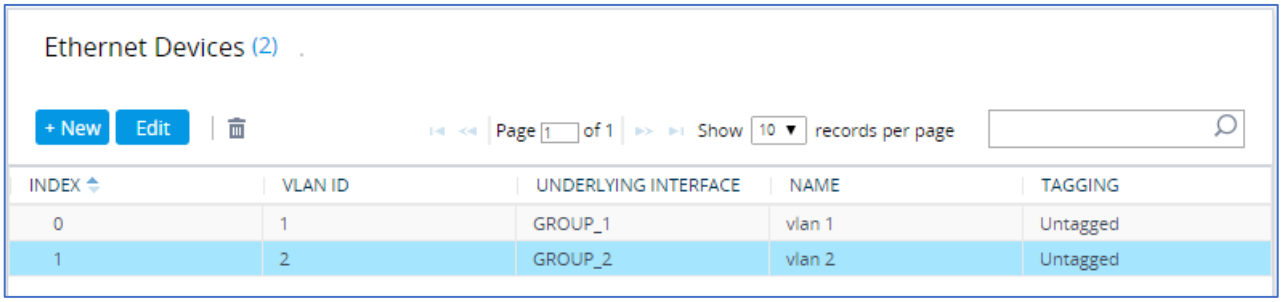
This section describes how to define VLANs for each of the following interfaces:

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

To configure the VLANs:

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

Figure 16: Configured VLAN IDs in Ethernet Device



2.5.4.3 Configuring Network Interfaces

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

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

To configure network parameters for both LAN and WAN interfaces:

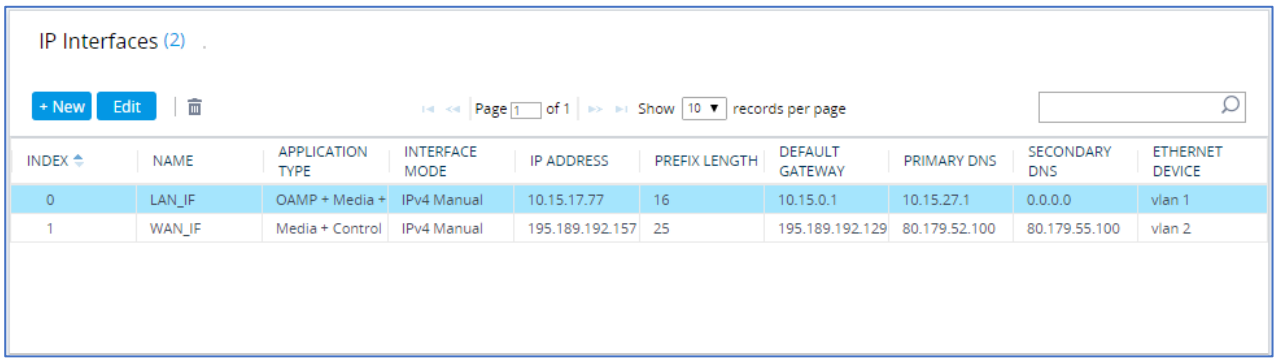
1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Configure the IP interfaces as follows (your network parameters might be different):

Table 3: Configuration Example of the Network Interface Table

Index	Name	Application Types	Interface Mode	IP Address	Prefix Length	Gateway	DNS	Ethernet Device
0	LAN_IF	OAMP+ Media + Control	IPv4 Manual	10.15.77.77	16	10.15.0.1	10.15.27.1	vlan 1
1	WAN_IF	Media + Control (as this interface points to the internet, enabling OAMP is not recommended)	IPv4 Manual	195.189.192.157 (DMZ IP address of SBC)	25	195.189.192.129 (router's IP address)	According to your Internet provider's instructions	vlan 2

The configured IP network interfaces are shown below:

Figure 17: Configuration Example of the Network Interface Table



2.5.5 Configuring 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

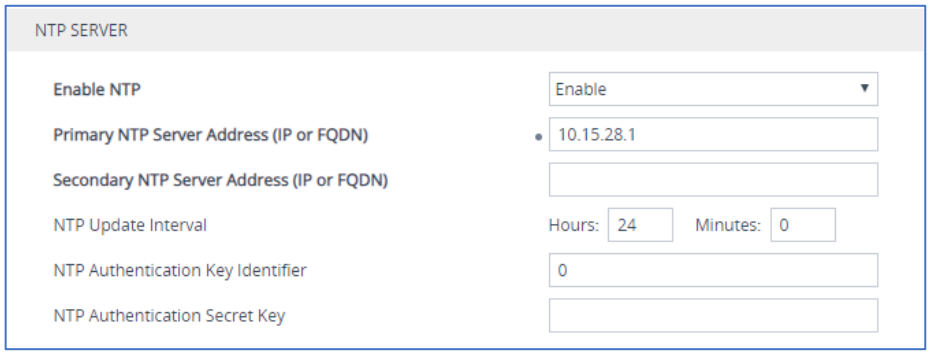
2.5.5.1 Configuring the NTP Server Address

This section describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or another global server) to ensure that the SBC receives the current date and time. This is necessary for validating certificates of remote parties. It is important, that NTP Server will locate on the OAMP IP Interface (LAN_IF in our case) or will be accessible through it.

To configure the NTP server address:

1. Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**).
2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., 10.15.28.1).

Figure 18: Configuring NTP Server Address



3. Click **Apply**.

2.5.5.2 Creating a TLS Context for Teams Direct Routing

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

The procedure involves the following main steps:

a. Creating a TLS Context for Teams Direct Routing.

b. Generating a Certificate Signing Request (CSR) and obtaining the certificate from a supported Certification Authority.

c. Deploying the SBC and Root/ Intermediate certificates on the SBC.

To create a TLS Context for Teams Direct Routing:

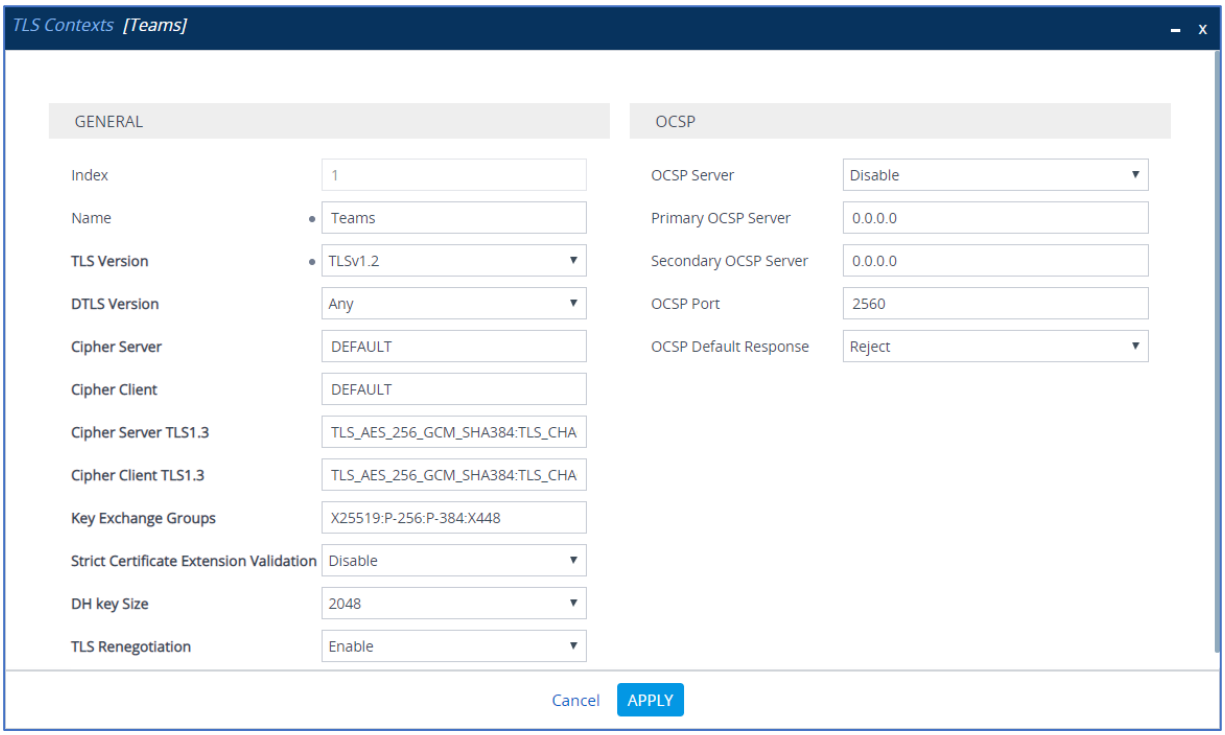
1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. Create a new TLS Context by clicking **+New** at the top of the interface, and then configure the parameters using the table below as reference.

Table 4: New TLS Context

Index	Name	TLS Version
1	Teams (arbitrary descriptive name)	TLSv1.2
All other parameters can be left unchanged with their default values.		

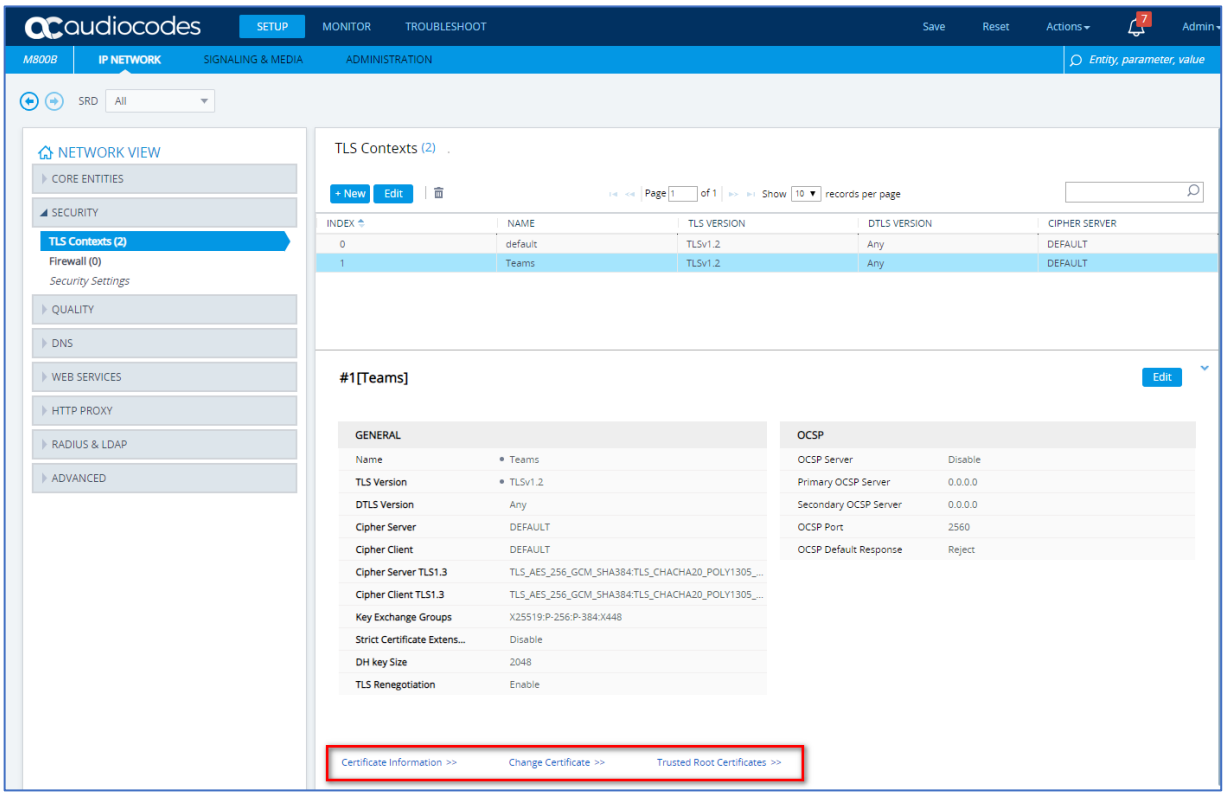
The table above exemplifies configuration focusing on interconnecting SIP and media. You might want to configure additional parameters according to your company's policies. For example, you might want to configure Online Certificate Status Protocol (OCSP) to check if SBC certificates presented in the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

Figure 19: 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 20: Configured TLS Context for Direct Routing and Interface to Manage the Certificates



2.5.5.3 Generating a CSR and Obtaining the Certificate from a Supported CA

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

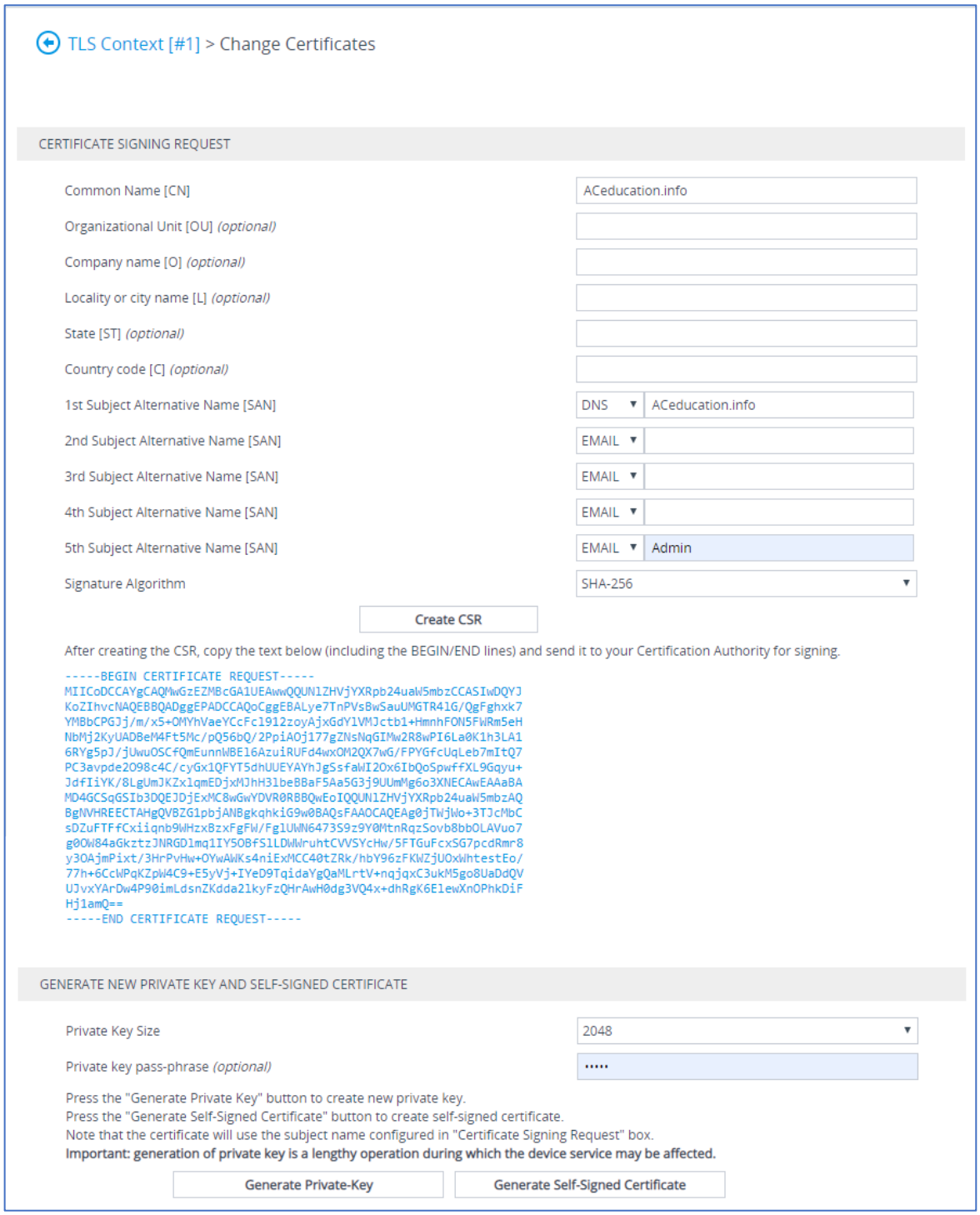
To generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority:

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the Teams TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
3. Under the **Certificate Signing Request** group, do the following:
   a. In the 'Common Name [CN]' field, enter the SBC FQDN name (based on example above, **ACeducation.info**).
   b. In the '1st Subject Alternative Name [SAN]' field, change the type to 'DNS', and then enter the SBC FQDN name (based on the example above, **ACeducation.info**).

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

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

Figure 21: Example of Certificate Signing Request – Creating CSR



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

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

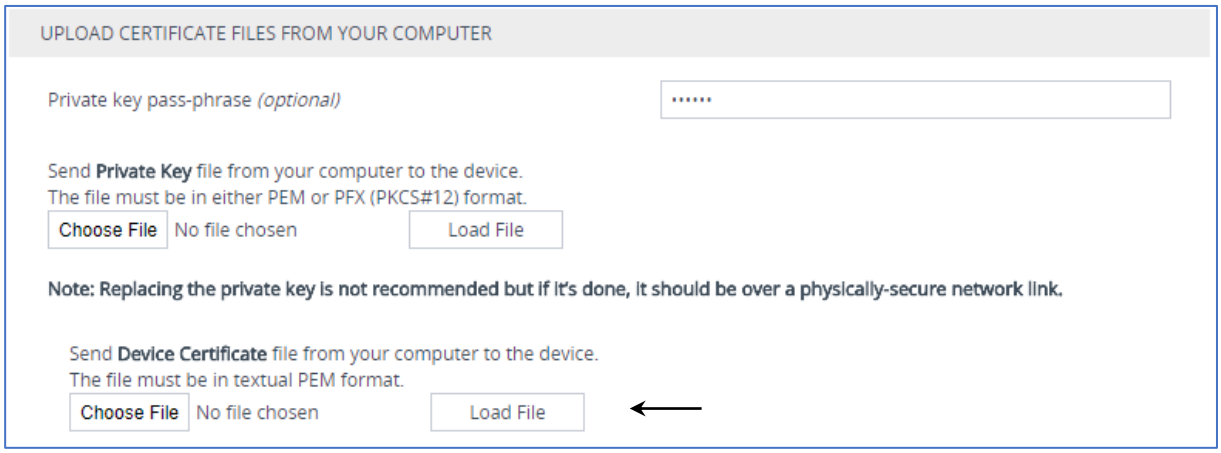
After obtaining the SBC signed and Trusted Root/Intermediate Certificate from the CA, install the following:

- SBC certificate
- Root / Intermediate certificates

To install the SBC certificate:

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

Figure 22: Uploading the Certificate Obtained from the Certification Authority

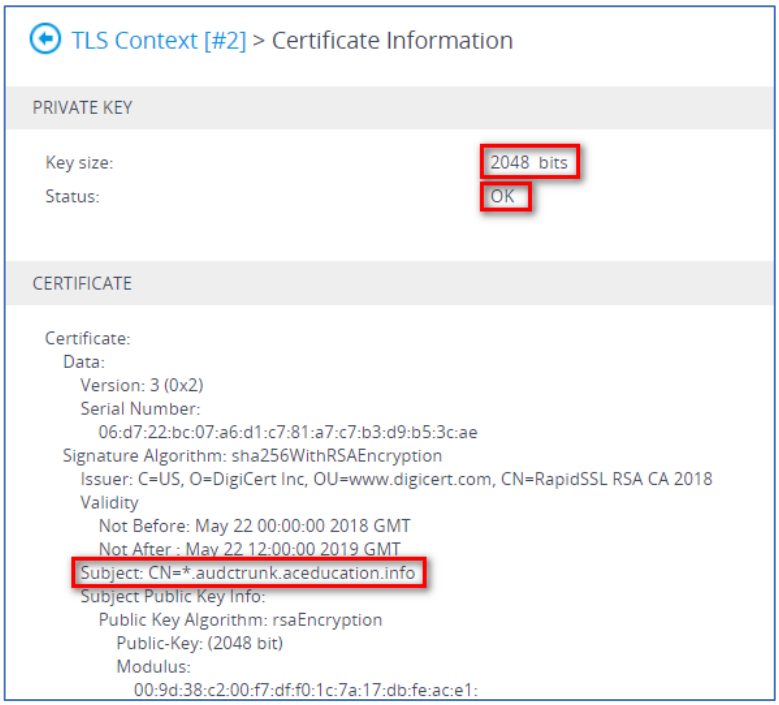


2. Validate that the certificate was uploaded correctly: A message indicating that the certificate was uploaded successfully is displayed in blue on the lower part of the page:

Figure 23: Message Indicating Successful Upload of the Certificate

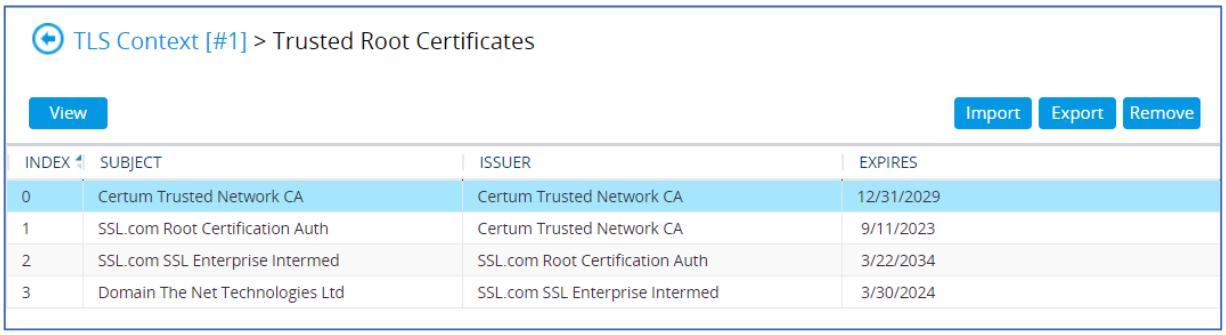
3. In the SBC's Web interface, return to the **TLS Contexts** page, select the required TLS Context index row, and then click the **Certificate Information** link, located at the bottom of the TLS. Then validate the Key size, certificate status and Subject Name:

Figure 24: Certificate Information Example



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

Figure 25: Example of Configured Trusted Root Certificates



2.5.6 Method for Generating and Installing the Wildcard Certificate

To use the same certificate on multiple devices, you may prefer using 3rd party application (e.g., DigiCert Certificate Utility for Windows) to process the certificate request from your Certificate Authority on another machine, with this utility installed.

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

To install the certificate:

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
3. Scroll down to the **Upload certificates files from your computer** group and do the following:
   a. Enter the password assigned during export with the DigiCert utility in the **'Private key pass-phrase**' field.
   b. Click the **Choose File** button corresponding to the 'Send **Private Key**...' field and then select the SBC certificate file exported from the DigiCert utility.

2.5.7 Deploying Trusted Root Certificate for MTLS connection

Loading Trusted Root Certificates to AudioCodes' SBC is mandatory when implementing an MTLS connection with the Microsoft Teams network.

Microsoft 365 is updating services powering messaging, meetings, telephony, voice, and video to use TLS certificates from a different set of Root Certificate Authorities (CAs). For more details of the new Root CAs, refer to Microsoft technical guidance at Office TLS Certificate Changes. Services began transitioning to the new Root CAs (e.g., DigiCert) beginning in January 2022 and will continue through October 2022. During this migration period, it's possible to load both the old (Baltimore) and the new (DigiCert) Root certificate to the same TLS Context.

The DNS name of the Teams Direct Routing interface is **sip.pstnhub.microsoft.com**. In this interface, a certificate is presented which is signed by **DigiCert** with:

Serial Number: 0x033af1e6a711a9a0bb2864b11d09fae5,
SHA-1 Thumbprint: DF3C24F9BFD666761B268073FE06D1CC8D4F82A4 and
SHA-256 Thumbprint: CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F.

To trust this certificate, your SBC *must* have the certificate in Trusted Certificates storage. Download the **DigiCert Global Root G2** (df3c) certificate in **PEM format** from https://www.digicert.com/kb/digicert-root-certificates.htm and follow the steps above to import the certificate to the Trusted Root storage.

Before importing the DigiCert Root Certificate into AudioCodes' SBC, make sure it's in .PEM or .PFX format. If it isn't, you need to convert it to .PEM or .PFX format, otherwise the 'Failed to load new certificate' error message is displayed. To convert to PEM format, use Windows local store on any Windows OS and then export it as 'Base-64 encoded X.509 (.CER) certificate'.

2.5.8 Configuring Media Realms

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

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

To configure Media Realms:

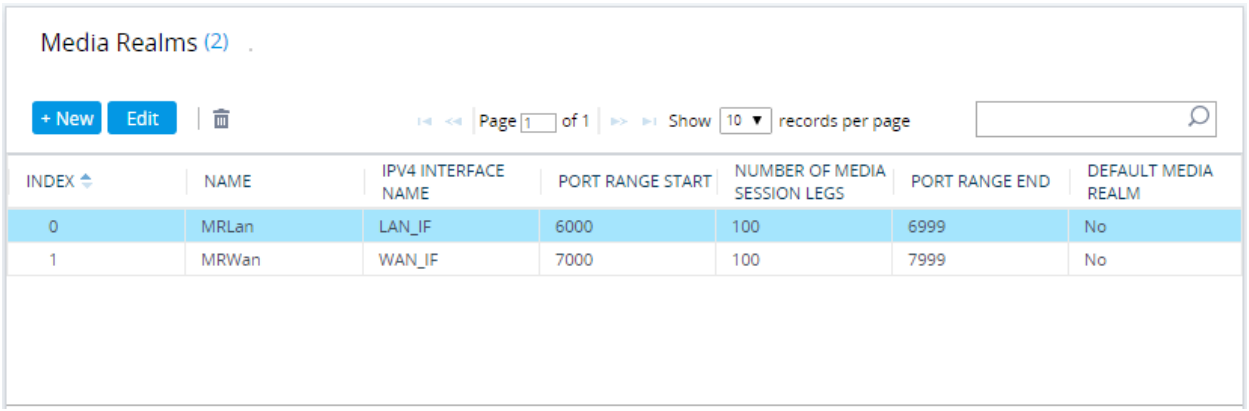
1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Configure Media Realms as follows (you can use the default Media Realm (Index 0), but modify it):

Table 5: Configuration Example Media Realms in Media Realms Table

Index	Name	Topology Location	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
0	MRLan (arbitrary name)		LAN_IF	6000	100 (media sessions assigned with port range)
1	MRWan (arbitrary name)	Up	WAN_IF	7000	100 (media sessions assigned with port range)

The configured Media Realms are shown in the figure below:

Figure 26: Configuration Example Media Realms in Media Realm Table



2.5.9 Configuring SIP Signaling Interfaces

This section shows how to configure a SIP Signaling Interfaces. A SIP Interface defines a listening port and type (UDP, TCP, or TLS) for SIP signaling traffic on a specific logical IP network interface (configured in the Interface Table above) and Media Realm.

Note that the configuration of a SIP interface for the SIP Trunk shows as an example and your configuration might be different. For specific configuration of interfaces pointing to SIP trunks and/or a third-party PSTN environment connected to the SBC, see the trunk / environment vendor documentation.

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

To configure SIP Interfaces:

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

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

Table 6: Configuration Example of SIP Signaling Interfaces

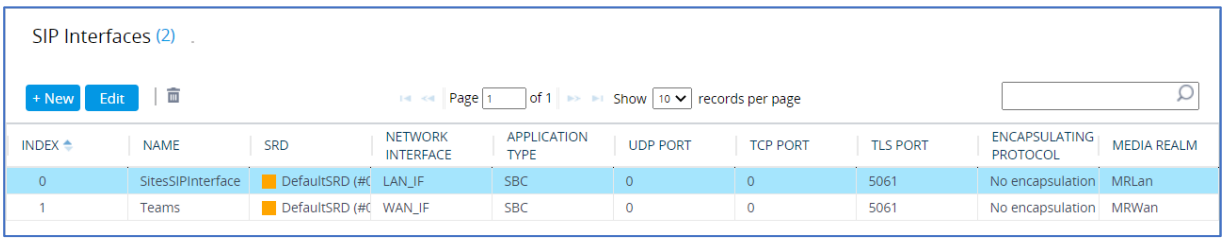
Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepalive	Classification Failure Response Type	Media Realm	TLS Context Name
0	SitesSIPInterface (arbitrary name)	LAN_IF	SBC	0	0	5061 (according to site requirement)	Disable (leave default value)	500 (leave default value)	MRLan	-
1	Teams (arbitrary name)	WAN_IF	SBC	0 (Phone System does not use UDP or TCP for SIP signaling)	0	5061 (as configured in the Office 365)	Enable	0 (Recommended to prevent DoS attacks)	MRWan	Teams

> For implementing an MTLS connection with the Microsoft Teams network, configure 'TLS Mutual Authentication' to "Enable" for the Teams SIP Interface.

> Loading DigiCert Trusted Root Certificates to AudioCodes' SBC is mandatory for implementing an MTLS connection with the Microsoft Teams network. Refer to Section 2.5.7 on page 27.

The configured SIP Interfaces are shown in the figure below:

Figure 27: Configuration Example of SIP Signaling Interfaces



2.5.10 Configuring Proxy Sets and Proxy Address

The Proxy Set and Proxy Address defines TLS parameters, IP interfaces, FQDN and the remote entity's port. Proxy Sets can also be used to configure load balancing between multiple servers. The example below covers configuration of a Proxy Sets for Teams Direct Routing and SIP Trunk. Note that the configuration of a Proxy Set for the SIP Trunk (through Site A SBC) shows as an example and your configuration might be different. For specific configuration of interfaces pointing to SIP trunks and/or the third-party PSTN environment connected to the SBC, see the trunk/environment vendor's documentation. AudioCodes also offers a comprehensive suite of documents covering the interconnection between different trunks and the equipment. The Proxy Sets will later be applied to the VoIP network by assigning them to IP Groups.

2.5.10.1 Configuring Proxy Sets

To support the Local Media Optimization handling, the Proxy Set that is paired as the Microsoft Teams Direct Routing interface is configured with an FQDN Host Name and each deployed remote (site) SBC is configured with an IP address.

To configure a Proxy Sets:

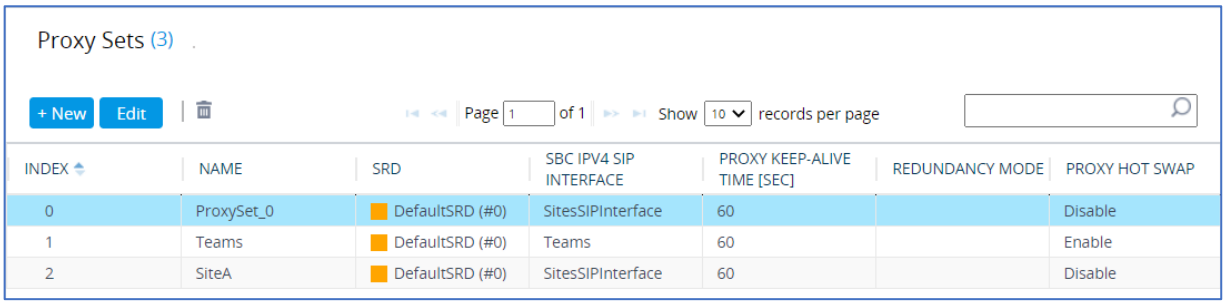
1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Configure Proxy Sets as shown in the table below:

Table 7: Configuration Example Proxy Sets in Proxy Sets Table

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

The configured Proxy Sets are shown in the figure below:

Figure 28: Configuration Example Proxy Sets in Proxy Sets Table



2.5.10.2 Configuring Proxy Addresses

This section shows how to configure the Proxy Addresses for the Proxy Sets in the Proxy SBC site towards the remote (site) SBC.

To configure a Proxy Address for Teams:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **Teams**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**;
3. Configure the address of the Proxy Set according to the parameters described in the table below:

Table 8: Configuration Proxy Address for Teams Direct Routing

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	sip.pstnhub.microsoft.com:5061	TLS	1	1
1	sip2.pstnhub.microsoft.com:5061	TLS	2	1
2	sip3.pstnhub.microsoft.com:5061	TLS	3	1

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

> If the SBC is deployed in Office 365 GCC DoD or GCC High environments, please contact AudioCodes deployment services, since these environments have different configurations (FQDNs) than the public Office 365 environment.

To configure a Proxy Address for remote (site) SBCs:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **SIPTrunk**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**;
3. Configure the IP address of the Proxy Set towards Remote SBC in Site A according to the parameters described in the table below:

Table 9: Configuration Proxy Address Towards Remote SiteA SBC

Index	Proxy Address	Transport Type
0	192.168.1.5:5061	TLS

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

2.5.11 Configuring Coder Groups

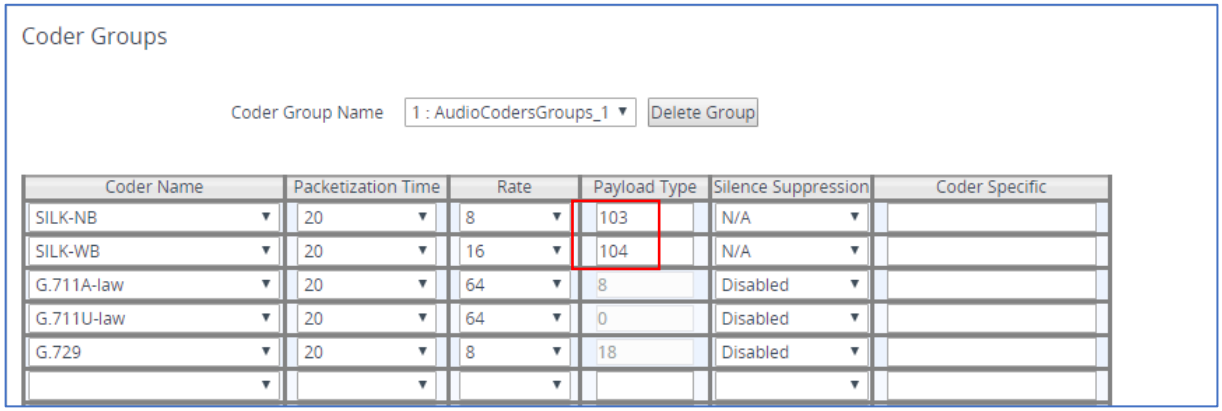
This section describes how to configure coders (known as *Coder Groups*). Teams Direct Routing supports the SILK and other coders while the network connection to the SIP Trunk may restrict operation with a dedicated coders list. You need to add a Coder Group with the supported coders for each of the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

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

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 29: Configuring Coder Group for Teams Direct Routing



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

2.5.12 Configuring IP Profiles

This section describes how to re-configure an IP Profiles in the Proxy SBC site. An IP Profile is a set of parameters with user-defined settings related to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder type). An IP Profile needs to be assigned to the specific IP Group. See Appendix C for a summary of all IP Profile configurations.

To configure IP Profiles Proxy SBC site:

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

Table 10: Configuration Example: Teams IP Profile

Parameter	Value
General	
Name	**Teams** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Secured**
SBC Early Media	
Remote Early Media RTP Detection Mode	**By Media** (required, as Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18x response)
SBC Media	
Extension Coders Group	**AudioCodersGroups_1**
RTCP Mode	**Generate Always** (required, as some ITSPs do not send RTCP packets during Hold, but Microsoft expects them)
ICE Mode	**Lite** (required only when Media Bypass enabled on Teams)
SBC Signaling	
SIP UPDATE Support	**Not Supported**
Remote re-INVITE Support	**Supported Only With SDP**
Remote Delayed Offer Support	**Not Supported**
Remote Representation Mode	**Add Routing Headers**
SBC Forward and Transfer	
Remote REFER Mode	**Regular**
Remote 3xx Mode	**Transparent**
SBC Hold	
Remote Hold Format	**Inactive** (some SIP Trunk may answer with a=inactive and IP=0.0.0.0 in response to the Re-Invite with Hold request from Teams. Microsoft Media Stack doesn't support this format. So, SBC will replace 0.0.0.0 with its IP address)
All other parameters can be left unchanged at their default values.	

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

4. Click **+New** to add the IP Profile for the SIP Trunk (through Site A SBC). Configure the parameters using the table below as a reference.

Table 11: Configuration Example: SIP Trunk IP Profile (toward remote Site A SBC)

Parameter	Value
General	
Name	**SiteA** (arbitrary name)
SBC Forward and Transfer	
Remote REFER Mode	**Regular**
Remote Replaces Mode	**Standard**
Remote 3xx Mode	**Transparent**
All other parameters can be left unchanged with their default values.	

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

2.5.13 Configuring IP Groups

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

To configure IP Group for Microsoft Teams Direct Routing for Media optimization:

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Click **Edit** to re-configure the IP Group for the Microsoft Teams Direct Routing paired SBC (Proxy SBC):

Table 12: Configuration Example: IP Group for Microsoft Teams Direct Routing

Parameter	Value
Name	**Teams** (arbitrary name)
Topology Location	**Up**
Type	**Server**
Proxy Set	**Teams**
IP Profile	**Teams**
Media Realm	**MRWan**
Internal Media Realm	**MRLan** This parameter is relevant when the 'Teams Local Media Optimization Handling' parameter (see below) is configured to any value other than "None" and the X-MS-UserLocation header in the incoming SIP message is set to 'Internal'. In this case, the Internal Media Realm determines the UDP port range and maximum sessions for Media traffic on this IP interface. If X-MS-UserLocation=Internal response is received from Teams, a new IP address/port is allocated using the Internal Media Realm only if the call is non-direct media i.e. media traverses the paired SBC to the remote SBCs.
Classify by Proxy Set	**Disable**
Local Host Name	**<FQDN name of the SBC in the enterprise tenant>** For example, *sbc.ACeducation.info* defines the host name (string) that the device uses in the SIP message's Via and Contact headers. This defines the FQDN as the host name that is recognized by Microsoft Teams. 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 the other configured IP Groups (SiteA and SiteB).
Teams Direct Routing Mode	**Enable** (Enables the SBC to include Microsoft's proprietary X-MS-SBC header in outgoing SIP INVITE and OPTIONS messages, in a Microsoft Teams Direct Routing environment. The header is used by Microsoft Teams to identify vendor equipment. The header's value is in the format 'Audiocodes/<model>/<firmware>').
Always Use Src Address	**Yes**
Teams Local Media Optimization Handling	**Teams Decides** (The routing decision is made according to the Microsoft Teams headers for the primary route)

Parameter	Value
Teams Local Media Optimization Initial Behavior	This parameter is relevant for inbound calls to Teams when "Teams Local Media Optimization Handling" is set to "Teams Decides" or "SBC Decides": ■ **Direct Media** (default) – Perform direct media call towards Teams. ■ **Internal** - Perform non-direct media call (media traverses the paired SBC from the remote SBC) towards Teams using Internal Media Realm. ■ **External** – Perform non-direct media call (media traverses the paired SBC from the remote SBC) towards Teams using external (regular) Media Realm. ■ **Note:** The value of this parameter can be variable depending on particular setup
Proxy Keep-Alive using IP Group settings	**Enable**
Inbound Message Manipulation Set	**0**
Outbound Message Manipulation Set	**1**
Call Setup Rules Set ID	**0**
All other parameters can be left unchanged with their default values.	

3. Click **+New** to add the IP Group for the SBC located at Site A and connected to the SIP Trunk. Configure the parameters using the table below as reference:

Table 13: Configuration Example: IP Group for Site A SBC

Parameter	Value
Name	**SiteA** (arbitrary name)
Topology Location	**Down**
Type	**Server**
Proxy Set	**SiteA**
IP Profile	**SiteA**
Media Realm	**MRLan**
Tags	**Site={RemotePSTNGateWayFQDN}**
All other parameters can be left unchanged with their default values.	

The Site Tag should be defined as the **remote** site SBC's FQDN and should be discoverable by DNS from the Proxy SBC.

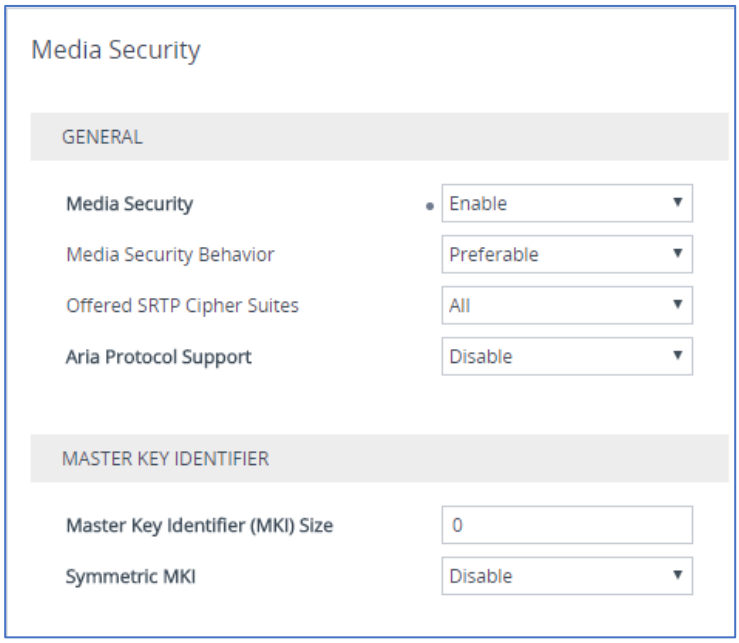
2.5.14 Configuring SRTP

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

To configure media security:

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

Figure 30: Configuring Media Security Parameter



3. Click **Apply**.

2.5.15 Configuring Message Condition Rules

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

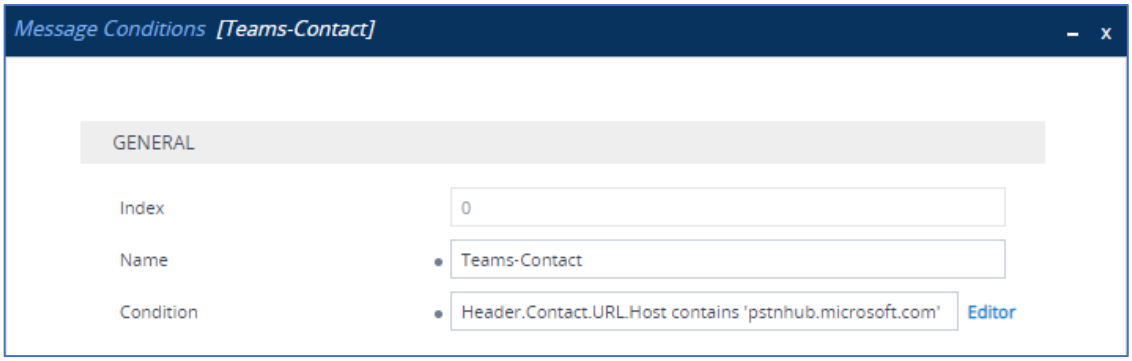
The following condition verifies that the Contact header contains Teams FQDN.

To configure a Message Condition rule:

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

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

Figure 31: Configuring Condition Table



3. Click **Apply**.

2.5.16 Configuring Classification Rules

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

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

To configure a Classification rule:

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

Table 14: Classification Rules

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

3. Click **Apply**.

2.5.17 Configuring Call Setup Rules

This section describes how to configure Call Setup Rules based on the site hostname, extracted from the Request-URI header. Call Setup rules define various sequences (site destination in this case) that are run upon receipt of an incoming call (dialog) at call setup, before the device routes the call to its destination.

Configured Call Setup Rules need be assigned to specific IP Group.

To configure a Call Setup Rules based on Site FQDN:

1. Open the Call Setup Rules table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Call Setup Rules**).
2. Click **New**
3. Configure a Call Setup rule according to the parameters described in the table below.

Table 15: Call Setup Rules Table

Index	Rules Set ID	Condition	Action Subject	Action Type	Action Value
0	0	Var.Session.0 == ''	Var.Session.0	Modify	Header.Request-URI.URL.Host.Name
1	0	Var.Session.0 != ''	DstTags.Site	Modify	Var.Session.0

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

2.5.18 Configuring Message Manipulation Rules

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

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

To configure SIP message manipulation rules:

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 0) for Teams IP Group. This rule applies to messages received from the Teams IP Group. This remove the privacy header to enable CLI identity.

Parameter	Value
Index	**0**
Name	**Privacy Header**
Manipulation Set ID	**0**
Condition	**Header.Privacy contains 'id'**
Action Subject	**Header.Privacy**
Action Type	**Remove**

3. Configure another manipulation rule (Manipulation Set 1) for Teams IP Group. This rule applies to messages sent to the Teams IP Group. This replaces the host part of the Contact Header with the value from the To Header.

Parameter	Value
Index	**1**
Name	**Replace Host in Contact**
Manipulation Set ID	**1**
Message Type	**Invite.Request**
Action Subject	**Header.Contact.URL.Host**
Action Type	**Modify**
Action Value	**Header.To.URL.Host**

4. Configure a new manipulation rule (Manipulation Set 2) for Teams IP Group. This rule applies to messages sent towards the Teams IP Group. This rule adds a routing policy rule towards Microsoft for handling different call forwarding scenarios (according to the action values shown below).

Parameter	Value
Index	**2**
Name	**Teams Routing Policy** (arbitrary name)
Manipulation Set ID	**1**
Condition	
Action Subject	**Header.X-MS-RoutingPolicies**
Action Type	**Add**
Action Value	One of the following values: ■ **'none'** ■ **'no_missed_call'** ■ **'disable_forwarding'** ■ **'disable_forwarding_except_phone'**

Implementation of this Message Manipulation rule with Microsoft Teams is optional according to site deployment requirements.

2.5.19 Configuring IP-to-IP Call Routing Rules

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

The example shown below only covers IP-to-IP routing, though you can route the calls from SIP Trunk (through Site A SBC) 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:

- Calls from Teams Direct Routing to SIP Trunk (through Site A SBC)
- Calls from SIP Trunk (through Site A SBC) to Teams Direct Routing

To re-configure IP-to-IP routing rules:

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

Table 16: IP-to-IP Call Routing Rules

Index	Name	Source IP Group	Request Type	Dest Type	Dest IP Group	Routing Tag Name	Internal Action
0	Terminate OPTIONS	Any	OPTIONS	Internal			Reply (Response='200')
1	Teams to SIP Trunk (arbitrary name)	Teams		Destination Tag		Site	
2	SIP Trunk to Teams (arbitrary name)	Any		IP Group	Teams		

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

2.5.20 Configuring Firewall Settings

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

To configure a firewall rule:

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

Table 17: Firewall Table Rules

Index	Source IP	Subnet Prefix	Start Port	End Port	Protocol	Use Specific Interface	Interface ID	Allow Type
0	<Public DNS Server IP> (e.g., 8.8.8.8)	32	0	65535	Any	Enable	WAN_IF	Allow
1	52.112.0.0	14	0	65535	TCP	Enable	WAN_IF	Allow
2	52.122.0.0	15	0	65535	TCP	Enable	WAN_IF	Allow
3	xxx.xxx.xxx.xxx	32	0	65535	UDP	Enable	WAN_IF	Allow
49	0.0.0.0	0	0	65535	Any	Enable	WAN_IF	Block

For information about prerequisites and planning your deployment, refer to Plan Direct Routing.

Be aware, that if in your configuration, connectivity to other entities (except Teams) is performed through the same IP Interface as Teams (WAN_IF in our example), you must add rules to allow traffic from these entities. See an example in the row of index 3.

2.6 Configuring SBC for Local Media Optimization (LMO) Remote Site SBCs

This section describes the configuration required for supporting Local Media Optimization handling on the remote site SBCs.

2.6.1 Configuring LAN and WAN IP Interfaces

Configuration of the SBC's IP network interfaces done in the same way as in Proxy SBC. Please refer to Section 2.5.4 on page 16 above.

2.6.2 Configuring Media Realms

Configuration of the SBC's IP network interfaces done in the same way as in Proxy SBC. Please refer to Section 2.5.8 on page 28 above.

2.6.3 Configuring SIP Interfaces

This section shows how to configure a SIP Signaling Interfaces on the remote site SBC.

To configure SIP interfaces:

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

Table 18: Configuration Example: Site SBC SIP Interfaces

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepalive	Classification Failure Response Type	Media Realm	TLS Context Name
0	SIPTrunk (arbitrary name)	WAN_IF	SBC	5060 (according to Service Provider requirement)	0	0	Disable (leave default value)	0 (Recommended to prevent DoS attacks)	MRWan	-
1	ProxySBC (arbitrary name)	LAN_IF	SBC	0	0	5061	Enable	500 (leave default value)	MRLan	-

2.6.4 Configuring Proxy Sets and Proxy Address

This section describes how to configure Proxy Sets and Proxy address for remote SBCs.

To configure a Proxy Sets:

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

Table 19: Configuration Example: Site Proxy Sets

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive
1	SIPTrunk (arbitrary name)	SIPTrunk	Default	Using Options
2	ProxySBC (arbitrary name)	ProxySBC	Default	Using Options
All other SIP configuration can be left unchanged with their default values.				

To configure a Proxy Address for SIP Trunk:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **SIPTrunk**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**;
3. Configure the address of the SIP Trunk according to the parameters described in the table below:

Table 20: Configuration Proxy Address for SIP Trunk

Index	Proxy Address	Transport Type
0	SIPTrunk.com:5060 (SIP Trunk IP / FQDN and port)	UDP
All other Proxy Addresses can be left unchanged with their default values.		

4. Click **Apply**.

To configure a Proxy Address for Proxy SBCs:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **ProxySBC**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Configure the address of the Proxy SBC according to the parameters described in the table below:

Table 21: Configuration Example: Proxy SBC Address

Index	Proxy Address	Transport Type
0	{ProxySBC IP}:5061	TLS
All other Proxy Addresses can be left unchanged with their default values.		

3. Click **Apply**.

2.6.5 Configuring IP Profiles

This section describes how to configure the IP Profiles for the SBC at the remote site. See Appendix C for a summary of all IP Profile configurations.

To configure IP Profile to each remote site SBC:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **+New** to add the IP Profile for the Microsoft Teams (through Proxy SBC). Configure the parameters using the table below as a reference.

Table 22: Configuration Example: Teams IP Profile (through the Proxy SBC)

Parameter	Value
General	
Name	**ProxySBC** (arbitrary name)
Media Security	
SBC Media Security Mode	**Secured**
SBC Media	
Extension Coders Group	**AudioCodersGroups_1**
ICE Mode	**Lite**
SBC Signaling	
SIP Update Support	**Not Supported**
Remote re-INVITE	**Supported Only With SDP**
Remote Delayed Offer Support	**Not Supported**
Remote Representation Mode	**Replace Contact**
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally**
Remote Replaces Mode	**Handle Locally**
Remote 3xx Mode	**Handle Locally**
SBC Hold	
Remote Hold Format	**Inactive**
All other parameters can be left unchanged at their default values.	

3. Click **Apply**.

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

Table 23: Configuration Example: SIP Trunk IP Profile (toward SIP Provider/ Media Gateway)

Parameter	Value
General	
Name	**SIPTrunk** (arbitrary name)
SBC Signaling	
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally**
Remote Replaces Mode	**Handle Locally**
Play RBT To Transferee	**Yes** (required, as some SIP Trunks do not play ring-back tone during transfer)
Remote 3xx Mode	**Handle Locally**
All other parameters can be left unchanged at their default values.	

5. Click **Apply**.

Teams Hold music is not supported by Microsoft in consultative transfer of a PSTN call. The transferee will hear silence during the transfer. To overcome this issue, it is possible to configure SBC to play music during a consultative transfer. To do this, refer to Section 2.6.9.

2.6.6 Configuring IP Groups

This section describes how to configure the IP Groups for the SBC in each remote site.

To configure an IP Groups:

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Click **+New** to add the IP Group for the SIP Trunk:

Table 24: Configuration Example: Site SBC IP Group towards SIP Trunk

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

3. Click **Apply**.
4. Click **+New** to add the IP Group towards Teams (through Proxy SBC) in the remote site SBC:

Table 25: Configuration Example: Site SBC IP Group towards Teams (through Proxy SBC)

Parameter	Value
Name	**ProxySBC** (arbitrary name)
Type	**Server**
Proxy Set	**ProxySBC**
IP Profile	**ProxySBC**
Media Realm	**MRLan**
SIP Group Name	**{MSFT - CsOnlinePSTNGateway }**
All other parameters can be left unchanged with their default values.	

5. Click **Apply**.

2.6.7 Configuring SRTP

Configuration of the SRTP done in the same way as in Proxy SBC. Please refer to Section 2.5.14 above.

2.6.8 Configuring IP-to-IP Call Routing Rules

This section describes how to configure IP-to-IP call routing rules on the remote site SBC.

To configure IP-to-IP routing rule:

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

Table 26: Site IP-to-IP Call Routing Rule

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

2.6.9 Configuring SBC To Play Music On Hold (Optional)

Teams Hold music is not supported by Microsoft in consultative transfer of a PSTN call. The transferee will hear silence during the transfer. To overcome this issue, it is possible to configure SBC to play music during a consultative transfer. To do this, a Prerecorded Tones (PRT) file needs to be prepared and loaded to the SBC. This section shows how to load a PRT file to the SBC. For a detailed procedure how to create a Prerecorded Tones (PRT) file, refer to appropriated AudioCodes' device *User Manual* document.

Update configuration of the SIP Trunk IP Profile:

1. Open the Proxy Sets table (Setup > Signaling and Media > Coders and Profiles > IP Profiles).
2. Choose SIP Trunk IP Profile, created in the Section 2.6.5 on the page 46. Configure the parameters using the table below as reference.

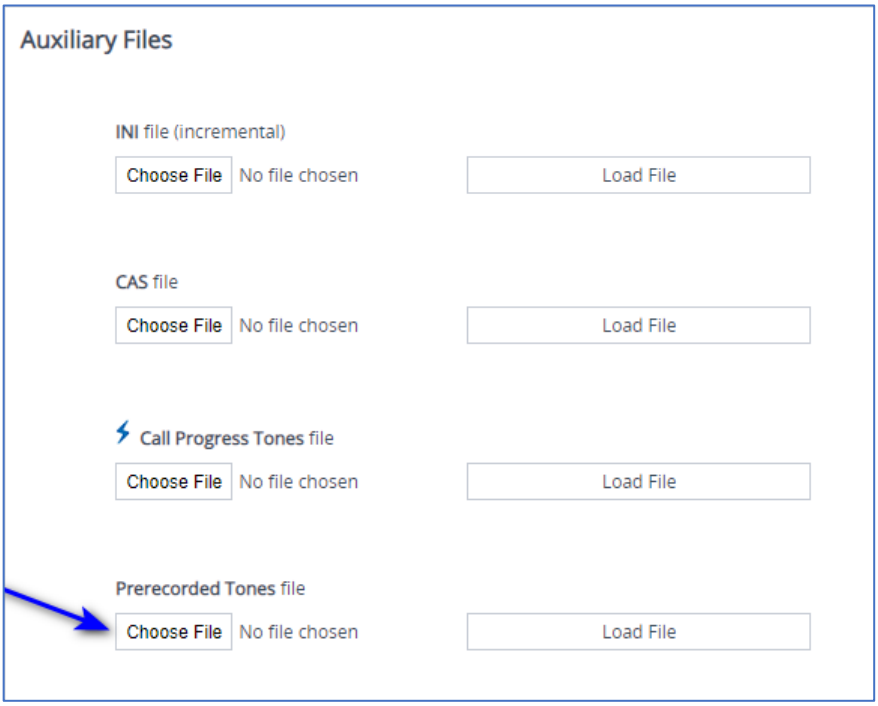
Table 27: Update Configuration of the SIP Trunk IP Profile

Parameter	Value
SBC Hold	
Remote Hold Format	**Send Only**
Reliable Held Tone Source	**No**
Play Held Tone	**Internal**

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

To load a PRT file to the device using the Web interface:

1. Open the Auxiliary Files page:
   - Toolbar: From the **Actions** drop-down menu, choose **Auxiliary Files**.
   - Navigation tree: **Setup** menu > **Administration** tab > **Maintenance** folder > **Auxiliary Files**.



2. Click the **Browse** button corresponding to the **Prerecorded Tones** file type that you want to load, navigate to the folder in which the file is located, and then click **Open**; the name and path of the file appear in the field next to the **Browse** button.
3. Click the **Load File** button corresponding to the file you want to load.
4. Save the loaded auxiliary files to flash memory.

> If in your configuration connectivity to SIP Trunks provided from the Proxy SBC, these changes are required on Proxy SBC.

2.7 Adapting Gateway to Work with Local Media Optimization

This section provides guidelines for configuring PSTN Gateway Application at the remote sites for supporting Local Media Optimization handling. To do this, SBC entities needed to be configured on the device.

- This section is only relevant for implementation, where the remote site is populated with PSTN connectivity (through Gateway Application).
- The Gateway configuration can vary from customer to customer, therefore in this document, we only provide the configuration changes that are necessary to adopt the Gateway to work with Local Media Optimization.
- Device should be populated with the appropriate (SBC session and IP security) licenses.

2.7.1 Configuring SBC SIP Signaling Interface

This section shows how to configure SBC SIP Signaling Interface. To configure SBC SIP interface:

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Click **+New** to add SBC SIP Interface (if there is already a configured SIP Interface with Application Type 'SBC', this interface can be used). You can change some parameters according to your requirements.

Table 28: Configuration Example: Site SIP Interface

Index	Name	Application Type	TLS Port
1	ProxySBC (arbitrary name)	SBC	5061 (arbitrary port)
All other SIP configuration can be left unchanged with their default values.			

2.7.2 Configuring SBC Proxy Set

This section describes how to configure SBC Proxy Set towards Proxy SBC.

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Click **+New** to add the **ProxySBC** Proxy Set as shown in the table:

Table 29: Configuration Example: Site Proxy Set

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive
1	ProxySBC	ProxySBC	Default	Using Options
All other Proxy Sets can be left unchanged with their default values.				

2.7.3 Configuring SBC Proxy Address

This section describes how to configure a Proxy address of the Proxy SBC.

To configure a Proxy Address for remote SBC:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **ProxySBC**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Configure Proxy Set Address as shown in the table:

Table 30: Configuration Example: Site Proxy Address

Index	Proxy Address	Transport Type
0	{ProxySBC IP}:5061	TLS
All other Proxy Addresses can be left unchanged with their default values.		

2.7.4 Configuring SBC IP Profile

This section describes how to configure the IP Profile for the Proxy SBC.

To configure IP Profile to the Proxy SBC:

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

Table 31: Configuration Example: Teams IP Profile (through the Proxy SBC)

Parameter	Value
General	
Name	**ProxySBC** (arbitrary name)
Media Security	
SBC Media Security Mode	**Secured**
SBC Media	
Extension Coders Group	**AudioCodersGroups_1**
ICE Mode	**Lite**
SBC Signaling	
Remote Update Support	**Not Supported**
Remote re-INVITE Support	**Supported Only With SDP**
Remote Delayed Offer Support	**Not Supported**
Remote Representation Mode	**Add Routing Headers**
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally**
Remote Replaces Mode	**Handle Locally**
Remote 3xx Mode	**Handle Locally**
SBC Hold	
Remote Hold Format	**Inactive**
All other parameters can be left unchanged at their default values.	

2.7.5 Configuring SBC IP Group

This section describes how to configure the IP group towards Proxy SBC in the remote site.

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 the IP Group towards Proxy SBC:

Table 32: Configuration Example: Site IP Group

Parameter	Value
Name	**ProxySBC** (arbitrary name)
Type	**Server**
Proxy Set	**ProxySBC**
IP Profile	**ProxySBC**
Media Realm	(according to your network environment)
SIP Group Name	**{MSFT - CsOnlinePSTNGateway }**
All other parameters can be left unchanged with their default values.	

2.7.6 Configuring SBC IP-to-IP Routing Rule

This section describes how to configure IP-to-IP routing rule for calls from Teams (through Proxy SBC) to the Gateway Application.

The following IP-to-IP Routing Rules are defined:

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

To configure SBC IP-to-IP routing rules:

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

Table 33: SBC IP-to-IP Routing Rules

Index	Name	Source IP Group	Request Type	Call Triger	ReRoute IP Group	Dest Type	Dest IP Group	Dest SIP Interface	Dest Address	Dest Port
0	Terminate OPTIONS	Any	OPTIONS			Dest Address			internal	
1	Refer from Teams (arbitrary name)	Any		REFER	ProxySBC	IP Group	ProxySBC			
2	Teams to GW (arbitrary name)	ProxySBC				Dest Address		{GW SIP Interface}	{GW IP Interface}	{GW SIP Interface port}

2.7.7 Configuring Gateway Tel-to-IP Routing Rule

This section describes how to configure Gateway Tel-to-IP routing rule for routing calls from PSTN to Teams through Proxy SBC.

To configure Tel-to-IP routing rules:

1. Open the Tel-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Routing** > **Tel > IP Routing**).
2. Click **New** and configure routing rule as shown in the table below:

Table 34: Gateway Tel-to-IP Routing Rule

Route Name	IP Profile	Dest IP Group Name
GW to Teams (arbitrary name)	Teams	ProxySBC
All other parameters can be left unchanged with their default values.		

3 Verifying 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 32: Proxy Set Status

Proxy Sets Status

This page refreshes every 60 seconds

PROXY SET ID	NAME	MODE	KEEP ALIVE	ADDRESS	PRIORITY	WEIGHT	SUCCESS COUNT	FAILURE COUNT	STATUS
0	ProxySet_0	Parking	Disabled						NOT RESOLVED
1	SIPTrunk	Parking	Enabled						ONLINE
				10.15.40.35(*)	-	-	1023	37	ONLINE
2	Teams	Load Balancing	Enabled						ONLINE
				sip.pstnhub.microsoft.com(52.114.75.24:5061)(*)	1	1.00	1	1	ONLINE
				sip2.pstnhub.microsoft.com(52.114.132.46:5061)(*)	2	1.00	1	0	ONLINE
				sip3.pstnhub.microsoft.com(52.114.7.24:5061)(*)	3	1.00	1	0	ONLINE

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

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

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

A.1 Terminology

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

A.2 Syntax Requirements for 'INVITE' Messages

Figure 33: Example of an 'INVITE' Message

```
INVITE sip:+97249888108@10.15.40.55;user=phone SIP/2.0
Via: SIP/2.0/TLS sbc.ACeducation.info:5068;alias;branch=z9hG4bKac496289557
Max-Forwards: 69
From: <sip:+97239762000@10.15.77.12>;tag=1c1642854452
To: <sip:+97249888108@10.15.40.55;user=phone>
Call-ID: 116796307628520199221 7@ACeducation.info
CSeq: 1 INVITE
Contact: <sip:+97239762000@sbc.ACeducation.info:5068;transport=tls>
Supported: em,100rel,timer,replaces,path,resource-priority,sdp-anat
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: 10.15.40.55/v.7.20A.250.273
Content-Type: application/sdp
Content-Length: 1114
```

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

A.3 Syntax Requirements for 'INVITE' Messages in Media Optimization

Figure 34: Example of an 'INVITE' Message (External user)

```
(N  3129751) ---- Incoming SIP Message from 52.114.132.46:4736 to SIPInterface #0 (SIPInterface_0) TLS TO(#3107) SocketID(93) --
INVITE sip:+122225888@mosbc71.audctrunk.aceducation.info:5061;user=phone;transport=tls SIP/2.0
FROM: MO2<sip:+15551002@sip.pstnhub.microsoft.com:5061;user=phone>;tag=98eca1f975c9499c95c2c9e66c317524
TO: <sip:+122225888@mosbc71.audctrunk.aceducation.info:5061;user=phone>
CSEQ: 1 INVITE
CALL-ID: 22d5c7b314c152cdb897d5ce79cec2de
MAX-FORWARDS: 70
VIA: SIP/2.0/TLS 52.114.132.46:5061;branch=z9hG4bK12f46b6
RECORD-ROUTE: <sip:sip-du-a-us.pstnhub.microsoft.com:5061;transport=tls;lr>
CONTACT: <sip:api-du-c-euwe.pstnhub.microsoft.com:443;transport=tls;x-i=71634df0-a8ef-40c8-865b-85039cc5e0df;x-c=/v1/ngc/call/22
CONTENT-LENGTH: 1781
USER-AGENT: Microsoft.PSTNHub.SIPProxy v.2019.11.28.2 i.USEA.4
CONTENT-TYPE: application/sdp
ALLOW: INVITE,ACK,OPTIONS,CANCEL,BYE,NOTIFY
P-ASSERTED-IDENTITY: <tel:+15551002>,<sip:mo2@mo.audctrunk.aceducation.info>
PRIVACY: id
X-MS-UserLocation: external
X-MS-MediaPath: mosbc.audctrunk.aceducation.info,mosbc71.audctrunk.aceducation.info
```

Figure 35: Example of an 'INVITE' Message (Internal User)

```
(N  3132353) ---- Incoming SIP Message from 52.114.132.46:4736 to SIPInterface #0 (SIPInterface_0) TLS TO(#3107) SocketID(93)
INVITE sip:+122225888@mosbc71.audctrunk.aceducation.info:5061;user=phone;transport=tls SIP/2.0
FROM: MO2<sip:+15551002@sip.pstnhub.microsoft.com:5061;user=phone>;tag=f254c0f24c624478b120351e5bb791ff
TO: <sip:+122225888@mosbc71.audctrunk.aceducation.info:5061;user=phone>
CSEQ: 1 INVITE
CALL-ID: 7cbcccdf073251b2a0837b7cd4739af4
MAX-FORWARDS: 70
VIA: SIP/2.0/TLS 52.114.132.46:5061;branch=z9hG4bK7c1c5f16
RECORD-ROUTE: <sip:sip-du-a-us.pstnhub.microsoft.com:5061;transport=tls;lr>
CONTACT: <sip:api-du-c-euwe.pstnhub.microsoft.com:443;transport=tls;x-i=6f0bb763-1eb1-4040-a787-d4bf2eb5019e;x-c=/v1/ngc/call/
CONTENT-LENGTH: 1777
USER-AGENT: Microsoft.PSTNHub.SIPProxy v.2019.11.28.2 i.USEA.4
CONTENT-TYPE: application/sdp
ALLOW: INVITE,ACK,OPTIONS,CANCEL,BYE,NOTIFY
P-ASSERTED-IDENTITY: <tel:+15551002>,<sip:mo2@mo.audctrunk.aceducation.info>
PRIVACY: id
X-MS-UserLocation: internal
X-MS-MediaPath: mosbc71.audctrunk.aceducation.info
X-MS-UserSite: MO.Site.71
```

- Privacy header removed
- X-MS- headers receive by Teams

A.4 Syntax Requirements for 'INVITE' Messages in site for Media Optimization

Figure 36: Example of an 'INVITE' Message From Site to Teams

```
(N  2672058) ---- Outgoing SIP Message to 52.114.75.24:5061 from SIPInterface #0 (SIPInterfa
INVITE sip:+15551002@mosbc71.audctrunk.aceducation.info;user=phone SIP/2.0
Via: SIP/2.0/TLS mosbc.audctrunk.aceducation.info:5061;alias;branch=z9hG4bKac275253736
Max-Forwards: 68
From: <sip:+122225888@10.15.40.29>;tag=1c1490933092
To: <sip:+15551002@mosbc71.audctrunk.aceducation.info;user=phone>
Call-ID: 11184345432212201913191@mosbc.audctrunk.aceducation.info
CSeq: 1 INVITE
Contact: <sip:+122225888@mosbc71.audctrunk.aceducation.info:5061;transport=tls>
Supported: em,100rel,timer,replaces,path,resource-priority,sdp-anat
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Mediant VE SBC/v.7.20A.254.975
Content-Type: application/sdp
Content-Length: 1109
```

- Contact header with Source Site FQDN

A.5 Requirements for 'OPTIONS' Messages Syntax

Figure 37: Example of 'OPTIONS' message

```
OPTIONS sip:195.189.192.171 SIP/2.0
Via: SIP/2.0/TLS sbc.ACeducation.info:5068;alias;branch=z9hG4bKac1385438539
Max-Forwards: 70
From: <sip:195.189.192.171>;tag=1c1890841146
To: <sip:195.189.192.171>
Call-ID: 595855232295201931O3@ACeducation.info
CSeq: 1 OPTIONS
Contact: <sip:sbc.ACeducation.info:5068;transport=tls>
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: 10.15.40.55/v.7.20A.250.273
Accept: application/sdp, application/simple-message-summary, message/sipfrag
Content-Length: 0
```

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

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

Table 35: Syntax Requirements for an 'OPTIONS' Message

Parameter	Where Configured	How to Configure
Contact	**Setup** > **Signaling and Media** > **Core Entities** > **IP Groups**> <Group Name> > **Local Host Name** In IP Group, 'Contact' must be configured. In this field ('Local Host Name'), define the local host name of the SBC as a string, for example, *sbc.ACeducation.info*. The name changes the host name in the call received from the IP Group.	See Section 2.12.

A.6 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 36: Teams Direct Routing Interface - Technical Characteristics

Category	Parameter	Value	Comments
Ports and IP ranges	SIP Interface FQDN Name	See Microsoft's document *Deploying Direct Routing Guide.*	-
	IP Addresses range for SIP interfaces	See Microsoft's document *Deploying Direct Routing Guide.*	-
	SIP Port	5061	-
	IP Address range for Media	See Microsoft's document *Deploying Direct Routing Guide.*	-
	Media port range on Media Processors	See Microsoft's document *Deploying Direct Routing Guide.*	-
	Media Port range on the client	See Microsoft's document *Deploying Direct Routing Guide.*	-
Transport and Security	SIP transport	TLS	-
	Media Transport	SRTP	-
	SRTP Security Context	DTLS, SIPS **Note:** Support for DTLS is pending. Currently, SIPS must be configured. When support for DTLS will be announced, it will be the recommended context.	https://tools.ietf.org/html/rfc5763
	Crypto Suite	AES_CM_128_HMAC_SHA1_80, non-MKI	-
	Control protocol for media transport	SRTCP (SRTCP-Mux recommended)	Using RTCP MUX helps reduce the number of required ports
	Supported Certification Authorities	See the *Deployment Guide*	-
	Transport for Media Bypass (of configured)	■ ICE-lite (RFC5245) – recommended ■ Client also has Transport Relays	-
	Audio codecs	■ G711 ■ Silk (Teams clients) ■ Opus (WebRTC clients) - only if Media Bypass is used ■ G729	-
Codecs	Other codecs	■ CN ■ Required narrowband and wideband ■ RED - Not required ■ DTMF - Required ■ Events 0-16 ■ Silence Suppression - Not required	-

B SIP Proxy Direct Routing Requirements

Teams Direct Routing has three FQDNs:

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

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

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

B.1 Failover Mechanism

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

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

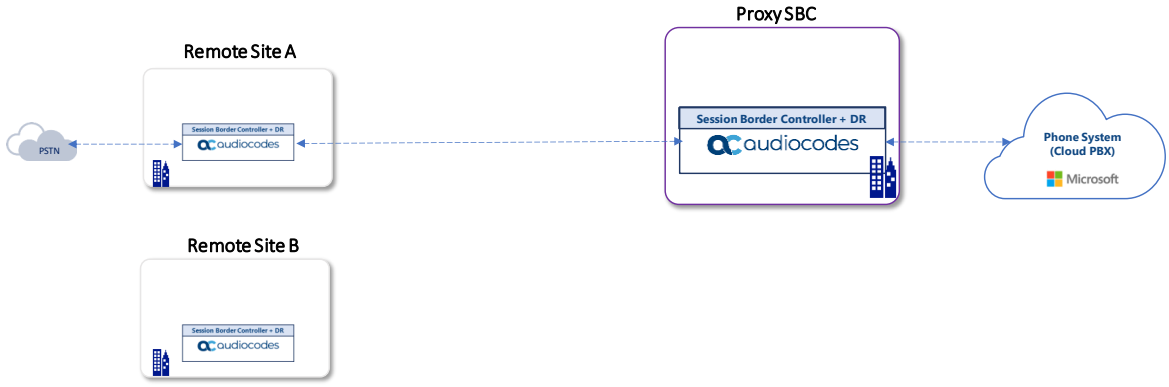
The SBC must send SIP OPTIONS to all IP addresses that are resolved from the three FQDNs, that is, **sip.pstnhub.microsoft.com**, **sip2.pstnhub.microsoft.com** and **sip3.pstnhub.microsoft.com**.

C Configuration Quick Guidelines

This appendix provides quick guidelines for configuring of the SBC's (Proxy SBC and the remote sites SBC's) to support Local Media Optimization.

C.1 Proxy SBC Scenario Topology

Figure 38: IP Profile for Remote Sites and Proxy SBC



C.2 SIP Interface

Table 37: SIP Interface Proxy SBC Configuration Summary

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepalive	Classification Failure Response Type	Media Realm	TLS Context Name
0	SitesSIPInterface (arbitrary name)	LAN_IF	SBC	0	0	5061 (according to site requirement)	Disable (leave default value)	500 (leave default value)	MRLan	-
1	Teams (arbitrary name)	WAN_IF	SBC	0	0	5061 (as configured in the Office 365)	Enable	0 (Recommended to prevent DoS attacks)	MRWan	Teams

Table 38: SIP Interface Remote SBC Configuration Summary

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepalive	Classification Failure Response Type	Media Realm	TLS Context Name
0	SIPTrunk (arbitrary name)	WAN_IF	SBC	5060 (according to Service Provider requirement)	0	0	Disable (leave default value)	0 (Recommended to prevent DoS attacks)	MRWan	-
1	ProxySBC (arbitrary name)	LAN_IF	SBC	0	0	5061	Enable	500 (leave default value)	MRLan	-

C.3 Proxy Set

Table 39: Proxy Set Proxy SBC Configuration Summary

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Proxy Hot Swap	Proxy Load Balancing Method	Proxy Address	Transport Type	Proxy Priority
1	Teams (arbitrary name)	Teams	Teams	Using Options	Enable	Random Weights	sip.pstnhub.microsoft.com:5061 sip2.pstnhub.microsoft.com:5061 sip3.pstnhub.microsoft.com:5061	TLS TLS TLS	1 2 3
2	SiteA (arbitrary name)	SitesSIPInterface (arbitrary name)	Default	Using Options	-	-	192.168.1.5:5061 (IP address of the SiteA SBC)	TLS	
3	SiteB (arbitrary name)	SitesSIPInterface (arbitrary name)	Default	Using Options	-	-	192.168.2.5:5061 (IP address of the SiteB SBC)	TLS	

Table 40: Proxy SET Remote SBC Configuration Summary

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Proxy Hot Swap	Proxy Load Balancing Method	Proxy Address	Transport Type	Proxy Priority
1	SIPTrunk (arbitrary name)	SIPTrunk	Default	Using Options	-	-	SIPTrunk.com:5060	UDP	-
2	ProxySBC (arbitrary name)	ProxySBC	Default	Using Options	-	-	{ProxySBC IP}:5061	TLS	-

C.4 IP Profile

Table 41: IP Profile Configuration Summary

	Remote SBC		Proxy SBC	
Parameter	**Value**	**Value**	**Value**	**Value**
General				
Name	**SIPTrunk** (toward SIP Provider/ MGW appl)	**ProxySBC**	**SiteA** (toward site A Remote SBC)	**Teams**
SBC Media Security				
SBC Media Security Mode	**Not Secured** (should be synchronized with SIP provider)	**Secured** (according to customer needs)	**Secured** (according to customer needs)	**Secured**
SBC Early Media				
Remote Early Media RTP Detection Mode	**By Signaling** (Default)	**By Signaling** (Default)	**By Signaling** (Default)	**By Media** (required, as Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18x response)
SBC Media				
Extension Coders Group	**AudioCodersGroups_1**	**AudioCodersGroups_1**	**AudioCodersGroups_1**	**AudioCodersGroups_1**
RTCP Mode	**Transparent** (Default)	**Transparent** (Default)	**Transparent** (Default)	**Generate Always** (required, as some ITSPs do not send RTCP packets during Hold, but Microsoft expects them)
ICE Mode	**Disable** (Default)	**Lite**	**Disable** (Default)	**Lite**
SBC Signaling				
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)	**As Is** (Default)	**As Is** (Default)	**As Is** (Default)
SIP UPDATE Support	**Supported** (Default)	**Not Supported**	**Supported** (Default)	**Not Supported**
Remote re-INVITE Support	**Supported** (Default)	**Supported Only With SDP**	**Supported** (Default)	**Supported Only With SDP**
Remote Delayed Offer Support	**Supported** (Default)	**Not Supported**	**Supported** (Default)	**Not Supported**

	Remote SBC		Proxy SBC	
Remote Representation Mode	**According to Operation Mode** (Default)	**Replace Contact**	**According to Operation Mode** (Default)	**Add Routing Headers**
SBC Forward and Transfer				
Remote REFER Mode	**Handle Locally**	**Handle Locally**	**Regular** (Default)	**Regular** (Default)
Remote Replaces Mode	**Handle Locally**	**Handle Locally**	**Standard** (Default)	**Standard** (Default)
Play RBT To Transferee	**Yes**	**No** (Default)	**No** (Default)	**No** (Default)
Remote 3xx Mode	**Handle Locally**	**Handle Locally**	**Transparent** (Default)	**Transparent** (Default)
SBC Hold				
Remote Hold Format	**Send Only** (Only in case, when you want that SBC will play Music On Hold)	**Inactive**	**Transparent** (Default)	**Inactive**
Reliable Held Tone Source	**No** (Only in case, when you want that SBC will play Music On Hold)	**Yes** (Default)	**Yes** (Default)	**Yes** (Default)
Play Held Tone	**Internal** (Only in case, when you want that SBC will play Music On Hold)	**No** (Default)	**No** (Default)	**No** (Default)
All other parameters can be left unchanged at their default values.				

C.5 IP Group

Table 42: IP Group Proxy SBC toward Teams Configuration Summary

Parameter	Value
Name	**Teams**
Type	**Server**
Proxy Set	**Teams**
IP Profile	**Teams**
Media Realm	**MRWan**
Internal Media Realm	**MRLan** (This parameter is relevant when the 'Teams Local Media Optimization Handling' parameter (see below) is configured to any value other than 'None' and the X-MS-UserLocation header in the incoming SIP message is set to 'Internal'). In this case, the Internal Media Realm determines the UDP port range and maximum sessions for Media traffic on this IP interface. If the 'X-MS-UserLocation=Internal' response is received from Teams, a new IP address/port is allocated using the Internal Media Realm only if the call is non-direct media - i.e., media traverses the paired SBC to the remote SBCs.)
Classify by Proxy Set	**Disable**
Local Host Name	**<FQDN name of the SBC in the enterprise tenant>** For example, sbc.ACeducation.info defines the host name (string) that the device uses in the SIP message's Via and Contact headers. This defines the FQDN as the host name that is recognized by Microsoft Teams. 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 the other configured IP Groups (SiteA and SiteB).
Teams Direct Routing Mode	**Enable** (Enables the SBC to include Microsoft's proprietary X-MS-SBC header in outgoing SIP INVITE and OPTIONS messages in a Microsoft Teams Direct Routing environment. The header is used by Microsoft Teams to identify vendor equipment. The header's value is in the format 'Audiocodes/<model>/<firmware>').
Always Use Src Address	**Yes**
Teams Local Media Optimization Handling	**Teams Decides** (The routing decision is made according to the Microsoft Teams headers for the primary route)
Teams Local Media Optimization Initial Behavior	This parameter is relevant for inbound calls to Teams when "Teams Local Media Optimization Handling" is set to "Teams Decides" or "SBC Decides": ■ **Direct Media** (default) – Perform direct media call towards Teams. ■ **Internal** - Perform non-direct media call (media traverses the paired SBC from the remote SBC) towards Teams using Internal Media Realm. ■ **External** – Perform non-direct media call (media traverses the paired SBC from the remote SBC) towards Teams using external (regular) Media Realm. **Note:** The value of this parameter can be variable depending on particular setup
Proxy Keep-Alive using IP Group settings	**Enable**
Inbound Message Manipulation Set	**0**
Outbound Message Manipulation Set	**1**
Call Setup Rules Set ID	**0**

Table 43: IP Group Proxy SBC toward Remote SBC's Configuration Summary

Parameter	Value
Name	**SiteA/SiteB**
Type	**Server**
Proxy Set	**SiteA/SiteB**
IP Profile	**SiteA/SiteB**
Media Realm	**MRLan**
Tags	**Site={RemotePSTNGateWayFQDN}** The Site Tag should be defined as the remote site SBC's FQDN and should be discoverable by DNS from the Proxy SBC.
All other parameters can be left unchanged with their default values.	

Table 44: IP Group Remote SBC toward Proxy SBC Configuration Summary

Parameter	Value
Name	**ProxySBC** (arbitrary name)
Topology Location	**Down**
Type	**Server**
Proxy Set	**ProxySBC**
IP Profile	**ProxySBC**
Media Realm	**MRLan**
SIP Group Name	**{MSFT - CsOnlinePSTNGateway }**
All other parameters can be left unchanged with their default values.	

Table 45: IP Group Remote SBC toward SIP Trunk (PSTN) Configuration Summary

Parameter	Value
Name	**SIPTrunk** (arbitrary name)
Topology Location	**Down**
Type	**Server**
Proxy Set	**SIPTrunk**
IP Profile	**SIPTrunk**
Media Realm	**MRWan**
Classify by Proxy Set	**Enable**
SIP Group Name	(according to ITSP requirement)
All other parameters can be left unchanged with their default values.	

C.6 IP-To-IP Routing

Table 46: IP-To-IP Routing in the Proxy SBC

Index	Name	Source IP Group	Request Type	Dest Type	Dest IP Group	Routing Tag Name	Internal Action
0	Terminate OPTIONS	Any	OPTIONS	Internal			Reply (Response='200')
1	Teams to SIP Trunk (arbitrary name)	Teams		Destination Tag		Site	
2	SIP Trunk to Teams (arbitrary name)	Any		IP Group	Teams		

Table 47: IP-To-IP Routing in the Remote Site SBC

Index	Name	Source IP Group	Request Type	Call Triger	ReRoute IP Group	Dest Type	Dest IP Group	Dest Address
0	Terminate OPTIONS	Any	OPTIONS			Internal		Reply (Response='200')
1	Terminate Refer (arbitrary name)	Any	Any	REFER	ProxySBC	IP Group	ProxySBC	
2	Teams to SIP Trunk (arbitrary name)	ProxySBC				IP Group	SIPTrunk	
3	SIP Trunk to Teams (arbitrary name)	SIPTrunk				IP Group	ProxySBC	

C.7 Message Manipulations

Table 48: Proxy SBC Message Manipulation Index 0

Parameter	Value
Index	**0**
Name	**Privacy Header**
Manipulation Set ID	**0**
Condition	**Header.Privacy contains 'id'**
Action Subject	**Header.Privacy**
Action Type	**Remove**

Table 49: Proxy SBC Message Manipulation Index 1

Parameter	Value
Index	**1**
Name	**Replace Host in Contact**
Manipulation Set ID	**1**
Message Type	**Invite.Request**
Action Subject	**Header.Contact.URL.Host**
Action Type	**Modify**
Action Value	**Header.To.URL.Host**

D AudioCodes ARM and SBCs with Teams Direct Local Media Optimization

This appendix describes how to provision all the system components involved in the ARM and SBC solution for Teams Direct Routing Local Media Optimization.

D.1 About AudioCodes Routing Manager (ARM)

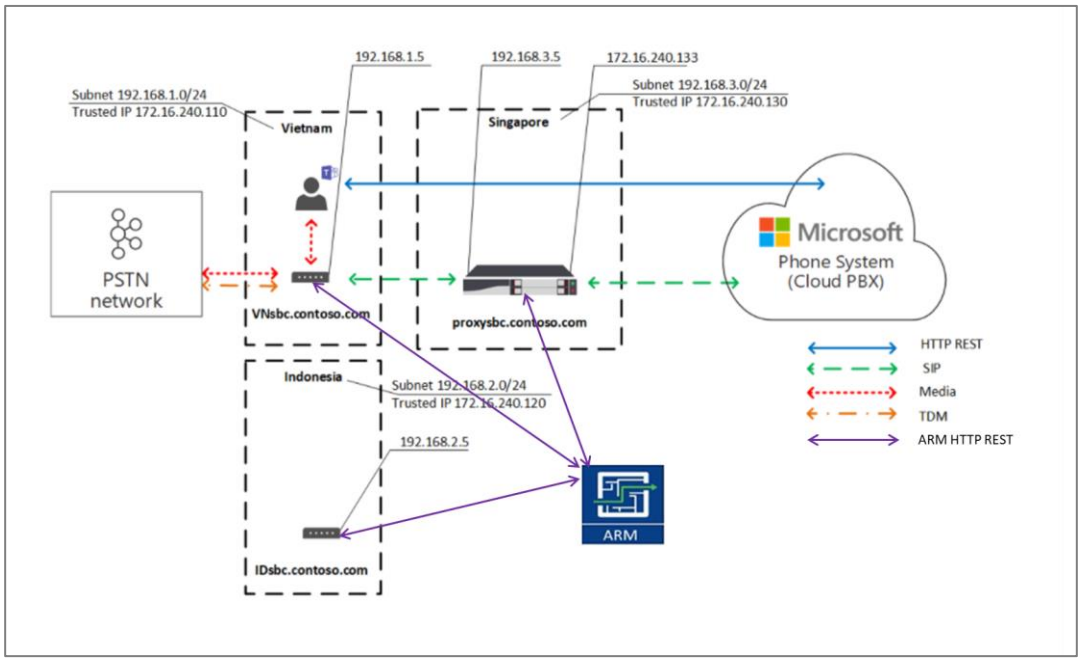
The ARM is a LINUX-based, software-only, telephony management product which expedites and streamlines IP telephony routing for enterprises with multiple globally distributed branches. The ARM determines the quickest, least expensive, and best call quality routes in packet networks. Routing data, previously located on the SBC, Unified Communications (UC) application (e.g., Microsoft's Skype for Business), or Media Gateway, is now located on the ARM server. If an enterprise has an SBC in every branch, a single ARM, deployed in HQ, can route all calls in the globally distributed corporate network to PSTN, the local provider, enterprise headquarters, or to the IP network. Routing rules, configured by the IT manager in the ARM's Routing Table, perform the routing.

If an enterprise has only one or two branches, its IT manager can easily independently implement maintenance changes. In globally distributed enterprises, IT managers until now had to laboriously implement changes, multiple times, per branch. With the ARM, IT managers implement changes only once, saving significant labor and time resources and costs.

D.2 Solution Overview

In Teams Direct Local Media Optimization, ARM handles call signaling for all solution SBCs (Proxy SBC and Remote SBCs). Remote SBCs handle the Local Media Optimization business logic. ARM significantly simplifies the provisioning of connectivity between the Proxy SBC and Regional SBC and visualizes the topology.

Figure 39: IP Profile for Remote Sites and Proxy SBC



The following sections describe the exact steps for configuring:

- Proxy and Remote SBCs
- ARM - Nodes, Connections, Routing Rules

D.3 Configuration of the SBCs

- Validate that your AudioCodes' Mediant SBCs are loaded with the correct firmware version (7.20A.258.354 or later).
- The following sections assumes that an SBC configuration is deployed in production working with Local Media Optimization and you wish to add support for working with ARM.

D.3.1 Configuring Proxy SBC for Local Media Optimization (LMO)

This section describes the configuration required for supporting Local Media Optimization handling on the **Proxy SBC**.

To configure LMO on Proxy SBC:

1. Configure the IP Interfaces as described in Section 2.5.4.
2. Configure the TLS Context as described in Section 2.5.5.
3. Generate and install a certificate as described in Section 2.5.6.
4. Load the Baltimore Trusted Root Certificates as described in Section 2.5.7.
5. Open the SRDs table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SRDs**) and set the 'Used by Routing Server' parameter to 'Used' for all SRDs.

   If the SBC is already provisioned to work with Local Media Optimization, and the solution is being extended to work with ARM, set the 'Used by Routing Server' parameter to 'Used' for all SRDs.
6. Configure the Media Realms as described in Section 2.5.8 and set the 'Used by Routing Server' parameter to 'Used' for both Media Realms.

   If the SBC is already provisioned to work with Local Media Optimization and the solution is being extended to work with ARM, set the 'Used by Routing Server' parameter to 'Used' for both Media Realms.
7. Configure SIP Interfaces as described in Section 2.5.9 and set the 'Used by Routing Server' parameter to 'Used' for both interfaces.

   If SBC is already provisioned to work with Local Media Optimization, and the solution is being extended to work with ARM, set the 'Used by Routing Server' parameter to 'Used' for both interfaces.
8. Add a Proxy Set towards Teams as described in Section 2.5.10.
   a. Configure the Proxy Set according to Table 2-6 (Teams).
   b. Configure the Proxy Address for this Proxy Set as described in Table 2-7.

   If SBC is already provisioned to work with Local Media Optimization, and the solution is being extended to work with ARM, delete all Proxy Sets towards sites.
9. Configure the Coder Groups as described in Section 2.5.11.
10. Add an IP Profiles for Teams as described in Section 2.5.12 according to Table 2-9.

11. Add an IP Group toward Teams as described in Section 2.5.13 according to Table 2-11 and set the 'Used by Routing Server' parameter to ‘Used’.

> If SBC is already provisioned to work with Local Media Optimization, and the solution is being extended to work with ARM, set the 'Used by Routing Server' parameter to ‘Used’ and delete all IP Groups towards sites.

12. Configure the SRTP as described in Section 2.5.14.
13. Add a Message Condition as described in Section 2.5.15.
14. Add a Classification Rules as described in Section 2.5.16.
15. Add Message Manipulations as described in Chapter 2.5.18.
16. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
17. Insert a new row to work with the ARM (should be before the other INVITE rules):

Index	Name	Source IP Group	Request Type	Destination Type
1	ARM	Any	INVITE	Routing Server

D.3.2 Configuring Remote Site SBCs for Local Media Optimization (LMO)

This section describes the configuration required for supporting Local Media Optimization handling on the **remote site** SBCs.

To configure remote site SBCs for LMO:

1. Configure the IP Interfaces as described in Section 2.6.1.
2. Open the SRDs table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SRDs**) and set the 'Used by Routing Server' parameter to 'Used' for all SRDs.

> If the SBC is already provisioned to work with Local Media Optimization, and the solution is now being extended to work with ARM, set the 'Used by Routing Server' parameter to 'Used' for all SRDs.

3. Configure the Media Realms as described in Section 2.6.2 and set the 'Used by Routing Server' parameter to 'Used' for both Media Realms.

> If the SBC is already provisioned to work with Local Media Optimization, and the solution is now being extended to work with ARM, set the 'Used by Routing Server' parameter to 'Used' for both Media Realms.

4. Configure SIP Interfaces as described in Section 2.6.3 and set 'Used by Routing Server' parameter to 'Used' for both interfaces.

> If the SBC is already provisioned to work with Local Media Optimization, and the solution is now being extended to work with ARM, set the 'Used by Routing Server' parameter to 'Used' for both interfaces.

5. Add a Proxy Set toward SIP Trunk as described in Section 2.6.4.
   a. Configure the Proxy Set according to Table 19.
   b. Configure the Proxy Address for this Proxy Set as described in Table 20.

> If SBC is already provisioned to work with Local Media Optimization, and now solution is extended with ARM, you have to delete Proxy Set towards Proxy SBC.

6. Add an IP Profiles for SIP Trunk as described in Section 2.6.5 according to Table 23.
7. Add an IP Group toward SIP Trunk as described in Section 2.6.6 according to Table 24 and set the 'Used by Routing Server' parameter to 'Used'.

> If the SBC is already provisioned to work with Local Media Optimization, and the solution is being extended to work with ARM, set the 'Used by Routing Server' parameter to 'Used' and delete IP Group towards Proxy SBC.

8. Configure the SRTP as described in Section 2.6.7.
9. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
10. Insert a new row to work with the ARM (should be before the other INVITE rules):

Index	Name	Source IP Group	Request Type	Destination Type
1	ARM	Any	INVITE	Routing Server

D.4 ARM Configuration

This section describes how to configure the ARM Web interface.

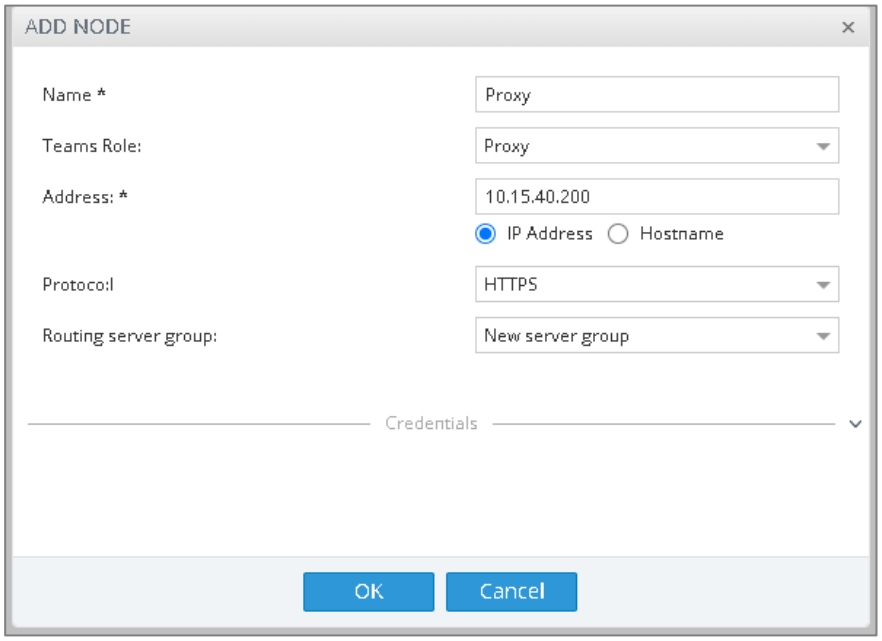
D.4.1 Defining SBC Nodes

This section describes how to define SBC nodes.

To define SBC nodes:

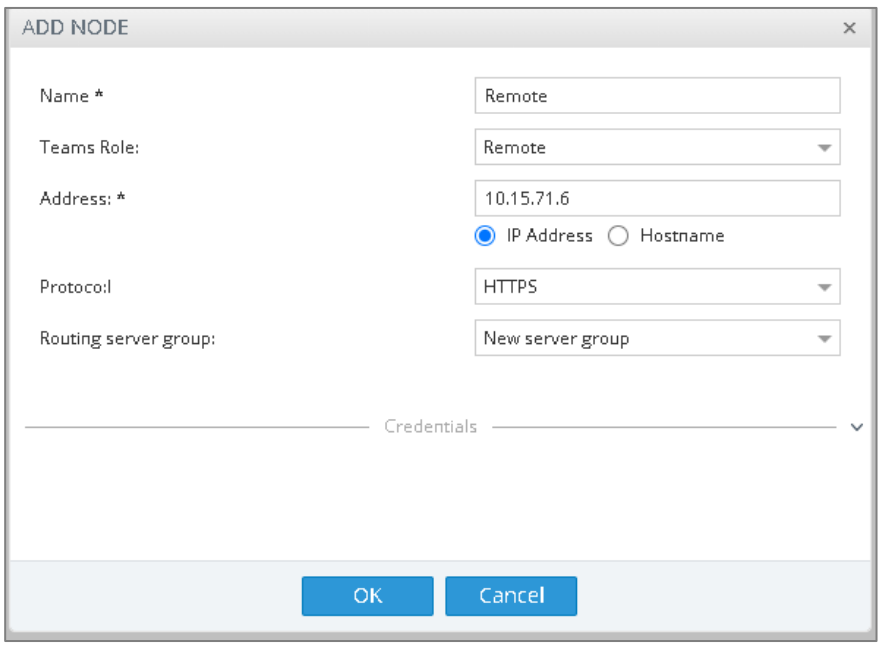
1. In ARM GUI Interface, add an AC Node for the Proxy_sbc.

Figure 40: AC Node for Proxy SBC



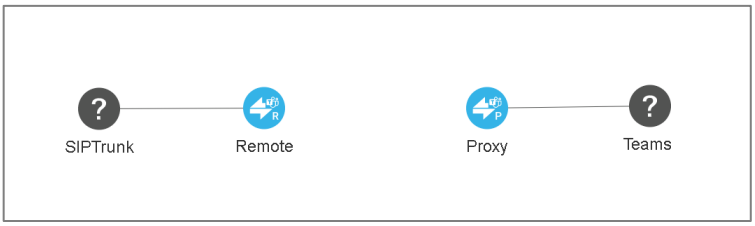
2. Add an AC Node for the Remote_SBC.

Figure 41: AC Node for Remote SBC



3. Unlock the Peer Connections. Wait for Sync. Nodes will be enabled.

Figure 42: Enable Nodes



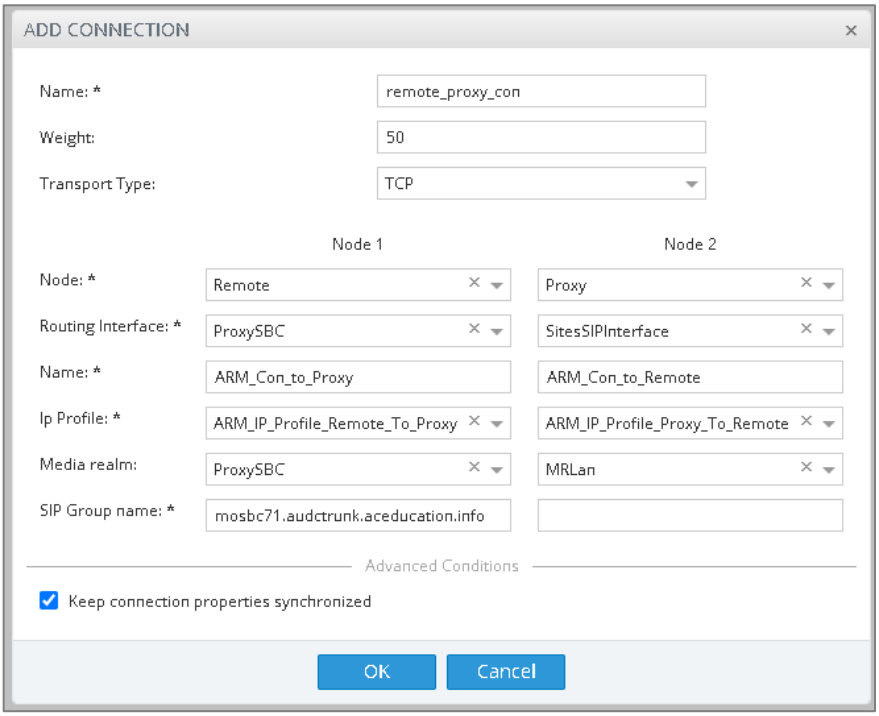
D.4.2 Defining Connection

This section describes how to define the connection between the remote SBC and the proxy SBC.

To define connection between the remote SBC and the proxy SBC:

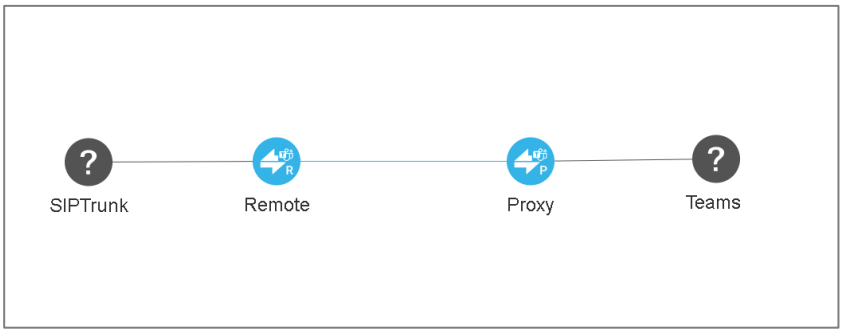
1. Drag a Connection from the Remote_SBC to the Proxy_sbc.
2. Select the protocol type, Routing Interface, Name, Ip Profile, Media Realm for both Nodes.
3. Configure Sip Group Name for the Remote Node.

Figure 43: Add Connection



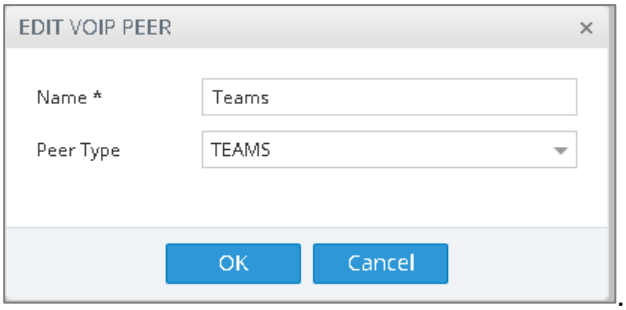
4. Wait for sync. The Connection will be enabled.

Figure 44: Established Connection



5. Edit the Teams Voip-Peer and select TEAMS.

Figure 45: Teams Voip-Peer



6. Edit the SIPTrunk Voip-Peer and select SIP_TRUNK.

Figure 46: SIPTrunk VoIP-Peer

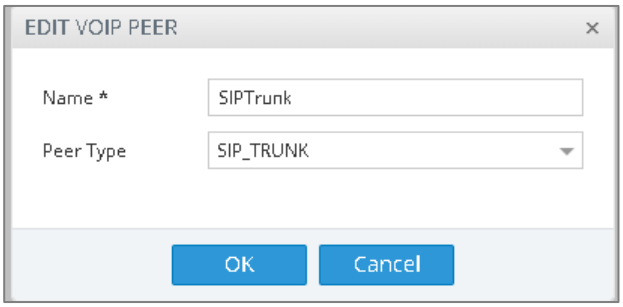


Figure 47: Established Connection

D.4.3 Defining Routing Rules

This section describes how to define routing rules.

D.4.3.1 Calls from Teams

This section describes how to define routing rules for calls from Teams.

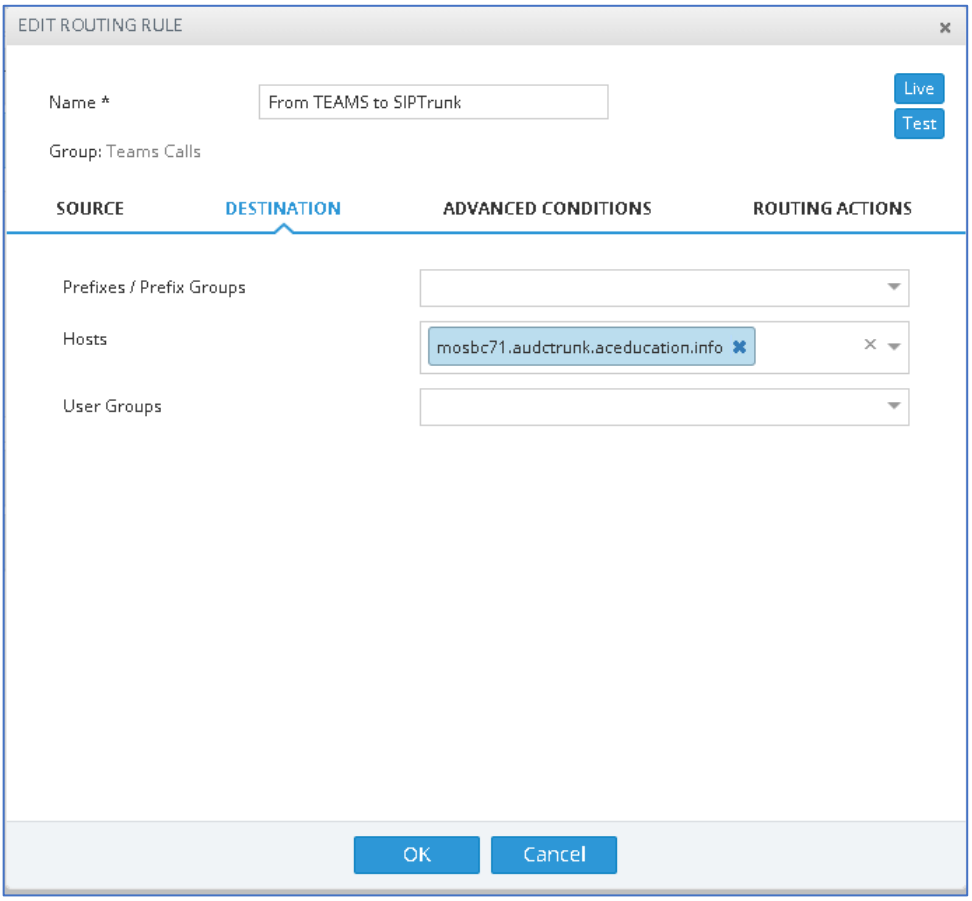
To define a routing rule for calls from Teams.

1. Add a Routing Rule for incoming call from Teams.

```
Name = From TEAMS to SIPTrunk
Source Peer Connection = The Peer Connection of Proxy_sbc toward Teams
Destination Host = {MSFT - CsOnlinePSTNGateway} of Remote_SBC
Routing Action = The Peer Connection of Remote_SBC toward SIPTrunk
```

2. Click **Live** to activate the routing rule; the rule is now activated in the ARM.

Figure 48: Add a Routing Rule for Incoming Call from Teams



D.4.3.2 Calls to Teams

This section describes how to define routing rules for calls to Teams.

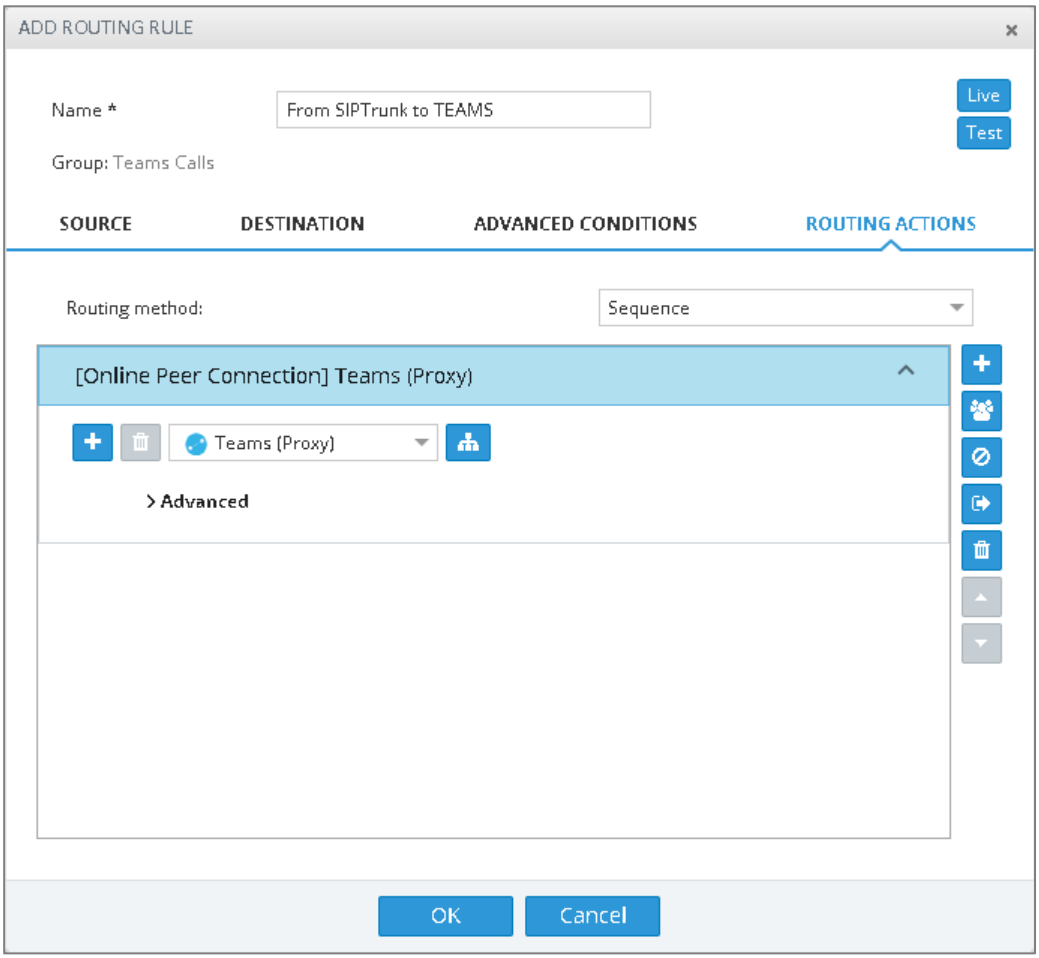
To define a routing rule for calls to Teams:

1. Add a Routing Rule for incoming call from SIPTrunk.

```
Name = From SIPTrunk to TEAMS
Source Peer Connection = The SIPTrunk Peer Connection of
Remote_SBC
Routing Action = The Peer Connection of Proxy_sbc toward TEAMS
```

2. Define the characteristics of the route request, e.g., the User Group and phone prefix of the originator/destination.
3. Click **Live** to activate the routing rule; the rule is now activated in the ARM.

Figure 49: Add a Routing Rule for Incoming Call from SIP Trunk



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

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

Document #: LTRT-33522