

## **Microsoft® Teams Direct Routing Enterprise Model and Swisscom SIP Trunk "Enterprise SIP" using AudioCodes Mediant™ SBC**

Version 7.4



## Table of Contents

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Introduction .....</b>  | <b>7</b>  |
| 1.1      | Intended Audience .....  | 7         |
| 1.2      | About AudioCodes SBC Product Series .....                                | 7         |
| 1.3      | About Microsoft Teams Direct Routing .....                               | 7         |
| <b>2</b> | <b>Component Information.....</b>  | <b>9</b>  |
| 2.1      | AudioCodes SBC Version.....  | 9         |
| 2.2      | Swisscom Enterprise SIP Trunking 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.....   | 12        |
| <b>3</b> | <b>Configuring Teams Direct Routing .....</b>                            | <b>13</b> |
| 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 Routing Policy .....                  | 20        |
| <b>4</b> | <b>Configuring AudioCodes SBC .....</b>                                  | <b>21</b> |
| 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 for Teams Direct Routing.....                       | 26        |
| 4.3.3    | Configure a Certificate .....  | 27        |
| 4.3.4    | Method of Generating and Installing the Wildcard Certificate .....       | 30        |
| 4.3.5    | Deploy Trusted Root Certificate for MTLS Connection .....                | 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 Sets.....  | 34        |
| 4.6.2    | Configure a Proxy Address.....   | 35        |
| 4.7      | Configure Coders .....   | 37        |
| 4.8      | Configure IP Profiles.....   | 40        |
| 4.9      | Configure IP Groups.....   | 43        |
| 4.10     | Configure SRTP .....   | 44        |
| 4.11     | Configuring Message Condition Rules.....                                 | 45        |
| 4.12     | Configuring Classification Rules .....                                   | 46        |
| 4.13     | Configure IP-to-IP Call Routing Rules .....                              | 47        |
| 4.14     | Configure Number Manipulation Rules .....                                | 48        |

---

|        |   |    |
|--------|---|----|
| 4.15   | Configure Message Manipulation Rules .....  | 50 |
| 4.16   | Miscellaneous Configuration.....  | 81 |
| 4.16.1 | Configure Call Forking Mode.....  | 81 |
| 4.16.2 | Optimizing CPU Cores Usage for a Specific Service (relevant for Mediant 9000 and Software SBC only) ..... | 82 |



## 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: April-07-2024

## 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   |
|-------|---|
| 12669 | Updated document for Version 7.4.   |
| 12681 | Updated Swisscom IP Profile (PRACK Mode parameter) according to Swisscom request. |
| 12682 | Replace Baltimore Root Certificates by DigiCert due to Microsoft notice.          |

## Documentation Feedback

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

**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 Swisscom's 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 Swisscom partners who are responsible for installing and configuring Swisscom's SIP Trunk and Microsoft's Teams Direct Routing Service for enabling VoIP calls using AudioCodes SBC.

## 1.2 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, 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 and Multi-Service Business Router platforms, or as a software-only solution for deployment with third-party hardware. The SBC can be offered as a Virtualized SBC, supporting the following platforms: Hyper-V, AWS, AZURE, AWP, KVM and VMWare.

## 1.3 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**

|                         |   |
|-------------------------|---|
| <b>SBC Vendor</b>       | AudioCodes  |
| <b>Models</b>           | <ul style="list-style-type: none"> <li>▪ Mediant 500 Gateway &amp; E-SBC</li> <li>▪ Mediant 500L Gateway &amp; E-SBC</li> <li>▪ Mediant 800B Gateway &amp; E-SBC</li> <li>▪ Mediant 1000B Gateway &amp; E-SBC</li> <li>▪ Mediant 2600 E-SBC</li> <li>▪ Mediant 4000 SBC</li> <li>▪ Mediant 4000B SBC</li> <li>▪ Mediant 9000 SBC</li> <li>▪ Mediant Software SBC (SE and VE)</li> </ul> |
| <b>Software Version</b> | 7.40A.100.114   |
| <b>Protocol</b>         | <ul style="list-style-type: none"> <li>▪ SIP/TCP (to the Swisscom SIP Trunk)</li> <li>▪ SIP/TLS (to the Teams Direct Routing)</li> </ul>  |
| <b>Additional Notes</b> | None  |

### 2.2 Swisscom Enterprise SIP Trunking Version

**Table 2-2: Swisscom Version**

|                                |  |
|--------------------------------|--|
| <b>Vendor/Service Provider</b> | Swisscom   |
| <b>SSW Model/Service</b>       | Enterprise SIP Standard and Enterprise SIP WAN with Cisco eSBC ISR4321 |
| <b>Software Version</b>        | IOS XE 17.2.1r   |
| <b>Protocol</b>                | SIP  |
| <b>Additional Notes</b>        | None   |

### 2.3 Microsoft Teams Direct Routing Version

**Table 2-3: Microsoft Teams Direct Routing Version**

|                         |                                   |
|-------------------------|-----------------------------------|
| <b>Vendor</b>           | Microsoft                         |
| <b>Model</b>            | Teams Phone System Direct Routing |
| <b>Software Version</b> |                                   |
| <b>Protocol</b>         | SIP                               |
| <b>Additional Notes</b> | None                              |

## 2.4 Interoperability Test Topology

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

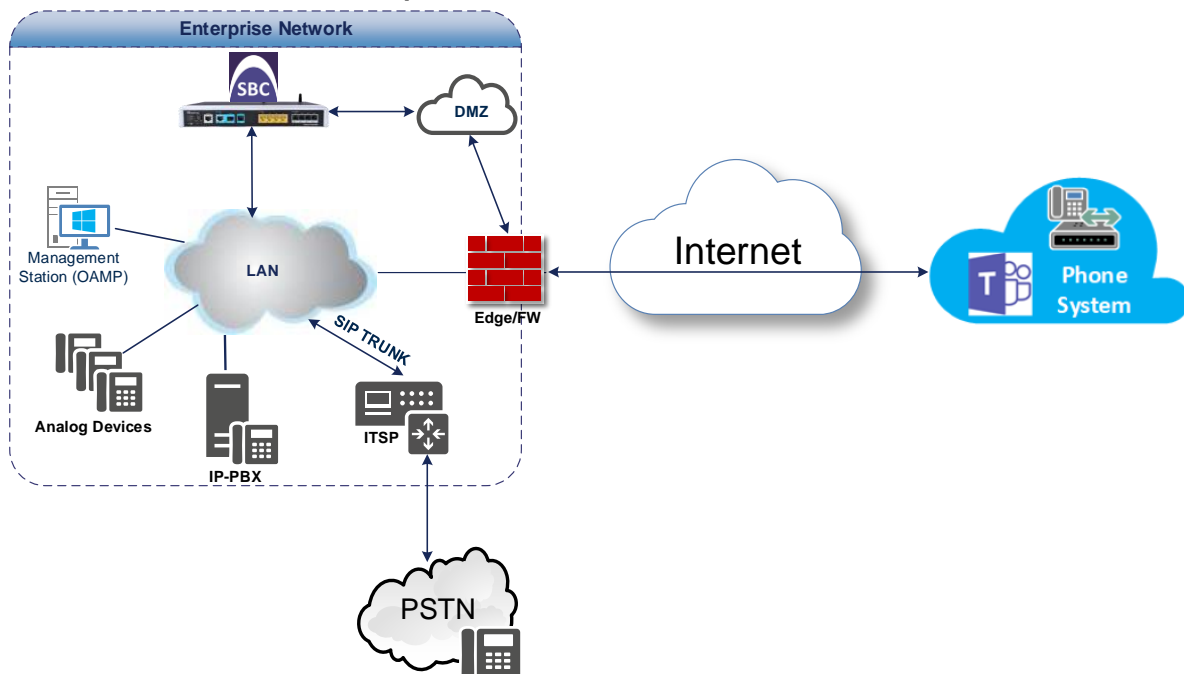
### 2.4.1 Enterprise Model Implementation

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

- Enterprise deployed with third-party IP-PBX, analog devices 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 Swisscom's SIP Trunking service
- AudioCodes SBC is implemented to interconnect between the 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 Swisscom's 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 Swisscom SIP Trunk**



## 2.4.2 Environment Setup

The interoperability test topology includes the following environment setup:

**Table 2-4: Environment Setup**

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

## 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 <i>Deploying Direct Routing Guide</i> . |
| SIP Trunks connected to the SBC                          |   |
| Office 365 Tenant  |   |
| Domains  |   |
| Public IP address for the SBC                            |   |
| Fully Qualified Domain Name (FQDN) for the SBC           |   |
| Public DNS entry for the SBC                             |   |
| Public trusted certificate for the SBC                   |   |
| Firewall ports for Direct Routing Signaling              |   |
| Firewall IP addresses and ports for Direct Routing Media |   |
| Media Transport Profile                                  |   |
| Firewall ports for Teams Clients Media                   |   |

#### 2.4.4 Known Limitations

The following limitations were observed during the interoperability tests done for the AudioCodes SBC interworking between Microsoft Teams Direct Routing and Swisscom 's SIP Trunk:

- As the Microsoft Teams client does not show the dialpad before the call is established (early-media scenario), it is not possible to send DTMF to interact with some IVR's.
- Calls with special arrangements will be billed on the trunk main number instead of the user number. This is because the SIP P-Asserted Identity header contains the same number as the SIP 'From' header. This limitation does not affect the completion of such calls.

## 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 Hosting 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

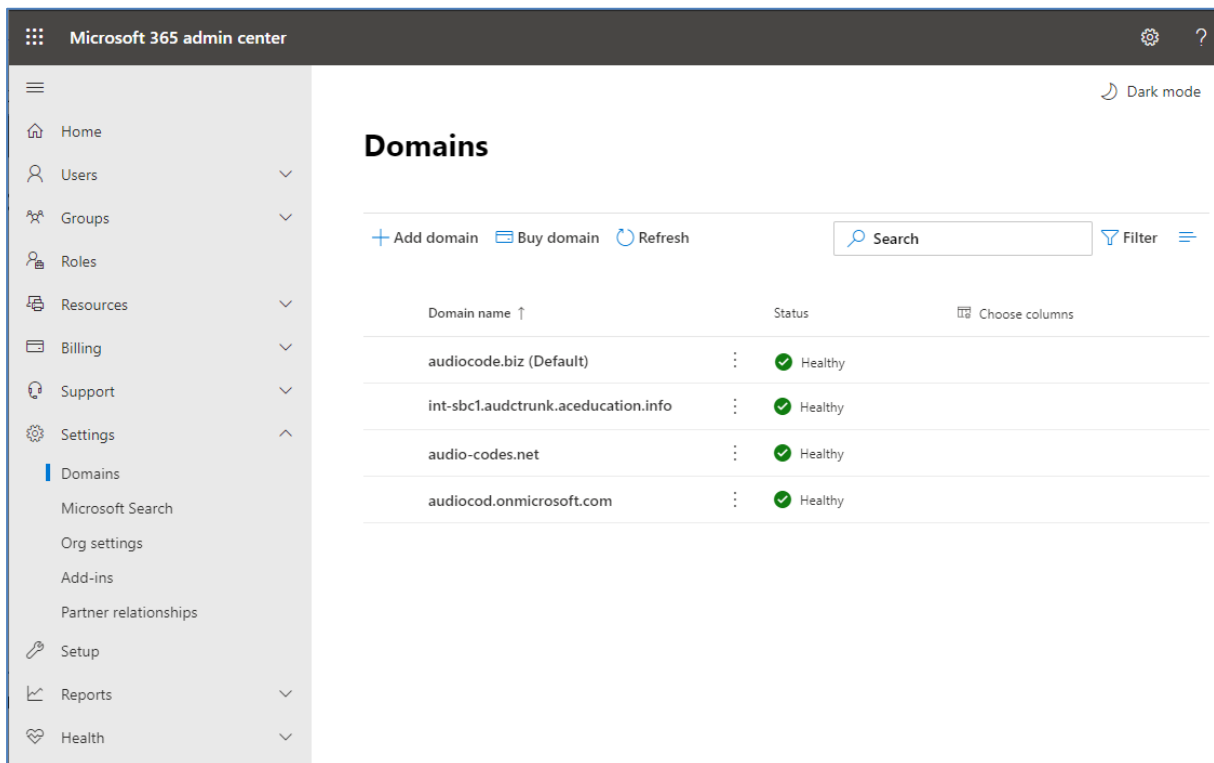
The SBC domain name must be from one of the names registered in 'Domains' of the tenant. You cannot use the **\*.onmicrosoft.com** tenant for the domain name. For example, in Figure 3-1, the administrator registered the following DNS names for the tenant:

**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                      | <b>Valid names:</b> <ul style="list-style-type: none"><li>▪ sbc.ACeducation.info</li><li>▪ ussbcs15.ACeducation.info</li><li>▪ europe.ACeducation.info</li></ul> <b>Invalid name:</b><br>sbc1.europe.ACeducation.info (requires registering domain name europe.atatum.biz in 'Domains' first)   |
| adatumbiz.onmicrosoft.com | No                       | Using <b>*.onmicrosoft.com</b> domains is not supported for SBC names   |
| hybridvoice.org           | Yes                      | <b>Valid names:</b> <ul style="list-style-type: none"><li>▪ sbc1.hybridvoice.org</li><li>▪ ussbcs15.hybridvoice.org</li><li>▪ europe.hybridvoice.org</li></ul> <b>Invalid name:</b><br>sbc1.europe.hybridvoice.org (requires registering domain name europe.hybridvoice.org in 'Domains' first) |

Users can be from any SIP domain registered for the tenant. For example, you can provide users [user@ACeducation.info](mailto: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**

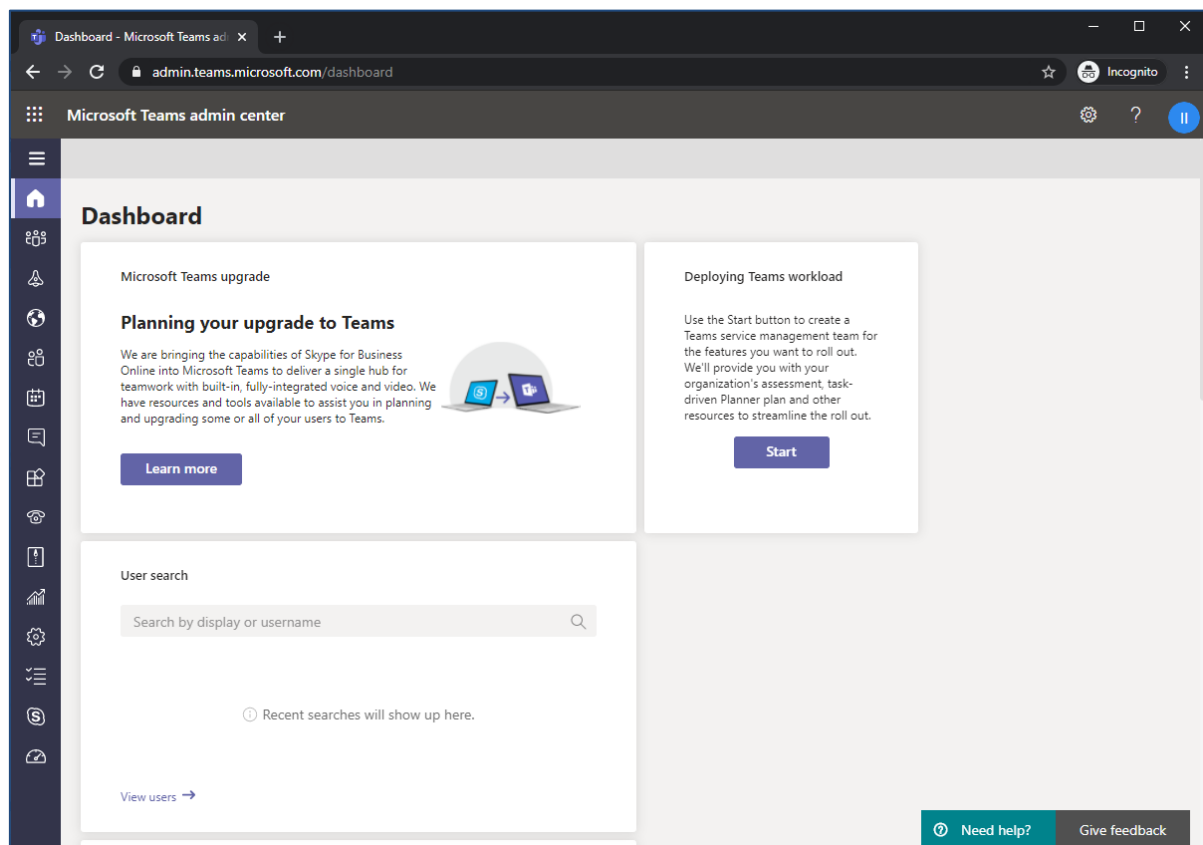


During creation of the Domain you will be forced to create public DNS record (**int-sbc1.audctrunk.aceducation.info** in our example.)

### 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



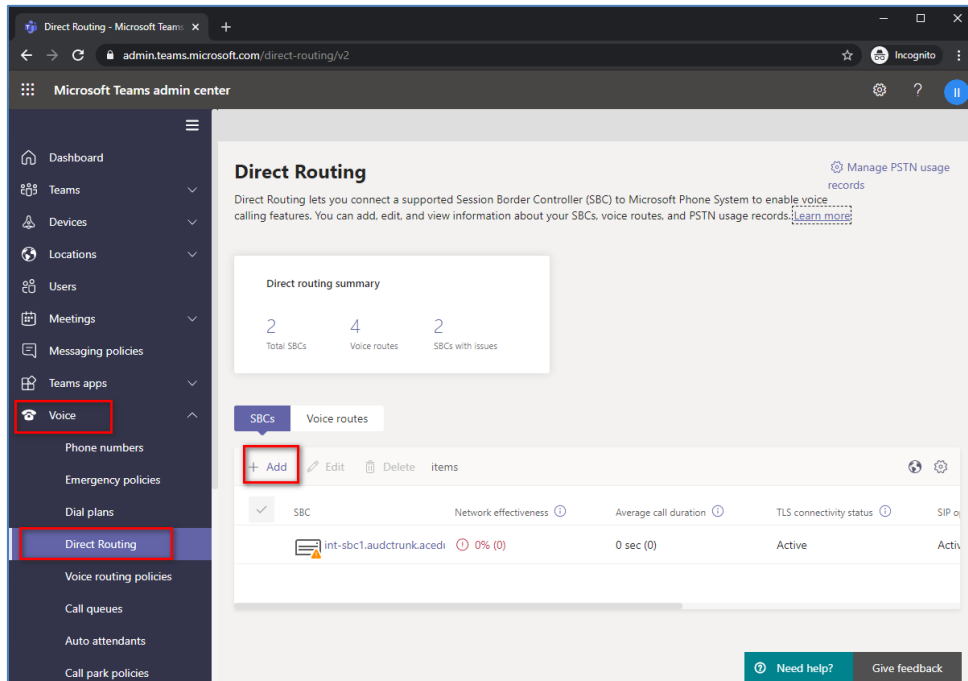
### 3.3.1 Add New SBC to Direct Routing

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

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

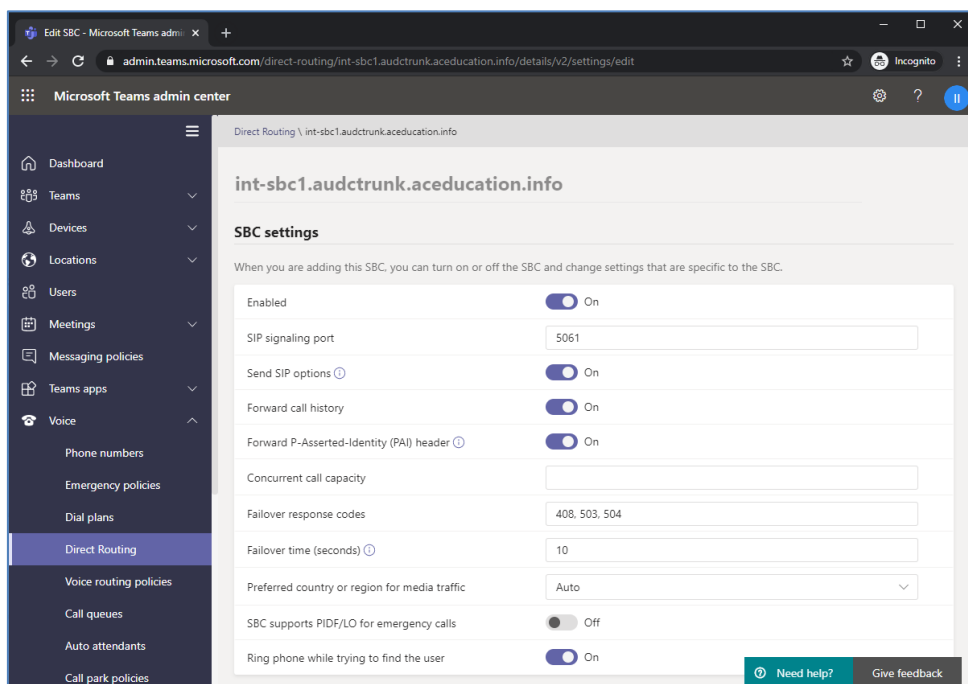
1. In the web interface, select **Voice**, and then click **Direct Routing**.
2. Under SBCs click **Add**.

**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 -SipSignalingPort 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**

**Direct Routing**

Direct Routing lets you connect a supported Session Border Controller (SBC) to Microsoft Phone System to enable voice calling features. You can add, edit, and view information about your SBCs, voice routes, and PSTN usage records. [Learn more](#)

**Direct routing summary**

|            |              |                  |
|------------|--------------|------------------|
| 2          | 4            | 2                |
| Total SBCs | Voice routes | SBCs with issues |

**Voice routes**

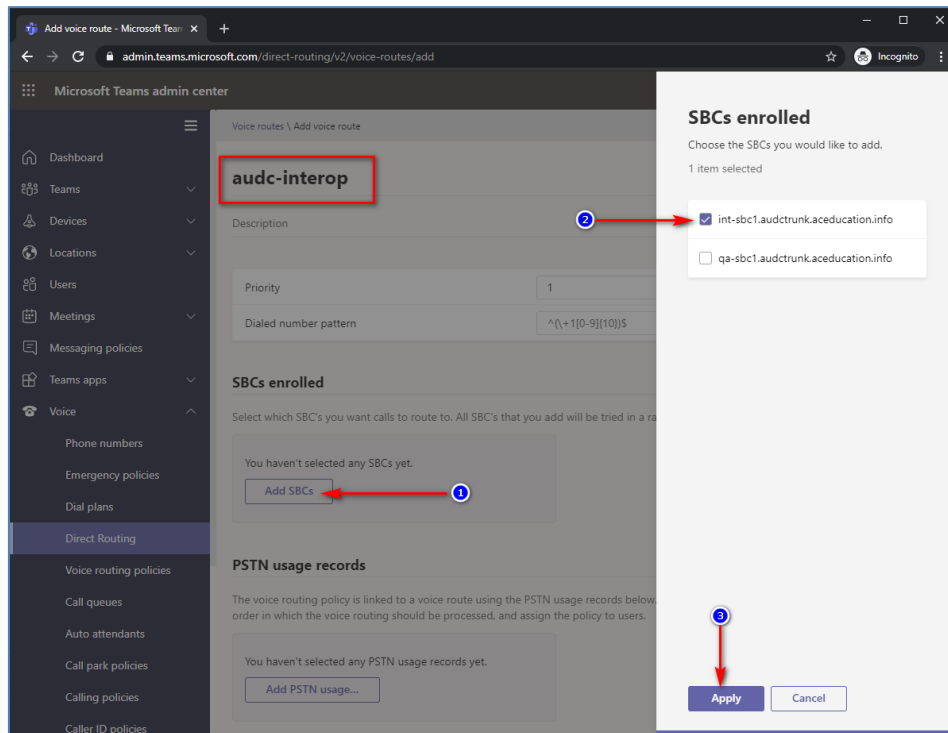
**+ Add** [Edit](#) [Move up](#) [Move down](#) [Delete](#) [Items](#)

| ✓ | Priority | Voice route   | Description  | Dialed number pattern | PSTN |
|---|----------|---------------|--------------|-----------------------|------|
|   | 1        | int-il        |              | ^\+                   | Inte |
|   | 2        | Israel        |              | ^\+972(\d{8})         | Isra |
|   | 3        | AC-SBCaaS-Any |              | \d+                   | SBC  |
|   | 4        | Test1         | Only Testing |                       |      |

[Need help?](#) [Give feedback](#)

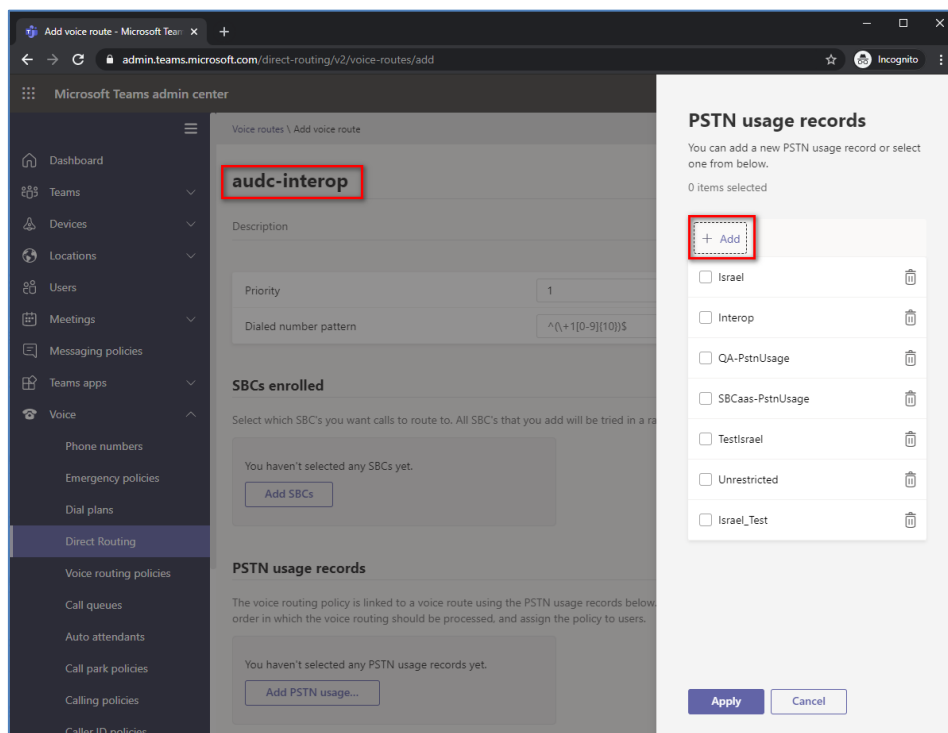
2. Create a new Voice Route and associate it with the SBC, configured in the previous step.

**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:

4. Creating an empty PSTN Usage:

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

5. 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"
```

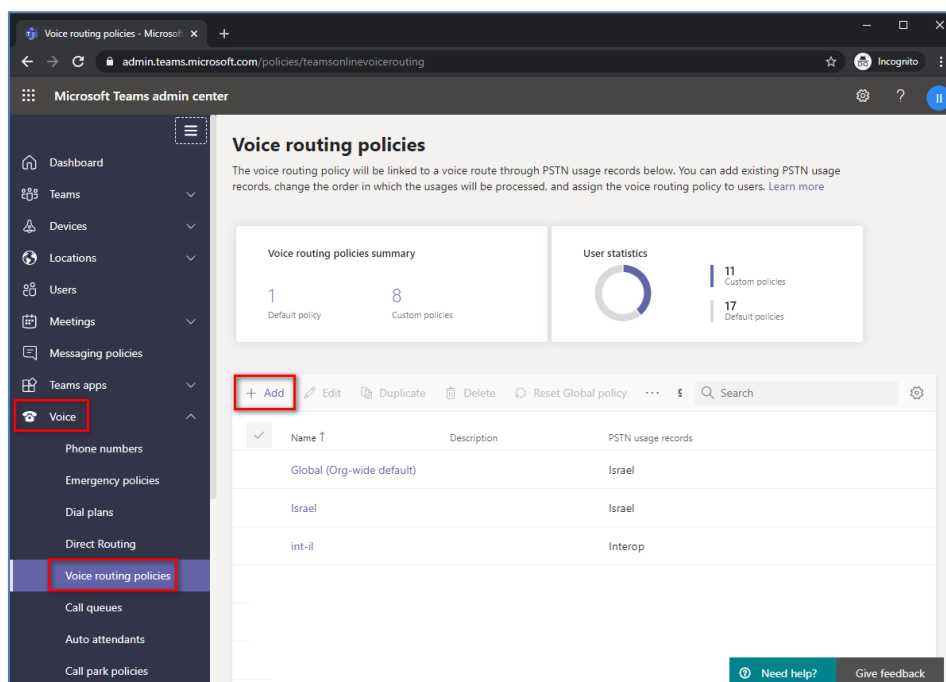
### 3.3.3 Add Voice Routing Policy

The procedure below describes how add a voice routing policy

- **To add voice routing policy:**

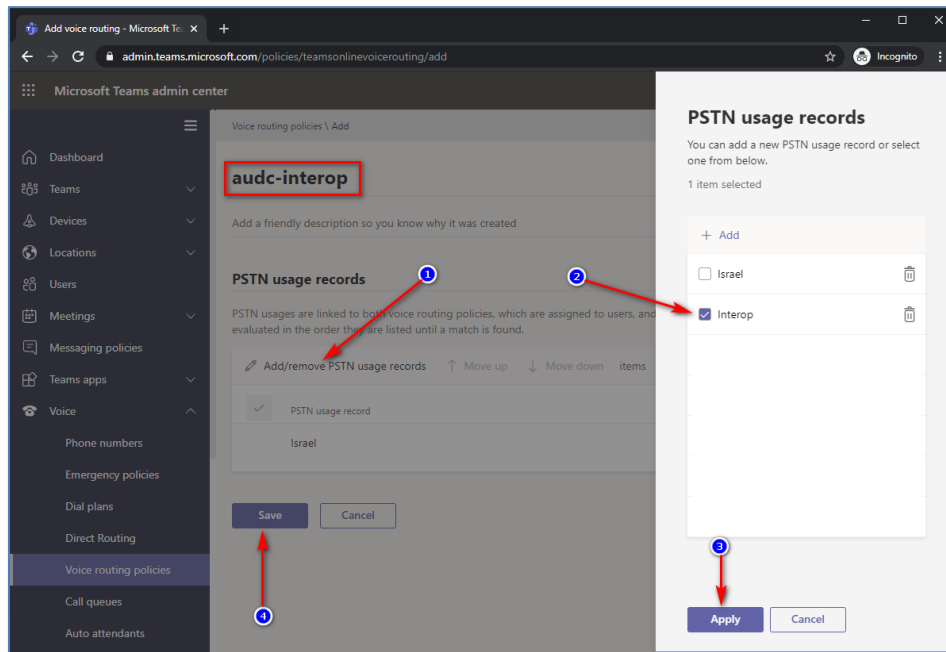
1. In the web interface, under **Voice**, select **Voice routing policies** and click **Add**.

**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 3.3.4 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 Routing Policy

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 Swisscom 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 - Swisscom SIP Trunking environment
- SBC WAN interface - 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 Swisscom 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.
- If your SBC is deployed in a virtual environment and transcoding is required, your virtual machine must have a minimum of two vCPUs. For more information, please refer to the appropriate *Installation Manual*, which can be found on AudioCodes website.
- 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**

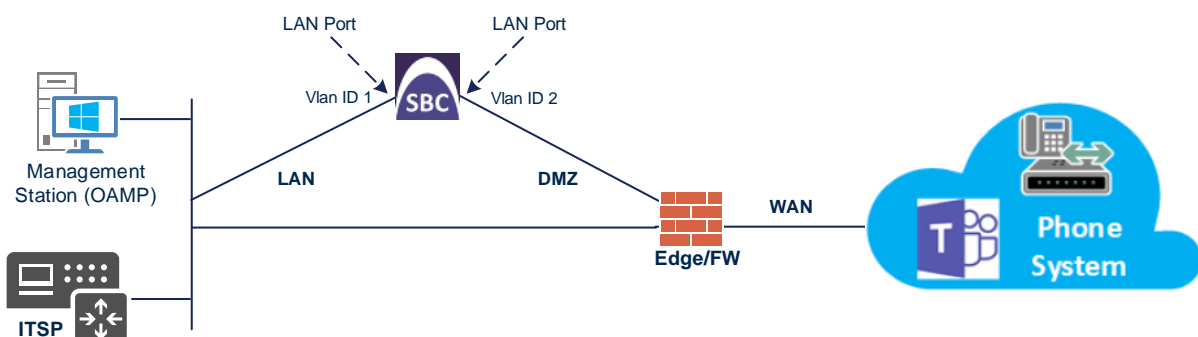


## 4.2 IP Network Interfaces Configuration

This step 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:
  - Teams Direct Routing, located on the WAN
  - Swisscom SIP Trunk, located on the LAN (or private VPN/MPLS connection to the Service Provider Network)
- 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 step 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 as follows:

**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 step describes how to configure the IP network interfaces for each of the following interfaces:

- LAN VoIP (assigned the name "LAN\_IF")
- WAN VoIP (assigned the name "WAN\_IF")

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

1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. 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                             | 10.15.27.1   | LAN_IF   | vlan 1          |
| 1     | Media + Control (as this interface points to the internet, enabling OAMP is not recommended) | IPv4 Manual    | 195.189.192.157 (DMZ IP address of SBC) | 25            | 195.189.192.129 (router's IP address) | According to your Internet provider's instructions | 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    | 10.15.17.77     | 16            | 10.15.0.1       | 10.15.27.1    | 0.0.0.0       | vlan 1          |
| 1     | WAN_IF | Media + Control  | IPv4 Manual    | 195.189.192.157 | 25            | 195.189.192.129 | 80.179.52.100 | 80.179.55.100 | vlan 2          |



## 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: int-sbc1.audctrunk.aceducation.info
- SAN: int-sbc1.audctrunk.aceducation.info

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 for Teams Direct Routing

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 version:**

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     |
| 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>.

**Figure 4-6: Configuring TLS Context for Teams Direct Routing**

3. Click **Apply**.

### 4.3.3 Configure a Certificate

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, 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 'Subject Name [CN]' field, enter the SBC FQDN name (based on example above, **int-sbc1.audctrunk.aceducation.info**).
  - b. In the '1<sup>st</sup> 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. Many CAs do not support private key of size 1024.
- d. To change the key size on TLS Context, go to: **Generate New Private Key**, change the 'Private Key Size' to the value required by your CA and then click **Generate Private-Key**. To use **2048** as a Private Key Size value, you can click **Generate Private-Key** without changing the default key size value.
- e. 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]

int-sbc1.audctrunk.aceducation.info

Organizational Unit [OU] (optional)

Company name [O] (optional)

Locality or city name [L] (optional)

State [ST] (optional)

Country code [C] (optional)

1st Subject Alternative Name [SAN]

DNS

int-sbc1.audctrunk.aceducation.info

2nd Subject Alternative Name [SAN]

EMAIL

3rd Subject Alternative Name [SAN]

EMAIL

4th Subject Alternative Name [SAN]

EMAIL

5th Subject Alternative Name [SAN]

EMAIL

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.

Generate Self-Signed Certificate

Create CSR

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

```

-----BEGIN CERTIFICATE REQUEST-----
MIICtDCCAzwCAQhwLjEsMCoGA1UEAwVjaH50LXN1YzEuYXVhY3Rydj5rLmFjZjZlR1
Y2F0aW9uLm1uZm8wggE1MA0GCgQGSiB3DQEBAAQAA4IBDwAwggEKAoIBAQQBAdaD
iQKgtqrj39RLJbY1RxtX9Zu80JUp9e1f1H3IeY6nY+kqFYSTIVFhm3SE5yU1sBd
J/p6EA6e0UaWLeZs1324VP+1nctA6a00Mz7uc+11p89ywnPk3+5rZlnXGZKKqpnF
P2Hw4h0px/dXX01VEwv+4Uf1St0072bZLppDIYDqZcxdT1r1zRqrP5mqATaTAI
zaFayjr80wB8nS10H6M09u+557e3J3UQxK+36rTRxU0o+qbdjiuHFP+dxrkzA5dBY
bIrmB27DA6RUXhwj1pw/sBSQn9FZuZpu3mZrth/EUCHEQ2tjJm96P/37mx358Fh
4CnrgXsu4HrXSQXAgHBAAGQTA/BgkqhkiG9w0BCQ4xHjAwHCAAGAUdEQQnMCJC
I21udC1zYmFuLmF1ZG00cnVuaYShY2VkdMlmd1vb15pbmZvMA0GCgQGSiB3DQEB
CwUAA4IBAQAjroPaX2yF/DSNjdrT+sZTEu2GkgeRNV3hzwDak3pLw0Hmw6upK9
UKv6E9/2GhniCmR200GkFvMReYL8xerjTdhRjctH1q/RP+1e3pm1N73xmD1sh/1WVx
shrw8G52jge18rQEBZIU70R48PW/xhCV3Te4ZYekDm33H0oG1Hy5Sud7WlyDUYHA
7x3wG1wFCMsF+CfAkW5vtAxVI6F9VOY1OGty71xMnMZG1McYP8P3U21S0yQoFyDC
jktQ8UEkDeHbyHg1H7S11A6g5fSHU1Y0AAKfhuvEoXUJ4kAMXcFnS7DASHTxFwulI
pRSjw21C08DHj1FZg0C+0oxC1Va8HOEJ
-----END CERTIFICATE REQUEST-----

```

GENERATE NEW PRIVATE KEY

Private Key Size

2048

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.

Generate Private-Key

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

Configuration Note

28

Document #: LTRT-12682

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, 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, 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, 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**

| <div>  TLS Context [#2] &gt; Trusted Root Certificates         </div> |                         |  |            |
|---|-------------------------|--|------------|
| <div>View</div>   |                         | <div> <div>Import</div> <div>Export</div> <div>Remove</div> </div> |            |
| 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 3<sup>rd</sup> 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 Trusted Root Certificate for MTLS Connection



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



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

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

0x033af1e6a711a9a0bb2864b11d09fae5, SHA-1 Thumbprint:

DF3C24F9BFD666761B268073FE06D1CC8D4F82A4 and SHA-256 Thumbprint:

CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F.

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



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

## 4.4 Configure Media Realms

This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➤ **To configure Media Realms:**

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

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

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

The configured Media Realms are shown in the figure below:

**Figure 4-11: Configured Media Realms in Media Realm Table**

| Media Realms (2)  |       |                     |                  |                              |                |                     |
|---|-------|---------------------|------------------|------------------------------|----------------|---------------------|
| <div> <span>+ New</span> <span>Edit</span> <span>🗑️</span> </div> <div> <span>⏪</span> <span>⏩</span> <span>Page 1 of 1</span> <span>Show 10 records per page</span> </div> |       |                     |                  |                              |                |                     |
| INDEX   | NAME  | IPv4 INTERFACE NAME | PORT RANGE START | NUMBER OF MEDIA SESSION LEGS | PORT RANGE END | DEFAULT MEDIA REALM |
| 0   | MRLan | LAN_IF              | 6000             | 100                          | 6999           | No                  |
| 1   | MRWan | WAN_IF              | 7000             | 100                          | 7999           | No                  |



## 4.5 Configure SIP Signaling Interfaces

This step describes how to configure SIP Interfaces. For the interoperability test topology, internal (towards the SIP Trunk) and external (towards the Teams Direct Routing Interface) SIP Interfaces must be configured for the SBC.

➤ **To configure SIP Interfaces:**

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



**Note:** The Direct Routing interface can only use TLS transport for a SIP. It does not support using TCP due to security reasons. The SIP port may 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 Interfaces 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 | TLS Context Name |
|-------|----------------------------------|-------------------|------------------|---|----------|--|----------------------------------|---|-------------|------------------|
| 0     | SwisscomESIP<br>(arbitrary name) | LAN_IF            | SBC              | 0   | 5060     | 0                                      | Disable<br>(leave default value) | 500 (leave default value)                 | MR Lan      | -                |
| 1     | Teams<br>(arbitrary name)        | WAN_IF            | SBC              | 0<br>(Phone System does not use UDP or TCP for SIP signaling) | 0        | 5061 (as configured in the Office 365) | Enable                           | 0<br>(Recommended to prevent DoS attacks) | MR Wan      | Teams            |

The configured SIP Interfaces are shown in the figure below:

**Figure 4-12: Configured SIP Interfaces in SIP Interface Table**

| SIP Interfaces (2)   |              |            |                   |                  |          |          |          |                        |             |
|--|--------------|------------|-------------------|------------------|----------|----------|----------|------------------------|-------------|
| <div> <span>+ New</span> <span>Edit</span> <span>🗑️</span> </div> <div> <span>⏪</span> <span>⏩</span> Page 1 of 1 <span>⏪</span> <span>⏩</span> Show 10 records per page <div>🔍</div> </div> |              |            |                   |                  |          |          |          |                        |             |
| INDEX  | NAME         | SRD        | NETWORK INTERFACE | APPLICATION TYPE | UDP PORT | TCP PORT | TLS PORT | ENCAPSULATION PROTOCOL | MEDIA REALM |
| 0  | SwisscomESIP | DefaultSRC | LAN_IF            | SBC              | 0        | 5060     | 0        | No encapsulation       | MR Lan      |
| 1  | Teams        | DefaultSRC | WAN_IF            | SBC              | 0        | 0        | 5061     | No encapsulation       | MR Wan      |

## 4.6 Configure Proxy Sets and Proxy Address

This step 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:

- Swisscom SIP Trunk
- Microsoft Teams Direct Routing

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

### 4.6.1 Configure a Proxy Sets

This section shows how to configure a Proxy Sets.

➤ 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 Keep-Alive Time [sec] | Proxy Hot Swap | Proxy Load Balancing Method |
|-------|-------------------------------|------------------------|------------------|------------------|-----------------------------|----------------|-----------------------------|
| 1     | SwisscomESIP (arbitrary name) | SwisscomESIP           | Default          | Using Options    | 10                          | -              | -                           |
| 2     | Teams (arbitrary name)        | Teams                  | Teams            | Using Options    | 60 (leave default value)    | Enable         | Random Weights              |

The configured Proxy Sets are shown in the figure below:

**Figure 4-13: Configured Proxy Sets in Proxy Sets Table**

| Proxy Sets (3)  |              |                 |                            |                        |                             |                 |                |
|---|--------------|-----------------|----------------------------|------------------------|-----------------------------|-----------------|----------------|
| <div> <span>+ New</span> <span>Edit</span> <span>🗑️</span> </div> <div> Page 1 of 1 Show 10 records per page </div> |              |                 |                            |                        |                             |                 |                |
| 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) | --                         | SwisscomESIP           | 60                          |                 | Disable        |
| 1   | SwisscomESIP | DefaultSRD (#0) | --                         | SwisscomESIP           | 10                          |                 | Disable        |
| 2   | Teams        | DefaultSRD (#0) | --                         | Teams                  | 60                          |                 | Enable         |

## 4.6.2 Configure a Proxy Address

This section shows how to configure a Proxy Address.

➤ **To configure a Proxy Address for the Swisscom SIP Trunk:**

1. Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets) and then click the Proxy Set **SwisscomESIP**, 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 4-14: Configuring Proxy Address for the Swisscom SIP Trunk**

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

**Table 4-6: Configuring Proxy Address for the Swisscom SIP Trunk**

| Index | Proxy Address                                     | Transport Type | Proxy Priority | Proxy Random Weight |
|-------|---|----------------|----------------|---------------------|
| 0     | 10.20.0.10:5060<br>(SIP Trunk IP / FQDN and port) | TCP            | 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 4-15: Configuring Proxy Address for Teams Direct Routing Interface**

The screenshot shows a 'Proxy Address' configuration window. It has a title bar with the text 'Proxy Address' and standard window controls. The main area is divided into a 'GENERAL' tab. Below the tab, there are five configuration fields, each with a label and a value field:

- Index:** 0
- Proxy Address:** sip.pstnhub.microsoft.com:5061
- Transport Type:** TLS (with a dropdown arrow)
- Proxy Priority:** 1
- Proxy Random Weight:** 1

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 step describes how to configure coders (termed *Coder Group*). As Teams Direct Routing supports the SILK and OPUS coders while the network connection to Swisscom 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 Teams Direct Routing and the Swisscom 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 Teams Direct Routing:

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

**Figure 4-16: Configuring Coder Group for 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.711A-law ▼     | 20 ▼               | 64 ▼                      | 8            | Disabled ▼          |                |  |
| G.711U-law ▼     | 20 ▼               | 64 ▼                      | 0            | Disabled ▼          |                |  |
| G.729 ▼          | 20 ▼               | 8 ▼                       | 18           | Disabled ▼          |                |  |
| ▼                | ▼                  | ▼                         |              | ▼                   |                |  |

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Swisscom 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 Swisscom SIP Trunk in the next step.

➤ **To set a preferred coder for the Swisscom 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 Swisscom SIP Trunk.

**Figure 4-17: Configuring Allowed Coders Group for Swisscom SIP Trunk**

The screenshot shows a configuration window titled "Allowed Audio Coders Groups [Swisscom-AllowedAudioCoders]". It has a "GENERAL" tab selected. Below the tab, there are two fields: "Index" with the value "0" and "Name" with the value "Swisscom-AllowedAudioCoders".

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:

| Parameter | Value              |
|-----------|--------------------|
| Index     | <b>0</b>           |
| Coder     | <b>G.711 A-law</b> |
| Index     | <b>1</b>           |
| Coder     | <b>G.729</b>       |
| Index     | <b>2</b>           |
| Coder     | <b>G.722</b>       |

**Figure 4-18: Configuring Allowed Coders for Swisscom SIP Trunk**

The screenshot shows a configuration window titled "Allowed Audio Coders". It has a "GENERAL" tab selected. Below the tab, there are three fields: "Index" with the value "0", "Coder" with a dropdown menu showing "G.711 A-law", and "User-defined Coder" which is empty.

- Open the Media Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Settings**).

**Figure 4-19: SBC Preferences Mode**

The screenshot displays the 'Media Settings' configuration page. It is divided into several sections: GENERAL, ROBUSTNESS, SBC SETTINGS, and GATEWAY SETTINGS. In the SBC SETTINGS section, the 'Preferences Mode' dropdown is set to 'Include Extensions', which is highlighted by a black arrow. Other settings include 'NAT Traversal' (Disable NAT), 'Enable Continuity Tones' (Disable), 'Inbound Media Latch Mode' (Dynamic), 'Number of Media Channels' (0), 'Enforce Media Order' (Disable), 'SDP Session Owner' (AudiocodesGW), 'New RTP Stream Packets' (3), 'New RTCP Stream Packets' (3), 'New SRTP Stream Packets' (3), 'New SRTCP Stream Packets' (3), 'Timeout To Relatch RTP (msec)' (200), 'Timeout To Relatch SRTP (msec)' (200), 'Timeout To Relatch Silence (msec)' (10000), 'Timeout To Relatch RTCP (msec)' (10000), 'Enable Early Media' (Disable), and 'Multiple Packetization Time Format' (None). At the bottom, there are 'Cancel' and 'APPLY' buttons.

| GENERAL                  |              | ROBUSTNESS                        |       |
|--------------------------|--------------|-----------------------------------|-------|
| NAT Traversal            | Disable NAT  | New RTP Stream Packets            | 3     |
| Enable Continuity Tones  | Disable      | New RTCP Stream Packets           | 3     |
| Inbound Media Latch Mode | Dynamic      | New SRTP Stream Packets           | 3     |
| Number of Media Channels | 0            | New SRTCP Stream Packets          | 3     |
| Enforce Media Order      | Disable      | Timeout To Relatch RTP (msec)     | 200   |
| SDP Session Owner        | AudiocodesGW | Timeout To Relatch SRTP (msec)    | 200   |
|                          |              | Timeout To Relatch Silence (msec) | 10000 |
|                          |              | Timeout To Relatch RTCP (msec)    | 10000 |

| SBC SETTINGS        |                      |
|---------------------|----------------------|
| Preferences Mode    | • Include Extensions |
| Enforce Media Order | Disable              |

| GATEWAY SETTINGS                   |         |
|------------------------------------|---------|
| Enable Early Media                 | Disable |
| Multiple Packetization Time Format | None    |

Cancel APPLY

- From the 'Preferences Mode' drop-down list, select **Include Extensions**.
- Click **Apply**.

## 4.8 Configure IP Profiles

This step 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 following IP entities:

- Swisscom SIP trunk – to operate in non-secure mode using RTP and SIP over TCP
- Microsoft Teams Direct Routing – to operate in secure mode using SRTP and SIP over TLS

### ➤ To configure an IP Profile for the Swisscom SIP Trunk:

1. Click **New**, and then configure the parameters as follows:

| Parameter                             | Value   |
|---------------------------------------|---|
| <b>General</b>                        |   |
| Index                                 | <b>1</b>  |
| Name                                  | <b>Swisscom</b>   |
| <b>Media Security</b>                 |   |
| SBC Media Security Mode               | <b>Not Secured</b>  |
| <b>SBC Early Media</b>                |   |
| Remote Early Media RTP Detection Mode | <b>By Media</b>   |
| <b>SBC Media</b>                      |   |
| Allowed Audio Coders                  | <b>Swisscom-AllowedAudioCoders</b>  |
| Allowed Coders Mode                   | <b>Restriction and Preference</b> (reorganize coders according to Allowed Coders list and restrict all other) |
| <b>SBC Signaling</b>                  |   |
| PRACK Mode                            | <b>Optional</b>   |
| <b>SBC Forward and Transfer</b>       |   |
| Remote REFER Mode                     | <b>Handle Locally</b>   |
| Remote Replaces Mode                  | <b>Handle Locally</b>   |
| Play RBT To Transferee                | <b>Yes</b>  |
| Remote 3xx Mode                       | <b>Handle Locally</b>   |
| <b>SBC Hold</b>                       |   |
| Remote Hold Format                    | <b>Send Only</b>  |
| <b>Media</b>                          |   |
| Broken Connection Mode                | <b>Ignore</b>   |



Figure 4-20: Configuring IP Profile for Swisscom SIP Trunk

2. Click **Apply**.

➤ **To configure IP Profile for the 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   |
|---------------------------------------|---|
| <b>General</b>                        |   |
| Index                                 | <b>2</b>  |
| Name                                  | <b>Teams</b> (arbitrary descriptive name)   |
| <b>Media Security</b>                 |   |
| SBC Media Security Mode               | <b>SRTP</b>   |
| <b>SBC Early Media</b>                |   |
| Remote Early Media RTP Detection Mode | <b>By Media</b> (required, as Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18x response) |
| <b>SBC Media</b>                      |   |
| Extension Coders Group                | <b>AudioCodersGroups_1</b>  |
| RTCP Mode                             | <b>Generate Always</b>  |
| ICE Mode                              | <b>Lite</b> (required only when Media Bypass enabled on Teams)  |
| <b>SBC Signaling</b>                  |   |
| SIP UPDATE Support                    | <b>Not Supported</b>  |
| Remote re-INVITE Support              | <b>Supported Only With SDP</b>  |
| Remote Delayed Offer Support          | <b>Not Supported</b>  |

| 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 4-21: Configuring IP Profile for Teams Direct Routing

IP Profiles [Teams]

| GENERAL                                 | SBC SIGNALING   |
|---|---|
| Index: 1                                | PRACK Mode: Transparent                                 |
| Name: Teams                             | P-Asserted-Identity Header Mode: As Is                  |
| Created by Routing Server: No           | Diversion Header Mode: As Is                            |
| Used By Routing Server: Not Used        | History-Info Header Mode: As Is                         |
|   | Session Expires Mode: Transparent                       |
| MEDIA SECURITY                          | SIP UPDATE Support: Not Supported                       |
| SBC Media Security Mode: Secured        | Remote re-INVITE: Supported only with SDP               |
| Gateway Media Security Mode: Preferable | Remote Delayed Offer Support: Not Supported             |
| Symmetric MKI: Disable                  | MSRP re-INVITE/UPDATE: Supported                        |
| MKI Size: 0                             | MSRP Offer Setup Role: ActPass                          |
| SBC Enforce MKI Size: Don't enforce     | MSRP Empty Message Format: Default                      |
| SBC Media Security Method: SDES         | Remote Representation Mode: According to Operation Mode |
| <p>Cancel <b>APPLY</b></p>              |   |

3. Click **Apply**.

## 4.9 Configure IP Groups

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

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

- Swisscom 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 Swisscom SIP Trunk:

| Parameter                                | Value  |
|--|--|
| Index                                    | <b>1</b>                                     |
| Name                                     | <b>SwisscomESIP</b>                          |
| Type                                     | <b>Server</b>                                |
| Proxy Set                                | <b>SwisscomESIP</b>                          |
| IP Profile                               | <b>Swisscom</b>                              |
| Media Realm                              | <b>MRLan</b>                                 |
| SIP Group Name                           | <b>10.20.0.10</b> (according to requirement) |
| Proxy Keep-Alive using IP Group settings | <b>Enable</b>                                |

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

| Parameter                                | Value   |
|--|---|
| Index                                    | <b>2</b>  |
| Name                                     | <b>Teams</b>  |
| Topology Location                        | <b>Up</b>   |
| Type                                     | <b>Server</b>   |
| Proxy Set                                | <b>Teams</b>  |
| IP Profile                               | <b>Teams</b>  |
| Media Realm                              | <b>MRWan</b>  |
| SIP Group Name                           | <b>teams-sbc.your.domain.com</b> (according to requirement)               |
| Classify By Proxy Set                    | <b>Disable</b>  |
| Local Host Name                          | <b>teams-sbc.your.domain.com</b><br>(FQDN name of your tenant in the SBC) |
| Always Use Src Address                   | <b>Yes</b>  |
| Proxy Keep-Alive using IP Group settings | <b>Enable</b>   |

The configured IP Groups are shown in the figure below:

**Figure 4-22: Configured IP Groups in IP Group Table**

| IP Groups (3) |              |            |        |                    |              |                          |             |                  |                       |                                  |                                   |
|---------------|--------------|------------|--------|--------------------|--------------|--------------------------|-------------|------------------|-----------------------|----------------------------------|-----------------------------------|
| + New Edit    |              |            |        | Page 1 of 1        |              | Show 10 records per page |             |                  |                       |                                  |                                   |
| INDEX         | NAME         | SRD        | TYPE   | SBC OPERATION MODE | PROXY SET    | IP PROFILE               | MEDIA REALM | SIP GROUP NAME   | CLASSIFY BY PROXY SET | INBOUND MESSAGE MANIPULATION SET | OUTBOUND MESSAGE MANIPULATION SET |
| 0             | Default_IPG  | DefaultSRD | Server | Not Configured     | ProxySet_0   | --                       | --          |                  | Disable               | -1                               | -1                                |
| 1             | SwisscomESIP | DefaultSRD | Server | Not Configured     | SwisscomESIP | Swisscom                 | MR-SIPTrunk | 10.20.0.10       | Enable                | -1                               | 4                                 |
| 2             | Teams        | DefaultSRD | Server | Not Configured     | Teams        | Teams                    | MR-Teams    | teams-sbc.your.c | Disable               | -1                               | -1                                |

## 4.10 Configure SRTP

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

➤ **To configure media security:**

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

**Figure 4-23: 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

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

## 4.11 Configuring Message Condition Rules

This step 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. Following Condition verifies that the Contact header contains Teams FQDN.

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

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

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

**Figure 4-24: Configuring Condition Table**

The screenshot shows a web interface window titled "Message Conditions [Teams-Contact]". Inside, there is a "GENERAL" tab. The configuration fields are as follows:

- Index:** A text input field containing the value "0".
- Name:** A text input field containing the value "Teams-Contact".
- Condition:** A text input field containing the value "header.contact.url.host contains 'pstnhub.micro:". To the right of this field is a blue link labeled "Editor".

3. Click **Apply**.

## 4.12 Configuring Classification Rules

This step 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:

| Parameter            | Value                     |
|----------------------|---------------------------|
| Index                | 0                         |
| Name                 | Teams                     |
| Source SIP Interface | Teams                     |
| Source IP Address    | 52.*.*                    |
| Destination Host     | teams-sbc.your.domain.com |
| Message Condition    | Teams-Contact             |
| Action Type          | Allow                     |
| Source IP Group      | Teams                     |

Figure 4-25: Configuring Classification Rule

The screenshot shows the 'Classification [Teams]' configuration window. At the top, there is a dropdown for 'SRD' set to '#0 [DefaultSRD]'. Below this, the window is divided into two main sections: 'MATCH' and 'ACTION'.

**MATCH Section:**

- Index: 0
- Name: Teams
- Source SIP Interface: #0 [Teams] (with a 'View' link)
- Source IP Address: 52.\*.\* (with a bullet point)
- Source Transport Type: Any (dropdown)
- Source Port: 0
- Source Username Pattern: \*
- Source Host: \*
- Destination Username Pattern: \*
- Destination Host: teams-sbc.your.domain.com (with a bullet point)

**ACTION Section:**

- Action Type: Allow (dropdown)
- Destination Routing Policy: -- (dropdown, with a 'View' link)
- IP Group Selection: Source IP Group (dropdown)
- Source IP Group: #0 [Teams] (with a bullet point and a 'View' link)
- IP Group Tag Name: default
- IP Profile: -- (dropdown, with a 'View' link')

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

3. Click **Apply**.

## 4.13 Configure IP-to-IP Call Routing Rules

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups (as configured in Section 4.9 on page 43) to denote the source and destination of the call.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Teams Direct Routing (WAN) and Swisscom SIP Trunk (LAN):

- 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 Swisscom SIP Trunk
- Calls from Swisscom 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 4-8: Configuration IP-to-IP Routing Rules**

| Index | Name                                | Source IP Group | Request Type | Call Trigger | 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-SwisscomESIP (arbitrary name) | Teams           |              |              |                  | IP Group    | Swisscom ESIP |                          |
| 3     | SwisscomESIP-Teams (arbitrary name) | Swisscom ESIP   |              |              |                  | 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**

| IP-to-IP Routing (4)  |                 |                |                           |                 |              |                         |                              |                  |                      |                           |                     |
|---|-----------------|----------------|---------------------------|-----------------|--------------|-------------------------|------------------------------|------------------|----------------------|---------------------------|---------------------|
| <div> <span>+ New</span> <span>Edit</span> <span>Insert</span> </div> <div> <span>Page 1 of 1</span> <span>Show 10 records per page</span> </div> |                 |                |                           |                 |              |                         |                              |                  |                      |                           |                     |
| INDEX   | NAME            | ROUTING POLICY | ALTERNATIVE ROUTE OPTIONS | SOURCE IP GROUP | REQUEST TYPE | SOURCE USERNAME PATTERN | DESTINATION USERNAME PATTERN | DESTINATION TYPE | DESTINATION IP GROUP | DESTINATION SIP INTERFACE | DESTINATION ADDRESS |
| 0   | Terminate OPTI  | Default_SBCRou | Route Row                 | Any             | OPTIONS      | *                       | *                            | Dest Address     | --                   | --                        | internal            |
| 1   | Refer Teams     | Default_SBCRou | Route Row                 | Any             | All          | *                       | *                            | Request URI      | Teams                | --                        |                     |
| 2   | Teams-Swisscom  | Default_SBCRou | Route Row                 | Teams           | All          | *                       | *                            | IP Group         | SwisscomESIP         | --                        |                     |
| 3   | SwisscomESIP-Ti | Default_SBCRou | Route Row                 | SwisscomESIP    | All          | *                       | *                            | IP Group         | Teams                | --                        |                     |



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

## 4.14 Configure Number Manipulation Rules

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 4.9 on page 43) to denote the source and destination of the call.



**Note:** Adapt the manipulation table according to your environment dial plan.

For example, for this interoperability test topology, manipulations are configured to add the “+41” prefix for emergency calls.

➤ **To configure a number manipulation rule:**

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

| Parameter                   | Value                               |
|-----------------------------|-------------------------------------|
| Index                       | <b>0</b>                            |
| Name                        | <b>add prefix emergency 3/4 dig</b> |
| Source IP Group             | <b>Teams</b>                        |
| Destination IP Group        | <b>SwisscomESIP</b>                 |
| Destination Username Prefix | <b>[1xx 1xxx]#</b>                  |
| Manipulated Item            | <b>Destination URI</b>              |
| Prefix to Add               | <b>+41</b>                          |

3. Click **Apply**.
4. Configure another manipulation rule as follows:

| Parameter                   | Value                                      |
|-----------------------------|--|
| Index                       | <b>1</b>                                   |
| Name                        | <b>add prefix emergency 3/4 dig with +</b> |
| Source IP Group             | <b>Teams</b>                               |
| Destination IP Group        | <b>SwisscomESIP</b>                        |
| Destination Username Prefix | <b>[+1xx +1xxx]#</b>                       |
| Manipulated Item            | <b>Destination URI</b>                     |
| Remove From Left            | <b>1</b>                                   |
| Prefix to Add               | <b>+41</b>                                 |

5. Click **Apply**.



The figure below shows an example of configured IP-to-IP outbound manipulation rules:

**Figure 4-27: Configured IP-to-IP Outbound Manipulation Rules**

| Outbound Manipulations (2) |               |                |                         |                 |                      |                         |                              |                 |                          |                   |                  |               |               |
|----------------------------|---------------|----------------|-------------------------|-----------------|----------------------|-------------------------|------------------------------|-----------------|--------------------------|-------------------|------------------|---------------|---------------|
| + New                      |               | Edit           | Insert                  | ↑               | ↓                    | 🗑️                      | Page 1 of 1                  |                 | Show 10 records per page |                   |                  |               |               |
| INDEX                      | NAME          | ROUTING POLICY | ADDITIONAL MANIPULATION | SOURCE IP GROUP | DESTINATION IP GROUP | SOURCE USERNAME PATTERN | DESTINATION USERNAME PATTERN | MANIPULATE ITEM | REMOVE FROM LEFT         | REMOVE FROM RIGHT | LEAVE FROM RIGHT | PREFIX TO ADD | SUFFIX TO ADD |
| 0                          | add prefix em | Default_SBCR   | No                      | Teams           | SwisscomESIF         | *                       | [1xx 1xxx]#                  | Destination U   | 0                        | 0                 | 255              | +41           |               |
| 1                          | add prefix em | Default_SBCR   | No                      | Teams           | SwisscomESIF         | *                       | [+1xx +1xxx]#                | Destination U   | 1                        | 0                 | 255              | +41           |               |

| Rule Index | Description  |
|------------|--|
| 0          | Calls with the prefix destination number "1xx" or "1xxx", add prefix "+41" to the destination number.                  |
| 1          | Calls with the prefix destination number "+1xx" or "+1xxx", remove "+" and add prefix "+41" to the destination number. |

## 4.15 Configure Message Manipulation Rules

This step 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 4) for Swisscom the SIP Trunk. This rule applies to messages sent to the Swisscom SIP Trunk IP Group in a Call Transfer scenario. This rule replaces the host part of the SIP Referred-By header with the value taken from the 'Group Name' field of the Swisscom SIP Trunk IP Group.

| Parameter           | Value                       |
|---------------------|-----------------------------|
| Index               | 0                           |
| Name                | Call Transfer               |
| 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 4-28: Configuring SIP Message Manipulation Rule 0 (for Swisscom SIP Trunk)**

The screenshot shows the 'Message Manipulations' configuration window for a rule named 'Call Transfer'. The window is divided into three main sections: GENERAL, ACTION, and MATCH. In the GENERAL section, the Index is 0, Name is 'Call Transfer', Manipulation Set ID is 4, and Row Role is 'Use Current Condition'. The ACTION section shows the Action Subject as 'header.referred-by.url.host', Action Type as 'Modify', and Action Value as 'param.ipg.dst.host'. The MATCH section shows the Message Type as 'invite.request' and the Condition as 'header.referred-by exists'. At the bottom, there are 'Cancel' and 'APPLY' buttons.

| GENERAL             |                       | ACTION         |                             |
|---------------------|-----------------------|----------------|-----------------------------|
| Index               | 0                     | Action Subject | header.referred-by.url.host |
| Name                | Call Transfer         | Action Type    | Modify                      |
| Manipulation Set ID | 4                     | Action Value   | param.ipg.dst.host          |
| Row Role            | Use Current Condition |                |                             |

| MATCH        |                           |
|--------------|---------------------------|
| Message Type | invite.request            |
| Condition    | header.referred-by exists |

Cancel APPLY

3. If the manipulation rule Index 0 (above) is executed, then the following rule is also executed. It adds the SIP Diversion header with values from the SIP Referred-by header.

| Parameter           | Value                  |
|---------------------|------------------------|
| Index               | 1                      |
| Name                | Call Transfer          |
| Manipulation Set ID | 4                      |
| Row Role            | Use Previous Condition |
| Message Type        |                        |
| Condition           |                        |
| Action Subject      | header.diversion       |
| Action Type         | Add                    |
| Action Value        | header.referred-by     |

Figure 4-29: Configuring SIP Message Manipulation Rule 1 (for Swisscom SIP Trunk)

Message Manipulations [Call Transfer]

GENERAL

Index 
Name 
Manipulation Set ID 
Row Role

ACTION

Action Subject  [Editor](#)
Action Type 
Action Value  [Editor](#)

MATCH

Message Type  [Editor](#)
Condition  [Editor](#)

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

4. If the manipulation rule Index 1 (above) is executed, then the following rule is also executed. It removes the SIP Referred-by header.

| Parameter           | Value                  |
|---------------------|------------------------|
| Index               | 2                      |
| Name                | Call Transfer          |
| Manipulation Set ID | 4                      |
| Row Role            | Use Previous Condition |
| Message Type        |                        |
| Condition           |                        |
| Action Subject      | header.referred-by     |
| Action Type         | Remove                 |
| Action Value        |                        |

Figure 4-30: Configuring SIP Message Manipulation Rule 2 (for Swisscom SIP Trunk)

Message Manipulations [Call Transfer]

GENERAL

Index 
Name • 
Manipulation Set ID • 
Row Role •

ACTION

Action Subject • 
Action Type • 
Action Value

MATCH

Message Type 
Condition

Cancel

APPLY

5. Configure another manipulation rule (Manipulation Set 4) for the Swisscom SIP Trunk. This rule applies to messages sent to the Swisscom SIP Trunk IP Group in a call forward scenario. This rule adds the SIP Diversion header with the value from the SIP History-Info Header.

| Parameter           | Value                                  |
|---------------------|--|
| Index               | <b>3</b>                               |
| Name                | <b>Call Forward</b>                    |
| Manipulation Set ID | <b>4</b>                               |
| Message Type        | <b>any</b>                             |
| Condition           | <b>Header.History-Info exists</b>      |
| Action Subject      | <b>Header.Diversion</b>                |
| Action Type         | <b>Add</b>                             |
| Action Value        | <b>Header.History-Info.HistoryInfo</b> |

**Figure 4-31: Configuring SIP Message Manipulation Rule 3 (for Swisscom SIP Trunk)**

Message Manipulations [Call Forward]

GENERAL

Index 
Name 
Manipulation Set ID 
Row Role

ACTION

Action Subject  Editor
Action Type 
Action Value  Editor

MATCH

Message Type  Editor
Condition  Editor

Cancel

6. If the manipulation rule Index 3 (above) is executed, then the following rule is also executed. It normalizes the SIP Diversion header.

| Parameter           | Value                  |
|---------------------|------------------------|
| Index               | 4                      |
| Name                | Call Forward           |
| Manipulation Set ID | 4                      |
| Row Role            | Use Previous Condition |
| Message Type        |                        |
| Condition           |                        |
| Action Subject      | Header.Diversion       |
| Action Type         | Normalize              |
| Action Value        |                        |

Figure 4-32: Configuring SIP Message Manipulation Rule 4 (for Swisscom SIP Trunk)

Message Manipulations [Call Forward]

GENERAL

Index 
Name 
Manipulation Set ID 
Row Role

ACTION

Action Subject  [Editor](#)
Action Type 
Action Value  [Editor](#)

MATCH

Message Type  [Editor](#)
Condition  [Editor](#)

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

7. If the manipulation rule Index 3 (above) is executed, then the following rule is also executed. It removes the SIP History-Info header.

| Parameter           | Value                         |
|---------------------|-------------------------------|
| Index               | <b>5</b>                      |
| Name                | <b>Call Forward</b>           |
| Manipulation Set ID | <b>4</b>                      |
| Row Role            | <b>Use Previous Condition</b> |
| Message Type        |                               |
| Condition           |                               |
| Action Subject      | <b>Header.History-Info</b>    |
| Action Type         | <b>Remove</b>                 |
| Action Value        |                               |

**Figure 4-33: Configuring SIP Message Manipulation Rule 5 (for Swisscom SIP Trunk)**

Message Manipulations [Call Forward]

GENERAL

Index 
Name 
Manipulation Set ID 
Row Role

ACTION

Action Subject  [Editor](#)
Action Type 
Action Value  [Editor](#)

MATCH

Message Type  [Editor](#)
Condition  [Editor](#)

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

8. Configure another manipulation rule (Manipulation Set 4) for the Swisscom SIP Trunk. This rule applies to messages sent to the Swisscom SIP Trunk IP Group. This rule replaces the host part of the SIP Diversion header with the value that was configured in the Swisscom SIP Trunk IP Group as Group Name.

| Parameter           | Value                     |
|---------------------|---------------------------|
| Index               | 6                         |
| Name                | Change Diversion Host     |
| Manipulation Set ID | 4                         |
| Message Type        | invite.request            |
| Condition           | header.diversion exists   |
| Action Subject      | header.diversion.url.host |
| Action Type         | Modify                    |
| Action Value        | param.ipg.dst.host        |

Figure 4-34: Configuring SIP Message Manipulation Rule 6 (for Swisscom SIP Trunk)

Message Manipulations [Change Diversion Host]

GENERAL

Index 
Name 
Manipulation Set ID 
Row Role

ACTION

Action Subject  Editor
Action Type 
Action Value  Editor

MATCH

Message Type  Editor
Condition  Editor

Cancel

APPLY



9. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to response messages sent to the Swisscom SIP Trunk IP Group. Sometimes Swisscom SIP Trunk send two media streams in the SIP INVITE message – m=audio (for audio stream) and m=image (for T.38 fax stream). In the response message, when only audio call is answered, AudioCodes SBC send 'm=image 0' and 'a=inactive' to clarify that T.38 fax will not be used. But the Swisscom SIP Trunk requests to remove 'a=inactive' and leave only 'm=image 0'.

| Parameter           | Value  |
|---------------------|--|
| Index               | 7  |
| Name                | Remove 'a=inactive'                                |
| Manipulation Set ID | 4  |
| Message Type        | any.response                                       |
| Condition           | body.sdp regex (.*)(m=image 0)(.*)(a=inactive)(.*) |
| Action Subject      | body.sdp   |
| Action Type         | Modify   |
| Action Value        | \$1+\$2+\$3+\$5                                    |

**Figure 4-35: Configuring SIP Message Manipulation Rule 7 (for Swisscom SIP Trunk)**

Message Manipulations [Remove 'a=inactive']

| GENERAL                         | ACTION   |
|---------------------------------|--|
| Index: 7                        | Action Subject: body.sdp <a href="#">Editor</a>      |
| Name: Remove 'a=inactive'       | Action Type: Modify                                  |
| Manipulation Set ID: 4          | Action Value: \$1+\$2+\$3+\$5 <a href="#">Editor</a> |
| Row Role: Use Current Condition |  |

| MATCH  |
|--|
| Message Type: any.response <a href="#">Editor</a>                                    |
| Condition: body.sdp regex (.*)(m=image 0)(.*)(a=inactive)(.*) <a href="#">Editor</a> |

Cancel [APPLY](#)

10. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to response messages sent to the Swisscom SIP Trunk IP Group for Call Forward of Anonymous Call initiated by the Microsoft Teams IP Group. This removes the user=phone variable from the SIP 'From' header.

| Parameter           | Value                                |
|---------------------|--------------------------------------|
| Index               | 8                                    |
| Name                | For Forward Anonymous                |
| Manipulation Set ID | 4                                    |
| Message Type        | any.request                          |
| Condition           | header.from.url contains 'anonymous' |
| Action Subject      | header.from.url.userphone            |
| Action Type         | Remove                               |
| Action Value        |                                      |

Figure 4-36: Configuring SIP Message Manipulation Rule 8 (for Swisscom SIP Trunk)

Message Manipulations [For Forward Anonymous]

GENERAL

Index 
Name 
Manipulation Set ID 
Row Role

ACTION

Action Subject  Editor
Action Type 
Action Value  Editor

MATCH

Message Type  Editor
Condition  Editor

Cancel

APPLY

11. If the manipulation rule Index 8 (above) is executed, then the following rule is also executed. This adds the SIP Privacy header with a value of 'id'.

| Parameter           | Value                         |
|---------------------|-------------------------------|
| Index               | <b>9</b>                      |
| Name                | <b>For Forward Anonymous</b>  |
| Manipulation Set ID | <b>4</b>                      |
| Row Role            | <b>Use Previous Condition</b> |
| Message Type        |                               |
| Condition           |                               |
| Action Subject      | <b>header.privacy</b>         |
| Action Type         | <b>Add</b>                    |
| Action Value        | <b>'id'</b>                   |

**Figure 4-37: Configuring SIP Message Manipulation Rule 9 (for Swisscom SIP Trunk)**

Message Manipulations [For Forward Anonymous]

GENERAL

Index 
Name 
Manipulation Set ID 
Row Role

ACTION

Action Subject  [Editor](#)
Action Type 
Action Value  [Editor](#)

MATCH

Message Type  [Editor](#)
Condition  [Editor](#)

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

12. If the manipulation rule Index 8 (above) is executed, then the following rule is also executed. This rule replaces the user part of the SIP P-Asserted-Identity header with the value from the SIP Diversion header.

| Parameter           | Value                                      |
|---------------------|--|
| Index               | <b>10</b>                                  |
| Name                | <b>For Forward Anonymous</b>               |
| Manipulation Set ID | <b>4</b>                                   |
| Row Role            | <b>Use Previous Condition</b>              |
| Message Type        |  |
| Condition           |  |
| Action Subject      | <b>header.p-asserted-identity.url.user</b> |
| Action Type         | <b>Modify</b>                              |
| Action Value        | <b>header.diversion.url.user</b>           |

Figure 4-38: Configuring SIP Message Manipulation Rule 10 (for Swisscom SIP Trunk)

Message Manipulations [For Forward Anonymous]

GENERAL

Index 
Name 
Manipulation Set ID 
Row Role

ACTION

Action Subject  Editor
Action Type 
Action Value  Editor

MATCH

Message Type  Editor
Condition  Editor

Cancel

13. If the manipulation rule Index 8 (above) is executed, then the following rule is also executed. This rule replaces the user part of the SIP P-Asserted-Identity header with the value from the SIP Diversion header.

| Parameter           | Value                  |
|---------------------|------------------------|
| Index               | 11                     |
| Name                | For Forward Anonymous  |
| Manipulation Set ID | 4                      |
| Row Role            | Use Previous Condition |
| Message Type        |                        |
| Condition           |                        |
| Action Subject      | header.from.url.host   |
| Action Type         | Modify                 |
| Action Value        | 'anonymous.invalid'    |

Figure 4-39: Configuring SIP Message Manipulation Rule 11 (for Swisscom SIP Trunk)

Message Manipulations [For Forward Anonymous]

GENERAL

Index
11

Name
For Forward Anonymous

Manipulation Set ID
4

Row Role
Use Previous Condition

ACTION

Action Subject
header.from.url.host
Editor

Action Type
Modify

Action Value
'anonymous.invalid'
Editor

MATCH

Message Type
Editor

Condition
Editor

Cancel
APPLY

14. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to 200 OK response messages sent to the Swisscom SIP Trunk IP Group. This adds a SIP Require header with a value of 'timer', if the SIP Session Expire header exists.

| Parameter           | Value                         |
|---------------------|-------------------------------|
| Index               | 12                            |
| Name                | Add Require=timer             |
| Manipulation Set ID | 4                             |
| Message Type        | any.response.200              |
| Condition           | header.session-expires exists |
| Action Subject      | header.require                |
| Action Type         | Add                           |
| Action Value        | 'timer'                       |

Figure 4-40: Configuring SIP Message Manipulation Rule 12 (for Swisscom SIP Trunk)

Message Manipulations [Add Require=timer]

GENERAL

Index
12

Name
Add Require=timer

Manipulation Set ID
4

Row Role
Use Current Condition

ACTION

Action Subject
header.require
Editor

Action Type
Add

Action Value
'timer'
Editor

MATCH

Message Type
any.response.200
Editor

Condition
header.session-expires exists
Editor

Cancel
APPLY

15. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule removes the Display Name.

| Parameter           | Value                        |
|---------------------|------------------------------|
| Index               | 13                           |
| Name                | Remove DisplayName           |
| Manipulation Set ID | 4                            |
| Message Type        | Invite                       |
| Action Subject      | Header.From.QuoteDisplayName |
| Action Type         | Remove                       |

Figure 4-41: Configuring SIP Message Manipulation Rule 13 (for Swisscom SIP Trunk)

Message Manipulations [Remove DisplayName]

GENERAL

Index

13

Name

Remove DisplayName

Manipulation Set ID

4

Row Role

Use Current Condition

ACTION

Action Subject

Header.From.QuoteDisplayName

Editor

Action Type

Remove

Action Value

Editor

MATCH

Message Type

Invite

Editor

Condition

Editor

Cancel

APPLY

16. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule normalizes the SDP body of each message.

| Parameter           | Value         |
|---------------------|---------------|
| Index               | 14            |
| Name                | Normalize SDP |
| Manipulation Set ID | 4             |
| Message Type        | any           |
| Action Subject      | body.sdp      |
| Action Type         | Normalize     |

Figure 4-42: Configuring SIP Message Manipulation Rule 14 (for Swisscom SIP Trunk)

Message Manipulations [Normalize SDP]

GENERAL

Index 
Name 
Manipulation Set ID 
Row Role

ACTION

Action Subject  Editor
Action Type 
Action Value  Editor

MATCH

Message Type  Editor
Condition  Editor

Cancel APPLY



17. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This replaces the host part of the SIP Request-URI header with the destination IP address.

| Parameter           | Value                                 |
|---------------------|---------------------------------------|
| Index               | 15                                    |
| Name                | To ITSP change R-URI Host to Dest. IP |
| Manipulation Set ID | 4                                     |
| Message Type        | any                                   |
| Condition           |                                       |
| Action Subject      | header.request-uri.url.host           |
| Action Type         | Modify                                |
| Action Value        | param.message.address.dst.address     |

**Figure 4-43: Configuring SIP Message Manipulation Rule 15 (for Swisscom SIP Trunk)**

Message Manipulations [To ITSP change R-URI Host to Dest. IP]

GENERAL

Index
15

Name
To ITSP change R-URI Host to Dest. IP

Manipulation Set ID
4

Row Role
Use Current Condition

MATCH

Message Type
any
Editor

Condition
Editor

ACTION

Action Subject
header.request-uri.url.host
Editor

Action Type
Modify

Action Value
param.message.address.dst.add
Editor

Cancel
APPLY

18. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule replaces the host part of the SIP To header with the Destination IP address.

| Parameter           | Value                              |
|---------------------|------------------------------------|
| Index               | 16                                 |
| Name                | To ITSP change To Host to Dest. IP |
| Manipulation Set ID | 4                                  |
| Message Type        | any                                |
| Condition           |                                    |
| Action Subject      | header.to.url.host                 |
| Action Type         | Modify                             |
| Action Value        | param.message.address.dst.address  |

Figure 4-44: Configuring SIP Message Manipulation Rule 16 (for Swisscom SIP Trunk)

Message Manipulations [To ITSP change To Host to Dest. IP]

GENERAL

Index 
Name 
Manipulation Set ID 
Row Role

ACTION

Action Subject  [Editor](#)
Action Type 
Action Value  [Editor](#)

MATCH

Message Type  [Editor](#)
Condition  [Editor](#)

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

19. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This replaces the host part of the SIP From header with the value from the SIP Contact header.

| Parameter           | Value                                |
|---------------------|--------------------------------------|
| Index               | 17                                   |
| Name                | To ITSP change From Host to local IP |
| Manipulation Set ID | 4                                    |
| Message Type        | any                                  |
| Condition           |                                      |
| Action Subject      | header.from.url.host                 |
| Action Type         | Modify                               |
| Action Value        | header.contact.url.host              |

**Figure 4-45: Configuring SIP Message Manipulation Rule 17 (for Swisscom SIP Trunk)**

Message Manipulations [To ITSP change From Host to local IP] - x

| GENERAL                                    | ACTION   |
|--|--|
| Index: 17                                  | Action Subject: header.from.url.host <a href="#">Editor</a>  |
| Name: To ITSP change From Host to local IP | Action Type: Modify  |
| Manipulation Set ID: 4                     | Action Value: header.contact.url.host <a href="#">Editor</a> |
| Row Role: Use Current Condition            |  |

| MATCH   |
|---|
| Message Type: any <a href="#">Editor</a>                                |
| Condition: header.from.url !contains 'anonymous' <a href="#">Editor</a> |

Cancel [APPLY](#)

20. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This replaces the host part of the SIP P-Asserted-Identity header with the value from the SIP Contact header.

| Parameter           | Value                               |
|---------------------|-------------------------------------|
| Index               | 18                                  |
| Name                | To ITSP change PAI Host to local IP |
| Manipulation Set ID | 4                                   |
| Message Type        | any                                 |
| Condition           |                                     |
| Action Subject      | header.p-asserted-identity.url.host |
| Action Type         | Modify                              |
| Action Value        | header.contact.url.host             |

Figure 4-46: Configuring SIP Message Manipulation Rule 18 (for Swisscom SIP Trunk)

Message Manipulations [To ITSP change PAI Host to local IP]

GENERAL

Index
18

Name
To ITSP change PAI Host to local IP

Manipulation Set ID
4

Row Role
Use Current Condition

MATCH

Message Type
any

Condition

ACTION

Action Subject
header.p-asserted-identity.url.host

Action Type
Modify

Action Value
header.contact.url.host

Cancel
APPLY

21. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This removes the 'ms-opaque' parameter from the SIP Contact header.

| Parameter           | Value                              |
|---------------------|------------------------------------|
| Index               | 19                                 |
| Name                | Remove ms-opaque from Contact      |
| Manipulation Set ID | 4                                  |
| Message Type        | Invite                             |
| Condition           |                                    |
| Action Subject      | Header.Contact.URL.Param.ms-opaque |
| Action Type         | Remove                             |
| Action Value        |                                    |

**Figure 4-47: Configuring SIP Message Manipulation Rule 19 (for Swisscom SIP Trunk)**

Message Manipulations [Remove ms-opaque from Contact] — x

**GENERAL**

Index: 19

Name: Remove ms-opaque from Contact

Manipulation Set ID: 4

Row Role: Use Current Condition ▼

**ACTION**

Action Subject: Header.Contact.URL.Param.ms-opaque [Editor](#)

Action Type: Remove ▼

Action Value: [Editor](#)

**MATCH**

Message Type: Invite [Editor](#)

Condition: [Editor](#)

Cancel **APPLY**

22. Configure another manipulation rule (Manipulation Set 3) for Swisscom SIP Trunk. This rule is applied to Re-INVITE request messages received from the Swisscom SIP Trunk IP Group during Hold, initiated by Microsoft Teams. In this rule RTP mode that is set to "sendonly" by Microsoft Teams, creates a variable and sets it to "1". This manages the call process handling for the state of the call.

| Parameter           | Value                                 |
|---------------------|---------------------------------------|
| Index               | 20                                    |
| Name                | Change RTP Mode                       |
| Manipulation Set ID | 3                                     |
| Message Type        | reinvite.request                      |
| Condition           | param.message.sdp.rtpmode=='sendonly' |
| Action Subject      | var.call.src.0                        |
| Action Type         | Modify                                |
| Action Value        | '1'                                   |

Figure 4-48: Configuring SIP Message Manipulation Rule 20 (for Swisscom SIP Trunk)

Message Manipulations [Change RTP Mode]

GENERAL

Index: 20  
Name: Change RTP Mode  
Manipulation Set ID: 3  
Row Role: Use Current Condition

ACTION

Action Subject: var.call.src.0  
Action Type: Modify  
Action Value: '1'

MATCH

Message Type: reinvite.request  
Condition: param.message.sdp.rtpmode=='sendonly'

Cancel

APPLY

23. Configure another manipulation rule (Manipulation Set 4) for Swisscom SIP Trunk. This rule is applied to 200 OK response on Re-INVITE request messages received from the Swisscom SIP Trunk IP Group during Hold, initiated by Microsoft Teams. A SIP Re-INVITE response while the current call state has a variable set to "1", sets within the SDP, an RTP mode of "recvonly". This rule normalizes call processing state back to Microsoft Teams for the proper reply to the initially received "sendonly".

| Parameter           | Value                     |
|---------------------|---------------------------|
| Index               | 21                        |
| Name                | Change RTP Mode           |
| Manipulation Set ID | 4                         |
| Message Type        | reinvite.response.200     |
| Condition           | var.call.src.0=='1'       |
| Action Subject      | param.message.sdp.rtpmode |
| Action Type         | Modify                    |
| Action Value        | 'recvonly'                |

Figure 4-49: Configuring SIP Message Manipulation Rule 21 (for Swisscom SIP Trunk)

Message Manipulations [Change RTP Mode]

| GENERAL                         | ACTION   |
|---------------------------------|--|
| Index: 21                       | Action Subject: param.message.sdp.rtpmode <a href="#">Editor</a> |
| Name: Change RTP Mode           | Action Type: Modify  |
| Manipulation Set ID: 4          | Action Value: 'recvonly' <a href="#">Editor</a>                  |
| Row Role: Use Current Condition |  |

| MATCH  |
|--|
| Message Type: reinvite.response.200 <a href="#">Editor</a> |
| Condition: var.call.src.0=='1' <a href="#">Editor</a>      |

Cancel [APPLY](#)

24. If the manipulation rule Index 21 (above) is executed, then the following rule is also executed. It checks the variable for its current state. If the variable is found to be set to "1", it then sets it to "0" to manage the call process handling for the state of the call.

| Parameter           | Value                         |
|---------------------|-------------------------------|
| Index               | <b>22</b>                     |
| Name                | <b>Change RTP Mode</b>        |
| Manipulation Set ID | <b>4</b>                      |
| Row Role            | <b>Use Previous Condition</b> |
| Message Type        |                               |
| Condition           |                               |
| Action Subject      | <b>var.call.src.0</b>         |
| Action Type         | <b>Modify</b>                 |
| Action Value        | <b>'0'</b>                    |

**Figure 4-50: Configuring SIP Message Manipulation Rule 22 (for Swisscom SIP Trunk)**

Message Manipulations [Change RTP Mode]

GENERAL

Index 
Name 
Manipulation Set ID 
Row Role

ACTION

Action Subject  Editor
Action Type 
Action Value  Editor

MATCH

Message Type  Editor
Condition  Editor

Cancel **APPLY**



25. Configure another manipulation rule (Manipulation Set 1) for Microsoft Teams. This rule applies to messages received from the Teams IP Group. This rule replaces user part of the second index (in the SIP URI format) of the SIP P-Asserted-Identity Header with the value from the first index (in the telephone format).

| Parameter           | Value                                 |
|---------------------|---------------------------------------|
| Index               | 23                                    |
| Name                | Build 1 PAI from 2                    |
| Manipulation Set ID | 1                                     |
| Message Type        |                                       |
| Condition           |                                       |
| Action Subject      | Header.P-Asserted-Identity.1.URL.User |
| Action Type         | Modify                                |
| Action Value        | Header.P-Asserted-Identity.0.URL.User |

**Figure 4-51: Configuring SIP Message Manipulation Rule 23 (for Microsoft Teams)**

Message Manipulations [Build 1 PAI from 2]

GENERAL

Index

23

Name

Build 1 PAI from 2

Manipulation Set ID

1

Row Role

Use Current Condition

MATCH

Message Type

Editor

Condition

Editor

ACTION

Action Subject

Header.P-Asserted-Identity.1.URL.User

Editor

Action Type

Modify

Action Value

Header.P-Asserted-Identity.0.URL.User

Editor

Cancel

APPLY

26. Configure another manipulation rule (Manipulation Set 1) for Microsoft Teams. This rule applies to messages received from the Teams IP Group. This rule removes the first index (in the telephone format) of the SIP P-Asserted-Identity Header.

| Parameter           | Value                        |
|---------------------|------------------------------|
| Index               | 24                           |
| Name                | Remove PAI tel               |
| Manipulation Set ID | 1                            |
| Message Type        |                              |
| Condition           |                              |
| Action Subject      | Header.P-Asserted-Identity.0 |
| Action Type         | Remove                       |
| Action Value        |                              |

Figure 4-52: Configuring SIP Message Manipulation Rule 24 (for Microsoft Teams)

Message Manipulations [Remove PAI tel]

GENERAL

Index 
Name 
Manipulation Set ID 
Row Role

ACTION

Action Subject  Editor
Action Type 
Action Value  Editor

MATCH

Message Type  Editor
Condition  Editor

Cancel

27. Configure another manipulation rule (Manipulation Set 1) for Teams. This rule applies to messages received from the Teams IP Group. This removes the SIP Privacy Header in all messages, except of call with presentation restriction.

| Parameter           | Value  |
|---------------------|--|
| Index               | <b>25</b>  |
| Name                | <b>Remove Privacy Header</b>   |
| Manipulation Set ID | <b>1</b>   |
| Condition           | <b>Header.Privacy exists And Header.From.URL !contains 'anonymous'</b> |
| Action Subject      | <b>Header.Privacy</b>  |
| Action Type         | <b>Remove</b>  |

**Figure 4-53: Configuring SIP Message Manipulation Rule 25 (for Microsoft Teams)**

Message Manipulations [Remove Privacy Header]

**GENERAL**

Index: 25

Name: Remove Privacy Header

Manipulation Set ID: 1

Row Role: Use Current Condition

**ACTION**

Action Subject: Header.Privacy

Action Type: Remove

Action Value:

**MATCH**

Message Type:

Condition: Header.Privacy exists And Header.From.U

Cancel APPLY

**Figure 4-54: Example of Configured SIP Message Manipulation Rules**

| Message Manipulations (26)   |                     |                     |                  |                      |                      |             |                      |                        |
|--|---------------------|---------------------|------------------|----------------------|----------------------|-------------|----------------------|------------------------|
| <div> + New Edit Insert </div> <div> Page 1 of 1 Show 30 records per page </div> |                     |                     |                  |                      |                      |             |                      |                        |
| INDEX  | NAME                | MANIPULATION SET ID | MESSAGE TYPE     | CONDITION            | ACTION SUBJECT       | ACTION TYPE | ACTION VALUE         | ROW ROLE               |
| 0  | Call Transfer       | 4                   | invite.request   | header.referred-by   | header.referred-by   | Modify      | param.ipg.dst.host   | Use Current Condition  |
| 1  | Call Transfer       | 4                   |                  |                      | header.diversion     | Add         | header.referred-by   | Use Previous Condition |
| 2  | Call Transfer       | 4                   |                  |                      | header.referred-by   | Remove      |                      | Use Previous Condition |
| 3  | Call Forward        | 4                   | any              | Header.History-Info  | Header.Diversion     | Add         | Header.History-Info  | Use Current Condition  |
| 4  | Call Forward        | 4                   |                  |                      | Header.Diversion     | Normalize   |                      | Use Previous Condition |
| 5  | Call Forward        | 4                   |                  |                      | Header.History-Info  | Remove      |                      | Use Previous Condition |
| 6  | Change Diversion H  | 4                   | invite.request   | header.diversion ex  | header.diversion.url | Modify      | param.ipg.dst.host   | Use Current Condition  |
| 7  | Remove 'a=inactive' | 4                   | any.response     | body.sdp regex (.*)i | body.sdp             | Modify      | \$1+\$2+\$3+\$5      | Use Current Condition  |
| 8  | For Forward Anonym  | 4                   | any.request      | header.from.url con  | header.from.url.use  | Remove      |                      | Use Current Condition  |
| 9  | For Forward Anonym  | 4                   |                  |                      | header.privacy       | Add         | 'id'                 | Use Previous Condition |
| 10   | For Forward Anonym  | 4                   |                  |                      | header.p-asserted-ri | Modify      | header.diversion.url | Use Previous Condition |
| 11   | For Forward Anonym  | 4                   |                  |                      | header.from.url.hos  | Modify      | 'anonymous.invalid'  | Use Previous Condition |
| 12   | Add Require=timer   | 4                   | any.response.200 | header.session-expi  | header.require       | Add         | 'timer'              | Use Current Condition  |
| 13   | Remove DisplayNam   | 4                   | Invite           |                      | Header.From.Quote    | Remove      |                      | Use Current Condition  |
| 14   | Normalize SDP       | 4                   | any              |                      | body.sdp             | Normalize   |                      | Use Current Condition  |
| 15   | To ITSP change R-Uf | 4                   | any              |                      | header.request-uri.t | Modify      | param.message.adc    | Use Current Condition  |
| 16   | To ITSP change To H | 4                   | any              |                      | header.to.url.host   | Modify      | param.message.adc    | Use Current Condition  |
| 17   | To ITSP change Fron | 4                   | any              | header.from.url.lcor | header.from.url.hos  | Modify      | header.contact.url.h | Use Current Condition  |

The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set IDs (1, 3 and 4) and which are executed for messages sent to or received from the Swisscom SIP Trunk IP as well as on messages received from Microsoft Teams. These rules are specifically required to enable proper interworking between Swisscom SIP Trunk and Microsoft Teams Direct Routing Interface. 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 sent to the Swisscom SIP Trunk IP Group in a Call Transfer scenario. This rule replaces the host part of the SIP Referred-By header with the value taken from the 'Group Name' field of the Swisscom SIP Trunk IP Group. | For Call Transfer scenarios, Swisscom SIP Trunk request SIP Diversion header instead of SIP Referred-By header, sent from the Microsoft Teams. |
| 1          | If manipulation rule index above is executed, then the following rule is also executed. It adds the SIP Diversion header with values from the SIP Referred-by header.  |  |
| 2          | If manipulation rule index above is executed, then the following rule is also executed. It removes the SIP Referred-by header.   |  |
| 3          | This rule applies to messages sent to the Swisscom SIP Trunk IP Group in a call forward scenario. This rule adds the SIP Diversion header with the value from the SIP History-Info Header.   | For Call Forward scenarios, Swisscom SIP Trunk request SIP Diversion header instead of SIP History-Info header, sent from the Microsoft Teams. |
| 4          | If the manipulation rule Index 3 (above) is executed, then the following rule is also executed. It normalizes the SIP Diversion header.  |  |
| 5          | If the manipulation rule Index 3 (above) is executed, then the following rule is also executed. It removes the SIP History-Info header.  |  |

| Rule Index | Rule Description  | Reason for Introducing Rule   |
|------------|---|---|
| 6          | This rule applies to messages sent to the Swisscom SIP Trunk IP Group. This rule replaces the host part of the SIP Diversion header with the value that was configured in the Swisscom SIP Trunk IP Group as Group Name.  | Swisscom SIP Trunk request that Host part of SIP Diversion header will be pre-configured.   |
| 7          | This rule is applied to response messages sent to the Swisscom SIP Trunk IP Group. It removes 'a=inactive' from responses sent to the Swisscom SIP Trunk.   | Swisscom The SIP Trunk sends two media streams in the SIP INVITE message – m=audio (for audio stream) and m=image (for T.38 fax stream). In the response message, when only the audio call is answered, the AudioCodes SBC sends 'm=image 0' and 'a=inactive' to clarify that T.38 fax will not be used. But the Swisscom SIP Trunk requests to remove 'a=inactive' and leave only 'm=image 0'. |
| 8          | This rule is applied to response messages sent to the Swisscom SIP Trunk IP Group for Call Forward of Anonymous Call initiated by the Microsoft Teams IP Group. This removes the user=phone variable from the SIP 'From' header.  | These rules are applied to normalize messages for Call Forward of an Anonymous Call initiated by the Microsoft Teams.   |
| 9          | If the manipulation rule index above is executed, then the following rule is also executed. This rule is applied to response messages sent to the Swisscom SIP Trunk IP Group for Call Forward of Anonymous Call initiated by the Microsoft Teams IP Group. This adds the SIP Privacy header with value 'id'. |   |
| 10         | If the manipulation rule index above is executed, then the following rule is also executed. This rule replaces the user part of the SIP P-Asserted-Identity header with the value from the SIP Diversion header.  |   |
| 11         | If the manipulation rule index above is executed, then the following rule is also executed. This rule replaces the host part of the SIP 'From' header with the value 'anonymous.invalid'.   |   |
| 12         | This rule is applied to 200 OK response messages sent to the Swisscom SIP Trunk IP Group. This adds the SIP Require header with a value of 'timer' if the SIP Session Expire header exists.   |   |
| 13         | This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule removes the Display Name.   |   |
| 14         | This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule normalizes the SDP body of each message.  |   |
| 15         | This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule replaces the host part of the SIP Request-URI header with the Destination IP address.   |   |

| Rule Index | Rule Description  | Reason for Introducing Rule |
|------------|---|-----------------------------|
| 16         | This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule replaces the host part of the SIP To header with destination IP address.  |                             |
| 17         | This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This rule replaces the host part of the SIP From header with the value from the SIP Contact header.   |                             |
| 18         | This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This replaces the host part of the SIP P-Asserted-Identity header with the value from the SIP Contact header.   |                             |
| 19         | This rule is applied to all messages sent to the Swisscom SIP Trunk IP Group. This removes 'ms-opaque' parameter from the SIP Contact header.   |                             |
| 20         | This rule is applied to Re-INVITE request messages received from the Swisscom SIP Trunk IP Group during Hold, initiated by Microsoft Teams. In this rule RTP mode that is set to "sendonly" by Microsoft Teams, creates a variable and sets it to "1". This manages the call process handling for the state of the call.  |                             |
| 21         | This rule is applied to 200 OK response on Re-INVITE request messages received from the Swisscom SIP Trunk IP Group during Hold, initiated by Microsoft Teams. A SIP Re-INVITE response while the current call state has a variable set to "1", sets within the SDP, an RTP mode of "recvonly". This rule normalizes call processing state back to Microsoft Teams for the proper reply to the initially received "sendonly". |                             |
| 22         | If the manipulation rule Index 21 (above) is executed, then the following rule is also executed. It checks the variable for its current state. If the variable is found to be set to "1", it then sets it to "0" to manage the call process handling for the state of the call.   |                             |
| 23         | This rule applies to messages received from the Teams IP Group. This rule replaces user part of the second index (in the SIP URI format) of the SIP P-Asserted-Identity Header with the value from the first index (in the telephone format).   |                             |
| 24         | This rule applies to messages received from the Teams IP Group. This rule removes the first index (in the telephone format) of the SIP P-Asserted-Identity Header.  |                             |
| 25         | This rule applies to messages received from the Teams IP Group. This removes the SIP Privacy Header in all messages, except for calls with presentation restriction.  |                             |

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

**Figure 4-55: Assigning Manipulation Set to the Microsoft Teams IP Group**

IP Groups [Teams]

SRD #0 [DefaultSRD]

| GENERAL              |                             | QUALITY OF EXPERIENCE     |         |
|----------------------|-----------------------------|---------------------------|---------|
| Index                | 0                           | QoE Profile               | -- View |
| Name                 | Teams                       | Bandwidth Profile         | -- View |
| Topology Location    | Up                          | User Voice Quality Report | Disable |
| Type                 | Server                      |                           |         |
| Proxy Set            | #0 [Teams] View             |                           |         |
| IP Profile           | #1 [Teams] View             |                           |         |
| Media Realm          | #0 [MRWan] View             |                           |         |
| Internal Media Realm | -- View                     |                           |         |
| Contact User         |                             |                           |         |
| SIP Group Name       | tsbc01.siptrunk.web-call.ch |                           |         |

MESSAGE MANIPULATION

|   |        |
|---|--------|
| Inbound Message Manipulation Set          | 1      |
| Outbound Message Manipulation Set         | -1     |
| Message Manipulation User-Defined String1 | 0      |
| Message Manipulation User-Defined String2 | 0      |
| Proxy Keep-Alive using IP Group settings  | Enable |

Cancel APPLY

- Click **Apply**.

29. Assign Manipulation Set IDs 3 and 4 to the Swisscom 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 Swisscom SIP Trunk IP Group, and then click **Edit**.
  - c. Set the 'Inbound Message Manipulation Set' field to **3**.
  - d. Set the 'Outbound Message Manipulation Set' field to **4**.

**Figure 4-56: Assigning Manipulation Set IDs to the Swisscom SIP Trunk IP Group**

The screenshot shows the 'IP Groups' configuration window for the group '[SwisscomESIP]'. At the top, there is a dropdown for 'SRD' set to '#0 [DefaultSRD]'. Below this, the configuration is divided into two main sections: 'GENERAL' and 'MESSAGE MANIPULATION'.

**GENERAL Section:**

- Index: 1
- Name: SwisscomESIP
- Topology Location: Down
- Type: Server
- Proxy Set: #1 [SwisscomESIP] (with a 'View' link)
- IP Profile: #2 [Swisscom] (with a 'View' link)
- Media Realm: #1 [MRLan] (with a 'View' link)
- Internal Media Realm: .. (with a 'View' link)
- Contact User: (empty field)
- SIP Group Name: 10.20.0.10

**MESSAGE MANIPULATION Section:**

- Inbound Message Manipulation Set: 3
- Outbound Message Manipulation Set: 4
- Message Manipulation User-Defined String1: 0
- Message Manipulation User-Defined String2: 0
- Proxy Keep-Alive using IP Group settings: Disable

At the bottom of the window, there are 'Cancel' and 'APPLY' buttons. The 'APPLY' button is highlighted in blue.

- e. Click **Apply**.



## 4.16 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

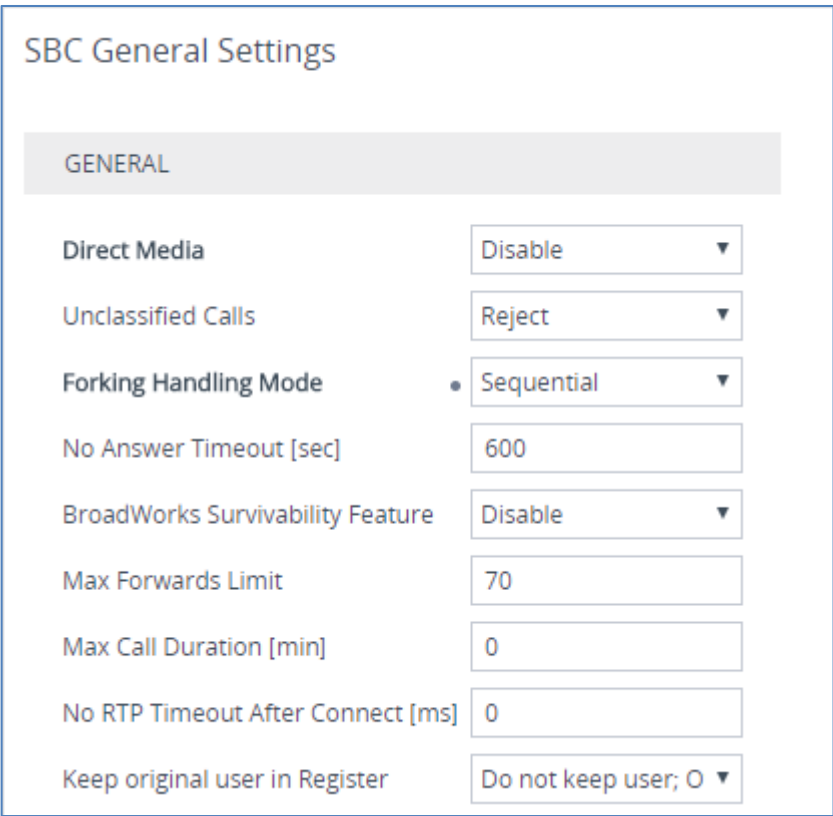
### 4.16.1 Configure Call Forking Mode

This step 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 4-57: Configuring Forking Mode**



The screenshot shows the 'SBC General Settings' page. A grey arrow points to the 'Forking Handling Mode' dropdown menu, which is currently set to 'Sequential'. The page has a 'GENERAL' tab selected. Other settings visible 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).

| SBC General Settings              |                       |
|-----------------------------------|-----------------------|
| GENERAL                           |                       |
| 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 (relevant for Mediant 9000 and Software SBC only)

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

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

### ➤ To optimize core allocation for a profile:

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

SBC Performance Profile

• Optimized for transcoding ▼ ⚡

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

**International Headquarters**

Naimi Park,  
Ofra Haza 6  
Or Yehuda, Israel  
Tel: +972-3-976-4000  
Fax: +972-3-976-4040

**AudioCodes Inc.**

80 Kingsbridge Road  
Piscataway NJ 08854, USA  
Tel: +1-732-469-0880  
Fax: +1-732-469-2298

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

**Website:** <https://www.audiocodes.com/>

©2024 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-12682

