

Microsoft® Teams Direct Routing Enterprise Model and Swisscom SIP Trunk "Smart Business Connect" using AudioCodes Mediant™ SBC

Version 7.2



Microsoft Partner
Gold Communications



Table of Contents

1	Introduction	7
1.1	Intended Audience	7
1.2	About AudioCodes SBC Product Series	7
1.3	About Microsoft Teams Direct Routing	7
2	Component Information.....	9
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
3	Configuring Teams Direct Routing.....	13
3.1	Prerequisites	13
3.2	SBC Domain Name in the Teams Enterprise Model	13
4	Configuring AudioCodes SBC	15
4.1	SBC Configuration Concept in Teams Direct Routing Enterprise Model	16
4.2	IP Network Interfaces Configuration	17
4.2.1	Configure VLANs	18
4.2.2	Configure Network Interfaces	18
4.3	SIP TLS Connection Configuration	20
4.3.1	Configure the NTP Server Address	21
4.3.2	Configure the TLS version	22
4.3.3	Configure a Certificate	23
4.3.4	Alternative Method of Generating and Installing the Certificate	26
4.3.5	Deploy Baltimore Trusted Root Certificate	26
4.4	Configure Media Realms	27
4.5	Configure SIP Signaling Interfaces	30
4.6	Configure Proxy Sets.....	32
4.7	Configure the Internal SRV Table	36
4.8	Configure Coders	38
4.9	Configure IP Profiles.....	41
4.10	Configure IP Groups.....	44
4.11	Configure SRTP	46
4.12	Configuring Message Condition Rules.....	47
4.13	Configuring Classification Rules	48
4.14	Configure IP-to-IP Call Routing Rules	49
4.15	Configure Number Manipulation Rules	55
4.16	Configure Message Manipulation Rules	57
4.17	Configure SIP OPTIONS Towards Teams.....	83
4.17.1	Configure FQDN in Contact Header of OPTIONS Message using Message Manipulations Set	83
4.17.2	Assigning Message Manipulation Set as Gateway Outbound Manipulation Set.....	85
4.18	Configure Registration Accounts	87

4.19	Miscellaneous Configuration.....	89
4.19.1	Configure Call Forking Mode.....	89
A	AudioCodes INI File	91

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-29-2019

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
14410	Initial document release for Version 7.2.
14411	Changes in TLS configuration according to Swisscom's request and new Microsoft requirement.
14412	Figure 2-1 was updated, G.722 codec was added to Table 2-4.

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 the AudioCodes website at <https://www.audiocodes.com/partners/sbc-interoperability-list>.

1.1 Intended Audience

The 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, PSTN access survivability, and third-party value-added services applications. This enables Enterprises to utilize the advantages of converged networks and eliminate the need for standalone appliances.

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

1.3 About Microsoft Teams Direct Routing

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

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

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes SBC Version

Table 2-1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500 Gateway & E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant 4000B SBC ▪ Mediant 9000 SBC ▪ Mediant Software SBC (SE and VE)
Software Version	7.20A.202.203
Protocol	▪ SIP/UDP (to the Swisscom SIP Trunk) ▪ SIP/TLS (to the Teams Direct Routing)
Additional Notes	None

2.2 Swisscom Enterprise SIP Trunking Version

Table 2-2: Swisscom Version

Vendor/Service Provider	Swisscom
SSW Model/Service	Smart Business Connect with Cisco eSBC
Software Version	IOS 15.6.3M4
Protocol	SIP
Additional Notes	None

2.3 Microsoft Teams Direct Routing Version

Table 2-3: Microsoft Teams Direct Routing Version

Vendor	Microsoft
Model	Teams Phone System Direct Routing
Software Version	
Protocol	SIP
Additional Notes	None

2.4 Interoperability Test Topology

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

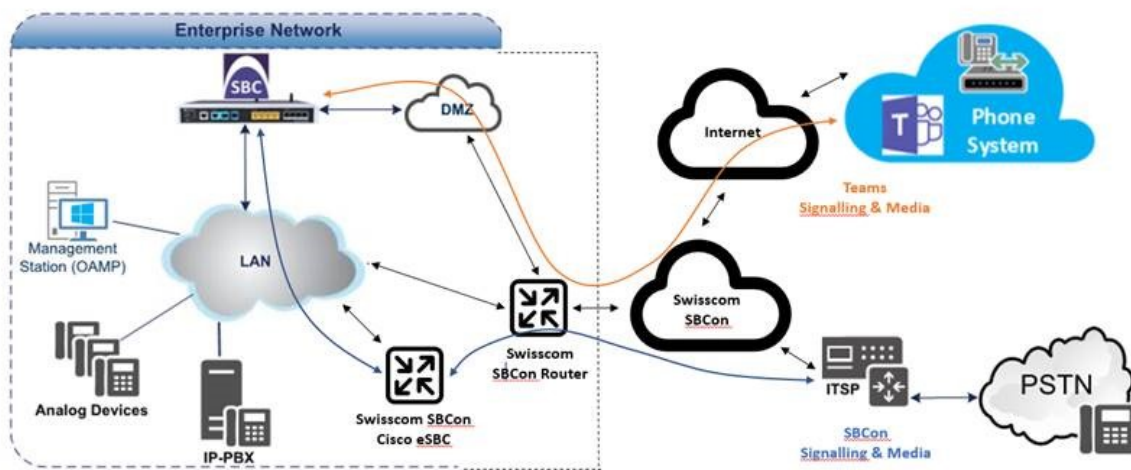
2.4.1 Enterprise Model Implementation

The interoperability testing between AudioCodes SBC and 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 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 Smart Business Connect SIP Trunk and Microsoft Teams Phone Systems, both 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 Smart Business Connect SIP Trunk



2.4.2 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	- Microsoft Teams Direct Routing environment is located on the Enterprise's (or Service Provider's) WAN - Swisscom SIP Trunk is located on the WAN
Signaling Transcoding	- Microsoft Teams Direct Routing operates with SIP-over-TLS transport type - Swisscom SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	- Microsoft Teams Direct Routing supports G.711A-law, G.711U-law, G.729, G.722, SILK (NB and WB) and OPUS coders - Swisscom SIP Trunk supports G.711A-law, G.711U-law, G.722 and G.729 coders
Media Transcoding	- Microsoft Teams Direct Routing operates with SRTP media type - Swisscom SIP Trunk operates with RTP media type

2.4.3 Infrastructure Prerequisites

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

Table 2-5: Infrastructure Prerequisites

Infrastructure Prerequisite	Details
Certified Session Border Controller (SBC)	See Microsoft's document <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 chapter describes how to configure Microsoft Teams Direct Routing to operate with AudioCodes SBC.

3.1 Prerequisites

Before you begin configuration, make sure you have these 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

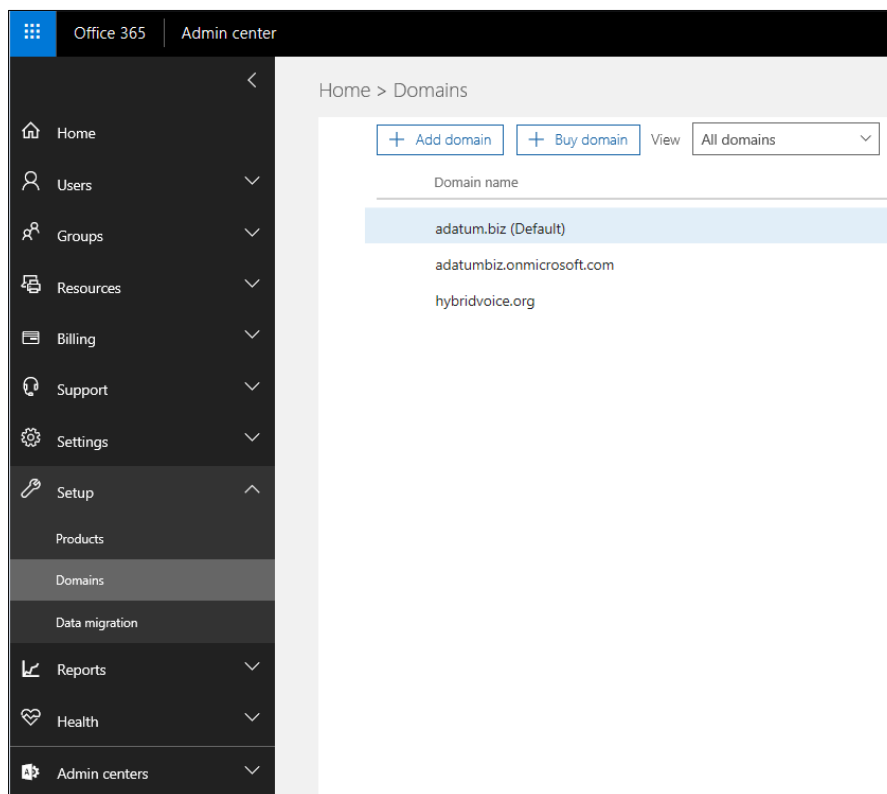
The SBC domain name must be from one of the names registered in 'Domains' of the tenant. You cannot use the ***.onmicrosoft.com** tenant for the domain name. For example, in Figure 2-2, the administrator registered the following DNS names for the tenant:

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

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

Figure 3-1: Example of Registered DNS Names



Use the following command on the Microsoft Teams Direct Routing Management Shell after reconfiguration to verify correct values:

■ **Get-CsOnlinePSTNGateway**

```
Identity           : sbc.ACeducation.info
Fqdn               : sbc.ACeducation.info
SipSignallingPort  : 5068
CodecPriority      : SILKWB, SILKNB, PCMU, PCMA
ExcludedCodecs    :
FailoverTimeSeconds : 10
ForwardCallHistory : True
ForwardPai        : False
SendSipOptions    : True
MaxConcurrentSessions :
Enabled           : True
MediaBypass       : False
```

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:

- ✓ **Microsoft**
- ✓ **Security**
- ✓ **DSP**
- ✓ **RTP**
- ✓ **SIP**
- ✓ **Number of SBC sessions** *[Based on requirements]*
- ✓ **Transcoding sessions** *[If media transcoding is needed]*
- ✓ **SILK and OPUS coders** *[Based on requirements]*

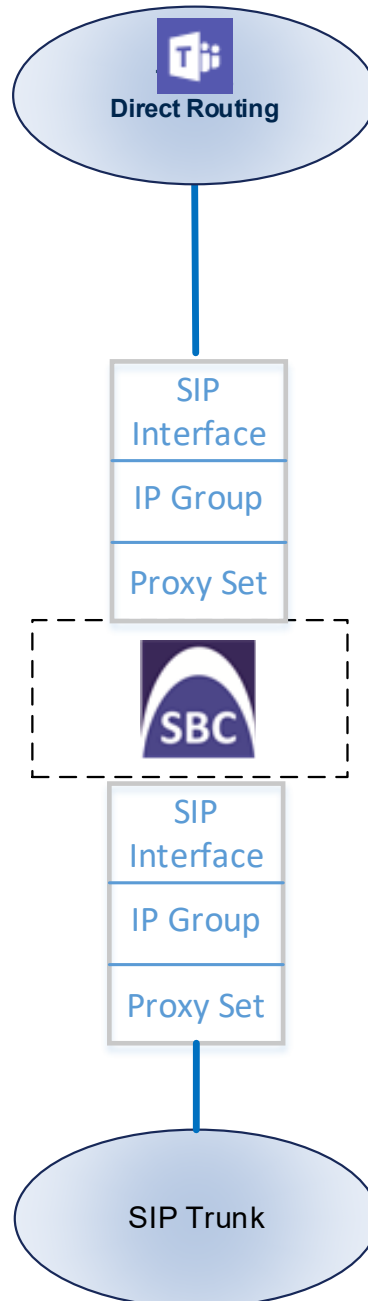
For more information about the License Key, contact your AudioCodes sales representative.

- The scope of this interoperability test and 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

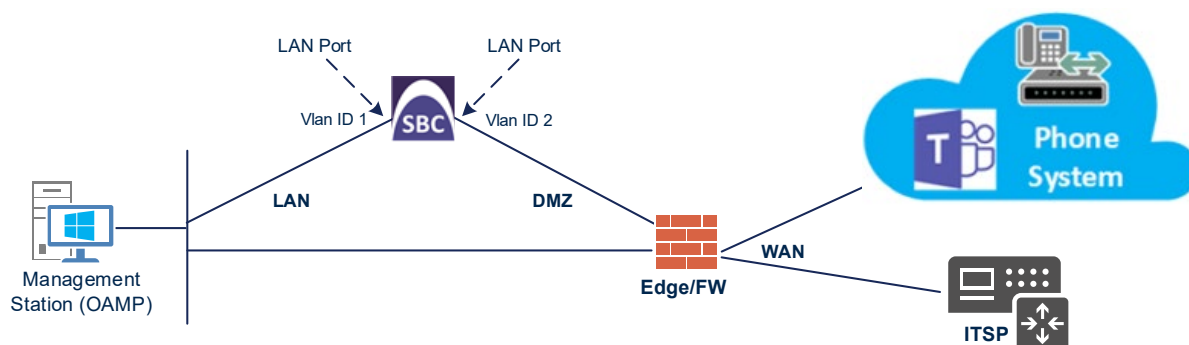


4.2 IP Network Interfaces Configuration

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:
 - Enterprise Management, located on the LAN
 - Swisscom SIP Trunk and Teams Direct Routing, located on the WAN
- SBC connects to the WAN through a DMZ network
- Physical connection: The type of physical connection to the LAN 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 LAN 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 define 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:

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

Figure 4-3: Configured VLAN IDs in Ethernet Device

Ethernet Devices (2)				
+ New Edit Delete				
Page 1 of 1 Show 10 records per page				
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. Modify the existing LAN network interface:
 - a. Select the 'Index' radio button of the **OAMP + Media + Control** table row, and then click **Edit**.

- b. Configure the interface as follows:

Parameter	Value
Name	LAN_IF (arbitrary descriptive name)
Ethernet Device	vlan 1
IP Address	10.15.17.77 (LAN IP address of SBC)
Prefix Length	16 (subnet mask in bits for 255.255.0.0)
Default Gateway	10.15.0.1
Primary DNS	10.15.27.1

3. Add a network interface for the WAN side:

- a. Click **New**.

- b. Configure the interface as follows:

Parameter	Value
Name	WAN_IF
Application Type	Media + Control
Ethernet Device	vlan 2
IP Address	195.189.192.157 (DMZ IP address of SBC)
Prefix Length	25 (subnet mask in bits for 255.255.255.128)
Default Gateway	195.189.192.129 (router's IP address)
Primary DNS	80.179.52.100
Secondary DNS	80.179.55.100

4. Click **Apply**.

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 Teams Direct Routing Phone System. This is essential for a secure SIP TLS connection. The configuration instructions in this section are based on the following domain structure example that must be implemented as part of the certificate which must be loaded to the host SBC:

- CN: ACeducation.info
- SAN: *.customers.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 step describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or some global server) to ensure that the SBC receives the accurate and current date and time. This is necessary for validating certificates of remote parties.

➤ **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., **pool.ntp.org**).

Figure 4-5: Configuring NTP Server Address

NTP SERVER	
Enable NTP	Enable ▼
Primary NTP Server Address (IP or FQDN)	• pool.ntp.org
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 Configure the TLS version

This step describes how to configure the SBC to use TLS Version 1.2 only. Microsoft requires implementing only TLS Version 1.2.

➤ **To configure the TLS version:**

1. Open the TLS Contexts table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts table, select the required TLS Context index row (usually default index 0 will be used), and then click **Edit**.
3. From the **'TLS Version'** drop-down list, select **'TLSv1.2'**

Figure 4-6: Configuring TLS version

The screenshot shows the 'TLS Contexts [default]' configuration window. It has two tabs: 'GENERAL' and 'OCSP'. The 'GENERAL' tab is selected, and it contains the following fields:

- Index: 0
- Name: default
- TLS Version: TLSv1.2 (indicated by an arrow)
- DTLS Version: Any
- Cipher Server: RC4:AE5128
- Cipher Client: DEFAULT
- Strict Certificate Extension Validation: Disable
- DH key Size: 1024

The 'OCSP' tab contains the following fields:

- OCSP Server: Disable
- Primary OCSP Server: 0.0.0.0
- Secondary OCSP Server: 0.0.0.0
- OCSP Port: 2560
- OCSP Default Response: Reject

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

4. Click **Apply**.

4.3.3 Configure a Certificate

This step 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 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.



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

➤ **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, **ACeducation.info**).
 - b. Change the 'Private Key Size' based on the requirements of your Certification Authority. Many CAs do not support private key of size 1024. In this case, you must change the key size to 2048.
 - c. To change the key size on TLS Context, go to: **Generate New Private Key and Self-Signed Certificate**, change the 'Private Key Size' to **2048** and then click **Generate Private-Key**. To use **1024** as a Private Key Size value, you can click **Generate Private-Key** without changing the default key size value.
 - d. Fill in the rest of the request fields according to your security provider's instructions.
 - e. 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 [#0] > Change Certificates

CERTIFICATE SIGNING REQUEST

Subject Name [CN]

1st Subject Alternative Name [SAN]

2nd Subject Alternative Name [SAN]

3rd Subject Alternative Name [SAN]

4th Subject Alternative Name [SAN]

5th Subject Alternative Name [SAN]

Organizational Unit [OU] (optional)

Company name [O] (optional)

Locality or city name [L] (optional)

State [ST] (optional)

Country code [C] (optional)

Signature Algorithm

AEducation.info

EMAIL ▼

EMAIL ▼

EMAIL ▼

EMAIL ▼

EMAIL ▼

Headquarters

Corporate

Poughkeepsie

New York

US

SHA-256 ▼

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-----
MIIBPjCCAVCAQAQwgbUxGTAXBgNVBAUwEWFEDZURlY2F0aH9uLm1uZm8xFATBgNV
BAsIDElh1YWRxdWlydG9ycyESMBAGAlUECgwJQ29ycG9yYXR1NRUwEwYDVQQHDAvQ
b3VnaGt1ZX8zZWJueETAPBgNVBAGhCE51dyB2b3JrMQswCQYDVQQGEwJUUzEZMhcG
CsqGS1b3DQE3CAWKMTAuNC41LjEyNjFlbWk6K5CSqGS1b3DQE3AgUM91dGVyLU1Q
U2VjHIGFMAGCSqGS1b3DQEBAQUAA4GNADCBiQKgODJCscN4x06hIeQuY20h8VPg
K4UKHUUV1d1j4zdFBKjkdgLakRZ6EK9nsENDMZFen00KF3UB8YNcXvISNre9Cnhj
DKN1XXGSoLOISLnP24oRP1okaZH0FohI3vW+W0j8/JJFn+uxhb2FSML7LGCU/b37
ps8qhVX+9G91SG6h1f8+5wIDAQABoAwwDQYJKoZIhvcNAQELBQADgYEAEtu8G/s
okk7ONgdOCiqlsY1ovdoQEHE9padxp3PeKaCVNHCH54cRVBNha9XE0J1ypR4UQRBC
9dbUCFx1mu91Pa3NZOH1lgtHz1KbjRHVFQ1lWQ0Z4JRGVnc131mmFskGRoaHjYlf
NeE1nAV7htST53naU2/Z8VURFY3oh4NbvyQ=
-----END CERTIFICATE REQUEST-----
```

GENERATE NEW PRIVATE KEY AND SELF-SIGNED CERTIFICATE

Private Key Size

Private key pass-phrase (optional)

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

2048

Generate Private-Key

Generate Self-Signed Certificate

4. Copy the CSR from the line "**-----BEGIN CERTIFICATE**" to "**END CERTIFICATE REQUEST**----" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, for example *certreq.txt*.
5. Send *certreq.txt* file to the Certified Authority Administrator for signing.
6. After obtaining 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. Validate that the certificate was uploaded correctly: A message indicating that the certificate was uploaded successfully is displayed in blue color lowermost in 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 [#2] > Certificate Information

PRIVATE KEY

Key size: 2048 bits

Status: OK

CERTIFICATE

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
06:d7:22:bc:07:a6:d1:c7:81:a7:c7:b3:d9:b5:3c:ae
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL RSA CA 2018
Validity
Not Before: May 22 00:00:00 2018 GMT
Not After : May 22 12:00:00 2019 GMT
Subject: CN=*.audctrunk.aceducation.info
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:9d:38:c2:00:f7:df:f0:1c:7a:17:db:fe:ac:e1:

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

TLS Context [#2] > Trusted Root Certificates			
View		Import Export Remove	
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

11. Reset the SBC with a burn to flash for your settings to take effect.

4.3.4 Alternative Method of Generating and Installing the Certificate

To use the same certificate on multiple devices, you may prefer using [DigiCert Certificate Utility for Windows](#) to process the certificate request from your Certificate Authority on another machine, with this utility installed.

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

➤ To install the certificate:

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

4.3.5 Deploy Baltimore Trusted Root Certificate

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

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



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

4.4 Configure Media Realms

This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for traffic toward SIP Trunk and one for traffic toward Teams.

➤ **To configure Media Realms:**

1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Add a Media Realm for the SIP Trunk. You can use the default Media Realm (Index 0), but modify it as shown below:

Parameter	Value
Index	0
Name	MR-SIPTrunk (descriptive name)
IPv4 Interface Name	WAN_IF
Port Range Start	6000
Number of Media Session Legs	100 (media sessions assigned with port range)

Figure 4-11: Configuring Media Realm for SIP Trunk

Media Realms [MR-SIPTrunk]

GENERAL

Index: 0

Name: MR-SIPTrunk

Topology Location: Down

IPv4 Interface Name: #1 [WAN_IF] [View](#)

Port Range Start: 6000

Number Of Media Session Legs: 100

Port Range End: 6999

Default Media Realm: No

QUALITY OF EXPERIENCE

QoS Profile: -- [View](#)

Bandwidth Profile: -- [View](#)

Cancel **APPLY**

3. Configure a Media Realm for the Teams:

Parameter	Value
Index	1
Name	MR-Teams (arbitrary name)
Topology Location	Up
IPv4 Interface Name	WAN_IF
Port Range Start	7000
Number of Media Session Legs	100 (media sessions assigned with port range)

Figure 4-12: Configuring Media Realm for Teams

Media Realms [MR-Teams]

GENERAL

Index
1
Name
MR-Teams
Topology Location
Up
IPv4 Interface Name
#1 [WAN_IF]
Port Range Start
7000
Number Of Media Session Legs
100
Port Range End
7999
Default Media Realm
No

QUALITY OF EXPERIENCE

QoE Profile
--
Bandwidth Profile
--

Cancel
APPLY

The configured Media Realms are shown in the figure below:

Figure 4-13: Configured Media Realms in Media Realm Table

Media Realms (2)						
+ New Edit 🗑️ ⏪ ⏩ Page 1 of 1 Show 10 records per page 🔍						
INDEX	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	MR-SIPTrunk	WAN_IF	6000	100	6999	No
1	MR-Teams	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, two SIP Interfaces must be configured for the SBC. One toward the SIP Trunk and another one toward Teams Direct Routing Interface.

➤ **To configure SIP Interfaces:**

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Add a SIP Interface for the SIP Trunk. You can use the default SIP Interface (Index 0), but modify it as shown below:

Parameter	Value
Index	0
Name	SwisscomSBCon (arbitrary descriptive name)
Network Interface	WAN_IF
Application Type	SBC
UDP Port	5060
TCP and TLS Port	0
Media Realm	MR-SIPTrunk



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 might be any port of your choice. When pairing the SBC with Office 365, the chosen port is specified in the pairing command.

3. Configure a SIP Interface for the Teams:

Parameter	Value
Index	1
Name	Teams (arbitrary descriptive name)
Network Interface	WAN_IF
Application Type	SBC
UDP and TCP Port	0
TLS Port	5061 (as configured in the Office 365)
Enable TCP Keepalive	Enable
Classification Failure Response Type	0
Media Realm	MR-Teams

The configured SIP Interfaces are shown in the figure below:

Figure 4-14: Configured SIP Interfaces in SIP Interface Table

SIP Interfaces (2)

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

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
0	SwisscomSBCon	 DefaultSRD	WAN_IF	SBC	5060	0	0	No encapsulation	MR-SIPTrunk
1	Teams	 DefaultSRD	WAN_IF	SBC	0	0	5061	No encapsulation	MR-Teams

4.6 Configure Proxy Sets

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 be later applying to the VoIP network by assigning them to IP Groups.

➤ To configure Proxy Sets:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Add a Proxy Set for the Swisscom SIP Trunk:

Parameter	Value
Index	1
Name	SwisscomSBCon
SBC IPv4 SIP Interface	SwisscomSBCon
Proxy Keep-Alive	Using Options
Proxy Keep-Alive Time [sec]	10

Figure 4-15: Configuring Proxy Set for Swisscom SIP Trunk

Proxy Sets [SwisscomSBCon]

SRD: #0 [DefaultSRD]

GENERAL	REDUNDANCY
Index: 1	Redundancy Mode: [Dropdown]
Name: SwisscomSBCon	Proxy Hot Swap: Disable [Dropdown]
Gateway IPv4 SIP Interface: [Dropdown] View	Proxy Load Balancing Method: Disable [Dropdown]
SBC IPv4 SIP Interface: #0 [SwisscomSBCon] View	Min. Active Servers for Load Balancing: 1
TLS Context Name: [Dropdown] View	
KEEP ALIVE	ADVANCED
Proxy Keep-Alive: Using OPTIONS [Dropdown]	Classification Input: IP Address only [Dropdown]
Proxy Keep-Alive Time [sec]: 10	DNS Resolve Method: [Dropdown]
Keep-Alive Failure Responses: [Text Field]	

Cancel APPLY

- a. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
- b. Click **New**; the following dialog box appears:

Figure 4-16: Configuring Proxy Address for Swisscom SIP Trunk

The screenshot shows a window titled "Proxy Address" with a "GENERAL" tab. The configuration fields are as follows:

Parameter	Value
Index	0
Proxy Address	10.1.200.3:5060
Transport Type	UDP

- c. Configure the address of the Proxy Set according to the parameters described in the table below.

Parameter	Value
Index	0
Proxy Address	10.1.200.3:5060 (IP address / FQDN and destination port)
Transport Type	UDP

- d. Click **Apply**.

3. Add a Proxy Set for the Teams Direct Routing as shown below:

Parameter	Value
Index	2
Name	Teams (arbitrary descriptive name)
SBC IPv4 SIP Interface	Teams
Proxy Keep-Alive	Using Options
Proxy Hot Swap	Enable
Proxy Load Balancing Method	Random Weights
DNS Resolve Method	SRV

Figure 4-17: Configuring Proxy Set for Microsoft Teams Direct Routing

- a. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
- b. Click **New**; the following dialog box appears:

Figure 4-18: Configuring Proxy Address for Microsoft Teams Direct Routing Interface

- c. Configure the address of the Proxy Set according to the parameters described in the table below.

Parameter	Value
Index	0
Proxy Address	teams.local (Teams Direct Routing FQDN)
Transport Type	TLS

- d. Click **Apply**.

The configured Proxy Sets are shown in the figure below:

Figure 4-19: Configured Proxy Sets in Proxy Sets Table

Proxy Sets (3)							
+ New		Edit					
				Page 1 of 1		Show 10 records per page	
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	--	SwisscomSBCon	60		Disable
1	SwisscomSBCon	DefaultSRD	--	SwisscomSBCon	10		Disable
2	Teams	DefaultSRD	--	Teams	60		Enable

4.7 Configure the Internal SRV Table

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

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

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

Table 4-1: Configuration Example of the Internal SRV Table

Parameter	Value
Domain Name	teams.local (FQDN is case-sensitive; configure in line with the configuration of the Teams Proxy Set)
Transport Type	TLS
1st ENTRY	
DNS Name 1	sip.pstnhub.microsoft.com
Priority 1	1
Weight 1	1
Port 1	5061
2nd ENTRY	
DNS Name 2	sip2.pstnhub.microsoft.com
Priority 2	2
Weight 2	1
Port 2	5061
3rd ENTRY	
DNS Name 3	sip3.pstnhub.microsoft.com
Priority 3	3
Weight 3	1
Port 3	5061

Figure 4-20: Example of the Internal SRV Table

The screenshot displays the AudioCodes M800B configuration interface. The top navigation bar includes tabs for SETUP, MONITOR, and TROUBLESHOOT. The left sidebar shows the NETWORK VIEW with categories like CORE ENTITIES, SECURITY, QUALITY, DNS, WEB SERVICES, HTTP PROXY, RADIUS & LDAP, and ADVANCED. The DNS section is expanded, showing Internal DNS (0) and Internal SRV (1). The Internal SRV (1) section displays a table with one entry (Index 0) for the domain teams.local, using TLS transport. Below the table, the configuration details for entry #0 are shown, including General settings (Domain Name: teams.local, Transport Type: TLS) and three entries (1ST, 2ND, and 3RD) with their respective DNS names, priorities, weights, and ports.

Internal SRV (1)

+ New Edit [trash icon] Page 1 of 1 Show 10 records per page

INDEX	DOMAIN NAME	TRANSPORT TYPE	DNS NAME 1	DNS NAME 2	DNS NAME 3
0	teams.local	TLS	sip.pstnhub.microsoft.com	sip2.pstnhub.microsoft.co	sip3.pstnhub.microsoft.co

#0 Edit

GENERAL

- Domain Name: teams.local
- Transport Type: TLS

1ST ENTRY

- DNS Name 1: sip.pstnhub.microsoft.com
- Priority 1: 1
- Weight 1: 1
- Port 1: 5061

2ND ENTRY

- DNS Name 2: sip2.pstnhub.microsoft.com
- Priority 2: 2
- Weight 2: 1
- Port 2: 5061

3RD ENTRY

- DNS Name 3: sip3.pstnhub.microsoft.com
- Priority 3: 3
- Weight 3: 1
- Port 3: 5061

4.8 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 assign 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	AudioCodersGroups_1
Coder Name	▪ SILK-NB ▪ SILK-WB ▪ G.711 A-law ▪ G.711 U-law ▪ G.729

Figure 4-21: 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 assign 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 4-22: 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	0
Coder	G.711 A-law
Index	1
Coder	G.729
Index	2
Coder	G.722

Figure 4-23: 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.

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

Figure 4-24: SBC Preferences Mode

Media Settings

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

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

4.9 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 UDP
- 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
General	
Index	1
Name	Swisscom
Media Security	
SBC Media Security Mode	RTP
SBC Media	
Allowed Audio Coders	Swisscom-AllowedAudioCoders
Allowed Coders Mode	Restriction and Preference (reorganize coders according to Allowed Coders list and restrict all other)
SBC Signaling	
P-Asserted-Identity Header Mode	Add (required for anonymous calls)
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally
Remote Replaces Mode	Handle Locally
Play RBT To Transferee	Yes
Remote 3xx Mode	Handle Locally
SBC Hold	
Remote Hold Format	Send Only

Figure 4-25: 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
General	
Index	2
Name	Teams (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	SRTP
SBC Early Media	
Remote Early Media RTP Detection Mode	By Media (required, as Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18x response)
Generate RTP	Until RTP Detected
SBC Media	
Extension Coders Group	AudioCodersGroups_1
ICE Mode	Lite (required only when Media Bypass enabled on Teams)
SBC Signaling	

Remote re-INVITE Support	Supported Only With SDP
Remote Delayed Offer Support	Not Supported
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally
Remote 3xx Mode	Handle Locally

Figure 4-26: Configuring IP Profile for Teams Direct Routing

IP Profiles [Teams]

GENERAL

Index: 2

Name: Teams

Created by Routing Server: No

MEDIA SECURITY

SBC Media Security Mode: SRTP

Gateway Media Security Mode: Preferable

Symmetric MKI: Enable

MKI Size: 0

SBC Enforce MKI Size: Don't enforce

SBC Media Security Method: SDES

Reset SRTP Upon Re-key: Disable

SBC SIGNALING

PRACK Mode: Transparent

P-Asserted-Identity Header Mode: As Is

Diversion Header Mode: As Is

History-Info Header Mode: As Is

Session Expires Mode: Transparent

Remote Update Support: Supported

Remote re-INVITE: Supported only with SDP

Remote Delayed Offer Support: Not Supported

Remote Representation Mode: According to Operation Mode

Keep Incoming Via Headers: According to Operation Mode

Keep Incoming Routing Headers: According to Operation Mode

Keep User-Agent Header: According to Operation Mode

Cancel APPLY

3. Click **Apply**.

4.10 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 WAN
- 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	1
Name	SwisscomSBCon
Type	Server
Proxy Set	SwisscomSBCon
IP Profile	Swisscom
Media Realm	MR-SIPTrunk
SIP Group Name	10.200.1.3 (according to requirement)

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

Parameter	Value
Index	2
Name	Teams
Topology Location	Up
Type	Server
Proxy Set	Teams
IP Profile	Teams
Media Realm	MR-Teams
SIP Group Name	teams-sbc.your.domain.com (according to requirement)
Classify By Proxy Set	Disable
Local Host Name	teams-sbc.your.domain.com (FQDN name of your tenant in the SBC)
Always Use Src Address	Yes
DTLS Context	default (TLS context, configured in Section 4.3.2)

The configured IP Groups are shown in the figure below:

Figure 4-27: 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	SwisscomSBCon	 DefaultSRD	Server	Not Configured	SwisscomSBCon	Swisscom	MR-SIPTrunk	10.200.1.3	Enable	-1	4
2	Teams	 DefaultSRD	Server	Not Configured	Teams	Teams	MR-Teams	teams-sbc.your.c	Disable	-1	-1

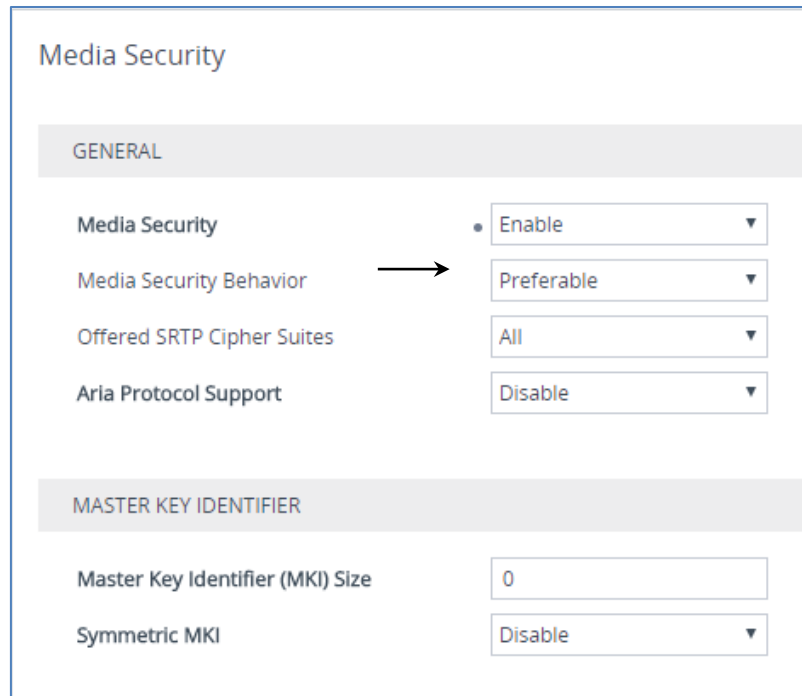
4.11 Configure SRTP

This step describes how to configure media security. The Direct Routing Interface require 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 4-28: Configuring SRTP



The screenshot shows the 'Media Security' configuration page. It is divided into two main sections: 'GENERAL' and 'MASTER KEY IDENTIFIER'.

GENERAL Section:

- Media Security:** A dropdown menu with 'Enable' selected.
- Media Security Behavior:** A dropdown menu with 'Preferable' selected. An arrow points from this field to the 'Media Security' dropdown.
- Offered SRTP Cipher Suites:** A dropdown menu with 'All' selected.
- Aria Protocol Support:** A dropdown menu with 'Disable' selected.

MASTER KEY IDENTIFIER Section:

- Master Key Identifier (MKI) Size:** A text input field with '0' entered.
- Symmetric MKI:** A dropdown menu with 'Disable' selected.

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

4.12 Configuring Message Condition Rules

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

Following Condition verifies that the Contact header contains Teams FQDN.

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

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

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

Figure 4-29: 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**.

4.13 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
Destination Host	teams-sbc.your.domain.com
Message Condition	Teams-Contact
Action Type	Allow
Source IP Group	Teams

Figure 4-30: Configuring Classification Rule

Classification [Teams]

SRD: #0 [DefaultSRD]

MATCH		ACTION	
Index	1	Action Type	Allow
Name	Teams	Destination Routing Policy	-- View
Source SIP Interface	#1 [Teams] View	Source IP Group	#2 [Teams] View
Source IP Address		IP Profile	--
Source Transport Type	Any		
Source Port	0		
Source Username Pattern	*		
Source Host	*		
Destination Username Pattern	*		
Destination Host	teams-sbc.your.domain.com		

Cancel APPLY

3. Click **Apply**.

4.14 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 4.10 on page 37,) 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 and Swisscom SIP Trunk:

- Terminate SIP OPTIONS messages on the SBC that are received from the DMZ
- 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 a rule to terminate SIP OPTIONS messages received from the both LAN and DMZ:
 - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	0
Name	Terminate OPTIONS (arbitrary descriptive name)
Source IP Group	Any
Request Type	OPTIONS
Destination Type	Dest Address
Destination Address	internal

Figure 4-31: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS

The screenshot shows the 'IP-to-IP Routing [Terminate OPTIONS]' configuration window. At the top, the 'Routing Policy' is set to '#0 [Default_SBCRoutingPolicy]'. The window is divided into two main sections: 'GENERAL' and 'ACTION'.

GENERAL Section:

- Index:** 0
- Name:** Terminate OPTIONS
- Alternative Route Options:** Route Row
- MATCH Section:**
 - Source IP Group:** Any
 - Request Type:** OPTIONS
 - Source Username Pattern:** *
 - Source Host:** *
 - Source Tag:** (empty)

ACTION Section:

- Destination Type:** Dest Address
- Destination IP Group:** --
- Destination SIP Interface:** --
- Destination Address:** internal
- Destination Port:** 0
- Destination Transport Type:** (empty)
- IP Group Set:** --
- Call Setup Rules Set ID:** -1
- Group Policy:** Sequential
- Cost Group:** --

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

- b. Click **Apply**.

3. Configure a rule to terminate REFER messages to Teams Direct Routing:
 - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	1
Route Name	Refer from Teams (arbitrary descriptive name)
Source IP Group	Any
Call Triger	REFER
ReRoute IP Group	Teams
Destination Type	Request URI
Destination IP Group	Teams

Figure 4-32: Configuring IP-to-IP Routing Rule for REFER from Teams

IP-to-IP Routing [Refer from Teams]

Routing Policy: #0 [Default_SBCRoutingPolicy]

GENERAL

Index: 1

Name: Refer from Teams

Alternative Route Options: Route Row

MATCH

Source IP Group: Any

Request Type: All

Source Username Pattern: *

Source Host: *

Source Tag:

ACTION

Destination Type: Request URI

Destination IP Group: #2 [Teams]

Destination SIP Interface: --

Destination Address:

Destination Port: 0

Destination Transport Type:

IP Group Set: --

Call Setup Rules Set ID: -1

Group Policy: Sequential

Cost Group: --

Cancel APPLY

- b. Click **Apply**.

4. Configure a rule to route calls from Teams Direct Routing to Swisscom SIP Trunk:
 - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	2
Route Name	Teams to SwisscomSBCon (arbitrary descriptive name)
Source IP Group	Teams
Destination Type	IP Group
Destination IP Group	SwisscomSBCon

Figure 4-33: Configuring IP-to-IP Routing Rule for Teams to SwisscomSBCon

The screenshot shows the 'IP-to-IP Routing' configuration window for a rule named 'Teams to SwisscomSBCon'. The window has a title bar with the rule name and standard window controls. Below the title bar, there is a 'Routing Policy' dropdown set to '#0 [Default_SBCRoutingPolicy]'. The configuration is divided into two main sections: 'GENERAL' and 'ACTION'.

GENERAL Section:

- Index:** 2
- Name:** Teams to SwisscomSBCon
- Alternative Route Options:** Route Row

MATCH Section:

- Source IP Group:** #2 [Teams] (with a 'View' link)
- Request Type:** All
- Source Username Pattern:** *
- Source Host:** *
- Source Tag:** (empty)

ACTION Section:

- Destination Type:** IP Group
- Destination IP Group:** #1 [SwisscomSBCon] (with a 'View' link)
- Destination SIP Interface:** .. (with a 'View' link)
- Destination Address:** (empty)
- Destination Port:** 0
- Destination Transport Type:** (empty)
- IP Group Set:** .. (with a 'View' link)
- Call Setup Rules Set ID:** -1
- Group Policy:** Sequential
- Cost Group:** .. (with a 'View' link)

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

- b. Click **Apply**.

5. Configure rule to route calls from Swisscom SIP Trunk to Teams Direct Routing:
 - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	3
Route Name	SwisscomSBCon to Teams (arbitrary descriptive name)
Source IP Group	SwisscomSBCon
Destination Type	IP Group
Destination IP Group	Teams

Figure 4-34: Configuring IP-to-IP Routing Rule for SwisscomSBCon to Teams

The screenshot shows the 'IP-to-IP Routing' configuration window for the rule 'SwisscomSBCon to Teams'. The window is divided into several sections:

- Routing Policy:** A dropdown menu showing '#0 [Default_SBCRoutingPolicy]'.
- GENERAL:**
 - Index: 4
 - Name: SwisscomSBCon to Teams
 - Alternative Route Options: Route Row
- MATCH:**
 - Source IP Group: #1 [SwisscomSBCon] (with a 'View' link)
 - Request Type: All
 - Source Username Pattern: *
 - Source Host: *
 - Source Tag: (empty)
- ACTION:**
 - Destination Type: IP Group
 - Destination IP Group: #2 [Teams] (with a 'View' link)
 - Destination SIP Interface: #1 [Teams] (with a 'View' link)
 - Destination Address: (empty)
 - Destination Port: 0
 - Destination Transport Type: (empty)
 - IP Group Set: -- (with a 'View' link)
 - Call Setup Rules Set ID: -1
 - Group Policy: Sequential
 - Cost Group: -- (with a 'View' link)

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

- b. Click **Apply**.

The configured routing rules are shown in the figure below:

Figure 4-35: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing (4)

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

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 O	Default_SBC	Route Row	Any	OPTIONS	*	*	Dest Address	--	--	internal
1	Refer from T	Default_SBC	Route Row	Any	All	*	*	Request URI	Teams	--	
2	Teams to Sw	Default_SBC	Route Row	Teams	All	*	*	IP Group	SwisscomSB	--	
4	SwisscomSB	Default_SBC	Route Row	SwisscomSB	All	*	*	IP Group	Teams	Teams	



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

4.15 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 4.10 on page 44) 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, a manipulation is configured to introduce anonymous call when dialing “+41*31” prefix from any IP Group to the Swisscom SIP Trunk IP Group.

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

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

Parameter	Value
Index	0
Name	For Anonymous Calls
Source IP Group	Any
Destination IP Group	SwisscomSBCon
Destination Username Prefix	+41*31
Manipulated Item	Source URI
Privacy Restriction Mode	Restrict

Figure 4-36: Configuring IP-to-IP Outbound Manipulation Rule

Outbound Manipulations [For Anonymous Calls]

Routing Policy: #0 [Default_SBCRoutingPolicy]

GENERAL

Index: 0

Name: For Anonymous Calls

Additional Manipulation: No

Call Trigger: Any

MATCH

Request Type: All

Source IP Group: Any

Destination IP Group: #1 [SwisscomSBCon]

Source Username Pattern: *

ACTION

Manipulated Item: Source URI

Remove From Left: 0

Remove From Right: 0

Leave From Right: 255

Prefix to Add:

Suffix to Add:

Privacy Restriction Mode: Restrict

Buttons: Cancel, APPLY

3. Click **Apply**.

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

Figure 4-37: 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 USER NAME / PATTERN	DESTINATION USER NAME / PATTERN	MANIPULATION ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT	PREFIX TO ADD	SUFFIX TO ADD
0	For Anon	Default_S	No	Any	Swisscom	*	+41*31	Source U	0	0	255		
1	For Anon	Default_S	No	Any	Swisscom	*	+41*31	Destinati	6	0	255		

Rule Index	Description
0	Calls from Any IP Group to SwisscomSBCOn IP Group with the prefix destination number "+41*31", apply restriction policy on the source number.
1	Calls from Any IP Group to SwisscomSBCOn IP Group with the prefix destination number "+41*31", remove 6 digits (+41*31) from this prefix.

4.16 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 4-38: Configuring SIP Message Manipulation Rule 0 (for Swisscom SIP Trunk)

Message Manipulations [Call Transfer]

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

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

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 4-39: 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 4-40: Configuring SIP Message Manipulation Rule 2 (for Swisscom SIP Trunk)

Message Manipulations [Call Transfer]

GENERAL

Index: 2

Name: • Call Transfer

Manipulation Set ID: • 4

Row Role: • Use Previous Condition ▼

ACTION

Action Subject: • header.referred-by

Action Type: • Remove ▼

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	3
Name	Call Forward
Manipulation Set ID	4
Message Type	any
Condition	Header.History-Info exists
Action Subject	Header.Diversion
Action Type	Add
Action Value	Header.History-Info.HistoryInfo

Figure 4-41: 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 APPLY

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

Message Manipulations [Call Forward] — x

GENERAL		ACTION	
Index	4	Action Subject	Header.Diversion Editor
Name	Call Forward	Action Type	Normalize ▼
Manipulation Set ID	4	Action Value	Editor
Row Role	Use Previous Condition ▼		

MATCH	
Message Type	Editor
Condition	Editor

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

5. 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	5
Name	Call Forward
Manipulation Set ID	4
Row Role	Use Previous Condition
Message Type	
Condition	
Action Subject	Header.History-Info
Action Type	Remove
Action Value	

Figure 4-43: 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](#)

7. 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 4-44: Configuring SIP Message Manipulation Rule 6 (for Swisscom SIP Trunk)

Message Manipulations [Change Diversion Host]

GENERAL

Index

6

Name

Change Diversion Host

Manipulation Set ID

4

Row Role

Use Current Condition

ACTION

Action Subject

header.diversion.url.host

Editor

Action Type

Modify

Action Value

param.ipg.dst.host

Editor

MATCH

Message Type

invite.request

Editor

Condition

header.diversion exists

Editor

Cancel

APPLY

8. 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 the audio call is answered, 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’.

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 4-45: Configuring SIP Message Manipulation Rule 7 (for Swisscom SIP Trunk)

Message Manipulations [Remove 'a=inactive']

GENERAL

Index

7

Name

Remove 'a=inactive'

Manipulation Set ID

4

Row Role

Use Current Condition

ACTION

Action Subject

body.sdp

Editor

Action Type

Modify

Action Value

\$1+\$2+\$3+\$5

Editor

MATCH

Message Type

any.response

Editor

Condition

body.sdp regex (.*)(m=image 0)(.*)(a=inactive)(.*)

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 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 4-46: 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

10. 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	9
Name	For Forward Anonymous
Manipulation Set ID	4
Row Role	Use Previous Condition
Message Type	
Condition	
Action Subject	header.privacy
Action Type	Add
Action Value	'id'

Figure 4-47: 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](#)

11. 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	10
Name	For Forward Anonymous
Manipulation Set ID	4
Row Role	Use Previous Condition
Message Type	
Condition	
Action Subject	header.p-asserted-identity.url.user
Action Type	Modify
Action Value	header.diversion.url.user

Figure 4-48: 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

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	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 4-49: Configuring SIP Message Manipulation Rule 11 (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. 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 4-50: Configuring SIP Message Manipulation Rule 12 (for Swisscom SIP Trunk)

Message Manipulations [Add Require=timer] — x

GENERAL	ACTION
Index: 12	Action Subject: header.require Editor
Name: Add Require=timer	Action Type: Add
Manipulation Set ID: 4	Action Value: 'timer' Editor
Row Role: Use Current Condition	

MATCH
Message Type: any.response.200 Editor
Condition: header.session-expires exists Editor

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

14. 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 4-51: 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
Action Type: Remove
Action Value:

MATCH

Message Type: Invite
Condition:

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 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 4-52: Configuring SIP Message Manipulation Rule 14 (for Swisscom SIP Trunk)

Message Manipulations [Normalize SDP]

GENERAL

Index

14

Name

Normalize SDP

Manipulation Set ID

4

Row Role

Use Current Condition

ACTION

Action Subject

body.sdp

Editor

Action Type

Normalize

Action Value

Editor

MATCH

Message Type

any

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 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 4-53: Configuring SIP Message Manipulation Rule 15 (for Swisscom SIP Trunk)

Message Manipulations [To ITSP change R-URI 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

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 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 4-54: Configuring SIP Message Manipulation Rule 16 (for Swisscom SIP Trunk)

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

GENERAL

Index
16

Name
To ITSP change To Host to Dest. IP

Manipulation Set ID
4

Row Role
Use Current Condition

MATCH

Message Type
any

Condition

ACTION

Action Subject
header.to.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 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 4-55: Configuring SIP Message Manipulation Rule 17 (for Swisscom SIP Trunk)

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

GENERAL

Index

17

Name

To ITSP change From Host to local IP

Manipulation Set ID

4

Row Role

Use Current Condition

ACTION

Action Subject

header.from.url.host

Editor

Action Type

Modify

Action Value

header.contact.url.host

Editor

MATCH

Message Type

any

Editor

Condition

header.from.url !contains 'anonymous'

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 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 4-56: 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

Editor

Condition

Editor

ACTION

Action Subject

▪ header.p-asserted-identity.url.host

Editor

Action Type

▪ Modify

▼

Action Value

▪ header.contact.url.host

Editor

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 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 4-57: Configuring SIP Message Manipulation Rule 19 (for Swisscom SIP Trunk)

Message Manipulations [Remove ms-opaque from Contact]

GENERAL

Index
19

Name
Remove ms-opaque from Contact

Manipulation Set ID
4

Row Role
Use Current Condition

MATCH

Message Type
Invite
Editor

Condition
Editor

ACTION

Action Subject
Header.Contact.URL.Param.ms-opaqu
Editor

Action Type
Remove

Action Value
Editor

Cancel
APPLY

21. Configure another manipulation rule (Manipulation Set 10). This rule is applied to OPTIONS 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	20
Name	Options to Swisscom
Manipulation Set ID	10 (This Set will be activated as described in Section 4.17.2 on page 85)
Message Type	Options
Condition	param.message.address.dst.sipinterface=='0' (per SIP Interface Index value assigned to the Swisscom SIP Trunk)
Action Subject	header.request-uri.url.host
Action Type	Modify
Action Value	param.message.address.dst.address

Figure 4-58: Configuring SIP Message Manipulation Rule 20

Message Manipulations [Options to Swisscom]

GENERAL		ACTION	
Index	20	Action Subject	header.request-uri.url.host Editor
Name	Options to Swisscom	Action Type	Modify
Manipulation Set ID	10	Action Value	param.message.address.dst.address Editor
Row Role	Use Current Condition		

MATCH	
Message Type	Options Editor
Condition	param.message.address.dst.sipinterface=='0' Editor

Cancel [APPLY](#)

22. Configure another manipulation rule (Manipulation Set 10). This rule is applied to OPTIONS messages sent to the Swisscom SIP Trunk IP Group. This replaces the host part of the SIP To header with the Destination IP address.

Parameter	Value
Index	21
Name	Options to Swisscom
Manipulation Set ID	10 (This Set will be activated as described in Section 4.17.2 on page 85)
Message Type	Options
Condition	param.message.address.dst.sipinterface=='0' (per SIP Interface Index value assigned to the Swisscom SIP Trunk)
Action Subject	header.to.url.host
Action Type	Modify
Action Value	param.message.address.dst.address

Figure 4-59: Configuring SIP Message Manipulation Rule 21

Message Manipulations [Options to Swisscom]

GENERAL	ACTION
Index: 21	Action Subject: header.to.url.host Editor
Name: Options to Swisscom	Action Type: Modify
Manipulation Set ID: 10	Action Value: param.message.address.dst.address Editor
Row Role: Use Current Condition	

MATCH
Message Type: Options Editor
Condition: param.message.address.dst.sipinterface=='0' Editor

Cancel [APPLY](#)

Figure 4-60: Example of Configured SIP Message Manipulation Rules

Message Manipulations (24)								
+ New Edit Insert ↑ ↓ 🗑️ ⏪ ⏩ Page 1 of 3 Show 10 records per page 🔍								
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.hc	Use Current Con
1	Call Transfer	4			header.diversion	Add	header.referred-by	Use Previous Cor
2	Call Transfer	4			header.referred-by	Remove		Use Previous Cor
3	Call Forward	4	any	Header.History-Info	Header.Diversion	Add	Header.History-Info	Use Current Con
4	Call Forward	4			Header.Diversion	Normalize		Use Previous Cor
5	Call Forward	4			Header.History-Info	Remove		Use Previous Cor
6	Change Diversion	4	invite.request	header.diversion	header.diversion	Modify	param.ipg.dst.hc	Use Current Con
7	Remove 'a=inacti	4	any.response	body.sdp regex (	body.sdp	Modify	\$1+\$2+\$3+\$5	Use Current Con
8	For Forward And	4	any.request	header.from.url	header.from.url	Remove		Use Current Con
9	For Forward And	4			header.privacy	Add	'Id'	Use Previous Cor

The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set ID 4 and which are executed for messages sent to the Swisscom SIP Trunk IP. 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.	
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.

Rule Index	Rule Description	Reason for Introducing Rule
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.	
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.	

Rule Index	Rule Description	Reason for Introducing Rule
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 the 'ms-opaque' parameter from the SIP Contact header.	
20	This rule is applied to OPTIONS messages sent to the Swisscom SIP Trunk IP Group. This replaces the host part of the SIP Request-URI header with destination IP address.	These rules are needed to ensure that the SIP OPTIONS requests are sent to the correct IP address.
21	This rule is applied to OPTIONS messages sent to the Swisscom SIP Trunk IP Group. This replaces the host part of the SIP To header with destination IP address.	
22	This rule is applied to OPTIONS messages sent to the Teams-Tenant-1 IP Group. This replaces the user part of the SIP From header with the predefined value.	These rules required by Microsoft Teams Interface and needed to be configured per each Tenant (Customer).
23	This rule is applied to OPTIONS messages sent to the Teams-Tenant-1 IP Group. This replaces the host part of the SIP Contact header with the SBC FQDN.	

23. Assign Manipulation Set ID 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 'Outbound Message Manipulation Set' field to **4**.

Figure 4-61: Assigning Manipulation Set 4 to the Swisscom SIP Trunk IP Group

The screenshot shows the 'IP Groups [SwisscomSBCon]' configuration window. At the top, there is a dropdown for 'SRD' set to '#0 [DefaultSRD]'. Below this are two main sections: 'GENERAL' and 'QUALITY OF EXPERIENCE'. The 'GENERAL' section includes fields for Index (1), Name (SwisscomSBCon), Topology Location (Down), Type (Server), Proxy Set (#1 [SwisscomSBCon]), IP Profile (#1 [Swisscom]), Media Realm (#0 [MR-SIPTrunk]), Contact User, SIP Group Name (10.200.1.3), and Created By Routing Server (No). The 'QUALITY OF EXPERIENCE' section includes QoE Profile and Bandwidth Profile, both set to '--'. Below these is the 'MESSAGE MANIPULATION' section, which contains 'Inbound Message Manipulation Set' (-1), 'Outbound Message Manipulation Set' (4), and two 'Message Manipulation User-Defined String' fields, both set to 0. At the bottom, there is a section for 'SBC REGISTRATION AND AUTHENTICATION'. The window has 'Cancel' and 'APPLY' buttons at the bottom right.

- d. Click **Apply**.

4.17 Configure SIP OPTIONS Towards Teams

SIP OPTIONS is an important mechanism used to monitor the connectivity between the AudioCodes SBC and the Microsoft Phone System. The Microsoft Phone System requires the FQDN of the trunk, sent in the host part of the Contact header of SIP OPTIONS. The FQDN of the trunk is the name that was specified during the pairing that was performed in the customer's tenant, for example:

New-CSOnlinePSTNGateway -FQDN sbcX.Customers.ACeducation.info

By default, AudioCodes SBC send its own IP address in the Contact header of the SIP OPTIONS message:

Contact: <sip:96.66.240.133>;tag=1c153541232

However, it's mandatory by Microsoft, that the Contact header contains the FQDN of the SBC. Message Manipulation Rules used to configure sending the FQDN in the Contact header of SIP OPTIONS.

4.17.1 Configure FQDN in Contact Header of OPTIONS Message using Message Manipulations Set

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

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

Contact:123456789@sbcX.Customers.ACeducation.info

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

➤ 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 10) for OPTIONS messages sent towards Microsoft Teams. This replaces the user part of the SIP From Header.

Parameter	Value
Index	22
Name	Options to Teams
Manipulation Set ID	10
Message Type	Options
Condition	param.message.address.dst.sipinterface=='1' (per SIP Interface Index value assigned to Teams)
Action Subject	header.from.url.user
Action Type	Modify
Action Value	'sip:admin@teams-sbc.your.domain.com' (per network configuration)

Figure 4-62: Configuring SIP Message Manipulation Rule 22 (for OPTIONS toward Teams)

Message Manipulations [Options to Teams]

GENERAL		ACTION	
Index	22	Action Subject	header.from.url Editor
Name	Options to Teams	Action Type	Modify
Manipulation Set ID	10	Action Value	'sip:admin@teams-sbc.your.domain.com' Editor
Row Role	Use Current Condition		

MATCH	
Message Type	Options Editor
Condition	param.message.address.dst.sipinterface=='1' Editor

Cancel **APPLY**

3. Configure another manipulation rule (Manipulation Set 10) for OPTIONS messages sent towards Microsoft Teams. This replaces the host part of the SIP Contact Header.

Parameter	Value
Index	23
Name	Options to Teams
Manipulation Set ID	10
Message Type	Options
Condition	param.message.address.dst.sipinterface=='1' (per SIP Interface Index value assigned to Teams)
Action Subject	header.contact.url.host
Action Type	Modify
Action Value	'teams-sbc.your.domain.com' (per network configuration)

Figure 4-63: Configuring SIP Message Manipulation Rule 23 (for OPTIONS toward Teams)

Message Manipulations [Options to Teams]

GENERAL		ACTION	
Index	23	Action Subject	header.contact.url.host Editor
Name	Options to Teams	Action Type	Modify
Manipulation Set ID	10	Action Value	'teams-sbc.your.domain.com' Editor
Row Role	Use Current Condition		

MATCH	
Message Type	Options Editor
Condition	param.message.address.dst.sipinterface=='1' Editor

Cancel **APPLY**



Note: If modification of the OPTIONS Request-URI header itself is required, for example, instead of sending **OPTIONS 99.66.240.132 SIP/2.0** you need to send **OPTIONS sip:admin@teams-sbc.your.domain.com SIP/2.0**, you must specify the Action Subject **header.request-uri.url**.

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

4.17.2 Assigning Message Manipulation Set as Gateway Outbound Manipulation Set

To apply changes to the SIP Options messages, Message Manipulation Set needed to be configured as Gateway Outbound Manipulation Set.

➤ **To configure the Gateway Outbound Manipulation Set:**

1. Open the Admin page.
2. Append the case-sensitive suffix 'AdminPage' to the device's IP address in your Web browser's URL field (e.g., `http:// <SBC FQDN or IP >/AdminPage`).
3. In the left pane of the page that opens, click **ini Parameters**.

Figure 4-64: Configuring GW Outbound Manipulation Set via AdminPage

Parameter Name: GWOUTBOUNDMANIPULATIONSET

Enter Value: 10

Apply New Value

Output Window

```
Parameter Name: GWOUTBOUNDMANIPULATIONSET
Parameter New Value: 10
Parameter Description: Outbound manipulation set ID for GW - If configured,
applies for all outgoing INVITE requests.
```

4. Enter these values in the 'Parameter Name' and 'Enter Value' fields:

Parameter	Value
GWOUTBOUNDMANIPULATIONSET	10 (Message Manipulation Set ID configured in the previous step)

5. Click the **Apply New Value** button.
6. Click on **Back to Main**. On the main page, don't forget to save the configuration.

4.18 Configure Registration Accounts

This step describes how to configure SIP registration accounts. This is required so that the SBC can register with the Swisscom SIP Trunk on behalf of Teams Direct Routing. The Swisscom Smart Business Connect SIP Trunk requires registration and authentication to provide service.

In the interoperability test topology, the Served IP Group is Teams Direct Routing IP Group and the Serving IP Group is Swisscom SIP Trunk IP Group.

➤ **To configure a registration account:**

1. Open the Accounts table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**).
2. Click **New**.
3. Configure the account according to the provided information from , for example:

Parameter	Value
Served IP Group	Teams
Application Type	SBC
Serving IP Group	SwisscomSBCon
Host Name	As provided by the SIP Trunk provider
Register	Regular
Contact User	+41441234567 (trunk main line)
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

Figure 4-65: Configuring a SIP Registration Account

The screenshot shows the 'Accounts' configuration window with two tabs: 'GENERAL' and 'CREDENTIALS'. The 'GENERAL' tab is selected and contains the following fields:

- Index: 0
- Served Trunk Group: -1
- Application Type: SBC
- Served IP Group: #2 [Teams] (with a 'View' link)
- Serving IP Group: #1 [SwisscomSBCon] (with a 'View' link)
- Host Name: (empty field)
- Contact User: +41441234567
- Register: Regular
- Registrar Stickiness: Disable
- Registrar Search Mode: Current Working Server
- Reg Event Package Subscription: Disable
- Register by Served IP Group Status: Register Always

The 'CREDENTIALS' tab is partially visible and contains:

- User Name: User
- Password: (empty field)

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

4. Click **Apply**.

This page is intentionally left blank.

4.19 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

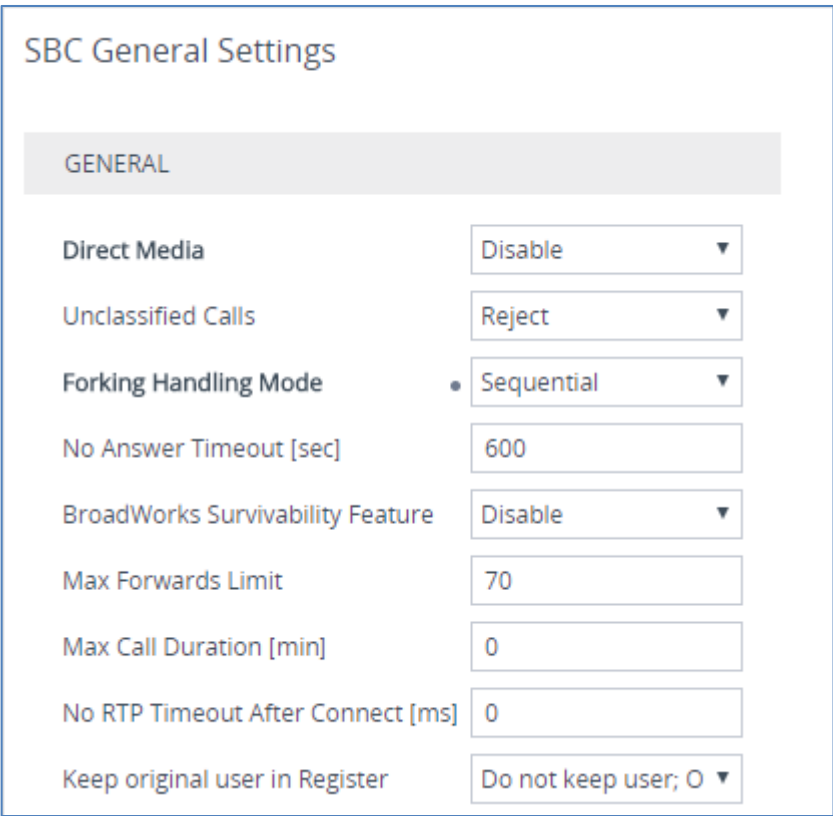
4.19.1 Configure Call Forking Mode

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 4-66: 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**.

This page is intentionally left blank.

A AudioCodes INI File

The *ini* configuration file of the SBC, corresponding to the Web-based configuration as described in Section 4 on page 15, is shown below:



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

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

;Board: Mediant VE SBC
;HW Board Type: 73 FK Board Type: 79
;Serial Number: 25865974047610
;Slot Number: 1
;Software Version: 7.20A.202.203
;ISO Version: Mediant Software E-SBC (ver 7.20A.156.028)
;DSP Software Version: SOFTDSP => 710.07
;Board IP Address: 10.1.62.250
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 10.1.62.1
;Ram size: 3803M   Flash size: 0M
;Num of DSP Cores: 1   Num DSP Channels: 1022
;Profile: NONE
;;;Key features;;Board Type: Mediant VE SBC ;DATA features: ;Coders: G723
G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB
G722 EG711 MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB OPUS_NB
OPUS_WB ;IP Media: Conf VXML VoicePromptAnnounc(H248.9) ;QOE features:
VoiceQualityMonitoring MediaEnhancement ;Channel Type: DspCh=50 ;HA ;DSP
Voice features: RTCP-XR AMRPolicyManagement ;Security: IPSEC
MediaEncryption StrongEncryption EncryptControlProtocol ;Control
Protocols: MSFT TRANSCODING=15 FEU=20 TestCall=10 SIPRec=5 CODER-
TRANSCODING=15 WebRTC MGCP SIP SBC=15 ;Default features;;Coders: G711
G726;

;MAC Addresses in use:
;-----
;GROUP_1 - 00:15:5d:00:7e:ba
;GROUP_2 - 00:15:5d:00:7e:bb
;GROUP_3 - 00:15:5d:00:7e:d1
;-----

[SYSTEM Params]

SyslogServerIP = 10.1.62.251
EnableSyslog = 1

[BSP Params]

PCMLawSelect = 3
UdpPortSpacing = 10
```

```

EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95
SbcPerformanceProfile = 2

[ControlProtocols Params]

AdminStateLockControl = 0

[Voice Engine Params]

PrerecordedTonesFileName = 'AC_PRT_SwisscomRingbackTone_Alwa_uLaw.dat'
ENABLEMEDIASECURITY = 1

[WEB Params]

UseProductName = 1
;HTTPSPKeyFileName is hidden but has non-default value
FaviconCurrentVersion = 4
Languages = 'en-US', '', '', '', '', '', '', '', ''

[SIP Params]

GWDEBUGLEVEL = 5
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENABLESYMMETRICMKI = 1
SBCPREFERENCESMODE = 1
GWOUTBOUNDMANIPULATIONSET = 10
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 104
ANSWERDETECTORCMD = 12582952
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[SNMP Params]

[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName,
DeviceTable_Tagging, DeviceTable_MTU;
DeviceTable 0 = 1, "GROUP_1", "vlan 1", 0, 1500;
DeviceTable 1 = 2, "GROUP_2", "vlan 2", 0, 1500;

[ \DeviceTable ]

[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.1.62.250, 24, 10.1.62.1, "LAN_IF", 8.8.8.8,
0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 212.243.144.61, 26, 212.243.144.1, "WAN_IF",
0.0.0.0, 0.0.0.0, "vlan 2";

```

```

[ \InterfaceTable ]

[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_CliSessionLimit, WebUsers_SessionTimeout, WebUsers_BlockTime,
WebUsers_UserLevel, WebUsers_PwNonce, WebUsers_SSHPublicKey;
WebUsers 0 = "Admin",
"$1$fR5GHLWwsLuw5uK27L6+vL287Lv1p/Sq8KDwrqH9+Kytq/+pxZaRkZCRkp/MnMvPnprMy
YjU0NWEjdfW3oyP3Yk=", 1, 0, 5, -1, 15, 60, 200,
"91813853665273bf4552f905ecaf1ca6", "";
WebUsers 1 = "User",
"$1$a1IKD1pZQhBHQkJNQRIZQE9JTB1JSrO0sbvn4bezvbq5vrTru7zzoKqip6Gioqih/6yp+
K2smZGblZeWl8WRz88=", 1, 0, 5, -1, 15, 60, 50,
"011e60c953b0a2238f7c737c9fc641b6", "";

[ \WebUsers ]

[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_DTLSVersion, TLSContexts_ServerCipherString,
TLSContexts_ClientCipherString, TLSContexts_RequireStrictCert,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse, TLSContexts_DHKeySize;
TLSContexts 0 = "default", 4, 0, "RC4:EXP", "ALL:!ADH", 0, 0, 0.0.0.0,
0.0.0.0, 2560, 0, 1024;

[ \TLSContexts ]

[ AudioCodersGroups ]

FORMAT AudioCodersGroups_Index = AudioCodersGroups_Name;
AudioCodersGroups 0 = "AudioCodersGroups_0";
AudioCodersGroups 1 = "AudioCodersGroups_1";

[ \AudioCodersGroups ]

[ AllowedAudioCodersGroups ]

FORMAT AllowedAudioCodersGroups_Index = AllowedAudioCodersGroups_Name;
AllowedAudioCodersGroups 0 = "Swisscom-AllowedAudioCoders";

[ \AllowedAudioCodersGroups ]

[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupName, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ,

```

```

IpProfile_RTPRedundancyDepth, IpProfile_CNGmode,
IpProfile_VxxTransportType, IpProfile_NSEMode, IpProfile_IsDTMFUsed,
IpProfile_PlayRBTone2IP, IpProfile_EnableEarlyMedia,
IpProfile_ProgressIndicator2IP, IpProfile_EnableEchoCanceller,
IpProfile_CopyDest2RedirectNumber, IpProfile_MediaSecurityBehaviour,
IpProfile_CallLimit, IpProfile_DisconnectOnBrokenConnection,
IpProfile_FirstTxDtmfOption, IpProfile_SecondTxDtmfOption,
IpProfile_RxDTMFOption, IpProfile_EnableHold, IpProfile_InputGain,
IpProfile_VoiceVolume, IpProfile_AddIEInSetup,
IpProfile_SBCExtensionCodersGroupName,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedAudioCodersGroupName,
IpProfile_SBCAllowedVideoCodersGroupName, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCSendMultipleDTMFMethods,
IpProfile_SBCAssertIdentity, IpProfile_AMDSensitivityParameterSuit,
IpProfile_AMDSensitivityLevel, IpProfile_AMDMaxGreetingTime,
IpProfile_AMDMaxPostSilenceGreetingTime, IpProfile_SBCDiversiionMode,
IpProfile_SBCHistoryInfoMode, IpProfile_EnableQSIGTunneling,
IpProfile_SBCFaxCodersGroupName, IpProfile_SBCFaxBehavior,
IpProfile_SBCFaxOfferMode, IpProfile_SBCFaxAnswerMode,
IpProfile_SbcPrackMode, IpProfile_SBCSessionExpiresMode,
IpProfile_SBCRemoteUpdateSupport, IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTtoTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay,
IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCSDPHandleRTCPAttribute,
IpProfile_SBCRemoveCryptoLifetimeInSDP, IpProfile_SBCIceMode,
IpProfile_SBCRTCPMux, IpProfile_SBCMediaSecurityMethod,
IpProfile_SBCHandleXDetect, IpProfile_SBCRTCPFeedback,
IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders,
IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCRemoteMultipleEarlyDialogs,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag,
IpProfile_SBCAdaptRFC2833BWtoVoiceCoderBW,
IpProfile_CreatedByRoutingServer, IpProfile_SBCFaxReroutingMode,
IpProfile_SBCMaxCallDuration, IpProfile_SBCGenerateRTP,
IpProfile_SBCISUPBodyHandling, IpProfile_SBCISUPVariant,
IpProfile_SBCVoiceQualityEnhancement, IpProfile_SBCMaxOpusBW,
IpProfile_SBCEnhancedPlc, IpProfile_LocalRingbackTone,
IpProfile_LocalHeldTone, IpProfile_SBCGenerateNoOp,
IpProfile_SBCRemoveUnKnownCrypto;
IpProfile 1 = "Swisscom", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0,
0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", "", 0, 0,
"", "Swisscom-AllowedAudioCoders", "", 2, 2, 0, 0, 0, 1, 0, 8, 300, 400,
0, 0, 0, "", 0, 0, 1, 3, 0, 2, 2, 1, 3, 2, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0,
0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 300, -1, -1, 0, 0,
0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -
1, -1, 0, 0;

```

```

IpProfile 2 = "Teams", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0, 0,
2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "",
"AudioCodersGroups_1", 0, 0, "", "", "", 0, 1, 0, 0, 0, 0, 0, 8, 300,
400, 0, 0, 0, 0, "", 0, 0, 1, 3, 0, 2, 1, 0, 3, 2, 1, 0, 1, 1, 0, 0, 1, 0,
1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1,
0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 1, 0, 0, 0,
0, 0, -1, -1, 0, 0;

[ \IpProfile ]

[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_RemoteIPv4IF,
CpMediaRealm_RemoteIPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile,
CpMediaRealm_TopologyLocation;
CpMediaRealm 0 = "MR-SIPTrunk", "WAN_IF", "", "", "", 6000, 100, 6999, 0,
"", "", 0;
CpMediaRealm 1 = "MR-Teams", "WAN_IF", "", "", "", 7000, 100, 7999, 0,
"", "", 1;

[ \CpMediaRealm ]

[ SBCRoutingPolicy ]

FORMAT SBCRoutingPolicy_Index = SBCRoutingPolicy_Name,
SBCRoutingPolicy_LCREnable, SBCRoutingPolicy_LCRAverageCallLength,
SBCRoutingPolicy_LCRDefaultCost, SBCRoutingPolicy_LdapServerGroupName;
SBCRoutingPolicy 0 = "Default_SBCRoutingPolicy", 0, 1, 0, "";

[ \SBCRoutingPolicy ]

[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations, SRD_SharingPolicy,
SRD_UsedByRoutingServer, SRD_SBCOperationMode, SRD_SBCRoutingPolicyName,
SRD_SBCDialPlanName, SRD_AdmissionProfile;
SRD 0 = "DefaultSRD", 0, -1, 1, 0, 0, 0, "Default_SBCRoutingPolicy", "",
"";

[ \SRD ]

[ MessagePolicy ]

FORMAT MessagePolicy_Index = MessagePolicy_Name,
MessagePolicy_MaxMessageLength, MessagePolicy_MaxHeaderLength,
MessagePolicy_MaxBodyLength, MessagePolicy_MaxNumHeaders,
MessagePolicy_MaxNumBodies, MessagePolicy_SendRejection,
MessagePolicy_MethodList, MessagePolicy_MethodListType,
MessagePolicy_BodyList, MessagePolicy_BodyListType,
MessagePolicy_UseMaliciousSignatureDB;
MessagePolicy 0 = "Malicious Signature DB Protection", -1, -1, -1, -1, -
1, 1, "", 0, "", 0, 1;

```

```
[ \MessagePolicy ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_AdditionalUDPPorts, SIPInterface_SRDName,
SIPInterface_MessagePolicyName, SIPInterface_TLSContext,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer, SIPInterface_TopologyLocation,
SIPInterface_PreParsingManSetName, SIPInterface_AdmissionProfile;
SIPInterface 0 = "SwisscomSBCon", "WAN_IF", 2, 5060, 0, 0, "",
"DefaultSRD", "", "default", -1, 0, 500, -1, 0, "MR-SIPTrunk", 0, -1, -1,
-1, 0, 0, "", "";
SIPInterface 1 = "Teams", "WAN_IF", 2, 0, 0, 5061, "", "DefaultSRD", "",
"default", 0, 1, 0, -1, 0, "MR-Teams", 0, -1, -1, -1, 0, 1, "", "";

[ \SIPInterface ]

[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap,
ProxySet_SRDName, ProxySet_ClassificationInput, ProxySet_TLSContextName,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName,
ProxySet_SBCIPv4SIPInterfaceName, ProxySet_GWIPv6SIPInterfaceName,
ProxySet_SBCIPv6SIPInterfaceName, ProxySet_MinActiveServersLB,
ProxySet_SuccessDetectionRetries, ProxySet_SuccessDetectionInterval,
ProxySet_FailureDetectionRetransmissions;
ProxySet 0 = "ProxySet_0", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"", "SwisscomSBCon", "", "", 1, 1, 10, -1;
ProxySet 1 = "SwisscomSBCon", 1, 10, 0, 0, "DefaultSRD", 0, "", -1, -1,
"", "", "SwisscomSBCon", "", "", 1, 1, 10, -1;
ProxySet 2 = "Teams", 1, 60, 2, 1, "DefaultSRD", 0, "", -1, 1, "", "",
"Teams", "", "", 1, 1, 10, -1;

[ \ProxySet ]

[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnablesSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
```

```

IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID,
IPGroup_TopologyLocation, IPGroup_SBCDialPlanName,
IPGroup_CallSetupRulesSetId, IPGroup_Tags, IPGroup_SBCUserStickiness,
IPGroup_UserUDPPortAssignment, IPGroup_AdmissionProfile;
IPGroup 0 = 0, "Default_IPG", "ProxySet_0", "", "", -1, 0, "DefaultSRD",
"", 0, "", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "",
0, "0", "0", 0, 0, "default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, "";
IPGroup 1 = 0, "SwisscomSBCon", "SwisscomSBCon", "10.200.1.3", "", -1, 0,
"DefaultSRD", "MR-SIPTrunk", 1, "Swisscom", -1, -1, 4, 0, 0, "", 0, -1, -
1, "", "Admin", "$1$aCkNBwIC", 0, "", "", 0, "0", "0", 0, 0, "default",
0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, "";
IPGroup 2 = 0, "Teams", "Teams", "teams-sbc.your.domain.com", "", -1, 0,
"DefaultSRD", "MR-Teams", 0, "Teams", -1, -1, -1, 0, 0, "", 0, -1, -1, "
teams-sbc.your.domain.com", "Admin", "$1$aCkNBwIC", 0, "", "", 1, "0",
"0", 0, 0, "default", 0, 0, -1, 0, 0, 1, "", -1, "", 0, 0, "";

[ \IPGroup ]

[ Srv2Ip ]

FORMAT Srv2Ip_Index = Srv2Ip_InternalDomain, Srv2Ip_TransportType,
Srv2Ip_Dns1, Srv2Ip_Priority1, Srv2Ip_Weight1, Srv2Ip_Port1, Srv2Ip_Dns2,
Srv2Ip_Priority2, Srv2Ip_Weight2, Srv2Ip_Port2, Srv2Ip_Dns3,
Srv2Ip_Priority3, Srv2Ip_Weight3, Srv2Ip_Port3;
Srv2Ip 0 = "teams.local", 2, "sip.pstnhub.microsoft.com", 1, 1, 5061,
"sip2.pstnhub.microsoft.com", 2, 1, 5061, "sip3.pstnhub.microsoft.com",
3, 1, 5061;

[ \Srv2Ip ]

[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 0 = "1", 0, "10.1.200.3:5060", 0;
ProxyIp 1 = "2", 0, "teams.local", 2;

[ \ProxyIp ]

[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroupName, Account_ServingIPGroupName, Account_Username,
Account_Password, Account_HostName, Account_ContactUser,
Account_Register, Account_RegistrarStickiness,
Account_RegistrarSearchMode, Account_RegEventPackageSubscription,
Account_ApplicationType, Account_RegByServedIPG,
Account_UDPPortAssignment;
Account 0 = -1, "Teams", "SwisscomSBCon", "User", "$1$8oKSh4aBmIqd", "",
"+41441234567", 1, 0, 0, 0, 2, 0, 0;

[ \Account ]

[ ConditionTable ]

```

```

FORMAT ConditionTable_Index = ConditionTable_Name,
ConditionTable_Condition;
ConditionTable 0 = "Teams-Contact", "header.contact.url.host contains
'pstnhub.microsoft.com'";

[ \ConditionTable ]

[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_RoutingPolicyName, IP2IPRouting_SrcIPGroupName,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageConditionName,
IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger,
IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType,
IP2IPRouting_DestIPGroupName, IP2IPRouting_DestSIPInterfaceName,
IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup, IP2IPRouting_DestTags,
IP2IPRouting_SrcTags, IP2IPRouting_IPGroupSetName,
IP2IPRouting_RoutingTagName, IP2IPRouting_InternalAction;
IP2IPRouting 0 = "Terminate OPTIONS", "Default_SBCRoutingPolicy", "Any",
"*, ", ", ", ", ", 6, ", ", "Any", 0, -1, 1, ", ", ", ", "internal", 0, -1, 0,
0, ", ", ", ", ", ", "default", ";
IP2IPRouting 1 = "Refer from Teams", "Default_SBCRoutingPolicy", "Any",
"*, ", ", ", ", ", 0, ", ", "Teams", 2, -1, 2, "Teams", ", ", ", ", 0, -1, 0,
0, ", ", ", ", ", ", "default", ";
IP2IPRouting 2 = "Teams to SwisscomSBCon", "Default_SBCRoutingPolicy",
"Teams", ", ", ", ", ", ", ", 0, ", ", "Any", 0, -1, 0, "SwisscomSBCon", ", ",
", ", 0, -1, 0, 0, ", ", ", ", ", ", "default", ";
IP2IPRouting 4 = "SwisscomSBCon to Teams", "Default_SBCRoutingPolicy",
"SwisscomSBCon", ", ", ", ", ", ", ", 0, ", ", "Any", 0, -1, 0, "Teams",
"Teams", ", ", 0, -1, 0, 0, ", ", ", ", ", ", "default", ";

[ \IP2IPRouting ]

[ Classification ]

FORMAT Classification_Index = Classification_ClassificationName,
Classification_MessageConditionName, Classification_SRDName,
Classification_SrcSIPInterfaceName, Classification_SrcAddress,
Classification_SrcPort, Classification_SrcTransportType,
Classification_SrcUsernamePrefix, Classification_SrcHost,
Classification_DestUsernamePrefix, Classification_DestHost,
Classification_ActionType, Classification_SrcIPGroupName,
Classification_DestRoutingPolicy, Classification_IpProfileName;
Classification 1 = "Teams", "Teams-Contact", "DefaultSRD", "Teams", ", ",
0, -1, ", ", ", ", ", ", "teams-sbc.your.domain.com", 1, "Teams", ", ", ";

[ \Classification ]

[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_RoutingPolicyName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupName,

```

```

IPOutboundManipulation_DestIPGroupName,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageConditionName,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupName,
IPOutboundManipulation_Trigger, IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode,
IPOutboundManipulation_DestTags, IPOutboundManipulation_SrcTags;
IPOutboundManipulation 0 = "For Anonymous Calls",
"Default_SBCRoutingPolicy", 0, "Any", "SwisscomSBCon", "*", "*",
"+41*31", "*", "*", "", 0, "Any", 0, 0, 0, 0, 255, "", "", 2, "", "";
IPOutboundManipulation 1 = "For Anonymous Calls",
"Default_SBCRoutingPolicy", 0, "Any", "SwisscomSBCon", "*", "*",
"+41*31", "*", "*", "", 0, "Any", 0, 1, 6, 0, 255, "", "", 0, "", "";

[ \IPOutboundManipulation ]

[ MessageManipulations ]

FORMAT MessageManipulations Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Call Transfer", 4, "invite.request",
"header.referred-by exists", "header.referred-by.url.host", 2,
"param.ipg.dst.host", 0;
MessageManipulations 1 = "Call Transfer", 4, "", "", "header.diversion",
0, "header.referred-by", 1;
MessageManipulations 2 = "Call Transfer", 4, "", "", "header.referred-
by", 1, "", 1;
MessageManipulations 3 = "Call Forward", 4, "any", "Header.History-Info
exists", "Header.Diversion", 0, "Header.History-Info.HistoryInfo", 0;
MessageManipulations 4 = "Call Forward", 4, "", "", "Header.Diversion",
7, "", 1;
MessageManipulations 5 = "Call Forward", 4, "", "", "Header.History-
Info", 1, "", 1;
MessageManipulations 6 = "Change Diversion Host", 4, "invite.request",
"header.diversion exists", "header.diversion.url.host", 2,
"param.ipg.dst.host", 0;
MessageManipulations 7 = "Remove 'a=inactive'", 4, "any.response",
"body.sdp regex (.*) (m=image 0) (.*) (a=inactive) (.*)", "body.sdp", 2,
"$1+$2+$3+$5", 0;
MessageManipulations 8 = "For Forward Anonymous", 4, "any.request",
"header.from.url contains 'anonymous'", "header.from.url.userphone", 1,
"", 0;
MessageManipulations 9 = "For Forward Anonymous", 4, "", "",
"header.privacy", 0, "'id'", 1;
MessageManipulations 10 = "For Forward Anonymous", 4, "", "", "header.p-
asserted-identity.url.user", 2, "header.diversion.url.user", 1;
MessageManipulations 11 = "For Forward Anonymous", 4, "", "",
"header.from.url.host", 2, "'anonymous.invalid'", 1;
MessageManipulations 12 = "Add Require=timer", 4, "any.response.200",
"header.session-expires exists", "header.require", 0, "'timer'", 0;

```

```

MessageManipulations 13 = "Remove DisplayName", 4, "Invite", "",
"Header.From.QuoteDisplayName", 1, "", 0;
MessageManipulations 14 = "Normalize SDP", 4, "any", "", "body.sdp", 7,
"", 0;
MessageManipulations 15 = "To ITSP change R-URI Host to Dest. IP", 4,
"any", "", "header.request-uri.url.host", 2,
"param.message.address.dst.address", 0;
MessageManipulations 16 = "To ITSP change To Host to Dest. IP", 4, "any",
"", "header.to.url.host", 2, "param.message.address.dst.address", 0;
MessageManipulations 17 = "To ITSP change From Host to local IP", 4,
"any", "header.from.url !contains 'anonymous'", "header.from.url.host",
2, "header.contact.url.host", 0;
MessageManipulations 18 = "To ITSP change PAI Host to local IP", 4,
"any", "", "header.p-asserted-identity.url.host", 2,
"header.contact.url.host", 0;
MessageManipulations 19 = "Remove ms-opaque from Contact", 4, "Invite",
"", "Header.Contact.URL.Param.ms-opaque", 1, "", 0;
MessageManipulations 20 = "Options to Swisscom", 10, "Options",
"param.message.address.dst.sipinterface=='0'", "header.request-
uri.url.host", 2, "param.message.address.dst.address", 0;
MessageManipulations 21 = "Options to Swisscom", 10, "Options",
"param.message.address.dst.sipinterface=='0'", "header.to.url.host", 2,
"param.message.address.dst.address", 0;
MessageManipulations 22 = "Options to Teams", 10, "Options",
"param.message.address.dst.sipinterface=='1'", "header.from.url", 2,
"'sip:admin@teams-sbc.your.domain.com'", 0;
MessageManipulations 23 = "Options to Teams", 10, "Options",
"param.message.address.dst.sipinterface=='1'", "header.contact.url.host",
2, "'teams-sbc.your.domain.com'", 0;

[ \MessageManipulations ]

[ GwRoutingPolicy ]

FORMAT GwRoutingPolicy_Index = GwRoutingPolicy_Name,
GwRoutingPolicy_LCREnable, GwRoutingPolicy_LCRAverageCallLength,
GwRoutingPolicy_LCRDefaultCost, GwRoutingPolicy_LdapServerGroupName;
GwRoutingPolicy 0 = "GwRoutingPolicy", 0, 1, 0, "";

[ \GwRoutingPolicy ]

[ ResourcePriorityNetworkDomains ]

FORMAT ResourcePriorityNetworkDomains_Index =
ResourcePriorityNetworkDomains_Name,
ResourcePriorityNetworkDomains_Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 1;
ResourcePriorityNetworkDomains 2 = "dod", 1;
ResourcePriorityNetworkDomains 3 = "drsn", 1;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 1;

[ \ResourcePriorityNetworkDomains ]

[ MaliciousSignatureDB ]

```

```

FORMAT MaliciousSignatureDB_Index = MaliciousSignatureDB_Name,
MaliciousSignatureDB_Pattern;
MaliciousSignatureDB 0 = "SIPVicious", "Header.User-Agent.content prefix
'friendly-scanner'";
MaliciousSignatureDB 1 = "SIPScan", "Header.User-Agent.content prefix
'sip-scan'";
MaliciousSignatureDB 2 = "Smap", "Header.User-Agent.content prefix
'smap'";
MaliciousSignatureDB 3 = "Sipsak", "Header.User-Agent.content prefix
'sipsak'";
MaliciousSignatureDB 4 = "Sipcli", "Header.User-Agent.content prefix
'sipcli'";
MaliciousSignatureDB 5 = "Sivus", "Header.User-Agent.content prefix
'SIVuS'";
MaliciousSignatureDB 6 = "Gulp", "Header.User-Agent.content prefix
'Gulp'";
MaliciousSignatureDB 7 = "Sipv", "Header.User-Agent.content prefix
'sipv'";
MaliciousSignatureDB 8 = "Sundayddr Worm", "Header.User-Agent.content
prefix 'sundayddr'";
MaliciousSignatureDB 9 = "VaxIPUserAgent", "Header.User-Agent.content
prefix 'VaxIPUserAgent'";
MaliciousSignatureDB 10 = "VaxSIPUserAgent", "Header.User-Agent.content
prefix 'VaxSIPUserAgent'";
MaliciousSignatureDB 11 = "SipArmyKnife", "Header.User-Agent.content
prefix 'siparmyknife'";

[ \MaliciousSignatureDB ]

[ AllowedAudioCoders ]

FORMAT AllowedAudioCoders_Index =
AllowedAudioCoders_AllowedAudioCodersGroupName,
AllowedAudioCoders_AllowedAudioCodersIndex, AllowedAudioCoders_CoderID,
AllowedAudioCoders_UserDefineCoder;
AllowedAudioCoders 0 = "Swisscom-AllowedAudioCoders", 0, 1, "";
AllowedAudioCoders 1 = "Swisscom-AllowedAudioCoders", 1, 3, "";
AllowedAudioCoders 2 = "Swisscom-AllowedAudioCoders", 2, 20, "";

[ \AllowedAudioCoders ]

[ AudioCoders ]

FORMAT AudioCoders_Index = AudioCoders_AudioCodersGroupId,
AudioCoders_AudioCodersIndex, AudioCoders_Name, AudioCoders_pTime,
AudioCoders_rate, AudioCoders_PayloadType, AudioCoders_Sce,
AudioCoders_CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 0, 1, 2, 90, -1, 0, "";
AudioCoders 1 = "AudioCodersGroups_1", 0, 35, 2, 19, 103, 0, "";
AudioCoders 2 = "AudioCodersGroups_1", 1, 36, 2, 43, 104, 0, "";
AudioCoders 3 = "AudioCodersGroups_1", 2, 1, 2, 90, -1, 0, "";
AudioCoders 4 = "AudioCodersGroups_1", 3, 2, 2, 90, -1, 0, "";
AudioCoders 5 = "AudioCodersGroups_1", 4, 3, 2, 19, -1, 0, "";

[ \AudioCoders ]

```

International Headquarters

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

AudioCodes Inc.

27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

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

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

Document #: LTRT-14412

