

Microsoft® Teams Direct Routing Enterprise Model and Twilio Elastic SIP Trunk using AudioCodes Mediant™ SBC

Version 7.2

Microsoft Partner

Gold Communications



Table of Contents

1	Introduction	7
1.1	Intended Audience	7
1.2	About Twilio	7
1.3	About AudioCodes SBC Product Series	7
1.4	About Microsoft Teams Direct Routing	7
2	Component Information.....	9
2.1	AudioCodes SBC Version.....	9
2.2	Twilio Elastic SIP Trunk Version	9
2.3	Microsoft Teams Direct Routing Version.....	9
2.4	Interoperability Test Topology	10
2.4.1	Enterprise Model Implementation.....	10
2.4.2	Environment Setup	11
2.4.3	Infrastructure Prerequisites.....	11
2.4.4	Known Limitations.....	11
3	Configuring Teams Direct Routing	13
3.1	Prerequisites	13
3.2	SBC Domain Name in the Teams Enterprise Model	13
3.3	Example of the Office 365 Tenant Direct Routing Configuration	15
3.3.1	Add New SBC to Direct Routing	16
3.3.2	Add Voice Route and PSTN Usage.....	17
3.3.3	Add Voice Routing Policy	19
3.3.4	Enable Online User.....	20
3.3.5	Assigning Online User to the Voice Route	20
4	Configuring AudioCodes SBC	21
4.1	SBC Configuration Concept in Teams Direct Routing Enterprise Model	22
4.2	IP Network Interfaces Configuration	22
4.2.1	Configure VLANs	23
4.2.2	Configure Network Interfaces	23
4.3	SIP TLS Connection Configuration	25
4.3.1	Configure the NTP Server Address	25
4.3.2	Create a TLS Context.....	26
4.3.3	Configure a Certificate for Operation with Microsoft Teams.....	27
4.3.4	Method of Generating and Installing the Wildcard Certificate	30
4.3.5	Deploy Baltimore Trusted Root Certificate	31
4.3.6	Configure a Certificate for Operation with Twilio Elastic SIP Trunk	31
4.4	Configure Media Realms	32
4.5	Configure SIP Signaling Interfaces	33
4.6	Configure Proxy Sets and Proxy Address.....	34
4.6.1	Configure a Proxy Address.....	35
4.7	Configure Coders	37
4.8	Configure IP Profiles.....	39
4.9	Configure IP Groups.....	42
4.10	Configure SRTP	43
4.11	Configuring Message Condition Rules.....	44
4.12	Configuring Classification Rules	45
4.13	Configure IP-to-IP Call Routing Rules	47

4.14 (Optional) Configuring Firewall Settings.....	48
4.15 Configure Message Manipulation Rules	49
4.16 Miscellaneous Configuration.....	57
4.16.1 Configure Call Forking Mode.....	57
4.16.2 Optimizing CPU Cores Usage for a Specific Service	58
A AudioCodes INI File	59

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: November-01-2020

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes



Abbreviations and Terminology

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

Document Revision Record

LTRT	Description
12414	Initial document release for Version 7.2.

Documentation Feedback

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

This page is intentionally left blank.

1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (hereafter, referred to as *SBC*) for interworking between Twilio's Elastic SIP Trunk and Microsoft's Teams Direct Routing environment.

You can also use AudioCodes' SBC Wizard tool to automatically configure the SBC based on this interoperability setup. However, it is recommended to read through this document to better understand the various configuration options. For more information on AudioCodes' SBC Wizard including the download option, visit AudioCodes Web site at <https://www.audiocodes.com/partners/sbc-interoperability-list>.

1.1 Intended Audience

This document is intended for engineers, or AudioCodes and Twilio partners who are responsible for installing and configuring Twilio's Elastic SIP Trunk and Microsoft's Teams Direct Routing Service in Enterprise Model for enabling VoIP calls using AudioCodes SBC.

1.2 About Twilio

Millions of developers around the world have used Twilio to unlock the magic of communications to improve any human experience. Twilio has democratized communications channels like voice, text, chat, video, and email by virtualizing the world's communications infrastructure through APIs that are simple enough for any developer to use, yet robust enough to power the world's most demanding applications. By making communications a part of every software developer's toolkit, Twilio is enabling innovators across every industry - from emerging leaders to the world's largest organizations - to reinvent how companies engage with their customers.

1.3 About AudioCodes SBC Product Series

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

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

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

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

1.4 About Microsoft Teams Direct Routing

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

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

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes SBC Version

Table 2-1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	<ul style="list-style-type: none"> ▪ Mediant 500 Gateway & E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800B/C Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000/B SBC ▪ Mediant 9000, 9030, 9080 SBC ▪ Mediant Software SBC (VE/SE/CE)
Software Version	7.20A.260.012 or later
Protocol	<ul style="list-style-type: none"> ▪ SIP/TCP or SIP/TLS (to the Twilio Elastic SIP Trunk) ▪ SIP/TLS (to the Teams Direct Routing)
Additional Notes	None

2.2 Twilio Elastic SIP Trunk Version

Table 2-2: Twilio Version

Vendor/Service Provider	Twilio
SSW Model/Service	Twilio
Software Version	
Protocol	SIP
Additional Notes	None

2.3 Microsoft Teams Direct Routing Version

Table 2-3: Microsoft Teams Direct Routing Version

Vendor	Microsoft
Model	Teams Phone System Direct Routing
Software Version	Release v.2020.9.21.1 i.ASSE.0
Protocol	SIP
Additional Notes	None

2.4 Interoperability Test Topology

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

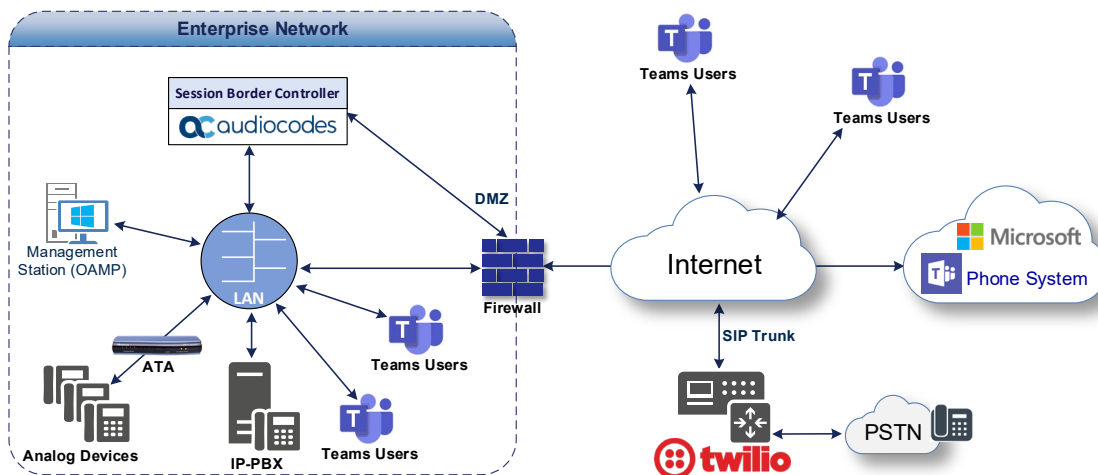
2.4.1 Enterprise Model Implementation

The interoperability testing between AudioCodes SBC and Twilio Elastic SIP Trunk with Teams Direct Routing Enterprise Model was done using the following topology setup:

- Enterprise deployed with third-party IP-PBX, analog devices (optional) and the administrator's management station, located on the LAN
- Enterprise deployed with Microsoft Teams Phone System Direct Routing Interface located on the WAN for enhanced communication within the Enterprise
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using Twilio's Elastic SIP Trunking service
- AudioCodes SBC is implemented to interconnect between the Elastic SIP Trunk in the Enterprise LAN and Microsoft Teams on the WAN
 - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
 - **Border:** IP-to-IP network border - the Twilio's Elastic SIP Trunk is located in the Enterprise LAN (or WAN) and the Microsoft Teams Phone Systems is located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Interoperability Test Topology between SBC and Microsoft Teams Direct Routing Enterprise Model with Twilio Elastic SIP Trunk



2.4.2 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	<ul style="list-style-type: none"> Both, Microsoft Teams Direct Routing and Twilio Elastic SIP Trunk environments are located on the Enterprise's (or Service Provider's) WAN
Signaling Transcoding	<ul style="list-style-type: none"> Microsoft Teams Direct Routing operates with SIP-over-TLS transport type Twilio Elastic SIP Trunk operates with SIP-over-TCP or SIP-over-TLS transport types
Codecs Transcoding	<ul style="list-style-type: none"> Microsoft Teams Direct Routing supports G.711A-law, G.711U-law, G.729, G.722, SILK (NB and WB) and OPUS coders Twilio Elastic SIP Trunk supports G.711A-law and G.711U-law coders
Media Transcoding	<ul style="list-style-type: none"> Microsoft Teams Direct Routing operates with SRTP media type Twilio Elastic SIP Trunk operates with RTP or SRTP media types

2.4.3 Infrastructure Prerequisites

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

Table 2-5: Infrastructure Prerequisites

Infrastructure Prerequisite	Details
Certified Session Border Controller (SBC)	See Microsoft's document Plan Direct Routing .
SIP Trunks connected to the SBC	
Office 365 Tenant	
Domains	
Public IP address for the SBC	
Fully Qualified Domain Name (FQDN) for the SBC	
Public DNS entry for the SBC	
Public trusted certificate for the SBC	
Firewall ports for Direct Routing Signaling	
Firewall IP addresses and ports for Direct Routing Media	
Media Transport Profile	
Firewall ports for Teams Clients Media	

2.4.4 Known Limitations

To implement anti-spoofing mechanism, the phone numbers, used by customers needs to be verified via Twilio's dashboard. No other limitations were observed in the interoperability tests done for the AudioCodes SBC interworking between Microsoft Teams Direct Routing and Twilio's Elastic SIP Trunk.

This page is intentionally left blank.

3 Configuring Teams Direct Routing

This section describes how to configure Microsoft Teams Direct Routing to operate with AudioCodes SBC.

3.1 Prerequisites

Before you begin configuration, make sure you have the following for every SBC you want to pair:

- Public IP address
- FQDN name matching SIP addresses of the users
- Public certificate, issued by one of the supported CAs

3.2 SBC Domain Name in the Teams Enterprise Model

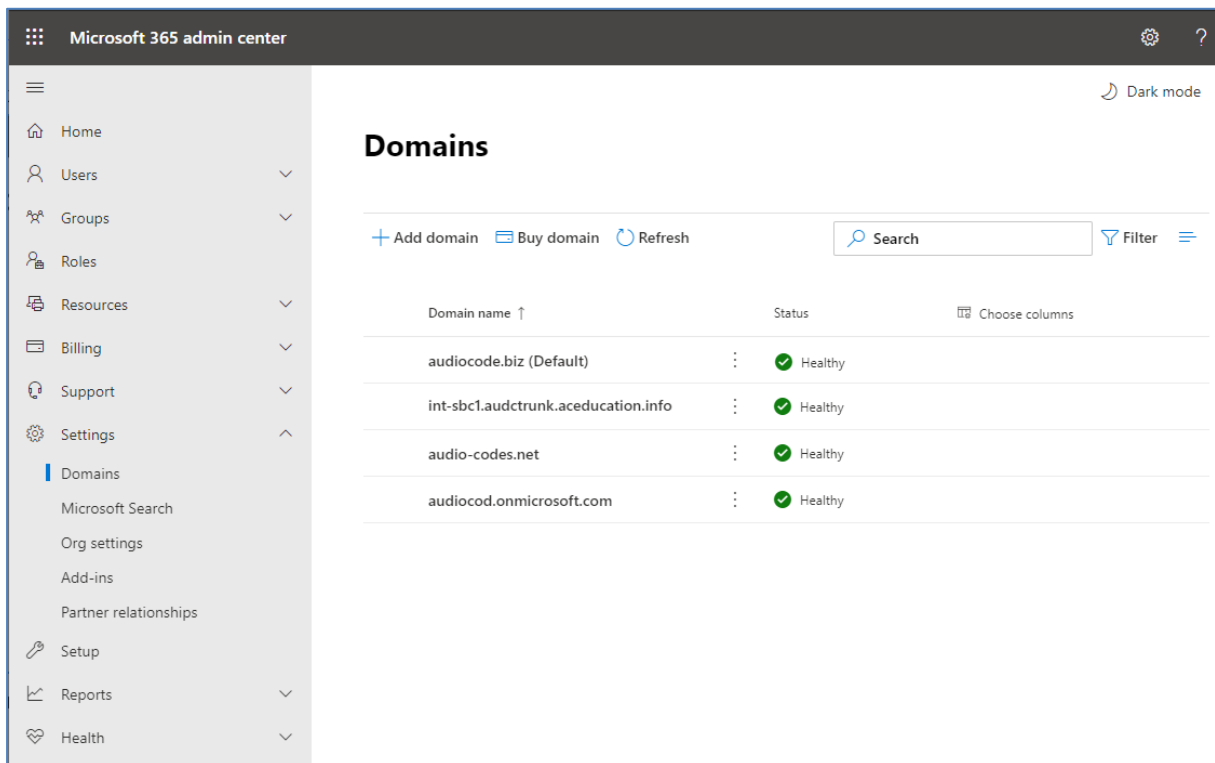
The SBC domain name must be from one of the names registered in 'Domains' of the tenant. You cannot use the *.onmicrosoft.com tenant for the domain name. For example, in Figure 3-1, the administrator registered the following DNS names for the tenant:

Table 3-1: DNS Names Registered by an Administrator for a Tenant

DNS Name	Can be used for SBC FQDN	Examples of FQDN Names
ACeducation.info	Yes	<p>Valid names:</p> <ul style="list-style-type: none"> ▪ sbc.ACeducation.info ▪ ussbcs15.ACeducation.info ▪ europe.ACeducation.info <p>Invalid name: sbc1.europe.ACeducation.info (requires registering domain name europe.atatum.biz in 'Domains' first)</p>
adatumbiz.onmicrosoft.com	No	Using *.onmicrosoft.com domains is not supported for SBC names
audctrunk.aceducation.info	Yes	<p>Valid names:</p> <ul style="list-style-type: none"> ▪ sbc1.audctrunk.aceducation.info ▪ ussbcs15.audctrunk.aceducation.info ▪ europe.audctrunk.aceducation.info <p>Invalid name: sbc1.europe.audctrunk.aceducation.info (requires registering domain name europe.hybridvoice.org in 'Domains' first)</p>

Users can be from any SIP domain registered for the tenant. For example, you can provide users user@ACeducation.info with the SBC FQDN `int-sbc1.audctrunk.aceducation.info` so long as both names are registered for this tenant.

Figure 3-1: Example of Registered DNS Names

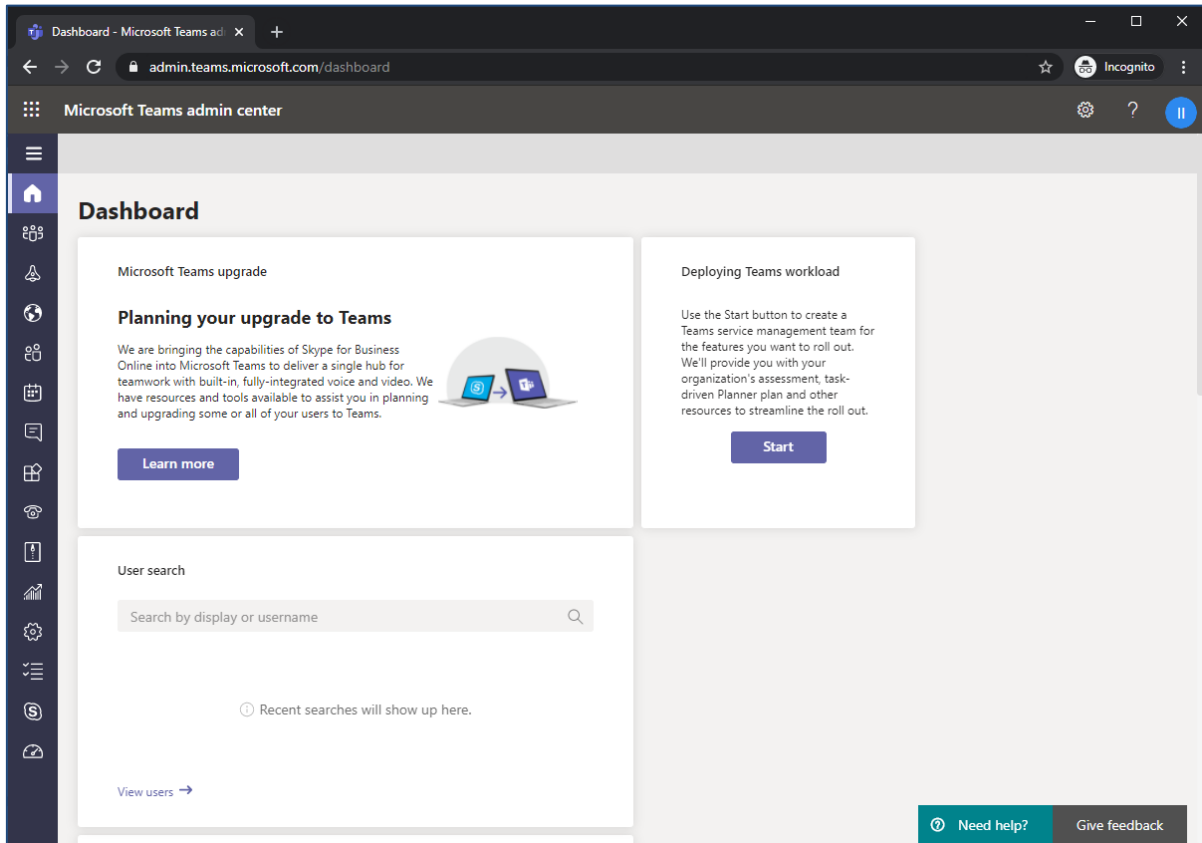


During creation of the Domain you will be forced to create public DNS record (**int-sbc1.audctrunk.aceducation.info** in our example.)

3.3 Example of the Office 365 Tenant Direct Routing Configuration

Configuration can be done using the web or with PowerShell. For the web, login to the Teams Admin Center (<https://admin.teams.microsoft.com>) with Tenant Administrator credentials.

Figure 3-2: Teams Admin Center



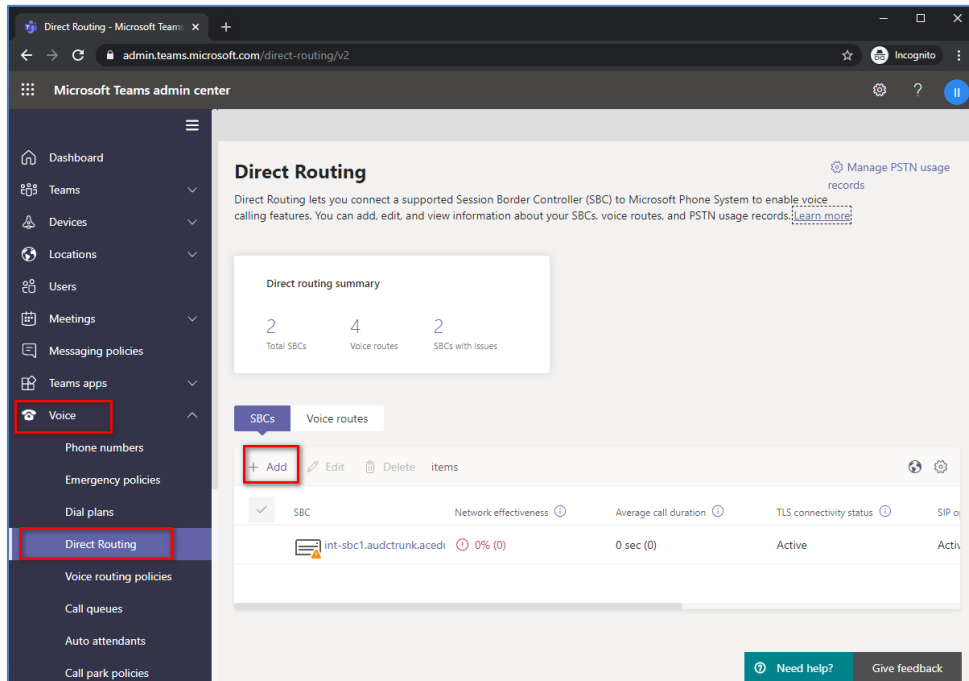
3.3.1 Add New SBC to Direct Routing

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

➤ **To add New SBC to Direct Routing:**

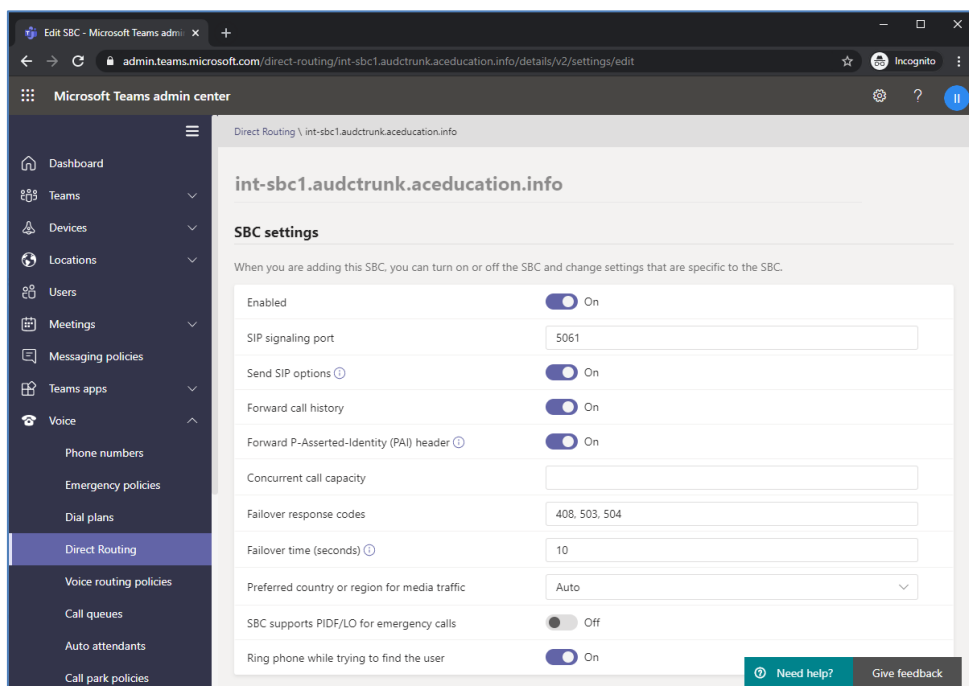
1. In the web interface, select **Voice**, and then click **Direct Routing**.
2. Under SBCs click **Add**.

Figure 3-3: Add new SBC to Direct Routing



3. Configure SBC.

Figure 3-4: Configure new SBC



You can use the following PowerShell command for creating a new Online PSTN Gateway:

```
New-CsOnlinePSTNGateway -Identity int-sbc1.audctrunk.aceducation.info -SipSignallingPort 5061 -ForwardCallHistory $True -ForwardPai $True -MediaBypass $True -Enabled $True
```



Note: Currently, enabling MediaBypass is available only through PowerShell.

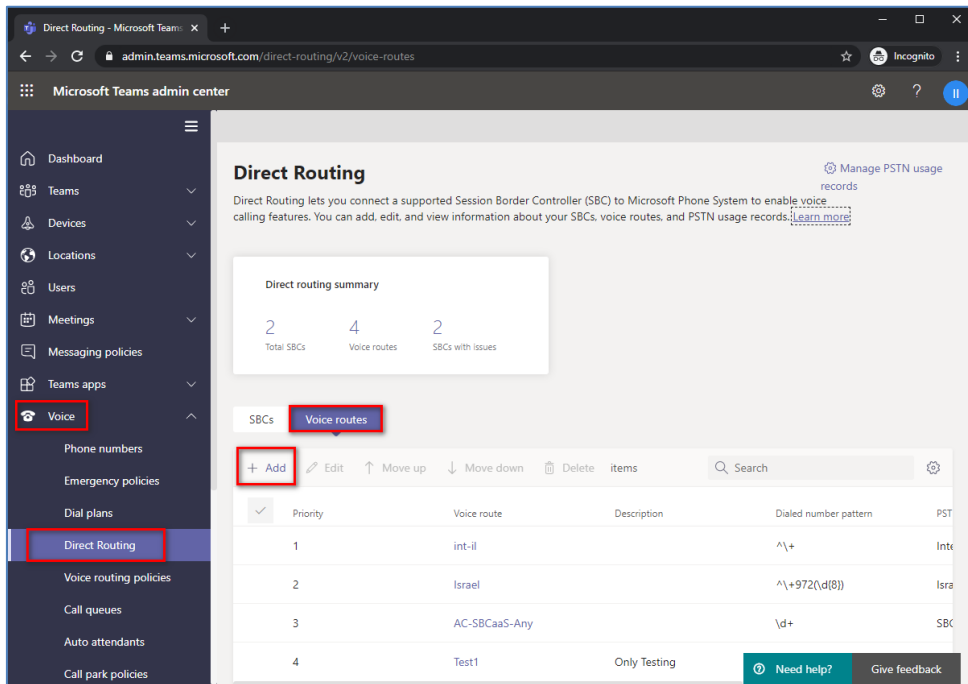
3.3.2 Add Voice Route and PSTN Usage

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

➤ **To add voice route and PSTN usage:**

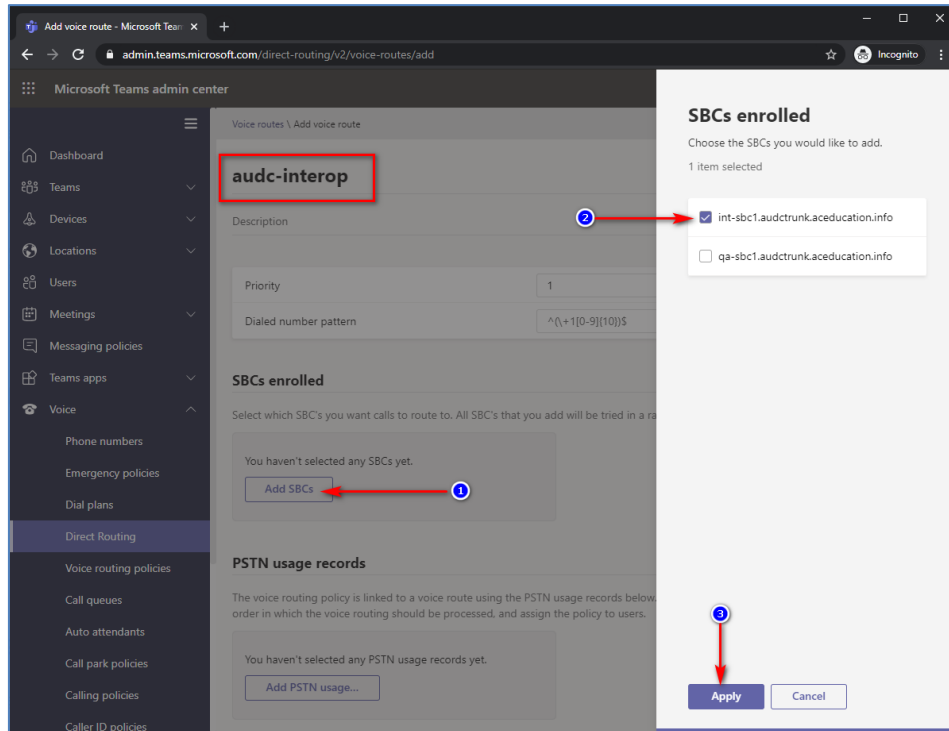
1. In the web interface, under **Direct Routing**, select **Voice routes**, and then click **Add**.

Figure 3-5: Add New Voice Route



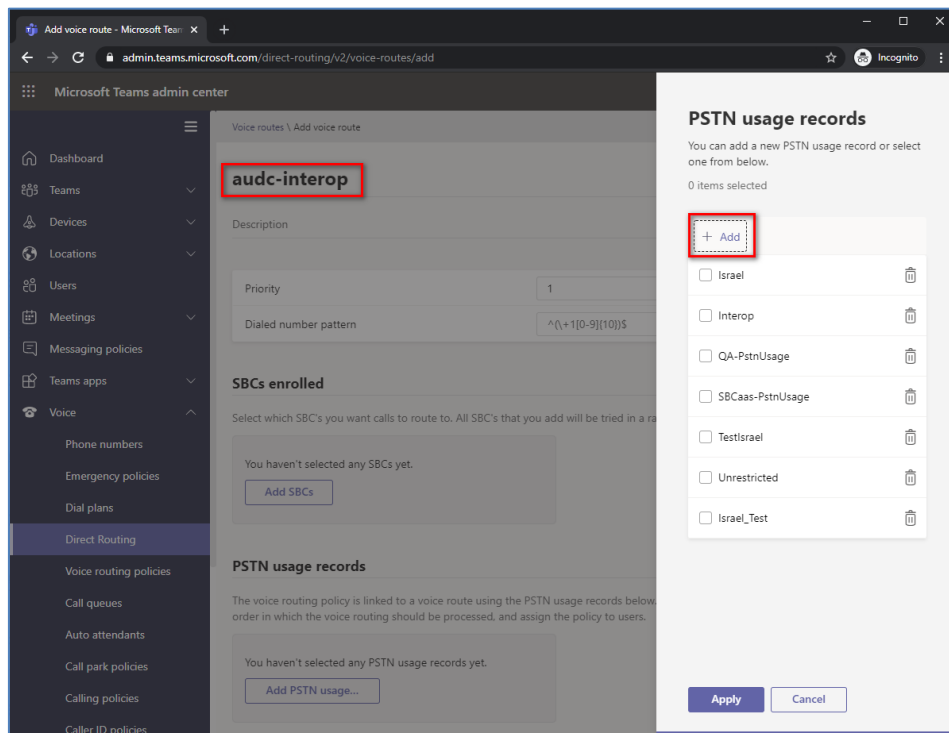
2. Create a new Voice Route and associate it with the SBC, configured in the previous step.

Figure 3-6: Associate SBC with new Voice Route



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

Figure 3-7: Associate PSTN Usage with New Voice Route



The same operations can be done using following PowerShell commands:

1. Creating an empty PSTN Usage:

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

2. Creating new Online Voice Route and associating it with PSTN Usage:

```
New-CsOnlineVoiceRoute -Identity "audc-interop" -NumberPattern
"^\\+" -OnlinePstnGatewayList int-
sbc1.audctrunk.aceducation.info -Priority 1 -OnlinePstnUsages
"Interop"
```

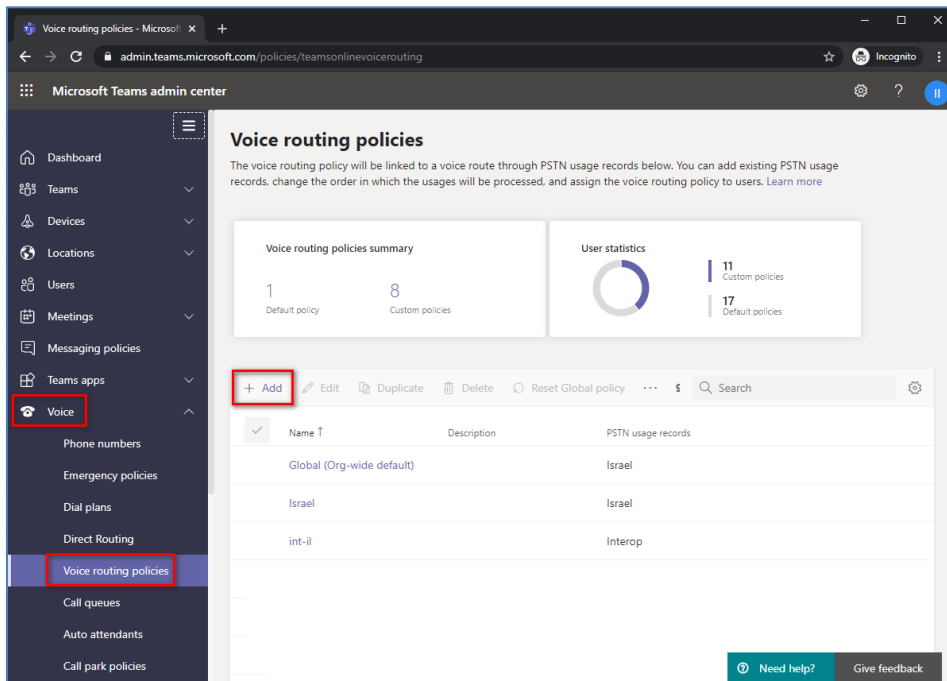
3.3.3 Add Voice Routing Policy

The procedure below describes how add a voice routing policy

- **To add voice routing policy:**

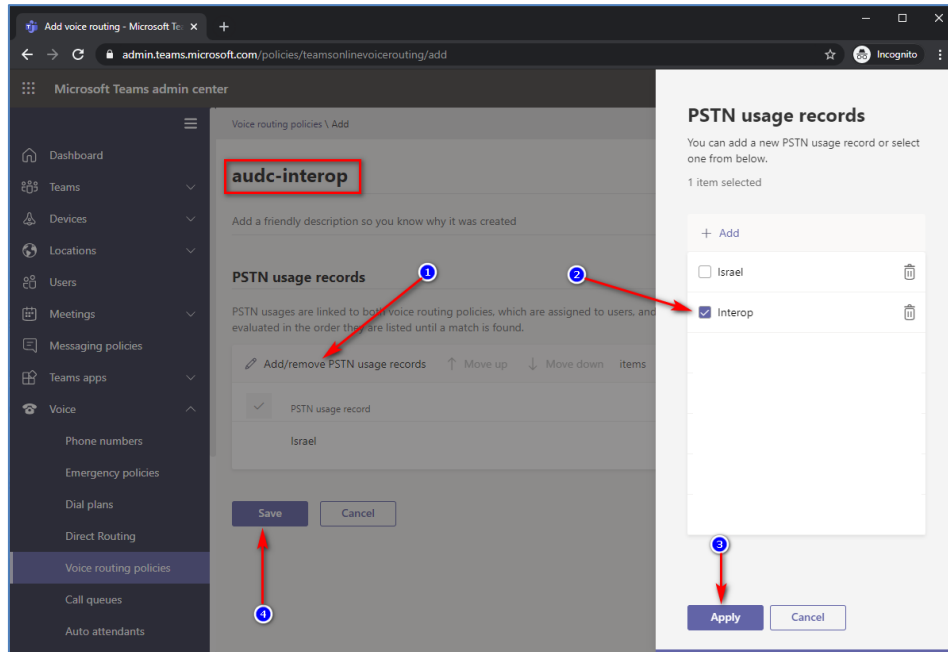
1. In the web interface, under **Voice**, select **Voice routing policies** and click **Add**.

Figure 3-8: Add New Voice Routing Policy



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

Figure 3-9: Associate PSTN Usage with New Voice Routing Policy



The same operations can be done using following PowerShell command:

```
New-CsOnlineVoiceRoutingPolicy "audc-interop" -OnlinePstnUsages "Interop"
```



Note: The commands specified in Sections 0 and 3.3.5, should be run **for each** Teams user in the company tenant. They are currently available through PowerShell **only**.

3.3.4 Enable Online User

Use the following PowerShell command for enabling online user:

```
Set-CsUser -Identity user1@company.com -EnterpriseVoiceEnabled $true -HostedVoiceMail $true -OnPremLineURI tel:+12345678901
```

3.3.5 Assigning Online User to the Voice Route

Use following PowerShell command for assigning online user to the Voice Route:

```
Grant-CsOnlineVoiceRoutingPolicy -PolicyName "audc-interop" -Identity user1@company.com
```

4 Configuring AudioCodes SBC

This section provides step-by-step procedures on how to configure AudioCodes SBC for interworking between Microsoft Teams Direct Routing and the Twilio Elastic SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

- SBC LAN interface – Management Station
- SBC WAN interface - Twilio Elastic SIP Trunk and Teams Direct Routing environment

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

Notes:

- For implementing Microsoft Teams Direct Routing and Twilio Elastic SIP Trunk based on the configuration described in this section, AudioCodes SBC must be installed with a License Key that includes the following software features:
 - **MSFT** (general Microsoft license)
Note: By default, all AudioCodes media gateways and SBCs are shipped with this license (except MSBR products, Mediant 500 SBC, and Mediant 500 Media Gateway).
 - **SW/TEAMS** (Microsoft Teams license)
 - **Number of SBC sessions** (based on requirements)
 - **Transcoding sessions** (only if media transcoding is needed)
 - **Coders** (based on requirements)
For more information about the License Key, contact your AudioCodes sales representative.
- The scope of this document does **not** cover all security aspects for configuring this topology. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document, which can be found at AudioCodes web site



4.1 SBC Configuration Concept in Teams Direct Routing Enterprise Model

The diagram below represents AudioCodes' device configuration concept in the Enterprise Model.

Figure 4-1: SBC Configuration Concept

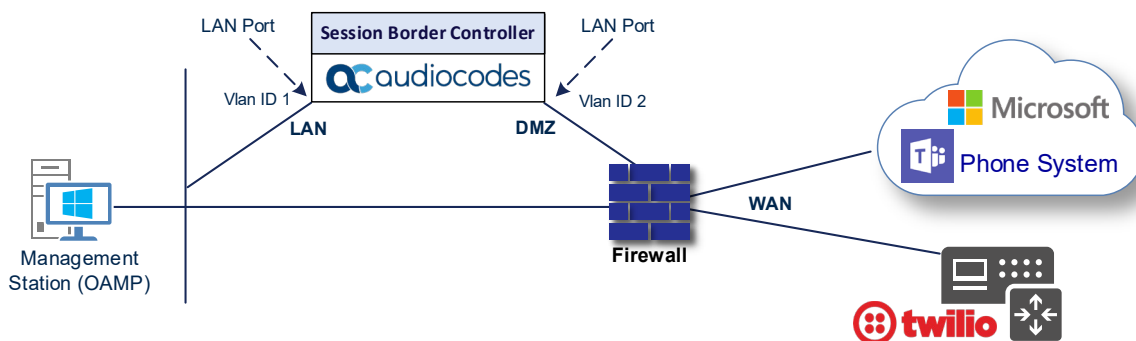


4.2 IP Network Interfaces Configuration

This section describes how to configure the SBC's IP network interfaces. There are several ways to deploy the SBC; however, this interoperability test topology employs the following deployment method:

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

Figure 4-2: Network Interfaces in Interoperability Test Topology



4.2.1 Configure VLANs

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

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

➤ **To configure the VLANs:**

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

Figure 4-3: Configured VLAN IDs in Ethernet Device

INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING
0	1	GROUP_1	vlan 1	Untagged
1	2	GROUP_2	vlan 2	Untagged

4.2.2 Configure Network Interfaces

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

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

➤ **To configure the IP network interfaces:**

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 4-1: Configuration Example of the Network Interface Table

Index	Application Types	Interface Mode	IP Address	Prefix Length	Gateway	DNS	I/F Name	Ethernet Device
0	OAMP+ Media + Control	IPv4 Manual	10.15.77.77	16	10.15.0.1	10.1.1.6	LAN_IF	vlan 1
1	Media + Control (as this interface points to the internet, enabling OAMP is not recommended)	IPv4 Manual	195.189.192.156 (DMZ IP address of SBC)	25	195.189.192.129 (router's IP address)	According to your Internet provider's instructions	WAN_IF	vlan 2

The configured IP network interfaces are shown below:

Figure 4-4: Configured Network Interfaces in IP Interfaces Table

IP Interfaces (2)

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

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	LAN_IF	OAMP + Media	IPv4 Manual	10.15.77.77	16	10.15.0.1	10.1.1.6		vlan 1
1	WAN_IF	Media + Control	IPv4 Manual	195.189.192.156	24	195.189.192.129	80.179.52.100	80.179.55.100	vlan 2

4.3 SIP TLS Connection Configuration

This section describes how to configure the SBC for using a TLS connection with the Microsoft Teams Direct Routing Phone System. This configuration is essential for a secure SIP TLS connection. The configuration instructions 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: sbc1.hybridvoice.org
- SAN: sbc1.hybridvoice.org

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

The Microsoft Phone System Direct Routing Interface allows **only** TLS connections from SBCs for SIP traffic with a certificate signed by one of the Trusted Certification Authorities.

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

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

4.3.1 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., **10.15.27.1**).

Figure 4-5: Configuring NTP Server Address

NTP SERVER	
Enable NTP	Enable
Primary NTP Server Address (IP or FQDN)	10.15.27.1
Secondary NTP Server Address (IP or FQDN)	
NTP Update Interval	Hours: 24 Minutes: 0
NTP Authentication Key Identifier	0
NTP Authentication Secret Key	

3. Click **Apply**.

4.3.2 Create a TLS Context

This section describes how to configure TLS Context in the SBC. AudioCodes recommends implementing only TLS to avoid flaws in SSL.

➤ **To configure the TLS Contexts:**

1. Open the TLS Contexts table (**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 4-2: New TLS Context

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



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

3. Click **Apply**.

The configured TLS Contexts are shown below:

Figure 4-6: Configured TLS Contexts

INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	default	TLSv1.0 TLSv1.1 and TLSv1.2	Any	DEFAULT
1	Teams	TLSv1.2	Any	DEFAULT
2	Twilio	TLSv1.2	Any	DEFAULT

4.3.3 Configure a Certificate for Operation with Microsoft Teams

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

The procedure involves the following main steps:

- a. Generating a Certificate Signing Request (CSR).
- b. Requesting Device Certificate from CA.
- c. Obtaining Trusted Root/ Intermediate Certificate from CA.
- d. Deploying Device and Trusted Root/ Intermediate Certificates on SBC.

➤ **To configure a certificate:**

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 (for Microsoft Teams), 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, **int-sbc1.audctrunk.aceducation.info**).
 - b. In the '1st Subject Alternative Name [SAN]' field, change the type to 'DNS' and enter the SBC FQDN name (based on example above, **int-sbc1.audctrunk.aceducation.info**).



Note: 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. Change the 'Private Key Size' based on the requirements of your Certification Authority.
- d. To change the key size on TLS Context, go to: **Generate New Private Key**, change the 'Private Key Size' to **1024** 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. Fill in 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 4-7: Example of Certificate Signing Request – Creating CSR

⬅️ TLS Context [#1] > Change Certificates

CERTIFICATE SIGNING REQUEST

Common Name [CN]	<input type="text" value="int-sbc1.audctrunk.aceducation.info"/>
Organizational Unit [OU] (optional)	<input type="text"/>
Company name [O] (optional)	<input type="text"/>
Locality or city name [L] (optional)	<input type="text"/>
State [ST] (optional)	<input type="text"/>
Country code [C] (optional)	<input type="text"/>
1st Subject Alternative Name [SAN]	DNS <input type="text" value="int-sbc1.audctrunk.aceducation.info"/>
2nd Subject Alternative Name [SAN]	EMAIL <input type="text"/>
3rd Subject Alternative Name [SAN]	EMAIL <input type="text"/>
4th Subject Alternative Name [SAN]	EMAIL <input type="text"/>
5th Subject Alternative Name [SAN]	EMAIL <input type="text"/>
Signature Algorithm	SHA-256

Press the "Generate Self-Signed Certificate" button to create self-signed certificate.
 Note that the certificate will use the subject name configured in "Certificate Signing Request" box.

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

```

-----BEGIN CERTIFICATE REQUEST-----
MIICtDCAZwCAQwIjE5MCoG41UFAwvjaH50LXNiYzEuYXVkyY3RydH5rLmFjZHR1
Y2F0aH9uLm1uZm8wggEiMA0GCsgGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQBAdA
iQKgtqrj39RL7bY1RxtX9Zu80JUp9e1f1H3IeY6nY+kqfYSTIVFhm3SEsYU1sBd
J/p6EA6e0UaWLeZsi324VP+1nctA6a00Mz7uc+1iP89yWlNpk3+5rZlNnXGZKKqpnF
P2Hw4h0px/dXX0IWEwv+4UF1St0072bZLppDIYDqQZcxdT1r1zRqrPSmqATaTAI
zaFayjr8ob085NQH6M09u+557eJ3UQxX+36rTRxUoo+qbdjiuMfP+dXrkzA5dBY
bIrcmB27DA6RUXhwj1pw/sBSQn9FZuZpu3mZrTl/EUCMEQ2tjjm96P/J7mx358Fh
4CnrXsu4HrXS6QxAgHBAAGQTA/BgkqhkIG9w08CQ4xMjAwMjC4G1UdEQQnMCWC
I21udC1zYmMxLmF1ZGN0cnVuay5hY2VkdWlhdG1vb15pbmZvMA0GCsgGSIb3DQEB
CwUAA4IBAQAjroPaX2yf/DSNjdrT-sZTEu2GNkgaorhV3hzwOaKJpLw0Hwv6upk9
UKv6E9/2GNh1cmR2oGkFvMrmYL8xerjTdhRjch1q/RP+1eJpm1N73xmD1sl/MVx
sIrw8G52jge18rQEBZIU7OR48PM/xhCV3Te4ZYekDm3JH0oG1HyS5ud7wlyDUYHA
7x3wG1wFCMsF+CfAkW5vtAxVI6F9VOYiOGty71xMnM2G1McYP8P3U21S0yQoFyDC
jktQ8UEkDeHbyNg1H7S11A6g5fSHU1Y0AAKfhwvEoXUJ4kAMXcfnS7DAShTxFuul
pRS5jw21C08DHj1fZgOC+OoxC1Va8HOEJ
-----END CERTIFICATE REQUEST-----
    
```

GENERATE NEW PRIVATE KEY

Private Key Size

Press the "Generate Private Key" button to create new private key.
 Important: generation of private key is a lengthy operation during which the device service may be affected.

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.

6. After obtaining an SBC signed and Trusted Root/Intermediate Certificate from the CA, in the SBC's Web interface, return to the **TLS Contexts** page and do the following:
 - a. In the TLS Contexts page, select the required TLS Context index row (for Microsoft Teams), 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 4-8: Uploading the Certificate Obtained from the Certification Authority

UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase (optional)

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

No file chosen

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

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

No file chosen ←

7. Confirm that the certificate was uploaded correctly. A message indicating that the certificate was uploaded successfully is displayed in blue in the lower part of the page.
8. In the SBC's Web interface, return to the **TLS Contexts** page, select the required TLS Context index row (for Microsoft Teams), 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 4-9: Certificate Information Example

⊕ TLS Context [#1] > Certificate Information

PRIVATE KEY

Key size: 2048 bits

Status: OK

CERTIFICATE

Certificate:

Data:

Version: 3 (0x2)

Serial Number:
45:be:53:11:ad:89:63:80:3b:ab:14:5e:34:34:57:53

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=IL, O=Domain The Net Technologies Ltd, CN=Domain The Net Technologies Ltd CA for SSL R2

Validity

Not Before: May 4 14:24:51 2020 GMT

Not After: May 4 14:24:51 2022 GMT

Subject: CN=int-sbc1.audctrunk.aceducation.info

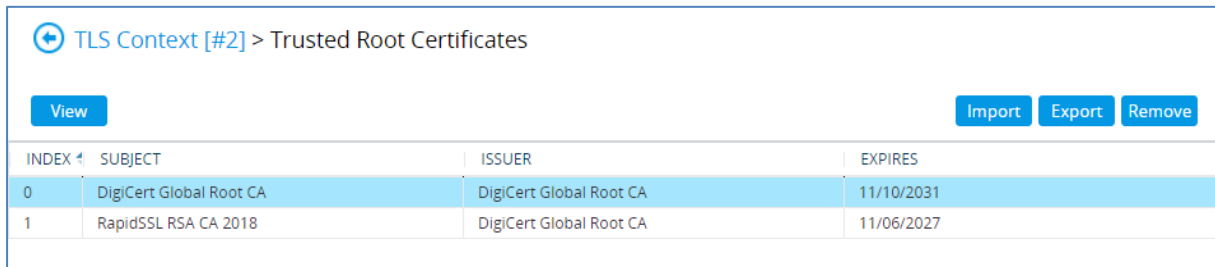
Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

9. 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 (for Microsoft Teams), 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.
10. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store:

Figure 4-10: Example of Configured Trusted Root Certificates



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

4.3.4 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.

4.3.5 Deploy Baltimore Trusted Root Certificate

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

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



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

4.3.6 Configure a Certificate for Operation with Twilio Elastic SIP Trunk

This section describes how to exchange a certificate with the Twilio Certificate Authority (CA). The certificate is used by the SBC to authenticate the connection with the Twilio Elastic SIP Trunk.

The procedure involves the following main steps:

- a. Generating a Private Key and Self-Signed Certificate
- b. Obtaining Trusted Root Certificate from Twilio CA
- c. Deploying Trusted Root Certificates on SBC

➤ **To configure a 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 (for Twilio Elastic SIP Trunk), 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 name, as configured at the Twilio Dashboard (e.g., **audc**).
 - b. Click the **Generate Self-Signed Certificate** button.
4. Under the **Generate New Private Key** group, click the **Generate Private Key** button to create new private key.
5. 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 (for Twilio Elastic SIP Trunk), 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 the certificate file to load. Twilio's Root/Intermediate Certificates can be loaded from the following link: <https://www.twilio.com/docs/sip-trunking#rootCA>

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

Figure 4-11: Example of Loaded Twilio’s Trusted Root Certificates

INDEX	SUBJECT	ISSUER	EXPIRES
0	GlobalSign Root CA	GlobalSign Root CA	1/28/2028
1	GlobalSign	GlobalSign	12/15/2021
2	VeriSign Class 3 Public Primary	VeriSign Class 3 Public Primary	7/16/2036
3	Entrust.net Certification Autho	Entrust.net Certification Autho	7/24/2029
4	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025
5	AddTrust Class 1 CA Root	AddTrust Class 1 CA Root	5/30/2020
6	AddTrust External CA Root	AddTrust External CA Root	5/30/2020

4.4 Configure Media Realms

This section describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for the Elastic SIP Trunk traffic and one for the Teams traffic. Due to fact that both, Microsoft Teams and Twilio Elastic SIP Trunk, are located at the WAN side of the SBC, only one Media Realm can be used. So, for specific interworking tests, the default Media Realm configuration was used.

➤ **To configure Media Realms:**

- Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
- Modify the default Media Realm (Index 0) as follows:

Table 4-3: Configuration Example Media Realm in Media Realm Table

Index	Name	IPv4 Interface Name
0	DefaultRealm	WAN_IF

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

The configured Media Realms are shown in the figure below:

Figure 4-12: Configured Media Realms in Media Realm Table

INDEX	NAME	IPv4 INTERFACE NAME	UDP PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	UDP PORT RANGE END	DEFAULT MEDIA REALM
0	DefaultRealm	WAN_IF	6000	5953	65529	No

4.5 Configure SIP Signaling Interfaces

This section describes how to configure SIP Interfaces. For specific interworking tests, the default SIP Interface (Index 0) configuration was used.

➤ **To configure SIP Interfaces:**

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



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

Table 4-4: Configured SIP Interface in SIP Interface Table

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepalive	Classification Failure Response Type	Media Realm
0	SIPInterface_0 (arbitrary name)	WAN_IF	SBC	0	0	5061 (as configured in the Office 365)	Enable	0 (Recommended to prevent DoS attacks)	DefaultRealm

The configured SIP Interfaces are shown in the figure below:

Figure 4-13: Configured SIP Interfaces in SIP Interface Table

SIP Interfaces (1)

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

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATION PROTOCOL	MEDIA REALM
0	SIPInterface_0	DefaultSRD	WAN_IF	SBC	0	0	5061	No encapsulation	DefaultRealm

4.6 Configure Proxy Sets and Proxy Address

This section describes how to configure Proxy Sets. The Proxy Set defines the destination address (IP address or FQDN) of the IP entity server. Proxy Sets can also be used to configure load balancing between multiple servers.

For the interoperability test topology, two Proxy Sets need to be configured for the following IP entities:

- Twilio Elastic SIP Trunk
- Teams Direct Routing

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

➤ **To configure 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 4-5: 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	Twilio (arbitrary name)	SIPInterface_0	Twilio	Using Options	Enable	-
2	Teams (arbitrary name)	SIPInterface_0	Teams	Using Options	Enable	Random Weights

The configured Proxy Sets are shown in the figure below:

Figure 4-14: Configured Proxy Sets in Proxy Sets Table

INDEX ↕	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#0)	--	SIPInterface_0	60		Disable
1	Twilio	DefaultSRD (#0)	--	SIPInterface_0	60		Enable
2	Teams	DefaultSRD (#0)	--	SIPInterface_0	60		Enable

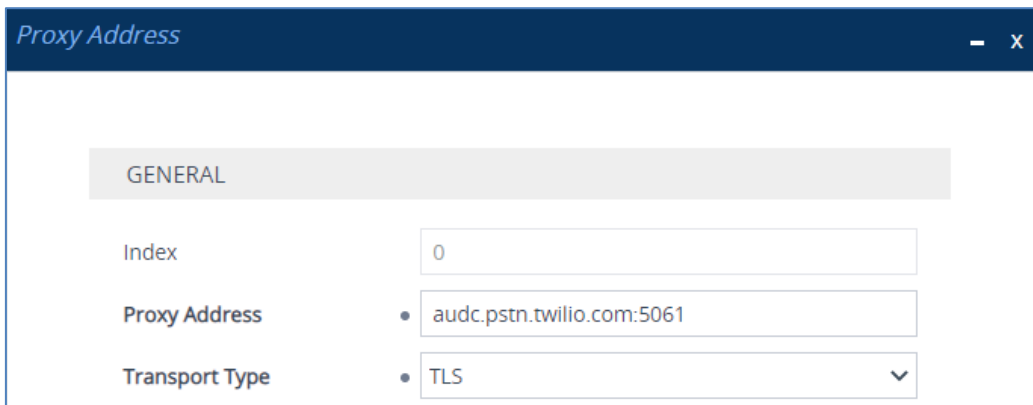
4.6.1 Configure a Proxy Address

This section shows how to configure a Proxy Address.

➤ **To configure a Proxy Address for Elastic SIP Trunk:**

1. Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets) and then click the Proxy Set **Twilio**, 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 4-15: Configuring Proxy Address for Twilio Elastic SIP Trunk



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

Table 4-6: Configuration Proxy Address for Twilio Elastic SIP Trunk

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	audc.pstn.twilio.com:5061	TLS	0	0

4. Click **Apply**.

➤ **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**; the following dialog box appears:

Figure 4-16: Configuring Proxy Address for Teams Direct Routing Interface

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

Table 4-7: 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**.

4.7 Configure Coders

This section describes how to configure coders (termed *Coder Group*). As Microsoft Teams Direct Routing supports the SILK and OPUS coders while the network connection to Twilio Elastic SIP Trunk may restrict operation with a dedicated coders list, you need to add a Coder Group with the supported coders for each leg, the Microsoft Teams Direct Routing and the Twilio Elastic SIP Trunk.

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

➤ **To configure coders:**

1. Open the Coder Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Coder Groups**).
2. Configure a Coder Group for Microsoft Teams Direct Routing:

Parameter	Value
Coder Group Name	AudioCodersGroups_1
Coder Name	<ul style="list-style-type: none"> ▪ SILK-NB ▪ SILK-WB ▪ G.729 ▪ G.711 A-law ▪ G.711 U-law

Figure 4-17: Configuring Coder Group for Microsoft Teams Direct Routing

Coder Groups

Coder Group Name: 1 : AudioCodersGroups_1 Delete Group

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

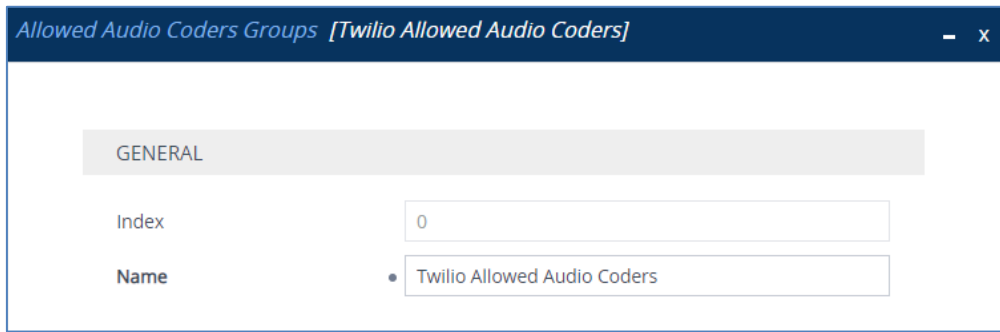
3. Click **Apply**, and then confirm the configuration change in the prompt that pops up.

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Twilio Elastic SIP Trunk uses the dedicated coders list whenever possible. Note that this Allowed Coders Group ID will be assigned to the IP Profile belonging to the Twilio Elastic SIP Trunk in the next step.

➤ **To set a preferred coder for the Twilio Elastic SIP Trunk:**

1. Open the Allowed Audio Coders Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Audio Coders Groups**).
2. Click **New** and configure a name for the Allowed Audio Coders Group for Twilio Elastic SIP Trunk.

Figure 4-18: Configuring Allowed Coders Group for Twilio Elastic SIP Trunk



3. Click **Apply**.
4. Select the new row that you configured, and then click the **Allowed Audio Coders** link located below the table; the Allowed Audio Coders table opens.
5. Click **New** and configure an Allowed Coders as follows:

Table 4-8: Allowed Coders for Twilio Elastic SIP Trunk

Index	Coder
0	G.711 A-law
1	G.711 U-law

4.8 Configure IP Profiles

This section describes how to configure IP Profiles. The IP Profile defines a set of call capabilities relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder and transcoding method).

In this interoperability test topology, IP Profiles need to be configured for the Twilio Elastic SIP Trunk as well as for Microsoft Teams Direct Routing.

➤ **To configure an IP Profile for the Twilio Elastic SIP Trunk:**

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

Parameter	Value
General	
Index	1
Name	Twilio
Media Security	
SBC Media Security Mode	Secured
SBC Enforce MKI Size	Enforce
SBC Media	
Allowed Audio Coders	Twilio Allowed Audio Coders
SBC Signaling	
P-Asserted-Identity Header Mode	Add (required for anonymous calls)
SIP UPDATE Support	Not Supported
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally
Remote Replaces Mode	Handle Locally
Remote 3xx Mode	Handle Locally

Figure 4-19: Configuring IP Profile for Twilio Elastic SIP Trunk

3. Click **Apply**.

➤ **To configure IP Profile for the Microsoft Teams Direct Routing:**

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

Parameter	Value
General	
Index	2
Name	Teams (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	Secured
SBC Early Media	
Remote Early Media RTP Detection Mode	By Media (required, as Microsoft Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18x response)
SBC Media	
Extension Coders Group	AudioCodersGroups_1
RTCP Mode	Generate Always (required, as some ITSPs do not send RTCP packets during while in Hold mode, but Microsoft expected to them)
ICE Mode	Lite (required only when Media Bypass enabled on Microsoft Teams)
SBC Signaling	
SIP UPDATE Support	Not Supported

Remote re-INVITE Support	Supported Only With SDP
Remote Delayed Offer Support	Not Supported
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally
Remote 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)

Figure 4-20: Configuring IP Profile for Microsoft Teams Direct Routing

The screenshot shows the configuration interface for an IP Profile. It is divided into two columns: GENERAL and SBC SIGNALING.

GENERAL Section:

- Index: 2
- Name: Teams
- Created by Routing Server: No

MEDIA SECURITY Section:

- SBC Media Security Mode: Secured
- Gateway Media Security Mode: Preferable
- Symmetric MKI: Disable
- MKI Size: 0
- SBC Enforce MKI Size: Don't enforce
- SBC Media Security Method: SDES
- Reset SRTP Upon Re-key: Disable

SBC SIGNALING Section:

- PRACK Mode: Transparent
- P-Asserted-Identity Header Mode: As Is
- Diversion Header Mode: As Is
- History-Info Header Mode: As Is
- Session Expires Mode: Transparent
- SIP UPDATE Support: Not Supported
- Remote re-INVITE: Supported only with SDP
- Remote Delayed Offer Support: Not Supported
- MSRP re-INVITE/UPDATE: Supported
- MSRP Offer Setup Role: ActPass
- MSRP Empty Message Format: Default
- Remote Representation Mode: According to Operation Mode

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

3. Click Apply.

4.9 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 ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

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

- Twilio Elastic SIP Trunk located on LAN
- Teams Direct Routing located on WAN

➤ **To configure IP Groups:**

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Configure an IP Group for the Twilio Elastic SIP Trunk:

Parameter	Value
Index	1
Name	Twilio
Type	Server
Proxy Set	Twilio
IP Profile	Twilio
Media Realm	DefaultRealm
SIP Group Name	audc1.pstn.twilio.com (according to ITSP requirement)

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

Parameter	Value
Index	2
Name	Teams
Topology Location	Up
Type	Server
Proxy Set	Teams
IP Profile	Teams
Media Realm	DefaultRealm
SIP Group Name	audc1.pstn.twilio.com (according to ITSP requirement)
Classify By Proxy Set	Disable
Local Host Name	< FQDN of the SBC in the Microsoft Teams tenant > (For example, int-sbc1.audctrunk.aceducation.info)
Always Use Src Address	Yes
Proxy Keep-Alive using IP Group settings	Enable

The configured IP Groups are shown in the figure below:

Figure 4-21: Configured IP Groups in IP Group Table

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATI SET	OUTBOUND MESSAGE MANIPULAT SET
0	Default_IPG	DefaultSR	Server	Not Configur	ProxySet_0	--	--		Disable	-1	-1
1	Twilio	DefaultSR	Server	Not Configur	Twilio	Twilio	DefaultRealm	audc1.pstn.tv	Enable	-1	4
2	Teams	DefaultSR	Server	Not Configur	Teams	Teams	DefaultRealm	audc1.pstn.tv	Disable	1	-1

4.10 Configure SRTP

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

- **To configure media security:**
 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 4-22: Configuring SRTP

Media Security

GENERAL

Media Security → Enable

Media Security Behavior Preferable

Offered SRTP Cipher Suites All

Aria Protocol Support Disable

MASTER KEY IDENTIFIER

Master Key Identifier (MKI) Size 0

Symmetric MKI Disable

3. Click **Apply**.

4.11 Configuring Message Condition Rules

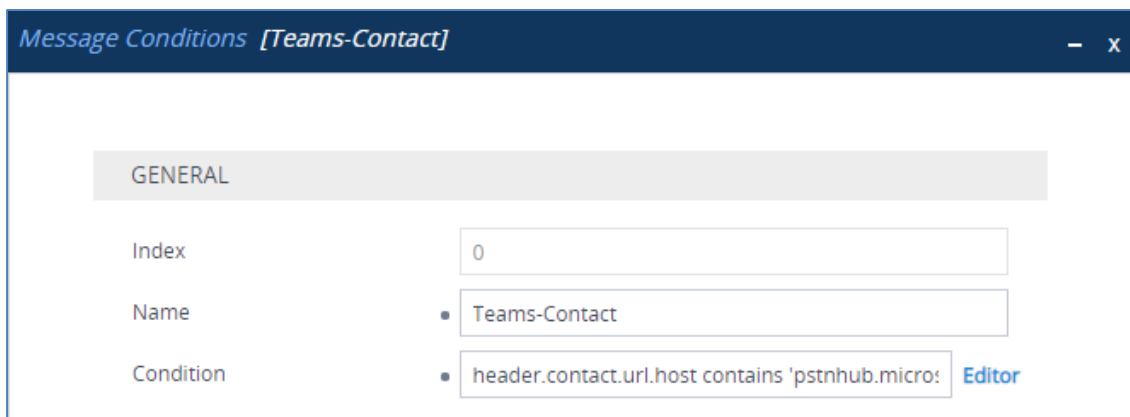
This section describes how to configure the Message Condition Rules. A Message Condition defines special conditions (pre-requisites) for incoming SIP messages. These rules can be used as additional matching criteria for the IP-to-IP routing rules in the IP-to-IP Routing table. The following condition verifies that the Contact header contains Microsoft Teams FQDN.

➤ **To configure a Message Condition rule:**

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 4-23: Configuring Condition Table



3. Click **Apply**.

4.12 Configuring Classification Rules

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

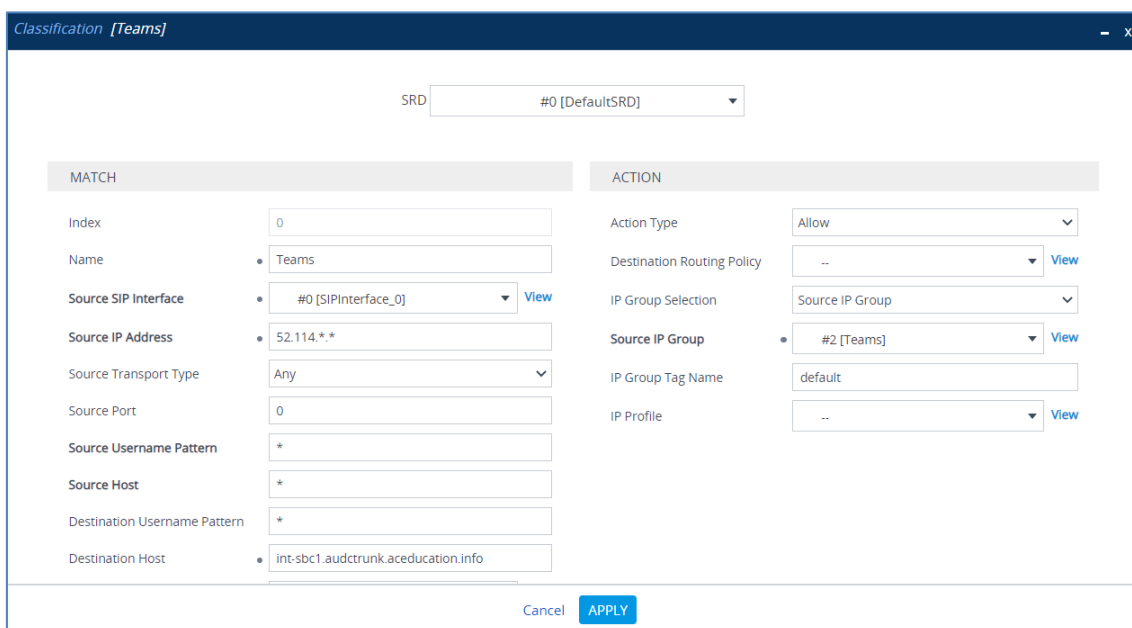
You can also use the Classification table for employing SIP-level access control for successfully classified calls, by configuring Classification rules with whitelist and blacklist settings. If a Classification rule is configured as a whitelist ("Allow"), the device accepts the SIP dialog and processes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

➤ **To configure a Classification rules:**

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

Parameter	Value
Index	0
Name	Teams
Source SIP Interface	SIPInterface_0
Source IP Address	52.114.*.*
Destination Host	< FQDN name of your SBC in the Microsoft Teams tenant > (e.g. int-sbc1.audctrunk.aceducation.info)
Message Condition	Teams-Contact
Action Type	Allow
Source IP Group	Teams

Figure 4-24: Configuring Classification Rule for Microsoft Teams



3. Click **Apply**.

- Click **New**, and then configure the parameters as follows for Twilio Elastic SIP Trunk:

Parameter	Value
Index	1
Name	Twilio Termination URI (arbitrary descriptive name)
Source SIP Interface	SIPInterface_0
Source Host	audc.pstn.twilio.com (Twilio FQDN)
Action Type	Allow
Source IP Group	Twilio

Figure 4-25: Configuring Classification Rule for Twilio Elastic SIP Trunk

Classification [Twilio Termination URI]

SRD #0 [DefaultSRD]

MATCH	ACTION
Index: 1	Action Type: Allow
Name: Twilio Termination URI	Destination Routing Policy: --
Source SIP Interface: #0 [SIPInterface_0]	IP Group Selection: Source IP Group
Source IP Address:	Source IP Group: #1 [Twilio]
Source Transport Type: Any	IP Group Tag Name: default
Source Port: 0	IP Profile: --
Source Username Pattern: *	
Source Host: audc.pstn.twilio.com	
Destination Username Pattern: *	
Destination Host: *	

Cancel APPLY

- Click **Apply**.

4.13 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.

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

- Terminate SIP OPTIONS messages on the SBC that are received from any entity
- Terminate REFER messages to Teams Direct Routing
- Calls from Teams Direct Routing to Twilio Elastic SIP Trunk
- Calls from Twilio Elastic 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 4-9: Configuration IP-to-IP Routing Rules

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

The configured routing rules are shown in the figure below:

Figure 4-26: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

INDEX	NAME	ROUTING POLICY	ALTERNATIV ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATIO USERNAME PATTERN	DESTINATIO TYPE	DESTINATIO IP GROUP	DESTINATIO SIP INTERFACE	DESTINATIO ADDRESS
0	Terminate O	Default_SBCF	Route Row	Any	OPTIONS	*	*	Internal	--	--	
1	Refer from T	Default_SBCF	Route Row	Any	All	*	*	Request URI	Teams	--	
2	Teams to SIP	Default_SBCF	Route Row	Teams	All	*	*	IP Group	Twilio	--	
3	SIP trunk to	Default_SBCF	Route Row	Twilio	All	*	*	IP Group	Teams	--	



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

4.14 (Optional) Configuring Firewall Settings



Note: AudioCodes highly advised to configure firewall with network traffic filtering rules **in front of** WAN interface of the SBC. For detailed list of ports, which needed to be open please refer to: <https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sip-signaling-fqdns-and-firewall-ports>.

As an extra security to the above note, **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 4-10: 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	52.114.148.0	32	0	65535	TCP	Enable	WAN_IF	Allow
2	52.114.132.46	32	0	65535	TCP	Enable	WAN_IF	Allow
3	52.114.75.24	32	0	65535	TCP	Enable	WAN_IF	Allow
4	52.114.76.76	32	0	65535	TCP	Enable	WAN_IF	Allow
5	52.114.7.24	32	0	65535	TCP	Enable	WAN_IF	Allow
6	52.114.14.70	32	0	65535	TCP	Enable	WAN_IF	Allow
49	0.0.0.0	0	0	65535	Any	Enable	WAN_IF	Block



Note: Be aware, that if in your configuration, connectivity to SIP Trunk (or other entities) is performed through the same IP Interface as Teams (WAN_IF in our example), you **must** add rules to allow traffic from these entities.

4.15 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.

➤ **To configure SIP message manipulation rule:**

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 Teams. This rule applies to messages received from the Teams IP Group. This remove 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

Figure 4-27: Configuring SIP Message Manipulation Rule 0 (for Teams)

The screenshot shows a configuration window titled "Message Manipulations [Remove PAI]". It is divided into three main sections: GENERAL, ACTION, and MATCH.

- GENERAL:**
 - Index: 0
 - Name: Remove PAI
 - Manipulation Set ID: 1
 - Row Role: Use Current Condition
- ACTION:**
 - Action Subject: Header.P-Asserted-Identity
 - Action Type: Remove
 - Action Value: (empty field)
- MATCH:**
 - Message Type: Any
 - Condition: (empty field)

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

- Configure another manipulation rule (Manipulation Set 4) for Twilio Elastic SIP Trunk. This rule applies to messages sent to the Twilio Elastic SIP Trunk IP. This remove the SIP Privacy Header in all messages, except of call with presentation restriction.

Parameter	Value
Index	1
Name	Remove Privacy Header
Manipulation Set ID	4
Condition	Header.Privacy exists And Header.From.URL !contains 'anonymous'
Action Subject	Header.Privacy
Action Type	Remove

Figure 4-28: Configuring SIP Message Manipulation Rule 1 (for Twilio Elastic SIP Trunk)

The screenshot shows a configuration window titled "Message Manipulations [Remove Privacy Header]". It is organized into three main sections: GENERAL, ACTION, and MATCH.

- GENERAL:**
 - Index: 1
 - Name: Remove Privacy Header
 - Manipulation Set ID: 4
 - Row Role: Use Current Condition
- ACTION:**
 - Action Subject: Header.Privacy
 - Action Type: Remove
 - Action Value: (empty)
- MATCH:**
 - Message Type: Any
 - Condition: Header.Privacy exists And Header.Fron

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

- Configure another manipulation rule (Manipulation Set 4) for Twilio Elastic SIP Trunk. This rule applies to messages sent to the Twilio Elastic SIP Trunk IP Group in a call forwarding scenario. This rule replaces the host part of the SIP History-Info Header with the value that was configured in the Twilio Elastic SIP Trunk IP Group.

Parameter	Value
Index	2
Name	Change Host of History-Info.0
Manipulation Set ID	4
Message Type	Invite.Request
Condition	Header.History-Info.0 regex (.*)(@)(.*)((;user=phone)(.*))
Action Subject	Header.History-Info.0
Action Type	Modify
Action Value	\$1+\$2+Param.IPG.Dst.Host+\$4+\$5

Figure 4-29: Configuring SIP Message Manipulation Rule 2 (for Twilio Elastic SIP Trunk)

The screenshot shows a configuration window titled "Message Manipulations [Change Host of History-Info.0]". It is divided into three main sections: GENERAL, MATCH, and ACTION.

- GENERAL:**
 - Index: 2
 - Name: Change Host of History-Info.0
 - Manipulation Set ID: 4
 - Row Role: Use Current Condition
- MATCH:**
 - Message Type: Invite.Request
 - Condition: Header.History-Info.0 regex (.*)(@)(.*)((;user=phone)(.***))
- ACTION:**
 - Action Subject: Header.History-Info.0
 - Action Type: Modify
 - Action Value: \$1+\$2+param.ipg.dst.host+\$4+\$5

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

- Configure another manipulation rule (Manipulation Set 4) for Twilio Elastic SIP Trunk. This rule also applies to messages sent to the Twilio Elastic SIP Trunk IP Group in a call forwarding scenario. This rule removes SIP History-Info.1 Header.

Parameter	Value
Index	3
Name	Remove History-Info.1
Manipulation Set ID	4
Message Type	Invite.Request
Action Subject	Header.History-Info.1
Action Type	Remove

Figure 4-30: Configuring SIP Message Manipulation Rule 3 (for Twilio Elastic SIP Trunk)

The screenshot shows a configuration window titled "Message Manipulations [Remove History-Info.1]". It is divided into three main sections: GENERAL, MATCH, and ACTION.

- GENERAL:**
 - Index: 3
 - Name: Remove History-Info.1
 - Manipulation Set ID: 4
 - Row Role: Use Current Condition
- MATCH:**
 - Message Type: Invite.Request
 - Condition: (empty)
- ACTION:**
 - Action Subject: Header.History-Info.1
 - Action Type: Remove
 - Action Value: (empty)

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

6. Configure another manipulation rule (Manipulation Set 4) for Twilio Elastic SIP Trunk. This rule applies to messages sent to the Twilio Elastic SIP Trunk IP Group in a call transfer scenario. This rule replaces the host part of the SIP Referred-by Header with the value that was configured in the Twilio Elastic SIP Trunk IP Group.

Parameter	Value
Index	4
Name	Change Referred-by Host
Manipulation Set ID	4
Message Type	Invite.Request
Condition	Header.Referred-By exists
Action Subject	Header.Referred-By.URL.Host
Action Type	Modify
Action Value	Param.IPG.Dst.Host

Figure 4-31: Configuring SIP Message Manipulation Rule 4 (for Twilio Elastic SIP Trunk)

The screenshot shows a configuration window titled "Message Manipulations [Change Referred-by Host]". It is organized into three main sections: GENERAL, ACTION, and MATCH. Each section contains several fields with corresponding values and "Editor" links for modification.

- GENERAL Section:**
 - Index: 4
 - Name: Change Referred-by Host
 - Manipulation Set ID: 4
 - Row Role: Use Current Condition
- ACTION Section:**
 - Action Subject: Header.Referred-By.URL.Host
 - Action Type: Modify
 - Action Value: Param.IPG.Dst.Host
- MATCH Section:**
 - Message Type: Invite.Request
 - Condition: Header.Referred-By exists

At the bottom of the window, there are two buttons: "Cancel" and "APPLY".

- Configure another manipulation rule (Manipulation Set 4) for Twilio Elastic SIP Trunk. This rule is applied to response messages sent to the Twilio Elastic SIP Trunk IP Group for Rejected Calls initiated by the Teams Direct Routing IP Group. This replaces the method types '488', '503' and '603' with the value '486', because Twilio Elastic SIP Trunk (or interconnected to it telephony provider) does not recognize these method types correctly.

Parameter	Value
Index	5
Name	Error Responses
Manipulation Set ID	4
Message Type	Any.Response
Condition	Header.Request-URI.MethodType=='488' OR Header.Request-URI.MethodType=='503' OR Header.Request-URI.MethodType=='603'
Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'486'

Figure 4-32: Configuring SIP Message Manipulation Rule 5 (for Twilio Elastic SIP Trunk)

The screenshot shows a configuration window titled "Message Manipulations [Error Responses]". It is divided into three main sections: GENERAL, MATCH, and ACTION.

- GENERAL:**
 - Index: 5
 - Name: Error Responses
 - Manipulation Set ID: 4
 - Row Role: Use Current Condition
- MATCH:**
 - Message Type: Any.Response
 - Condition: Header.Request-URI.MethodType=='488' C
- ACTION:**
 - Action Subject: Header.Request-URI.MethodType
 - Action Type: Modify
 - Action Value: '486'

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

Figure 4-33: Example of Configured SIP Message Manipulation Rules

INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	Remove PAI	1			Header.P-Asserted	Remove		Use Current Condit
1	Remove Privacy	4		Header.Privacy exi	Header.Privacy	Remove		Use Current Condit
2	Change Host of His	4	Invite.Request	Header.History-Inf	Header.History-Inf	Modify	\$1+\$2+Param.IPG.	Use Current Condit
3	Remove History-In	4	Invite.Request		Header.History-Inf	Remove		Use Current Condit
4	Change Referred-b	4	Invite.Request	Header.Referred-B	Header.Referred-B	Modify	Param.IPG.Dst.Hos	Use Current Condit
5	Error Responses	4	Any.Response	Header.Request-U	Header.Request-U	Modify	'486'	Use Current Condit

The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set IDs (Manipulation Set IDs 1, and 4) and which are executed for messages sent to and from the Twilio Elastic SIP Trunk IP Group as well as the Teams Direct Routing IP Group. These rules are specifically required to enable proper interworking between Twilio Elastic SIP Trunk and Teams Direct Routing. Refer to the *User’s Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule applies to messages received from the Teams IP Group. This removes the SIP P-Asserted-Identity Header.	Microsoft Office 365 may be configured to send the PAI header, but we recommend to do this in the SBC for better interoperability.
1	This rule applies to messages sent to the Twilio Elastic SIP Trunk IP. This removes the SIP Privacy Header in all messages, except for a call with presentation restrictions.	The same as in the previous rule.
2	This rule applies to messages sent to the Elastic SIP Trunk IP Group in a call forwarding scenario. This rule replaces the host part of the SIP History-Info Header with the value, configured in the Twilio Elastic SIP Trunk IP Group.	To introduce Topology Hiding in the Call Forward scenarios, the host part of the SIP History-Info Header should be replaced with the value that was configured in the Elastic SIP Trunk IP Group.
3	This rule also applies to messages sent to the Elastic SIP Trunk IP Group in a call forwarding scenario. This rule removes the SIP History-Info.1 Header.	To introduce Topology Hiding in the Call Forward scenarios, the SIP History-Info.1 Header should be removed.
4	This rule applies to messages sent to the Elastic SIP Trunk IP Group in a call transfer scenario. This replaces the host part of the SIP Referred-by Header with the value, configured in the Twilio Elastic SIP Trunk IP Group.	To introduce Topology Hiding in the Call Transfer scenarios, the host part of the SIP Referred-by Header should be replaced with the value that was configured in the Elastic SIP Trunk IP Group.
5	This replaces the method types '488', '503' and '603' with the value '486'.	Twilio Elastic SIP Trunk (or interconnected to it telephony provider) does not recognize these method types correctly.

8. Assign Manipulation Set ID 1 to the Teams Direct Routing IP Group:
 - a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
 - b. Select the row of the Teams Direct Routing IP Group, and then click **Edit**.
 - c. Set the 'Inbound Message Manipulation Set' field to 1.

Figure 4-34: Assigning Manipulation Set to the Teams Direct Routing IP Group

The screenshot shows the configuration page for an IP Group named 'Teams'. The 'MESSAGE MANIPULATION' section is expanded, showing the following settings:

- Inbound Message Manipulation Set: 1
- Outbound Message Manipulation Set: -1
- Message Manipulation User-Defined String 1: (empty)
- Message Manipulation User-Defined String 2: (empty)
- Proxy Keep-Alive using IP Group settings: Enable

Other visible settings include: SRD: #0 [DefaultSRD], Index: 2, Name: Teams, Topology Location: Up, Type: Server, Proxy Set: #2 [Teams], IP Profile: #2 [Teams], Media Realm: #0 [DefaultRealm], Internal Media Realm: --, Contact User: (empty), SIP Group Name: (empty). Buttons for 'Cancel' and 'APPLY' are at the bottom.

- d. Click **Apply**.
9. Assign Manipulation Set ID 4 to the Twilio Elastic SIP Trunk IP Group:
 - a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
 - b. Select the row of the Twilio Elastic SIP Trunk IP Group, and then click **Edit**.
 - c. Set the 'Outbound Message Manipulation Set' field to 4.

Figure 4-35: Assigning Manipulation Set 4 to the Twilio Elastic SIP Trunk IP Group

The screenshot shows the configuration page for an IP Group named 'Twilio'. The 'MESSAGE MANIPULATION' section is expanded, showing the following settings:

- Inbound Message Manipulation Set: -1
- Outbound Message Manipulation Set: 4
- Message Manipulation User-Defined String 1: (empty)
- Message Manipulation User-Defined String 2: (empty)
- Proxy Keep-Alive using IP Group settings: Disable

Other visible settings include: SRD: #0 [DefaultSRD], Index: 1, Name: Twilio, Topology Location: Down, Type: Server, Proxy Set: #1 [Twilio], IP Profile: #1 [Twilio], Media Realm: #0 [DefaultRealm], Internal Media Realm: --, Contact User: (empty), SIP Group Name: (empty). Buttons for 'Cancel' and 'APPLY' are at the bottom.

- d. Click **Apply**.

4.16 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

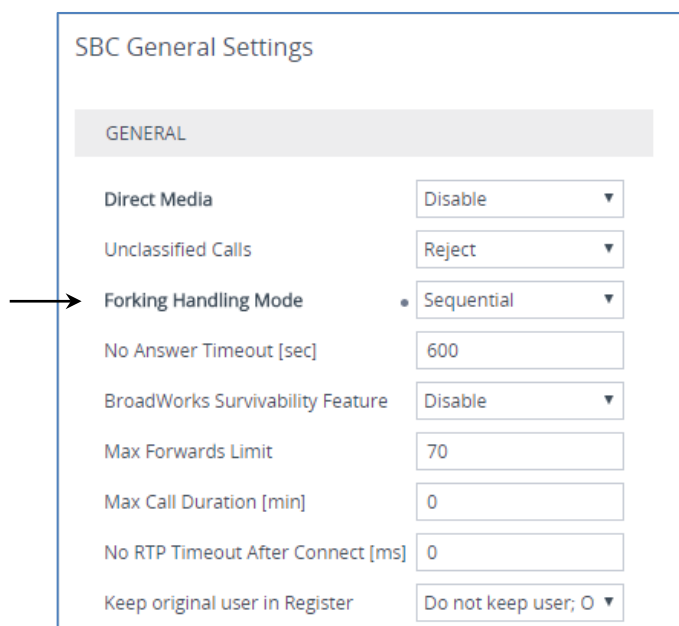
4.16.1 Configure Call Forking Mode

This section describes how to configure the SBC's handling of SIP 18x responses received for call forking of INVITE messages. For the interoperability test topology, if a SIP 18x response with SDP is received, the SBC opens a voice stream according to the received SDP. The SBC re-opens the stream according to subsequently received 18x responses with SDP or plays a ringback tone if a 180 response without SDP is received. It is mandatory to set this field for the Teams Direct Routing environment.

➤ **To configure call forking:**

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).
2. From the 'SBC Forking Handling Mode' drop-down list, select **Sequential**.

Figure 4-36: Configuring Forking Mode



The screenshot shows the 'SBC General Settings' page with the 'GENERAL' tab selected. The 'Forking Handling Mode' dropdown menu is highlighted with a black arrow pointing to it, and the value 'Sequential' is selected. Other settings include: Direct Media (Disable), Unclassified Calls (Reject), No Answer Timeout [sec] (600), BroadWorks Survivability Feature (Disable), Max Forwards Limit (70), Max Call Duration [min] (0), No RTP Timeout After Connect [ms] (0), and Keep original user in Register (Do not keep user; 0).

Setting	Value
Direct Media	Disable
Unclassified Calls	Reject
Forking Handling Mode	Sequential
No Answer Timeout [sec]	600
BroadWorks Survivability Feature	Disable
Max Forwards Limit	70
Max Call Duration [min]	0
No RTP Timeout After Connect [ms]	0
Keep original user in Register	Do not keep user; 0

3. Click **Apply**.

4.16.2 Optimizing CPU Cores Usage for a Specific Service



Note: This section is applicable to Mediant 9000 and Mediant 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.

A AudioCodes INI File

The *ini* configuration file of the SBC, corresponding to the Web-based configuration as described in Section 4 on page 21, is shown below:



Note: To load or save an *ini* file, use the Configuration File page (**Setup** menu > **Administration** tab > **Maintenance** folder > **Configuration File**).

```
;*****
;** Ini File **
;*****

;Time & Date: 25/10/2020 11:38:58
;Device Up Time: 11d:20h:47m:14s
;Board: M800B
;Board Type: 72
;Serial Number: 4807217
;Software Version: 7.20A.260.012
;DSP Software Version: 5014AE3_R => 723.06
;Board IP Address: 10.15.77.77
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;CPU: Cavium Networks Octeon V0.1 @ 300Mhz, total 2 cores, 2 cpus, 1
sockets
;Cores mapping:
;core #0, on cpu #0, on socket #0
;core #1, on cpu #1, on socket #0
;Memory: 512 MB
;Flash size: 64 MB
;Num of DSP Cores: 3
;Num of physical LAN ports: 4
;;;Key features;;Board Type: M800B ;QOE features: VoiceQualityMonitoring
MediaEnhancement ;DSP Voice features: RTCP-XR ;Security: IPSEC
MediaEncryption StrongEncryption EncryptControlProtocol ;Coders: G723
G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB
G722 EG711 MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB OPUS_NB
OPUS_WB EVS ;IP Media: Conf VXML ;Channel Type: DspCh=30 IPMediaDspCh=30
;HA ;BRITrunks=4 ;ElTrunks=1 ;T1Trunks=1 ;FXSPorts=4 ;FXOPorts=0 ;Control
Protocols: MGCP SIP SBC=100 MSFT TRANSCODING=100 FEU=100 TestCall=100
SIPRec=10 CODER-TRANSCODING=100 SBC-SIGNALING=100 ELIN HttpProxy TEAMS
;Default features;;Coders: G711 G726;

;----- HW components -----
;
; Slot # : Module type : # of ports
;-----
;      1 : FALC56      : 1
;      2 : FXS         : 4
;      3 : BRI         : 4
;-----

;USB Port 1: Empty
;USB Port 2: Empty
;-----
```

```

[SYSTEM Params]

SyslogServerIP = 10.15.77.100
EnableSyslog = 1
NTPServerUTCOffset = 7200
HALocalMAC = '00908f495a31'
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '10.15.27.1'
Tr069VerifyCommonName = 0
SBCWizardFilename = 'templates4.zip'

[BSP Params]

PCMLawSelect = 3
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]

[ControlProtocols Params]

AdminStateLockControl = 0

[PSTN Params]

V5ProtocolSide = 0

[Voice Engine Params]

ENABLEMEDIASECURITY = 1
PLThresholdLevelsPerMille_0 = 5
PLThresholdLevelsPerMille_1 = 10
PLThresholdLevelsPerMille_2 = 20
PLThresholdLevelsPerMille_3 = 50
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

Languages = 'en-US', '', '', '', '', '', '', '', ''

[SIP Params]

GWDEBUGLEVEL = 5
MSLDAPPRIMARYKEY = 'telephoneNumber'
MEDIACDRREPORTLEVEL = 1
SBCFORKINGHANDLINGMODE = 1
ANSWERDETECTORCMD = 10486144

[SNMP Params]

[ PhysicalPortsTable ]

```

```

FORMAT Index = Port, Mode, SpeedDuplex, PortDescription, GroupMember;
PhysicalPortsTable 0 = "GE_4_1", 1, 4, "User Port #0", "GROUP_1";
PhysicalPortsTable 1 = "GE_4_2", 1, 4, "User Port #1", "GROUP_1";
PhysicalPortsTable 2 = "GE_4_3", 1, 4, "User Port #2", "GROUP_2";
PhysicalPortsTable 3 = "GE_4_4", 1, 4, "User Port #3", "GROUP_2";

[ \PhysicalPortsTable ]

[ EtherGroupTable ]

FORMAT Index = Group, Mode, Member1, Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";

[ \EtherGroupTable ]

[ DeviceTable ]

FORMAT Index = VlanID, UnderlyingInterface, DeviceName, Tagging, MTU;
DeviceTable 0 = 1, "GROUP_1", "vlan 1", 0, 1500;
DeviceTable 1 = 2, "GROUP_2", "vlan 2", 0, 1500;

[ \DeviceTable ]

[ InterfaceTable ]

FORMAT Index = ApplicationTypes, InterfaceMode, IPAddress, PrefixLength,
Gateway, InterfaceName, PrimaryDNSServerIPAddress,
SecondaryDNSServerIPAddress, UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.77.77, 16, 10.15.0.1, "LAN_IF", 10.1.1.6,
, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.156, 24, 195.189.192.129, "WAN_IF",
80.179.52.100, 80.179.55.100, "vlan 2";

[ \InterfaceTable ]

[ WebUsers ]

FORMAT Index = Username, Password, Status, PwAgeInterval, SessionLimit,
CliSessionLimit, SessionTimeout, BlockTime, UserLevel, PwNonce,
SSHPublicKey;
WebUsers 0 = "Admin",
"$1$bgtdFkgQREJNFRNJHUhDGRtPTuPju+bhteClubG4vby9t7fy9fbloqfyoKmt+KP5/qz9m
ZSTlpyUkpDNzMudz54=", 1, 0, 5, -1, 15, 60, 200,
"e4064f90b5b26631d46fbcdb79f2b7a0", ".fc";
WebUsers 1 = "User",
"$1$Cj46OmhtN3E1JiolcSQnfXh4Ii5+Jn4ZRBQRHR0fHx4bTB9ITE8aVgRQVQUGAAEPXvKCD
w0GWSEgIHN0dHB2LHE=", 1, 0, 5, -1, 15, 60, 50,
"c26a27dd91a886b99de5e81b9a736232", "";

[ \WebUsers ]

```

```

[ TLSContexts ]

FORMAT Index = Name, TLSVersion, DTLSVersion, ServerCipherString,
ClientCipherString, ServerCipherTLS13String, ClientCipherTLS13String,
KeyExchangeGroups, RequireStrictCert, TlsRenegotiation,
MiddleboxCompatMode, OcspEnable, OcspServerPrimary, OcspServerSecondary,
OcspServerPort, OcspDefaultResponse, DHKeySize;
TLSContexts 0 = "default", 7, 0, "DEFAULT", "DEFAULT",
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA2
56",
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA2
56", "X25519:P-256:P-384:X448", 0, 1, 0, 0, 0.0.0.0, 0.0.0.0, 2560, 0,
2048;
TLSContexts 1 = "Teams", 4, 0, "DEFAULT", "DEFAULT",
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA2
56",
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA2
56", "X25519:P-256:P-384:X448", 0, 1, 0, 0, 0.0.0.0, 0.0.0.0, 2560, 0,
2048;
TLSContexts 2 = "Twilio", 4, 0, "DEFAULT", "DEFAULT",
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA2
56",
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA2
56", "X25519:P-256:P-384:X448", 0, 1, 0, 0, 0.0.0.0, 0.0.0.0, 2560, 0,
2048;

[ \TLSContexts ]

[ AudioCodersGroups ]

FORMAT Index = Name;
AudioCodersGroups 0 = "AudioCodersGroups_0";
AudioCodersGroups 1 = "AudioCodersGroups_1";

[ \AudioCodersGroups ]

[ AllowedAudioCodersGroups ]

FORMAT Index = Name;
AllowedAudioCodersGroups 0 = "Twilio Allowed Audio Coders";

[ \AllowedAudioCodersGroups ]

[ IpProfile ]

FORMAT Index = ProfileName, IpPreference, CodersGroupName, IsFaxUsed,
JitterBufMinDelay, JitterBufOptFactor, IPDiffServ, SigIPDiffServ,
RTPRedundancyDepth, CNGmode, VxxTransportType, NSEMode, IsDTMFUsed,
PlayRBTone2IP, EnableEarlyMedia, ProgressIndicator2IP,
EnableEchoCanceller, CopyDest2RedirectNumber, MediaSecurityBehaviour,
CallLimit, DisconnectOnBrokenConnection, FirstTxDtmfOption,
SecondTxDtmfOption, RxDTMFOption, EnableHold, InputGain, VoiceVolume,
AddIEInSetup, SBCExtensionCodersGroupName, MediaIPVersionPreference,
TranscodingMode, SBCEAllowedMediaTypes, SBCEAllowedAudioCodersGroupName,
SBCEAllowedVideoCodersGroupName, SBCEAllowedCodersMode,
SBCEMediaSecurityBehaviour, SBCERFC2833Behavior, SBCEAlternativeDTMFMethod,
    
```

```

SBCSendMultipleDTMFMethods, SBCAssertIdentity,
AMDSensitivityParameterSuit, AMDSensitivityLevel, AMDMaxGreetingTime,
AMDMaxPostSilenceGreetingTime, SBCDiversioMode, SBCHistoryInfoMode,
EnableQSIGTunneling, SBCFaxCodersGroupName, SBCFaxBehavior,
SBCFaxOfferMode, SBCFaxAnswerMode, SbcPrackMode, SBCSessionExpiresMode,
SBCRemoteUpdateSupport, SBCRemoteReinviteSupport,
SBCRemoteDelayedOfferSupport, SBCRemoteReferBehavior,
SBCRemote3xxBehavior, SBCRemoteMultiple18xSupport,
SBCRemoteEarlyMediaResponseType, SBCRemoteEarlyMediaSupport,
EnableSymmetricMKI, MKISize, SBCEnforceMKISize, SBCRemoteEarlyMediaRTP,
SBCRemoteSupportsRFC3960, SBCRemoteCanPlayRingback, EnableEarly183,
EarlyAnswerTimeout, SBC2833DTMFPayloadType, SBCUserRegistrationTime,
ResetSRTPStateUponRekey, AmdMode, SBCReliableHeldToneSource,
GenerateSRTPKeys, SBCPlayHeldTone, SBCRemoteHoldFormat,
SBCRemoteReplacesBehavior, SBCSDPptimeAnswer, SBCPreferredPTime,
SBCUseSilenceSupp, SBCRTPRedundancyBehavior, SBCPlayRBTToTransferee,
SBCRTPCompensation, SBCJitterCompensation, SBCRemoteRenegotiateOnFaxDetection,
JitterBufMaxDelay, SBCUserBehindUdpNATRegistrationTime,
SBCUserBehindTcpNATRegistrationTime, SBCSDPHandlerTCPAttribute,
SBCRemoveCryptoLifetimeInSDP, SBCIceMode, SBCRTCPMux,
SBCMediaSecurityMethod, SBCHandleXDetect, SBCRTCPFeedback,
SBCRemoteRepresentationMode, SBCKeepVIAHeaders, SBCKeepRoutingHeaders,
SBCKeepUserAgentHeader, SBCRemoteMultipleEarlyDialogs,
SBCRemoteMultipleAnswersMode, SBCDirectMediaTag,
SBCAdaptRFC2833BWToVoiceCoderBW, CreatedByRoutingServer,
SBCFaxReroutingMode, SBCMaxCallDuration, SBCGenerateRTP,
SBCISUPBodyHandling, SBCISUPVariant, SBCVoiceQualityEnhancement,
SBCMaxOpusBW, SBCEnhancedPlc, LocalRingbackTone, LocalHeldTone,
SBCGenerateNoOp, SBCRemoveUnknownCrypto, SBCMultipleCoders, DataDiffServ,
SBCMSRPReinviteUpdateSupport, SBCMSRPOfferSetupRole, SBCMSRPEmpMsg;
IpProfile 1 = "Twilio", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0,
0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", "", 0, 1,
"", "Twilio Allowed Audio Coders", "", 0, 1, 0, 0, 0, 1, 0, 8, 300, 400,
0, 0, 0, "", 0, 0, 1, 3, 0, 0, 2, 1, 3, 2, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0,
0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1, 0, 0,
0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -
1, -1, 0, 0, 0, 0, 1, 2, 0;
IpProfile 2 = "Teams", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0, 0,
2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "",
"AudioCodersGroups_1", 0, 0, "", "", "", 0, 1, 0, 0, 0, 0, 8, 300,
400, 0, 0, 0, "", 0, 0, 1, 3, 0, 0, 1, 0, 3, 2, 1, 0, 1, 0, 0, 0, 1, 0,
0, 0, 0, 0, 0, 0, 1, 0, 0, 3, 1, 0, 0, 0, 0, 1, 0, 0, 300, -1, -1,
0, 0, 1, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, -1, -1, 0, 0, 0, 0, 1, 2, 0;

[ \IpProfile ]

[ CpMediaRealm ]

FORMAT Index = MediaRealmName, IPv4IF, IPv6IF, RemoteIPv4IF,
RemoteIPv6IF, PortRangeStart, MediaSessionLeg, PortRangeEnd,
TCPPortRangeStart, TCPPortRangeEnd, IsDefault, QoeProfile, BWProfile,
TopologyLocation;
CpMediaRealm 0 = "DefaultRealm", "WAN_IF", "", "", "", 6000, 5953, 65529,
0, 0, 0, "", "", 0;

[ \CpMediaRealm ]

[ SBCRoutingPolicy ]

FORMAT Index = Name, LCREnable, LCRAverageCallLength, LCRDefaultCost,
LdapServerGroupName;

```

```

SBCRoutingPolicy 0 = "Default_SBCRoutingPolicy", 0, 1, 0, "";

[ \SBCRoutingPolicy ]

[ SRD ]

FORMAT Index = Name, BlockUnRegUsers, MaxNumOfRegUsers,
EnableUnAuthenticatedRegistrations, SharingPolicy, UsedByRoutingServer,
SBCOperationMode, SBCRoutingPolicyName, SBCDialPlanName,
AdmissionProfile;
SRD 0 = "DefaultSRD", 0, -1, 1, 0, 0, 0, "Default_SBCRoutingPolicy", "",
"";

[ \SRD ]

[ MessagePolicy ]

FORMAT Index = Name, MaxMessageLength, MaxHeaderLength, MaxBodyLength,
MaxNumHeaders, MaxNumBodies, SendRejection, MethodList, MethodListType,
BodyList, BodyListType, UseMaliciousSignatureDB;
MessagePolicy 0 = "Malicious Signature DB Protection", -1, -1, -1, -1, -
1, 1, "", 0, "", 0, 1;

[ \MessagePolicy ]

[ SIPInterface ]

FORMAT Index = InterfaceName, NetworkInterface,
SCTPSecondaryNetworkInterface, ApplicationType, UDPPort, TCPPort,
TLSPort, SCTPPort, AdditionalUDPPorts, AdditionalUDPPortsMode, SRDName,
MessagePolicyName, TLSContext, TLSMutualAuthentication,
TCPKeepaliveEnable, ClassificationFailureResponseType,
PreClassificationManSet, EncapsulatingProtocol, MediaRealm,
SBCDirectMedia, BlockUnRegUsers, MaxNumOfRegUsers,
EnableUnAuthenticatedRegistrations, UsedByRoutingServer,
TopologyLocation, PreParsingManSetName, AdmissionProfile,
CallSetupRulesSetId;
SIPInterface 0 = "SIPInterface_0", "WAN_IF", "", 2, 0, 0, 5061, 0, "", 0,
"DefaultSRD", "", "default", -1, 1, 0, -1, 0, "DefaultRealm", 0, -1, -1,
-1, 0, 0, "", "", -1;

[ \SIPInterface ]

[ ProxySet ]

FORMAT Index = ProxyName, EnableProxyKeepAlive, ProxyKeepAliveTime,
ProxyLoadBalancingMethod, IsProxyHotSwap, SRDName, ClassificationInput,
TLSContextName, ProxyRedundancyMode, DNSResolveMethod,
KeepAliveFailureResp, GWIPv4SIPInterfaceName, SBCIPv4SIPInterfaceName,
GWIPv6SIPInterfaceName, SBCIPv6SIPInterfaceName, MinActiveServersLB,
SuccessDetectionRetries, SuccessDetectionInterval,
FailureDetectionRetransmissions;
ProxySet 0 = "ProxySet_0", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"", "SIPInterface_0", "", "", 1, 1, 10, -1;
ProxySet 1 = "Twilio", 1, 60, 0, 1, "DefaultSRD", 0, "Twilio", -1, -1,
"", "", "SIPInterface_0", "", "", 1, 1, 10, -1;
    
```



```

ProxySet 2 = "Teams", 1, 60, 2, 1, "DefaultSRD", 0, "Teams", -1, -1, "",
"", "SIPInterface_0", "", "", 1, 1, 10, -1;

[ \ProxySet ]

[ IPGroup ]

FORMAT Index = Type, Name, ProxySetName, VoiceAIConnector, SIPGroupName,
ContactUser, SipReRoutingMode, AlwaysUseRouteTable, SRDName, MediaRealm,
InternalMediaRealm, ClassifyByProxySet, ProfileName, MaxNumOfRegUsers,
InboundManSet, OutboundManSet, RegistrationMode, AuthenticationMode,
MethodList, SBCServerAuthType, OAuthHTTPService, EnableSBCClientForking,
SourceUriInput, DestUriInput, ContactName, Username, Password, UIFormat,
QOEProfile, BWProfile, AlwaysUseSourceAddr, MsgManUserDef1,
MsgManUserDef2, SIPConnect, SBCPSAPMode, DTLContext,
CreatedByRoutingServer, UsedByRoutingServer, SBCOperationMode,
SBCRouteUsingRequestURIPort, SBCKeepOriginalCallID, TopologyLocation,
SBCDialPlanName, CallSetupRulesSetId, Tags, SBCUserStickiness,
UserUDPPortAssignment, AdmissionProfile, ProxyKeepAliveUsingIPG,
SBCAltRouteReasonsSetName, TeamsLocalMediaOptimization,
TeamsLocalMOInitialBehavior, SIPSourceHostName;
IPGroup 0 = 0, "Default_IPG", "ProxySet_0", "", "", "", -1, 0,
"DefaultSRD", "", "", 0, "", -1, -1, -1, 0, 0, "", -1, "", 0, -1, -1, "",
"", "$l$gQ=", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 0,
"", -1, "", 0, 0, "", 0, "", 0, 0, "";
IPGroup 1 = 0, "Twilio", "Twilio", "", "audcl.pstn.twilio.com", "", -1,
0, "DefaultSRD", "DefaultRealm", "", 1, "Twilio", -1, -1, 4, 0, 0, "", -
1, "", 0, -1, -1, "", "", "$l$gQ=", 0, "", "", 0, "", "", 0, 0,
"default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, "", 0, "", 0, 0, "";
IPGroup 2 = 0, "Teams", "Teams", "", "audcl.pstn.twilio.com", "", -1, 0,
"DefaultSRD", "DefaultRealm", "", 0, "Teams", -1, 1, -1, 0, 0, "", -1,
"", 0, -1, -1, "int-sbcl.audctrunk.aceducation.info", "", "$l$gQ=", 0,
"", "", 1, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 1, "", -1, "", 0, 0,
"", 1, "", 0, 0, "";

[ \IPGroup ]

[ ProxyIp ]

FORMAT Index = ProxySetId, ProxyIpIndex, IpAddress, TransportType,
Priority, Weight;
ProxyIp 0 = "1", 0, "audcl.pstn.twilio.com:5061", 2, 0, 0;
ProxyIp 1 = "2", 0, "sip.pstnhub.microsoft.com:5061", 2, 1, 1;
ProxyIp 2 = "2", 1, "sip2.pstnhub.microsoft.com:5061", 2, 2, 1;
ProxyIp 3 = "2", 2, "sip3.pstnhub.microsoft.com:5061", 2, 3, 1;

[ \ProxyIp ]

[ ConditionTable ]

FORMAT Index = Name, Condition;
ConditionTable 0 = "Teams-Contact", "Header.Contact.URL.Host contains
'pstnhub.microsoft.com'";

[ \ConditionTable ]

[ IP2IPRouting ]

```

```

FORMAT Index = RouteName, RoutingPolicyName, SrcIPGroupName,
SrcUsernamePrefix, SrcHost, DestUsernamePrefix, DestHost, RequestType,
MessageConditionName, ReRouteIPGroupName, Trigger, CallSetupRulesSetId,
DestType, DestIPGroupName, DestSIPInterfaceName, DestAddress, DestPort,
DestTransportType, AltRouteOptions, GroupPolicy, CostGroup, DestTags,
ModifiedDestUserName, SrcTags, IPGroupSetName, RoutingTagName,
InternalAction;
IP2IPRouting 0 = "Terminate OPTIONS", "Default_SBCRoutingPolicy", "Any",
"*,"*,"*,*, 6, "", "Any", 0, -1, 13, "", "", "", 0, -1, 0, 0, "",
"", "", "", "", "default", "Reply (Response='200')";
IP2IPRouting 1 = "Refer from Teams", "Default_SBCRoutingPolicy", "Any",
"*,"*,"*,*, 0, "", "Teams", 2, -1, 2, "Teams", "", "", 0, -1, 0,
0, "", "", "", "", "default", "";
IP2IPRouting 2 = "Teams to SIP Trunk", "Default_SBCRoutingPolicy",
"Teams","*,"*,*,*, 0, "", "Any", 0, -1, 0, "Twilio", "", "", 0,
-1, 0, 0, "", "", "", "", "default", "";
IP2IPRouting 3 = "SIP Trunk to Teams", "Default_SBCRoutingPolicy",
"Twilio","*,"*,*,*, 0, "", "Any", 0, -1, 0, "Teams", "", "", 0,
-1, 0, 0, "", "", "", "", "default", "";

[ \IP2IPRouting ]

[ Classification ]

FORMAT Index = ClassificationName, MessageConditionName, SRDName,
SrcSIPInterfaceName, SrcAddress, SrcPort, SrcTransportType,
SrcUsernamePrefix, SrcHost, DestUsernamePrefix, DestHost, ActionType,
SrcIPGroupName, DestRoutingPolicy, IpProfileName, IPGroupSelection,
IpGroupTagName;
Classification 0 = "Teams", "Teams-Contact", "DefaultSRD",
"SIPInterface_0", "52.114.*.*", 0, -1, "*", "*", "*", "int-
sbcl.audctrunk.aceducation.info", 1, "Teams", "", "", 0, "default";
Classification 1 = "Twilio Termination URI", "", "DefaultSRD",
"SIPInterface_0", "", 0, -1, "*", "audcl.pstn.twilio.com", "*", "*", 1,
"Twilio", "", "", 0, "default";

[ \Classification ]

[ MessageManipulations ]

FORMAT Index = ManipulationName, ManSetID, MessageType, Condition,
ActionSubject, ActionType, ActionValue, RowRole;
MessageManipulations 0 = "Remove PAI", 1, "", "", "Header.P-Asserted-
Identity", 1, "", 0;
MessageManipulations 1 = "Remove Privacy", 4, "", "Header.Privacy exists
And Header.From.URL !contains 'anonymous'", "Header.Privacy", 1, "", 0;
MessageManipulations 2 = "Change Host of History-Info.0", 4,
"Invite.Request", "Header.History-Info.0 regex
(.*)@(.) (;user=phone) (.)", "Header.History-Info.0", 2,
"$1+$2+Param.IPG.Dst.Host+$4+$5", 0;
MessageManipulations 3 = "Remove History-Info.1", 4, "Invite.Request",
"", "Header.History-Info.1", 1, "", 0;
MessageManipulations 4 = "Change Referred-by Host", 4, "Invite.Request",
"Header.Referred-By exists", "Header.Referred-By.URL.Host", 2,
"Param.IPG.Dst.Host", 0;
MessageManipulations 5 = "Error Responses", 4, "Any.Response",
"Header.Request-URI.MethodType=='488' OR Header.Request-
URI.MethodType=='503' OR Header.Request-URI.MethodType=='603'",
"Header.Request-URI.MethodType", 2, "'486'", 0;
    
```

```
[ \MessageManipulations ]

[ GwRoutingPolicy ]

FORMAT Index = Name, LCREnable, LCRAverageCallLength, LCRDefaultCost,
LdapServerGroupName;
GwRoutingPolicy 0 = "GwRoutingPolicy", 0, 1, 0, "";

[ \GwRoutingPolicy ]

[ LoggingFilters ]

FORMAT Index = FilterType, Value, LogDestination, CaptureType, Mode;
LoggingFilters 0 = 1, "", 1, 2, 0;

[ \LoggingFilters ]

[ ResourcePriorityNetworkDomains ]

FORMAT Index = Name, Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 1;
ResourcePriorityNetworkDomains 2 = "dod", 1;
ResourcePriorityNetworkDomains 3 = "drsn", 1;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 1;

[ \ResourcePriorityNetworkDomains ]

[ MaliciousSignatureDB ]

FORMAT Index = Name, Pattern;
MaliciousSignatureDB 0 = "SIPVicious", "Header.User-Agent.content prefix
'friendly-scanner'";
MaliciousSignatureDB 1 = "SIPScan", "Header.User-Agent.content prefix
'sip-scan'";
MaliciousSignatureDB 2 = "Smapi", "Header.User-Agent.content prefix
'smap'";
MaliciousSignatureDB 3 = "Sipsak", "Header.User-Agent.content prefix
'sipsak'";
MaliciousSignatureDB 4 = "Sipcli", "Header.User-Agent.content prefix
'sipcli'";
MaliciousSignatureDB 5 = "Sivus", "Header.User-Agent.content prefix
'SIVuS'";
MaliciousSignatureDB 6 = "Gulp", "Header.User-Agent.content prefix
'Gulp'";
MaliciousSignatureDB 7 = "Sipv", "Header.User-Agent.content prefix
'sipv'";
MaliciousSignatureDB 8 = "Sundayddr Worm", "Header.User-Agent.content
prefix 'sundayddr'";
MaliciousSignatureDB 9 = "VaxIPUserAgent", "Header.User-Agent.content
prefix 'VaxIPUserAgent'";
MaliciousSignatureDB 10 = "VaxSIPUserAgent", "Header.User-Agent.content
prefix 'VaxSIPUserAgent'";
```

```

MaliciousSignatureDB 11 = "SipArmyKnife", "Header.User-Agent.content
prefix 'siparmyknife'";

[ \MaliciousSignatureDB ]

[ AllowedAudioCoders ]

FORMAT Index = AllowedAudioCodersGroupName, AllowedAudioCodersIndex,
CoderID, UserDefineCoder;
AllowedAudioCoders 0 = "Twilio Allowed Audio Coders", 0, 1, "";
AllowedAudioCoders 1 = "Twilio Allowed Audio Coders", 1, 2, "";

[ \AllowedAudioCoders ]

[ AudioCoders ]

FORMAT Index = AudioCodersGroupId, AudioCodersIndex, Name, pTime, rate,
PayloadType, Sce, CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 0, 1, 2, 90, -1, 0, "";
AudioCoders 1 = "AudioCodersGroups_1", 0, 35, 2, 19, 103, 0, "";
AudioCoders 2 = "AudioCodersGroups_1", 1, 36, 2, 43, 104, 0, "";
AudioCoders 3 = "AudioCodersGroups_1", 2, 3, 2, 19, -1, 0, "";
AudioCoders 4 = "AudioCodersGroups_1", 3, 1, 2, 90, -1, 0, "";
AudioCoders 5 = "AudioCodersGroups_1", 4, 2, 2, 90, -1, 0, "";
AudioCoders 6 = "AudioCodersGroups_0", 1, 2, 2, 90, -1, 0, "";

[ \AudioCoders ]
    
```

This page is intentionally left blank.

International Headquarters

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

AudioCodes Inc.

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

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

website: <https://www.audiocodes.com>

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

Document #: LTRT-12414

