Configuration Note

AudioCodes Mediant™ Family of Media Gateways & Session Border Controllers

Connecting AudioCodes' SBC to Microsoft Azure Communication Services

Microsoft Partner
Gold Communications

audiocodes

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: January-05-2023

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
AudioCodes Configuration Notes

Document Revision Record

LTRT	Description
39470	Initial document release
39471	Change "ACS SIP interface" to "Azure Communication Services direct routing" per Microsoft request and add links to Microsoft docs in Section 3
39472	Minor fixes per Microsoft request

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 the Microsoft Azure Communication Services (ACS) and refers to the AudioCodes SBC configuration only. For more information about Microsoft Azure Communication Services, please refer to https://docs.microsoft.com/en-us/azure/communication-services/.

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 Microsoft Azure Communication Services

Azure Communication Services allows you to easily add real-time voice, video, and telephone communication to your applications. Communication Services SDKs also allow you to add SMS functionality to your communications solutions. Azure Communication Services is identity agnostic; you have complete control over how end users are identified and authenticated. You can connect people to the communication data plane or services (bots).

Applications include:

- **Business to Consumer (B2C)**. Business employees and services can interact with consumers using voice, video, and rich text chat in a custom browser or mobile application. An organization can send and receive SMS messages or operate an interactive voice response system (IVR) using a phone number acquired through Azure. Integration with Microsoft Teams allows consumers to join Teams meetings hosted by employees; ideal for remote healthcare, banking, and product support scenarios where employees might already be familiar with Teams.
- **Consumer to Consumer**. Build engaging social spaces for consumer-to-consumer interaction with voice, video, and rich text chat. Any type of user interface can be built on Azure Communication Services SDKs. Complete application samples and UI assets are available to help you get started quickly.

1.2 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.

1.3 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*.

For implementing Microsoft Azure Communication Services based on the configuration described in this document, AudioCodes SBC must be installed with a License Key that includes the following features:

- **MSFT** (general Microsoft license)
  Note: By default, all AudioCodes media gateways and SBCs are shipped with this license (except MSBR products, Mediant 500 SBC, and Mediant 500 Media Gateway).
- **SW/TEAMS** (Microsoft Teams license)
- **Number of SBC sessions** (based on requirements)
- **Transcoding sessions** (only if media transcoding is needed)
- **Coders** (based on requirements)

For more information about the License Key, contact your AudioCodes sales representative.

2 Topology Example

ACS PSTN Telephony Voice Calling allow users to interact with a traditional telephone number, facilitated by PSTN (Public Switched Telephone Network) for voice calling. ACS supports a "SIP Interface". This allows you to connect, via a certified SBC, PBXs, Analog Telephony Adapters, or another PSTN carrier.

Figure 1: Azure Communication Services direct routing

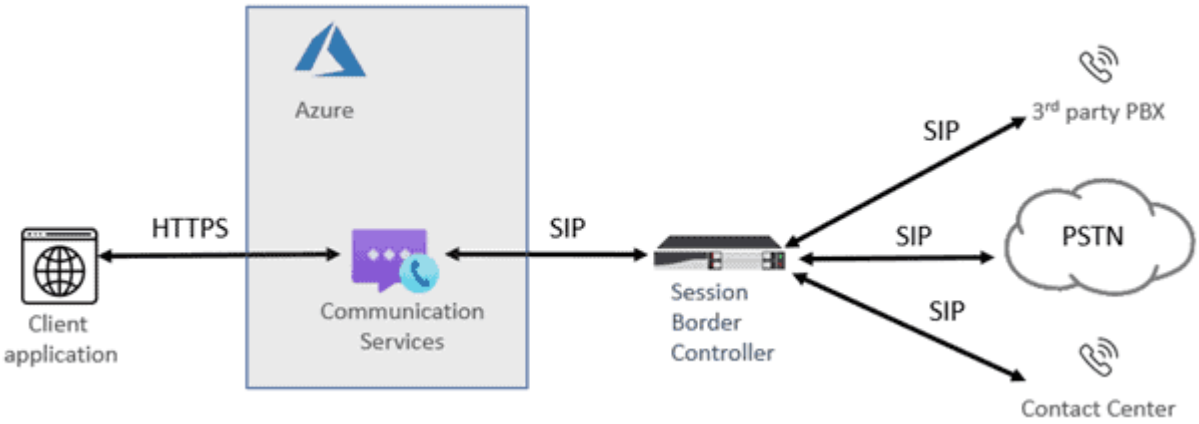
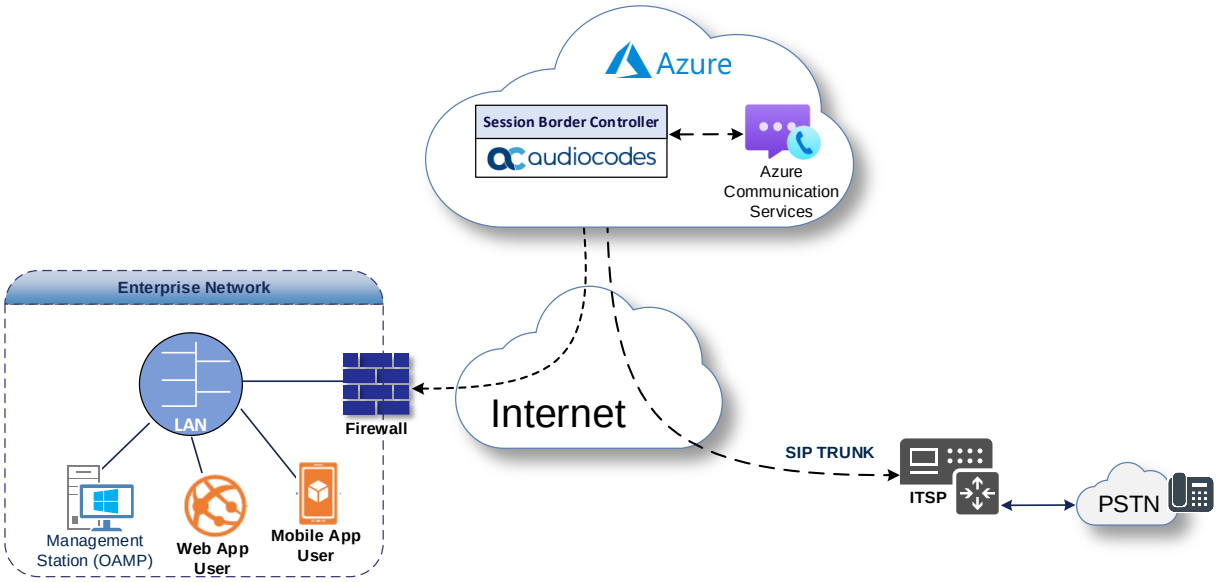


Figure 2: Interoperability Test Topology



This document shows how to configure the connection between AudioCodes' SBC and the Microsoft Azure Communication Services (ACS) 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).

2.1 Environment Setup

The topology example includes the following environment setup:

Table 1: Environment Setup

Area	Setup
Network	■ Both, Company SIP Trunk and ACS environment, are located on the Enterprise's (or Service Provider's) WAN
Signaling Transcoding	■ ACS operates with SIP-over-TLS transport type ■ Generic SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	■ ACS supports G.711A-law, G.711U-law, G.722, G.729 and SILK (NB and WB) coders ■ Generic SIP Trunk supports G.711A-law, G.711U-law, and G.729 coders
Media Transcoding	■ ACS operates with SRTP media type ■ Generic SIP Trunk operates with RTP media type

2.2 Infrastructure Prerequisites

The table below shows the list of infrastructure prerequisites required for deploying connection to Azure Communication Services. These are the same requirement as for interconnect with Teams Direct Routing.

Table 2-2: Infrastructure Prerequisites

Infrastructure Prerequisite	Details
Certified Session Border Controller (SBC)	See Microsoft's document *Plan Direct Routing*.
SIP Trunks connected to the SBC	
Azure Communication resource	
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 ACS Clients Media	

3 Configuring Azure Communication Services direct routing

Currently, a configuration description of the Microsoft Azure Communication Services direct routing is not available, it will be added in the future. The following links can be used to start working with the SIP Interface for interconnect to Microsoft Azure Communication Services:

- About Direct Routing
- Azure direct routing infrastructure requirements
- Provision SBC and configure voice routing
- What is Azure Communication Services
- How to create an ACS resource
- Build your own app quickstart
- Web app with calling capabilities

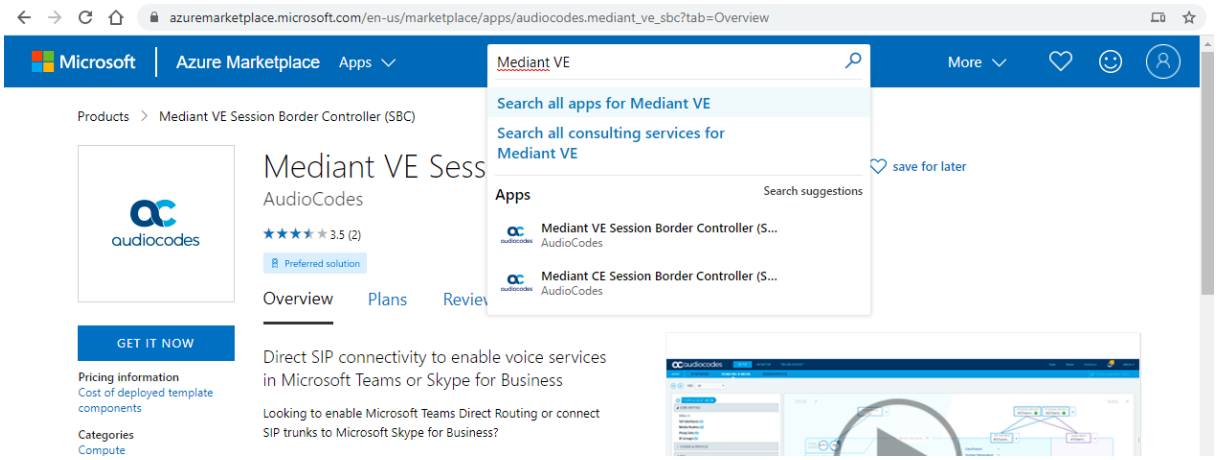
4 Deploying Mediant VE Via Azure Marketplace

This section describes the deployment of a standalone Mediant VE through the Azure Marketplace. This deployment method uses a graphical user interface and is therefore, most suited if you are not familiar with the Azure cloud environment.

To deploy a standalone Mediant VE through Azure Marketplace:

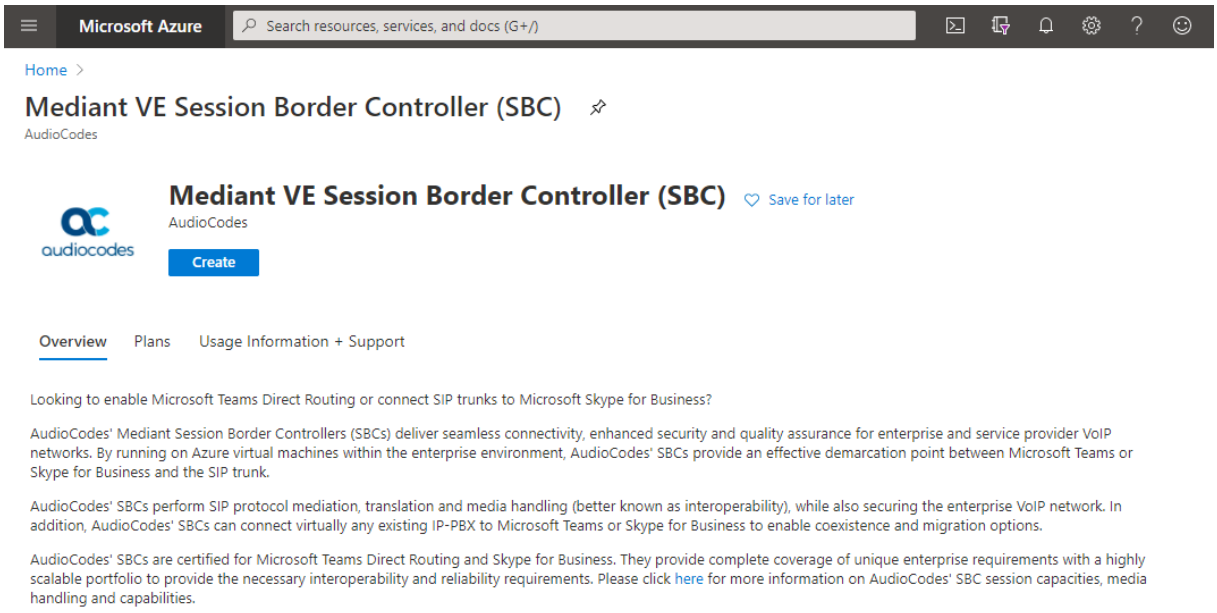
1. Open the Azure Marketplace at https://azuremarketplace.microsoft.com/.
2. Search for the product "Mediant VE Session Border Controller (SBC)" published by AudioCodes.

Figure 3: Azure Marketplace



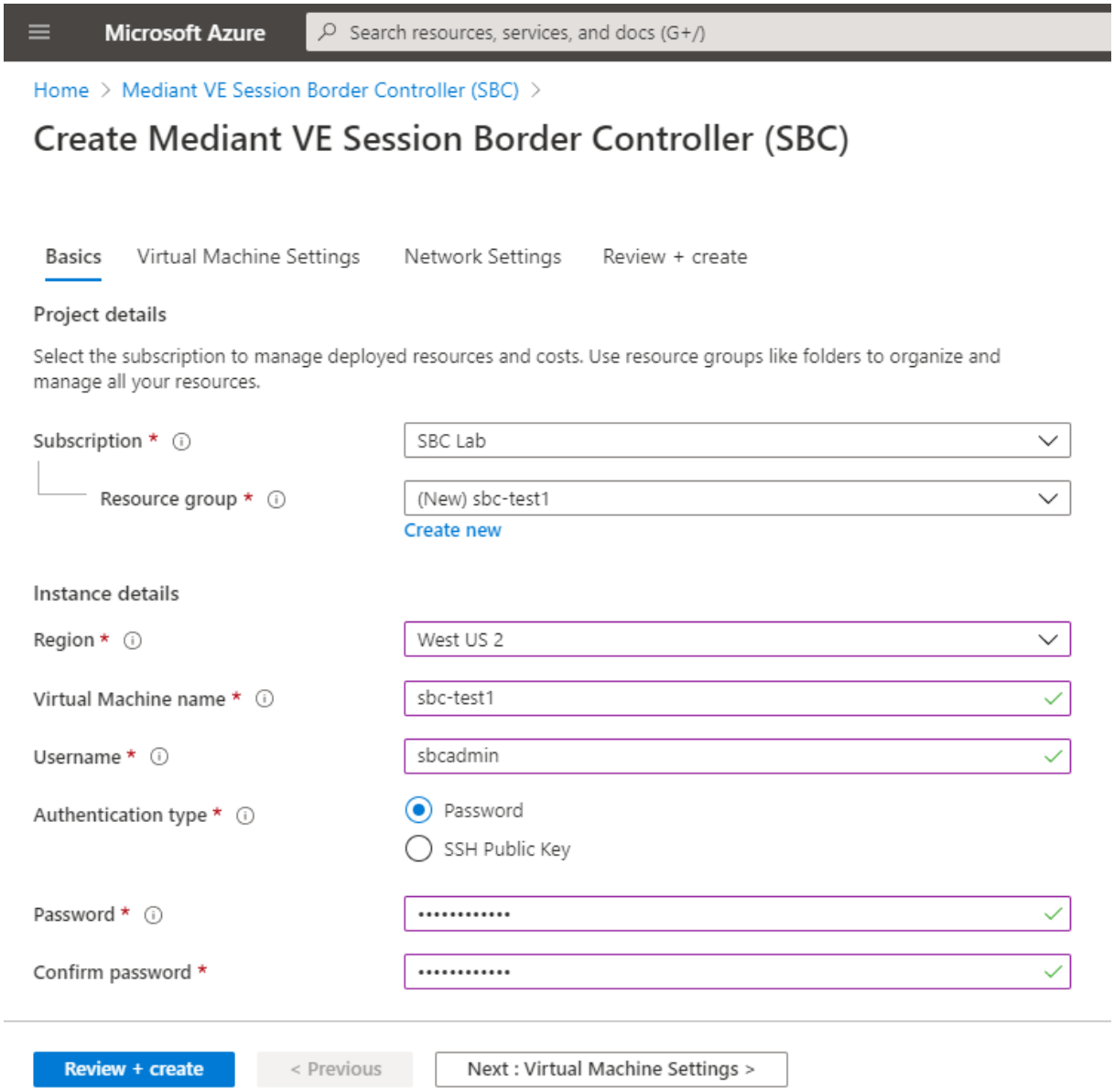
3. Click **GET IT NOW**; the Azure portal and Mediant VE SBC Product Overview screen appears:

Figure 4: Mediant VE SBC Product Overview



4. Click **Create** to start a new Mediant VE deployment.
The Create AudioCodes Mediant VE SBC for Microsoft Azure dialog appears. The dialog contains multiple steps. Complete each step according to the description below.

Figure 5: Basics Step



5. In the **Basics** step, do the following:
   a. In the 'Subscription' field, select a proper subscription for your deployment.
   b. In the 'Resource group' field, click **Create new** and then enter a unique name for the new resource group. Alternatively, you may select an existing empty resource group from the list.
   c. In the 'Region' field, select a proper region for your deployment.
   d. In the 'Virtual Machine name' field, enter a unique name for the new VM.
   e. In the 'Username' field, enter a username.
   f. For 'Authentication type', select **Password**.
   g. In the 'Password' field, enter a password, and then enter it again in the 'Confirm password' field.

These credentials are used to connect to the management interface of the deployed Mediant VE (instead of the default **Admin**/**Admin** credentials used in other environments).

Azure imposes some limitations on username and password. For example, it prohibits the use of "Admin" for username and requires you to use a strong password that meets the following policy:

- A minimum of 12 characters
- Use three out of the following characters:
  - lowercase characters
  - uppercase characters
  - numbers
  - symbols

h. Click **OK**.

6. In the **Virtual Machine Settings** step, do the following:

a. Choose the virtual machine size.
For a list of supported virtual machine sizes and corresponding capacity figures, refer to the *SBC-Gateway-MSBR Series Release Notes*.

b. Choose the disk type for the virtual machine.
As SBC software typically doesn't perform extensive disk activity, **Standard HDD** disk type is adequate for most deployments. However, if you plan to use SBC for transcoding, then a virtual machine should have a minimum of 2 vCPUs.

c. Choose the OS version for the deployed SBC software:

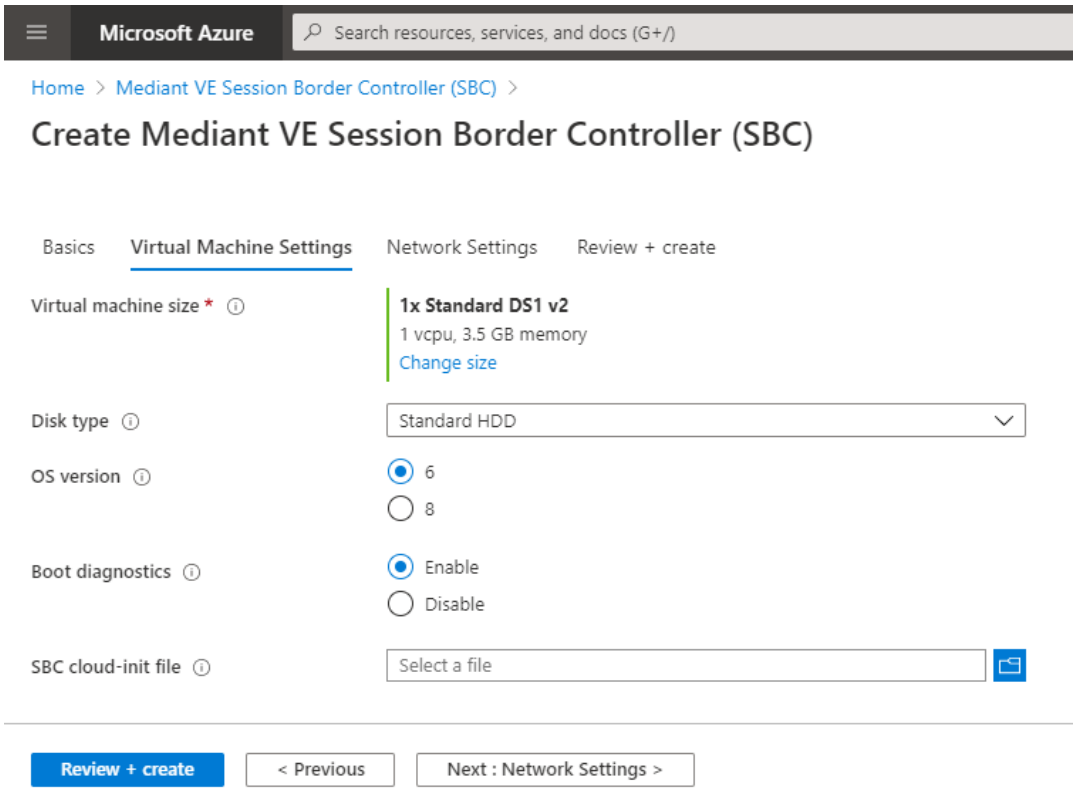
- **6** – this version corresponds to the 7.20A stream, which is based on CentOS 6.
- **8** – this version corresponds to the new 7.40A stream, which is based on CentOS Stream 8 and provides significantly better performance and capacity (refer to the *SBC-Gateway Series Release Notes* for details).

d. Choose whether to enable virtual machine's boot diagnostics.

e. (Optionally), provide Mediant VE automatic configuration script (cloud-init file).
For more information, refer to the *Automatic Provisioning of Mediant VE SBC via Cloud-Init Configuration Note*.

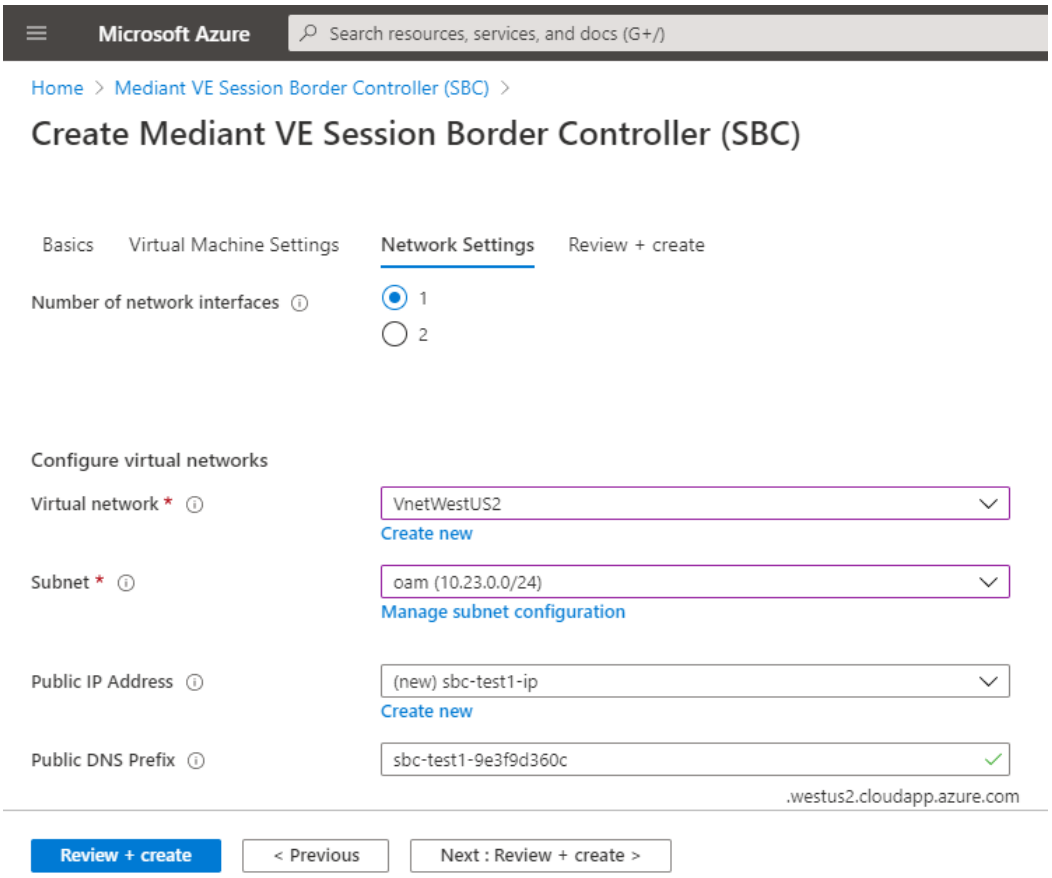
f. Click **OK**.

Figure 6: Virtual Machine Settings Step



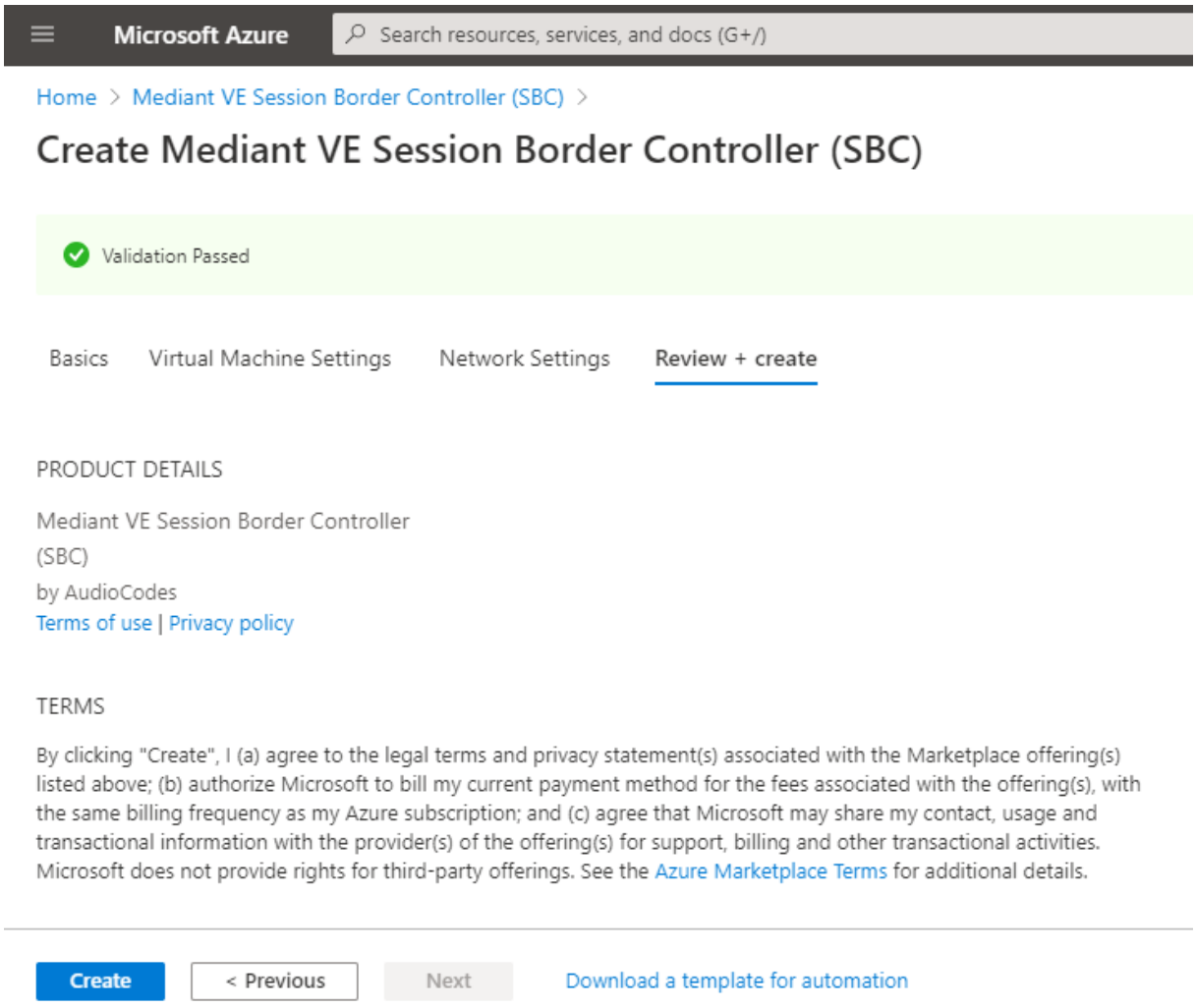
7. In the **Network Settings** step, do the following:
   a. Choose the number of network interfaces for the new virtual machine.
   Deployment via Azure Marketplace supports up to two network interfaces. If you need more interfaces, perform deployment via the PowerShell CLI, as described in the *Mediant Virtual Edition SBC for Microsoft Azure Installation Manual*.
   b. Configure the virtual network where the new VM will be deployed.
   You may either create a new virtual network or select an existing one. Azure virtual machine is always connected to a single virtual network, regardless of the number of its network interfaces.
   c. Configure the subnet for each network interface.
   You may either create a new subnet (for new virtual network) or select an existing one. If you choose two network interfaces, you must connect each interface to a different subnet. This is a limitation of Azure Marketplace UI and may be overcome by performing the deployment via the PowerShell CLI, as described in the *Mediant Virtual Edition SBC for Microsoft Azure Installation Manual.* You can then access the SBC management interfaces (Web and SSH) through the 1st network interface only.
   d. Configure the virtual machine's Public IP Address.
   You may either create a new Public IP Address or select an existing one.
      - If you create a new Public IP Address, select **Static Assignment**. This ensures that the IP address remains unchanged if you stop the virtual machine.
      - If you choose two network interfaces, the public IP address will be attached to the 1st network interface.
   e. Click **OK**

Figure 7: Network Settings Step



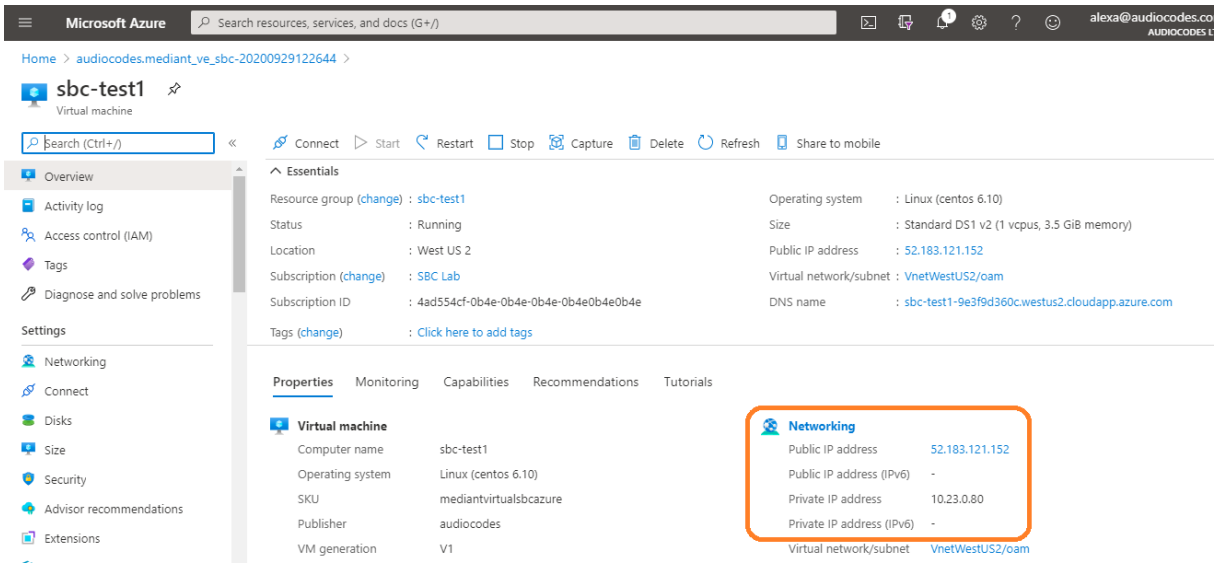
8. In the **Review + create** step, review the Mediant VE SBC terms of use and virtual machine configuration, and then click **Create**.

Figure 8: Review + Create Step



9. Wait until the virtual machine deployment is complete, and then determine the IP address that is assigned to your virtual machine that can be used to access management interface:
   - If you assigned a public IP address to the VM, you may use it to access the management interface.
   - Alternatively, you may use a private IP address of the 1st network interface.

Figure 9: Determining IP Address of Deployed VM



10. Log in to the management interface (through Web or SSH) using the credentials that you configured during the virtual machine set up.

5 Configuring AudioCodes' SBC

This section provides example of step-by-step procedures on how to configure AudioCodes SBC for interworking between Microsoft Azure Communication Services (ACS) and the Generic SIP Trunk. These configuration procedures are based on the topology example described in Section 2.1 on page 9, and includes the following main topics:

- SBC LAN interface – administrator's management station and Generic SIP Trunking (depend on topology) environment
- SBC WAN interface - Generic SIP Trunking (depend on topology) and Teams Direct Routing environment

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

- For implementing connection to ACS based on the configuration described in this section, AudioCodes SBC must be installed with a License Key. For more information, see Section 1.3 on page 7.
- The scope of this document does **not** cover all security aspects for configuring this topology. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document, which can be found at AudioCodes web site.

5.1 SBC Configuration Concept with ACS

The diagram below represents AudioCodes' device configuration concept.

Figure 10: SBC Configuration Concept

5.2 IP Network Interfaces Configuration

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

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

Figure 11: Network Interfaces in the Topology with SIP Trunk on the LAN

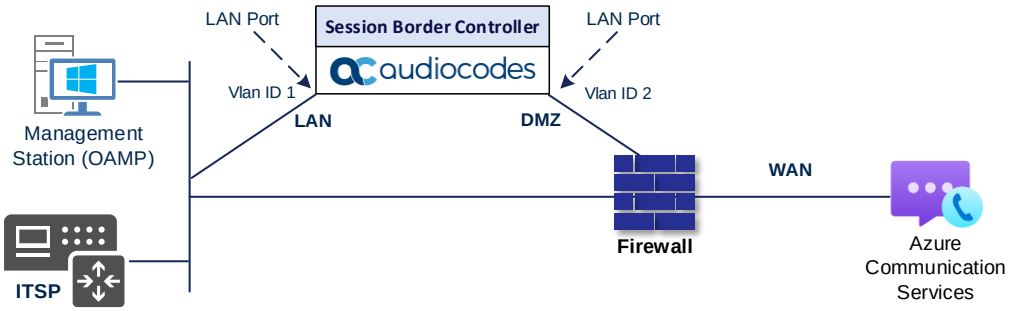
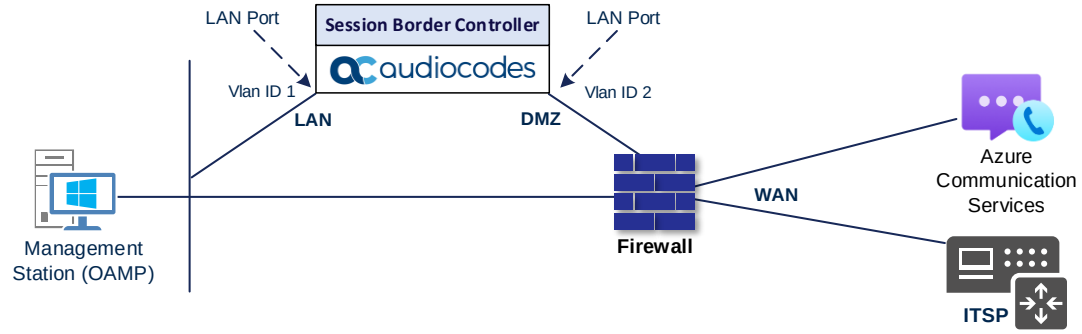


Figure 12: Network Interfaces in the Topology with SIP Trunk on the WAN



This document provides an example of the following deployment method:

- SBC implemented in the Azure with one IP interface, used for all purposes:
  - Management (OAMP)
  - Signaling and media connectivity to Generic SIP Trunk and ACS

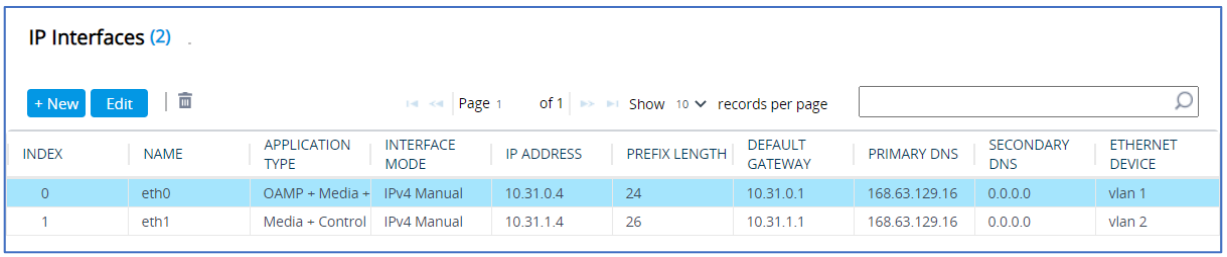
5.2.1 Configure VLANs

Since default VLANs configuration was used in this interoperability test topology, no additional configuration is needed.

5.2.2 Configure Network Interfaces

Network Interfaces are configured automatically in the Azure implementation. Refer to the *Mediant Virtual Edition SBC for Microsoft Azure Installation Manual* document, which can be found at AudioCodes web site. The example of the configured IP network interface are shown below:

Figure 13: Configuration Example of the Network Interface Table



5.2.3 Configure NAT Translation

The SBC, located in the Azure Cloud, implements private IP addresses. The NAT Translation table lets you configure network address translation (NAT) rules for translating source IP addresses into NAT IP addresses (*global - public*). These are used in front of the Azure firewall facing the Generic SIP Trunk and the ACS.

A NAT Translation Table is created automatically during the implementation process (as described in step 7 on page 14 above.) But if it is required to configure manually, follow next steps.

To configure the NAT translation rules:

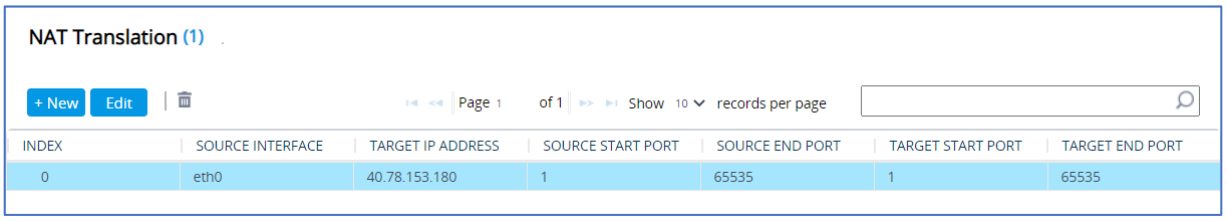
1. Open the NAT Translation table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **NAT Translation**).
2. Add a new NAT Translation rule by clicking **+New** at the top of the interface, and then configure the parameters using the table below as reference.

Table 3: NAT Translation Rule

Index	Source Interface	Source Start Port	Source End Port	Target IP Address	Target Start Port	Target End Port
0	eth0	1	65535	<Public IP Address>	1	65535

3. Click **Apply**.

Figure 14: Example of the NAT Translation Table



5.3 SIP TLS Connection Configuration

This section describes how to configure the SBC for using a TLS connection with the ACS. This configuration is essential for a secure SIP TLS connection. The configuration instructions example in this section are based on the following domain structure that must be implemented as part of the certificate which must be loaded to the host SBC:

- CN: acstest.audiocodes.be
- SAN: acstest.audiocodes.be

This certificate module is based on the Service Provider's own TLS Certificate. For more certificate structure options, see Microsoft Teams Direct Routing documentation.

The Azure Communication Services direct routing allows ***only*** TLS connections from SBCs for SIP traffic with a certificate signed by one of the Trusted Certification Authorities.

Currently, supported Certification Authorities can be found in the following link:

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc

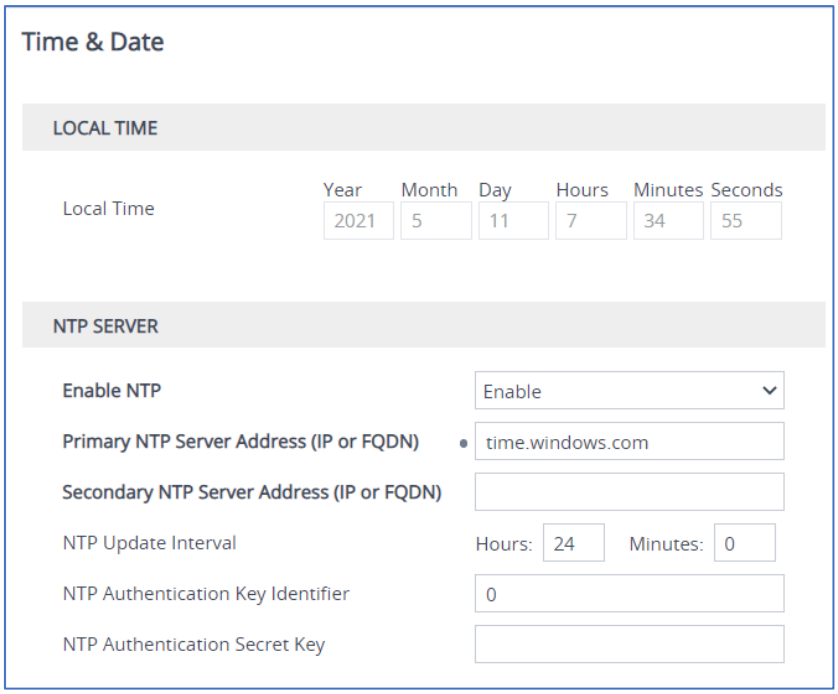
5.3.1 Configure the NTP Server Address

This section describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (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., **time.windows.com**).

Figure 15: Configuring NTP Server Address



3. Click **Apply**.

5.3.2 Create a TLS Context for ACS (same as 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 SSL.com Global Root CA. The certificate is used by the SBC to authenticate the connection with ACS.

The procedure involves the following main steps:

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

To create a TLS Context for ACS:

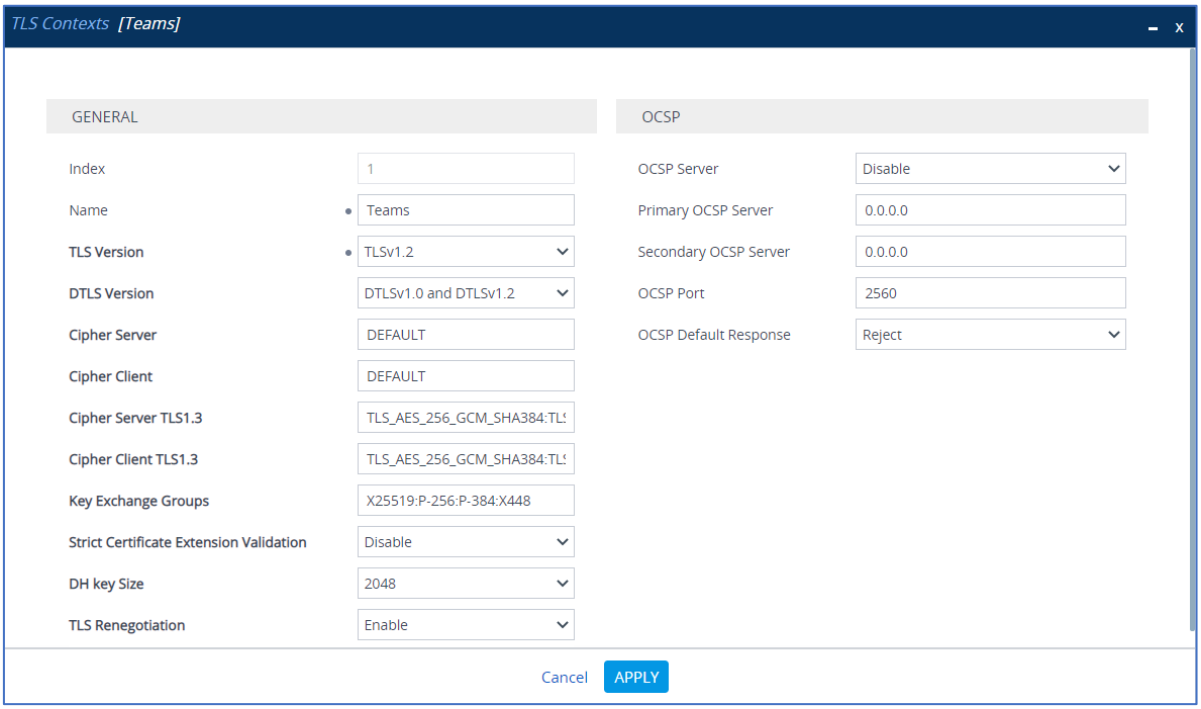
1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. Create a new TLS Context by clicking **+New** at the top of the interface, and then configure the parameters using the table below as reference.

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.		

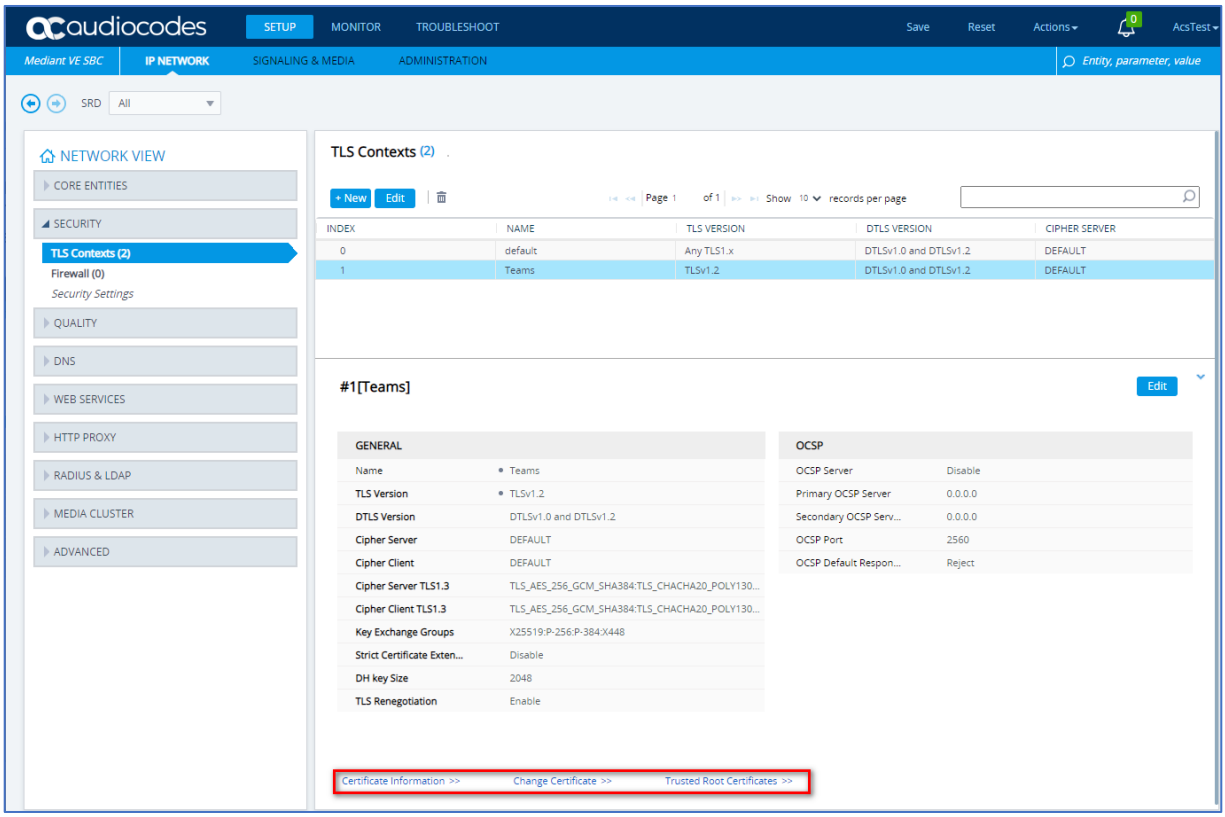
The table above exemplifies configuration focusing on interconnecting SIP and media. You might want to configure additional parameters according to your company's policies. For example, you might want to configure Online Certificate Status Protocol (OCSP) to check if SBC certificates presented in the 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 16: Configuration of TLS Context for ACS



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

Figure 17: Configured TLS Context for ACS and Interface to Manage the Certificates



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

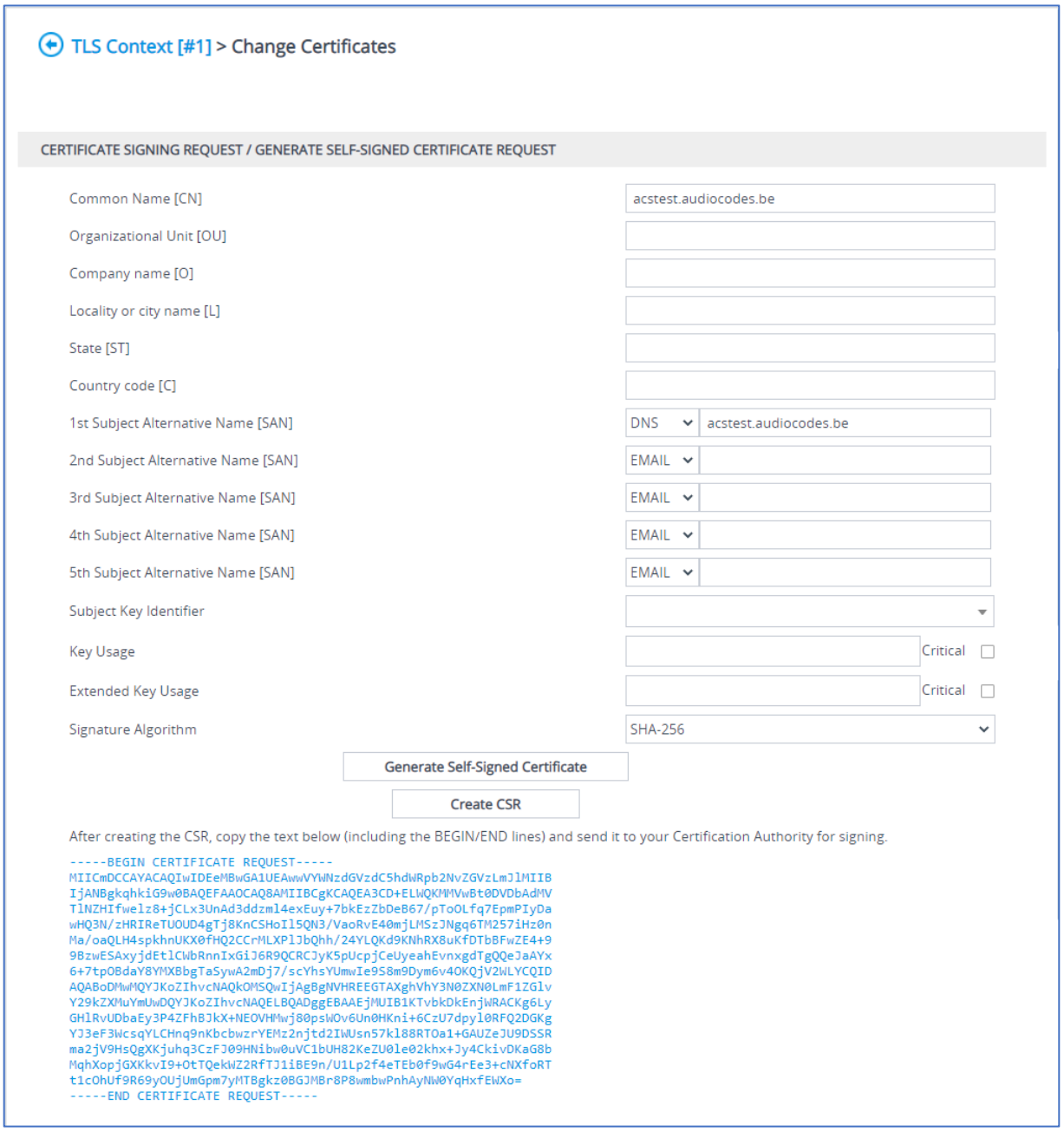
This section shows how to generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority.

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

1. 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, **acstest.audiocodes.be**).
   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, **acstest.audiocodes.be**).
   c. Change the 'Private Key Size' based on the requirements of your Certification Authority. Many CAs do not support private key of size **1024**.
   d. To change the key size on TLS Context, go to: **Generate New Private Key and Self-Signed Certificate**, change the 'Private Key Size' to **1024** (if this required by CA) and then click **Generate Private-Key**. To use **2048** as a Private Key Size value, you can click **Generate Private-Key** without changing the default key size value.
   e. Enter the rest of the request fields according to your security provider's instructions.

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

Figure 18: 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.

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

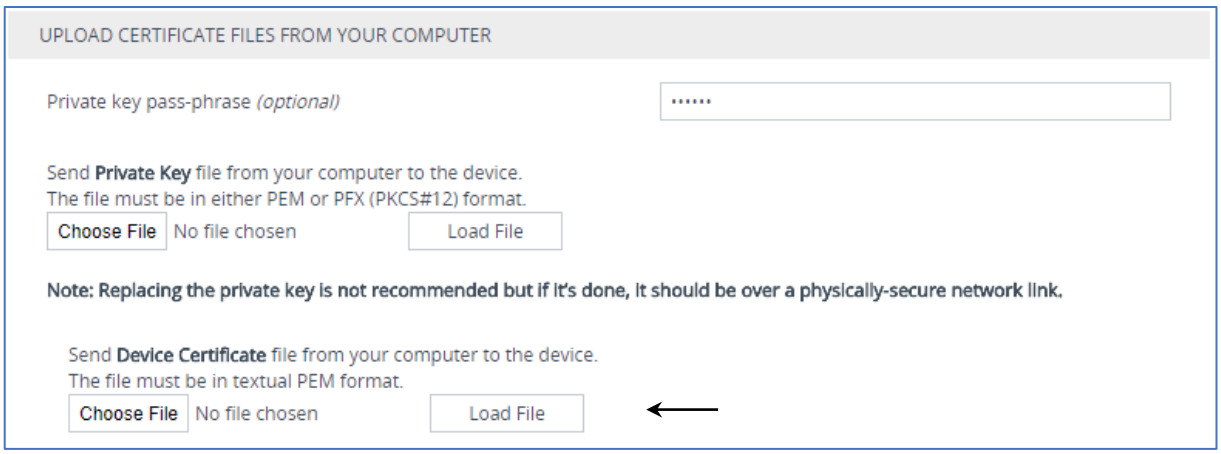
After obtaining the SBC signed and Trusted Root/Intermediate Certificate from the CA, install the following:

- SBC certificate
- Root / Intermediate certificates

To install the SBC certificate:

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

Figure 19: 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:

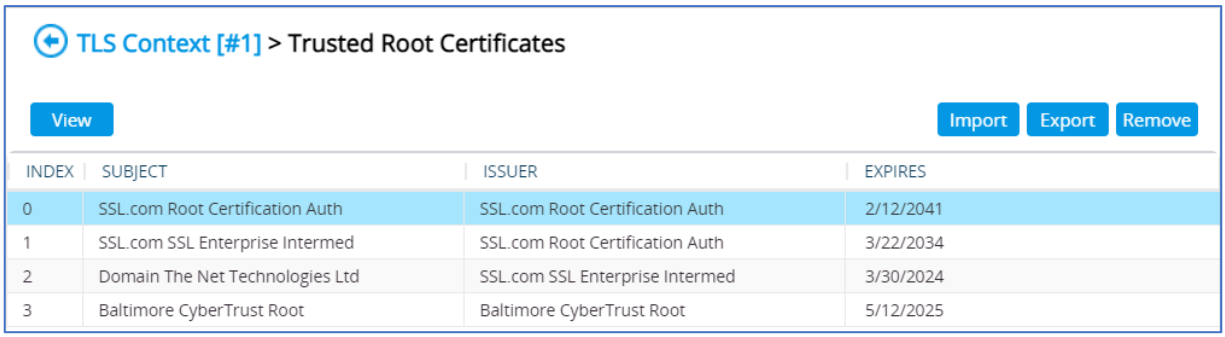
Figure 20: Message Indicating Successful Upload of the Certificate

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 21: 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 22: Example of Configured Trusted Root Certificates



5.3.5 Method of Generating and Installing the Wildcard Certificate

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

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

To install the certificate:

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

5.3.6 Deploy Trusted Root Certificate for MTLS Connection

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

Microsoft 365 updated services such as, messaging, meetings, telephony, voice, and video to use TLS certificates from a different set of Root Certificate Authorities (CAs). For more details of the new Root CAs, refer to Microsoft technical guidance at Office TLS Certificate Changes.

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

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

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

Before importing the DigiCert Root Certificate into AudioCodes' SBC, make sure it's in .PEM or .PFX format. If it isn't, you need to convert it to .PEM or .PFX format, otherwise 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'.

5.4 Configure Media Realm

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

- One for the WAN 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:

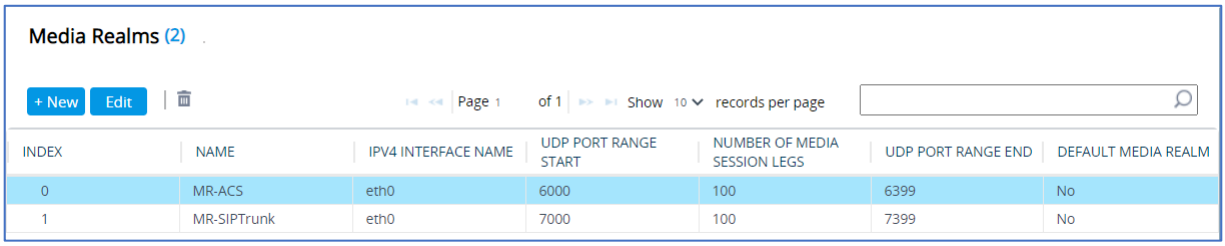
1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Configure Media Realms as follows (you can use the default Media Realm (Index 0), but modify it):

Table 5: Configuration Example Media Realms in Media Realm Table

Index	Name	Topology Location	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
0	MR-ACS (arbitrary name)	Up	eth0	6000	100 (media sessions assigned with port range)
1	MR-SIPTrunk (arbitrary name)		eth0	7000	100 (media sessions assigned with port range)

The configured Media Realms are shown in the figure below:

Figure 23: Configuration Example Media Realms in Media Realm Table



5.5 Configure 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 Azure Communication Services direct routing 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.

Table 6: Configuration Example of SIP Signaling Interfaces

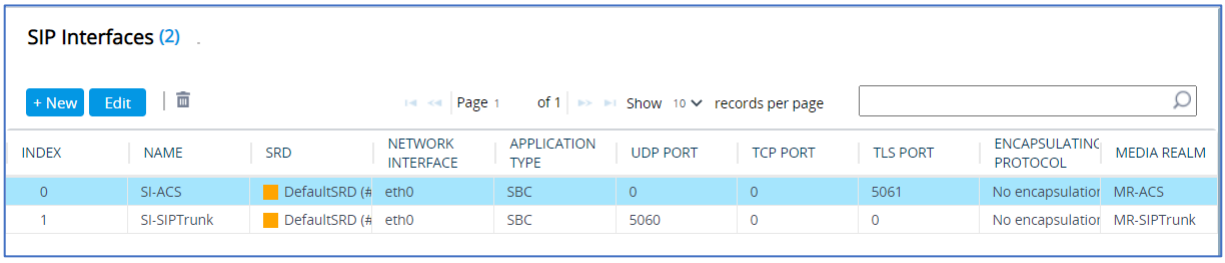
Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepalive	Classification Failure Response Type	Media Realm	TLS Context Name
0	SI-ACS (arbitrary name)	eth0	SBC	0 (Phone System does not use UDP or TCP for SIP signaling)	0	5061 (as configured in the Office 365)	Enable	0 (Recommended to prevent DoS attacks)	MR-ACS	Teams
1	SI-SIPTrunk (arbitrary name)	eth0	SBC	5060 (according to Service Provider requirement)	0	0	Disable (leave default value)	0 (Recommended to prevent DoS attacks)	MR-SIPTrunk	-

> For implementing an MTLS connection with the Microsoft Teams network, configure 'TLS Mutual Authentication' to "Enable" for the Azure Communication Services direct routing.

> Loading DigiCert Trusted Root Certificates to AudioCodes' SBC is mandatory for implementing an MTLS connection with the Microsoft Teams network. Refer to Section 5.3.6 on page 27.

The configured SIP Interfaces are shown in the figure below:

Figure 24: Configuration Example of SIP Signaling Interfaces



5.6 Configure Proxy Sets and Proxy Address

5.6.1 Configure Proxy Sets

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 ACS and SIP Trunk. Note that the configuration of a Proxy Set 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 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.

> For devices with PSTN interface (Hybrid SBC) it is highly recommended that you do not configure Proxy Set ID 0 and IP Group ID 0. The only time that you should configure this specific Proxy Set and IP Group is when it is used for the Gateway Interface (e.g., PSTN fallback).

To configure a Proxy Sets:

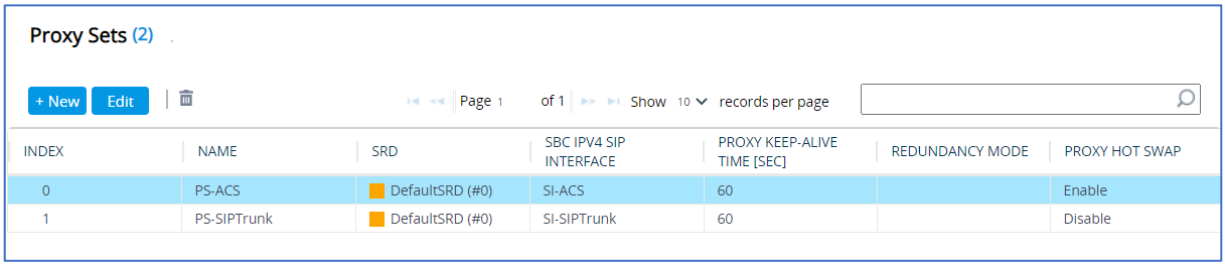
1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Configure Proxy Sets as shown in the table below:

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
0	PS-ACS (arbitrary name)	SI-ACS	Teams	Using Options	Enable	Random Weights
1	PS-SIPTrunk (arbitrary name)	SI-SIPTrunk	Default	Using Options	-	-

The configured Proxy Sets are shown in the figure below:

Figure 25: Configuration Example Proxy Sets in Proxy Sets Table



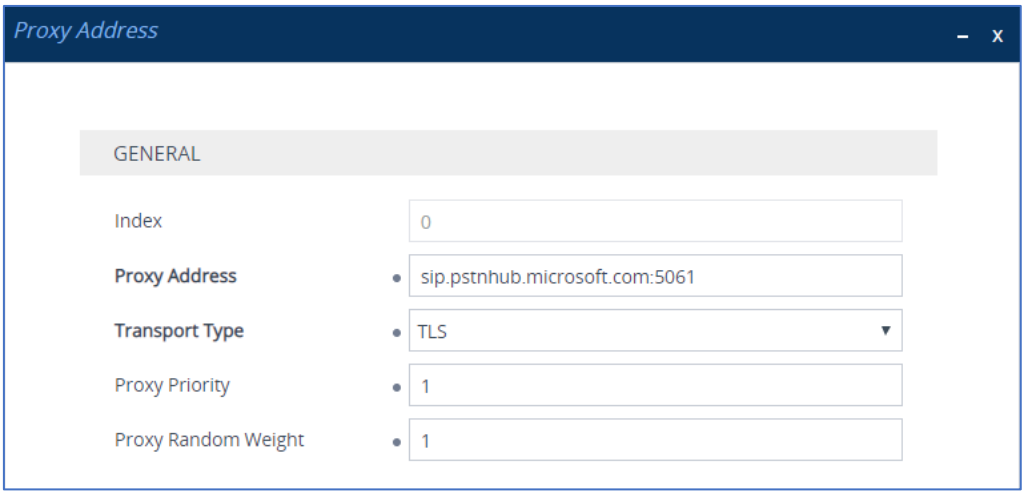
5.6.2 Configure Proxy Addresses

This section shows how to configure a Proxy Address.

To configure a Proxy Address for ACS (same as for Teams Direct Routing):

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **PS-ACS**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**; the following dialog box appears:

Figure 26: Configuring Proxy Address for Azure Communication Services direct routing



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

Table 8: Configuration Proxy Address for ACS

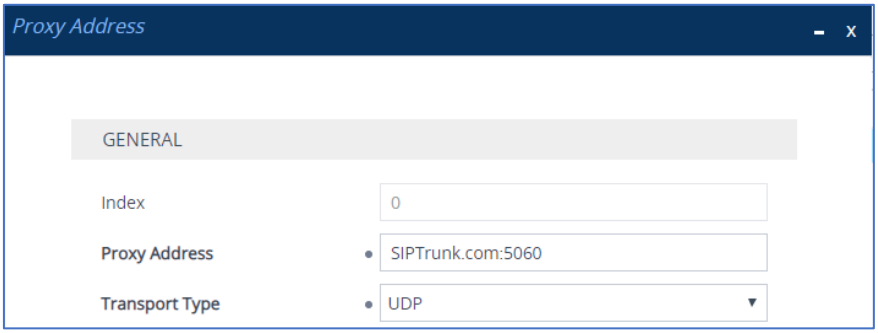
Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	sip.pstnhub.microsoft.com:5061	TLS	1	1
1	sip2.pstnhub.microsoft.com:5061	TLS	2	1
2	sip3.pstnhub.microsoft.com:5061	TLS	3	1

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

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**; the following dialog box appears:

Figure 27: Configuring Proxy Address for SIP Trunk



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

Table 9: Configuration Proxy Address for SIP Trunk

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	SIPTrunk.com:5060 (SIP Trunk IP / FQDN and port)	UDP	0	0

4. Click **Apply**.

5.7 Configure Coder Groups

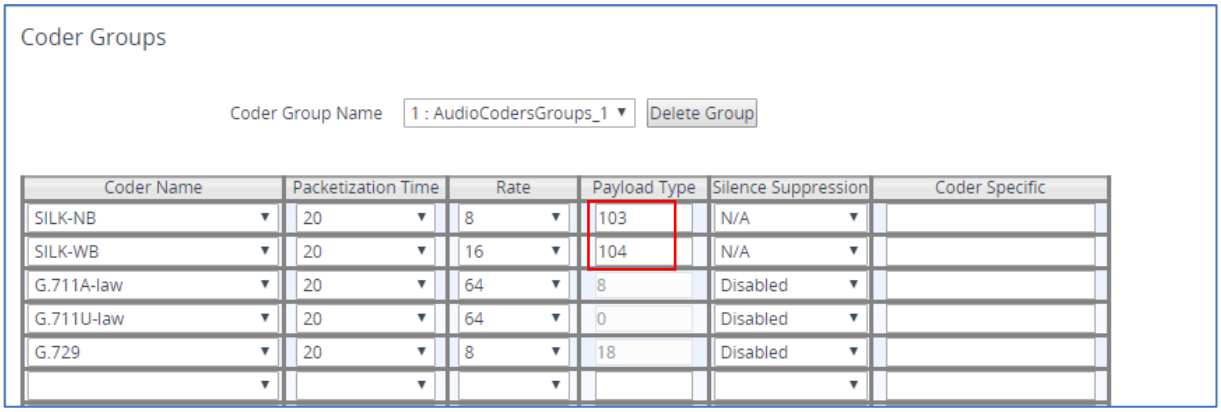
This section describes how to configure coders (known as *Coder Groups*). ACS supports the SILK and G.722 coders while the network connection to the SIP Trunk may restrict operation with a dedicated coders list. You need to add a Coder Group with the supported coders for each of the following leg, the ACS and the SIP Trunk.

> The Coder Group ID for this entity will be assigned to its corresponding IP Profile in Section 5.8.

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 28: Configuring Coder Group for ACS



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

5.8 Configure IP Profiles

This section describes how to configure IP Profiles. 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.

To configure an IP Profile:

1. Open the Proxy Sets table (**Setup** menu > **Signaling and Media** tab > **Coders and Profiles** folder > IP Profiles).
2. Click **+New** to add the IP Profile for the Azure Communication Services direct routing. Configure the parameters using the table below as reference.

Table 10: Configuration Example: ACS IP Profile

Parameter	Value
General	
Name	**ACS** (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**
RFC 2833 Mode	**Extended**
RTCP Mode	**Generate Always** (required, as some ITSPs do not send RTCP packets during Hold, but Microsoft expects them)
ICE Mode	**Lite**
SBC Signaling	
SIP UPDATE Support	**Not Supported**
Remote re-INVITE Support	**Supported Only With SDP**
Remote Delayed Offer Support	**Not Supported**
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally**
Remote Replaces Mode	**Handle Locally**
Remote 3xx Mode	**Handle Locally**
SBC Hold	
Remote Hold Format	**Inactive** (some SIP Trunk may answer with a=inactive and IP=0.0.0.0 in response to the Re-Invite with Hold request from Teams. Microsoft Media Stack doesn't support this format. So, SBC will replace 0.0.0.0 with its IP address)
All other parameters can be left unchanged at their default values.	

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

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

Table 11: Configuration Example: SIP Trunk IP Profile

Parameter	Value
General	
Name	**SIPTrunk**
Media Security	
SBC Media Security Mode	**Not Secured**
SBC Signaling	
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally**
Remote Replaces Mode	**Handle Locally**
Remote 3xx Mode	**Handle Locally**
All other parameters can be left unchanged with their default values.	

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

5.9 Configure 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.

> For devices with PSTN interface (Hybrid SBC) it is highly recommended that you do not configure Proxy Set ID 0 and IP Group ID 0. The only time that you should configure this specific Proxy Set and IP Group is when it is used for the Gateway Interface (e.g., PSTN fallback).

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 ACS:

Parameter	Value
Name	**IPG-ACS**
Topology Location	**Up**
Type	**Server**
Proxy Set	**PS-ACS**
IP Profile	**ACS**
Media Realm	**MR-ACS**
Classify by Proxy Set	**Disable**
Local Host Name	**<FQDN name of the SBC>** (based on our example, *acstest.audiocodes.be*).
Always Use Src Address	**Yes**
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>').
Inbound Message Manipulation Set	**1**
Proxy Keep-Alive using IP Group settings	**Enable**
All other parameters can be left unchanged with their default values.	

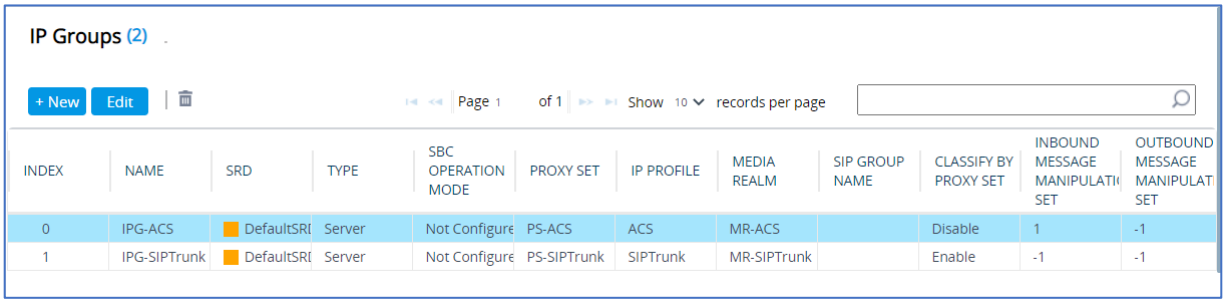
3. Click **+New** to add the IP Group for the SIP Trunk:

Parameter	Value
Name	**IPG-SIPTrunk**
Type	**Server**
Proxy Set	**PS-SIPTrunk**
IP Profile	**SIPTrunk**
Media Realm	**MR-SIPTrunk**
SIP Group Name	(according to ITSP requirement)
All other parameters can be left unchanged with their default values.	

The configuration of the SIP Trunk 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.

The configured IP Groups are shown in the figure below:

Figure 29: Configured IP Groups in IP Group Table



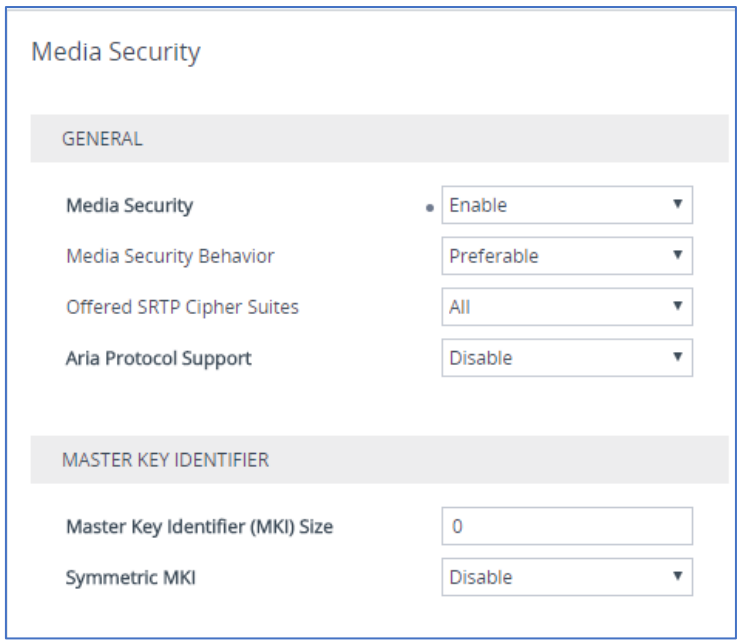
5.10 Configure SRTP

This section describes how to configure media security. The Azure Communication Services direct routing 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**.

5.11 Configure Message Manipulation Rules

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

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

Implementation of the Message Manipulation rule with ACS (shown below) is optional according to site deployment requirements.

To configure SIP message manipulation rule for ACS:

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 1) for ACS. This rule applies to messages received from the ACS IP Group. This rule removes the SIP P-Asserted-Identity header.

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

3. Configure another manipulation rule (Manipulation Set 1) for ACS. This rule applies to messages received from the ACS IP Group. This rule remove the SIP Privacy Header in all messages, except for calls with presentation restriction.

Parameter	Value
Index	**1**
Name	**Remove Privacy Header**
Manipulation Set ID	**1**
Condition	**Header.Privacy exists And Header.From.URL !contains 'anonymous'**
Action Subject	**Header.Privacy**
Action Type	**Remove**

5.12 Configure Message Condition Rules

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

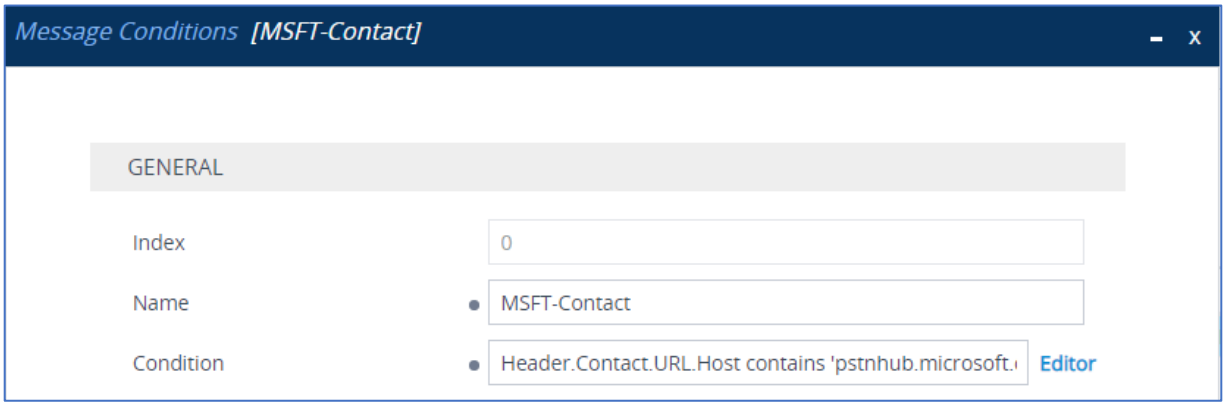
The following condition verifies that the Contact header contains Microsoft FQDN.

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	**MSFT-Contact** (arbitrary descriptive name)
Condition	**Header.Contact.URL.Host contains 'pstnhub.microsoft.com'**

Figure 31: Configuring Condition Table



3. Click **Apply**.

5.13 Configure 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 5-12: 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)	SI-ACS	52.112.*.*	acstest.audiocodes.be (example)	MSFT-Contact	Allow	IPG-ACS
1	Teams_52_113 (arbitrary name)	SI-ACS	52.113.*.*	acstest.audiocodes.be (example)	MSFT-Contact	Allow	IPG-ACS
2	Teams_52_114 (arbitrary name)	SI-ACS	52.114.*.*	acstest.audiocodes.be (example)	MSFT-Contact	Allow	IPG-ACS
3	Teams_52_115 (arbitrary name)	SI-ACS	52.115.*.*	acstest.audiocodes.be (example)	MSFT-Contact	Allow	IPG-ACS
4	Teams_52_120 (arbitrary name)	SI-ACS	52.120.*.*	acstest.audiocodes.be (example)	MSFT-Contact	Allow	IPG-ACS
5	Teams_52_121 (arbitrary name)	SI-ACS	52.121.*.*	acstest.audiocodes.be (example)	MSFT-Contact	Allow	IPG-ACS
6	Teams_52_122 (arbitrary name)	SI-ACS	52.122.*.*	acstest.audiocodes.be (example)	MSFT-Contact	Allow	IPG-ACS
7	Teams_52_123 (arbitrary name)	SI-ACS	52.123.*.*	acstest.audiocodes.be (example)	MSFT-Contact	Allow	IPG-ACS

3. Click **Apply**.

5.14 Configure IP-to-IP Call Routing Rules

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

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

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

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

To configure IP-to-IP routing rules:

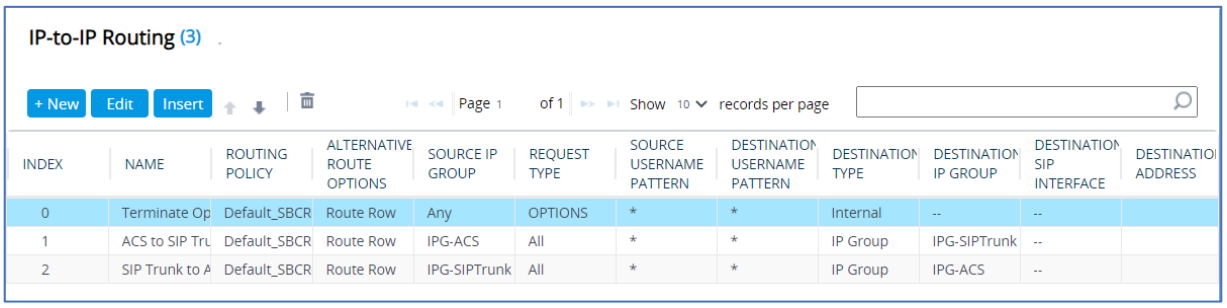
1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure routing rules as shown in the table below:

Table 13: IP-to-IP Call Routing Rules

Index	Name	Source IP Group	Request Type	Call Triger	Reroute IP Group	Dest Type	Dest IP Group	Internal Action
0	Terminate Options	Any	OPTIONS			Internal		Reply (Response='200')
1	ACS to SIP Trunk (arbitrary name)	IPG-ACS				IP Group	IPG-SIPTrunk	
2	SIP Trunk to ACS (arbitrary name)	IPG-SIPTrunk				IP Group	IPG-ACS	

The configured routing rules are shown in the figure below:

Figure 32: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



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

5.15 Configure Number Manipulation Rules

This section describes how to configure IP-to-IP number manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 5.9 on page 36) to denote the source and destination of the call.

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

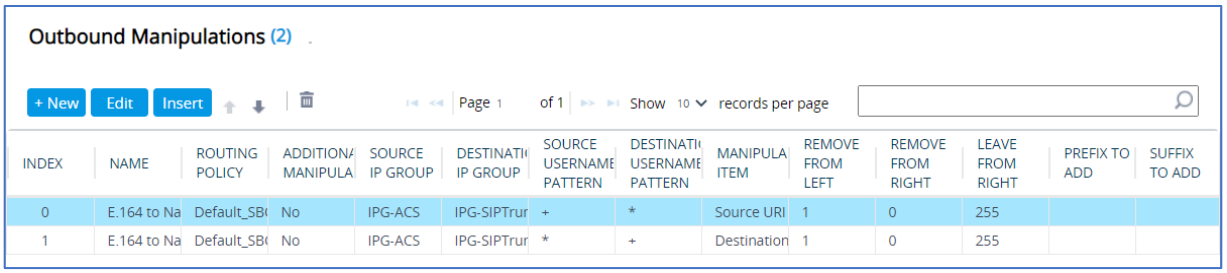
For example, for this interoperability test topology, a manipulation is configured to convert E.164 phone numbers format, used by ACS to national telephone number format, used by the SIP Trunk. To do this, the "+" (plus sign) will be removed from the destination and source numbers (if it exists) for calls from the ACS IP Group to the Generic SIP Trunk IP Group.

To configure a number manipulation rule:

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

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between ACS IP Group and Generic SIP Trunk IP Group:

Figure 33: Example of Configured IP-to-IP Outbound Manipulation Rules



Rule Index	Description
0	Calls from ACS IP Group to SIP Trunk IP Group with the prefix source number "+", remove one digit from left.
1	Calls from ACS IP Group to SIP Trunk IP Group with the prefix destination number "+", remove one digit from left.

5.16 Miscellaneous Configuration

This section describes miscellaneous SBC configurations.

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

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

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

To optimize core allocation for a profile:

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

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

6 Verify the Pairing Between the SBC and ACS

After you have paired the SBC with ACS, validate that the SBC can successfully exchange OPTIONS with ACS.

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 PS-ACS and verify that 'Status' is online. If you see a failure, you need to troubleshoot the connection first.

Figure 34: 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	PS-ACS	Load Balancing	Enabled						ONLINE
				sip.pstnhub.microsoft.com(52.114.132.46:5061) (*)	1	1.00	1135	0	ONLINE
				sip2.pstnhub.microsoft.com(52.114.76.76:5061) (*)	2	1.00	1135	0	ONLINE
				sip3.pstnhub.microsoft.com(52.114.7.24:5061) (*)	3	1.00	1133	0	ONLINE
1	PS-SIPTrunk	Parking	Enabled						ONLINE
				195.189.192.154(*)	-	-	1116	49	ONLINE

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

The syntax of SIP messages must conform with Microsoft 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 35: Example of an 'INVITE' Message

```
INVITE sip:+16132606017@vendor4.lab.internetvoice.ca SIP/2.0
Via: SIP/2.0/TLS int-sbc1.audctrunk.aceducation.info:5061;alias;branch=z9hG4bKac659089971
Max-Forwards: 18
From: <sip:+97239764347@siptrunking.bell.ca;user=phone>;tag=1c132512889
To: "USER 6132606017" <sip:+16132606017@vendor4.lab.internetvoice.ca>
Call-ID: 20651257111120201029 26@int-sbc1.audctrunk.aceducation.info
CSeq: 1 INVITE
Contact: <sip:+97239764347@int-sbc1.audctrunk.aceducation.info:5061;transport=tls>
Supported: 100rel,sdp-anat
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
User-Agent: M800B/v.7.20A.258.271
P-Asserted-Identity: <sip:+97239764347@siptrunking.bell.ca;user=phone>
Accept: application/media_control+xml,application/sdp,multipart/mixed
Recv-Info: x-broadworks-client-session-info
Content-Type: application/sdp
Content-Length: 1131
```

- **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 Requirements for 'OPTIONS' Messages Syntax

Figure 36: Example of 'OPTIONS' message

```
OPTIONS sip:vendor4.lab.internetvoice.ca SIP/2.0
Via: SIP/2.0/TLS int-sbc1.audctrunk.aceducation.info:5061;alias;branch=z9hG4bKac886439183
Max-Forwards: 70
From: <sip:195.189.192.160>;tag=1c1860024667
To: <sip:195.189.192.160>
Call-ID: 6389312301111202010 2946@int-sbc1.audctrunk.aceducation.info
CSeq: 1 OPTIONS
Contact: <sip:int-sbc1.audctrunk.aceducation.info:5061;transport=tls>
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: M800B/v.7.20A.258.271
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 14: 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, *int-sbc1.audctrunk.aceducation.info*. The name changes the host name in the call received from the IP Group.	See Section 5.9.

A.4 Connectivity Interface Characteristics

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

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

Microsoft has a partnership with some SBC vendors and guarantees their devices' interoperability with the interface. All validated devices are listed on Microsoft's website. Microsoft only supports devices *that are validated* 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 15: 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 (ACS 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**.

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

©2023 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-39472