Configuration Note

AudioCodes Professional Services – Interoperability Lab

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

Version 7.2

Table of Contents

Notice

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

This document is subject to change without notice.

Date Published: July-17-2019

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.

Document Revision Record

LTRT	Description
33410	Initial document release for Version 7.2.

Documentation Feedback

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

This page is intentionally left blank.

1 Introduction

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

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

1.1 Intended Audience

This document is intended for engineers, or AudioCodes and autphone partners who are responsible for installing and configuring autphone's SIP Trunk and Microsoft's Teams Direct Routing Service in Enterprise Model 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 the Microsoft Phone System. The customer-provided SBC can be connected to almost any telephony trunk, or connect with third-party PSTN equipment. The connection allows:

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

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes SBC Version

Table 2-1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500 Gateway & E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 800C Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant 4000B SBC ▪ Mediant 9000 SBC ▪ Mediant 9030 SBC ▪ Mediant 9080 SBC ▪ Mediant Software SBC (VE/SE/CE)
Software Version	7.20A.250.273
Protocol	▪ SIP/UDP (to the autphone SIP Trunk) ▪ SIP/TLS (to the Teams Direct Routing)
Additional Notes	None

2.2 autphone SIP Trunking Version

Table 2-2: autphone Version

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

2.3 Microsoft Teams Direct Routing Version

Table 2-3: Microsoft Teams Direct Routing Version

Vendor	Microsoft
Model	Teams Phone System Direct Routing
Software Version	Release v.2019.4.24.4 i.EUWE.1
Protocol	SIP
Additional Notes	None

2.4 Interoperability Test Topology

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

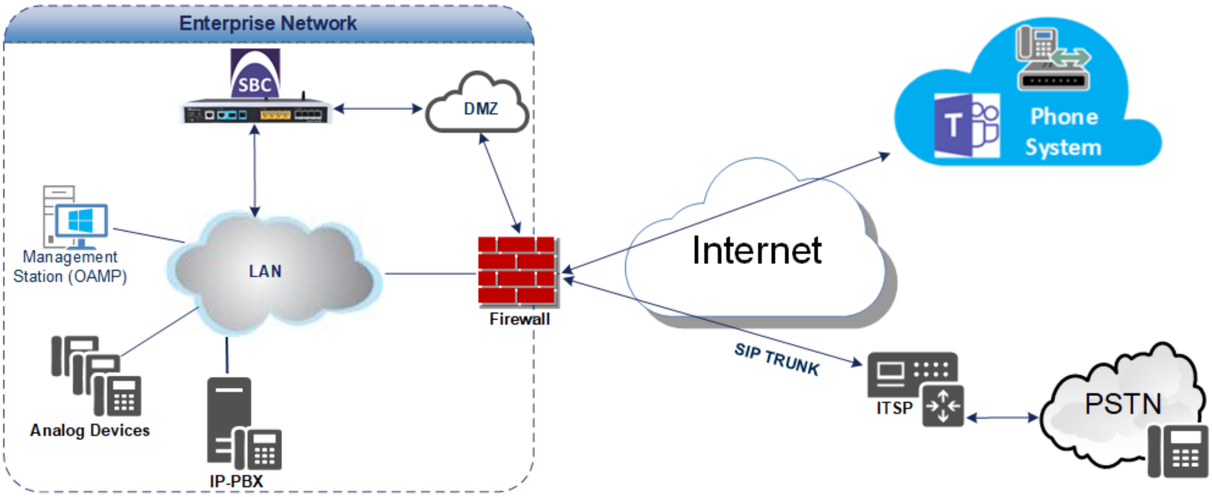
2.4.1 Enterprise Model Implementation

The interoperability testing between AudioCodes SBC and autphone 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 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 autphone's SIP Trunking service
- AudioCodes SBC is implemented to interconnect between the SIP Trunk and Teams Direct Routing located in the WAN
    - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
    - **Border:** IP-to-IP network border - the autphone's SIP Trunk is located in the Enterprise LAN (or WAN) and the Teams Phone Systems is located in the public network.

The figure below illustrates this interoperability test topology:

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



2.4.2 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

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

2.4.3 Infrastructure Prerequisites

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

Table 2-5: Infrastructure Prerequisites

Infrastructure Prerequisite	Details
Certified Session Border Controller (SBC)	See Microsoft's document *Deploying Direct Routing Guide.*
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 limitation was observed during interoperability tests performed for AudioCodes SBC interworking between Microsoft Teams Direct Routing and autphone's SIP Trunk:

- If the Microsoft Teams Direct Routing sends one of the following error responses:
  - 500 Server Internal Error
  - 503 Service Unavailable
  - 603 Decline

  autphone SIP Trunk still sends re-INVITEs and does not disconnect the call.

  To disconnect the call, a message manipulation rule is used to replace the above error response with the '486 Busy Here' response (see Section 4.15 on page 59).

3 Configuring Teams Direct Routing

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

3.1 Prerequisites

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

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

3.2 SBC Domain Name in the Teams Enterprise Model

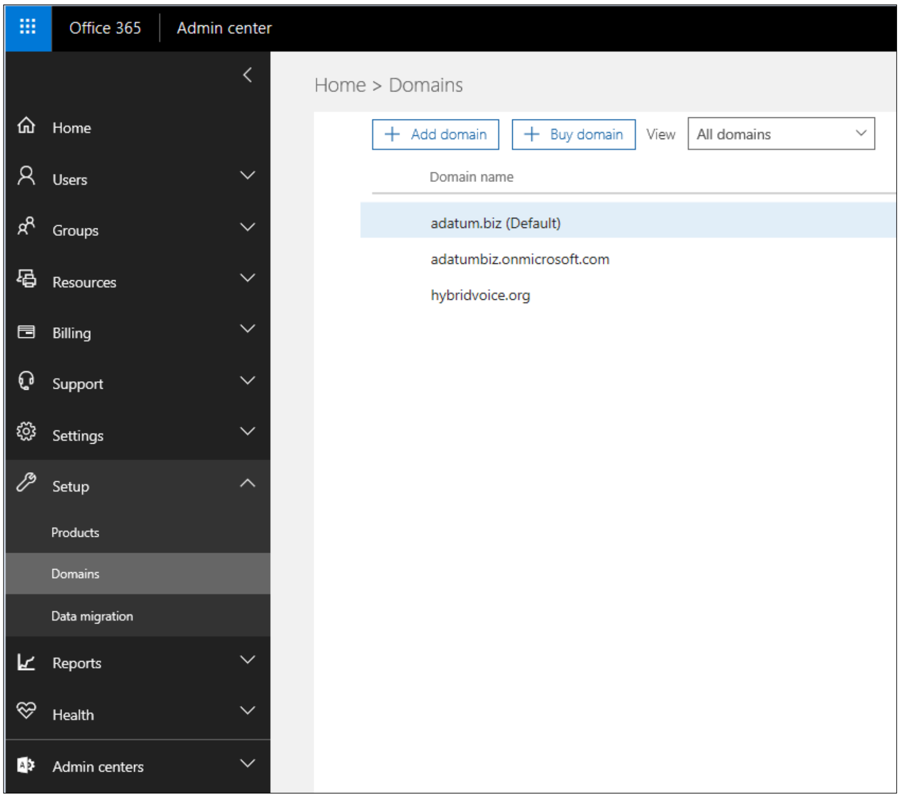
The SBC domain name must be from one of the names registered in 'Domains' of the tenant. You cannot use the ***.onmicrosoft.com** tenant for the domain name. For example, in Figure 2-2, the administrator registered the following DNS names for the tenant:

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



3.3 Example of the Office 365 Tenant Direct Routing Configuration

3.3.1 Online PSTN Gateway Configuration

Use following PowerShell command for creating new Online PSTN Gateway:

New-CsOnlinePSTNGateway *-Identity* ***sbc.aceducation.info*** *-SipSignallingPort* ***5061*** *-ForwardCallHistory $True -ForwardPai $True -MediaBypass $True -Enabled $True*

3.3.2 Online PSTN Usage Configuration

Use following PowerShell command for creating an empty PSTN Usage:

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

3.3.3 Online Voice Route Configuration

Use following PowerShell command for creating new Online Voice Route and associate it with PSTN Usage:

New-CsOnlineVoiceRoute *-Identity* ***"audc-interop"*** *-NumberPattern "^\+" -OnlinePstnGatewayList* ***sbc.aceducation.info*** *-Priority 1 -OnlinePstnUsages* ***"Interop"***

3.3.4 Online Voice Routing Policy Configuration

Use following PowerShell command for assigning the Voice Route to the PSTN Usage:

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

> **Note:** The commands specified in Sections 3.3.5 and 3.3.6, should be run for each Teams user in the company tenant.

3.3.5 Enable Online User

Use following PowerShell command for enabling online user:

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

3.3.6 Assigning Online User to the Voice Route

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

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

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

- **Get-CsOnlinePSTNGateway**

```
Identity                          : sbc.ACeducation.info
Fqdn                              : sbc.ACeducation.info
SipSignallingPort                 : 5061
FailoverTimeSeconds               : 10
ForwardCallHistory                : True
ForwardPai                        : True
SendSipOptions                    : True
Enabled                           : True
MediaBypass                       : True
GatewaySiteLbrEnabled             : False
FailoverResponseCodes             : 408,503,504
GenerateRingingWhileLocatingUser  : True
PidfLoSupported                   : False
BypassMode                        : None
```

This page is intentionally left blank.

4 Configuring AudioCodes SBC

This section provides step-by-step procedures on how to configure AudioCodes SBC for interworking between Teams Direct Routing and the autphone 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 WAN interface - autphone SIP Trunking and Teams Direct Routing environment

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

Notes:

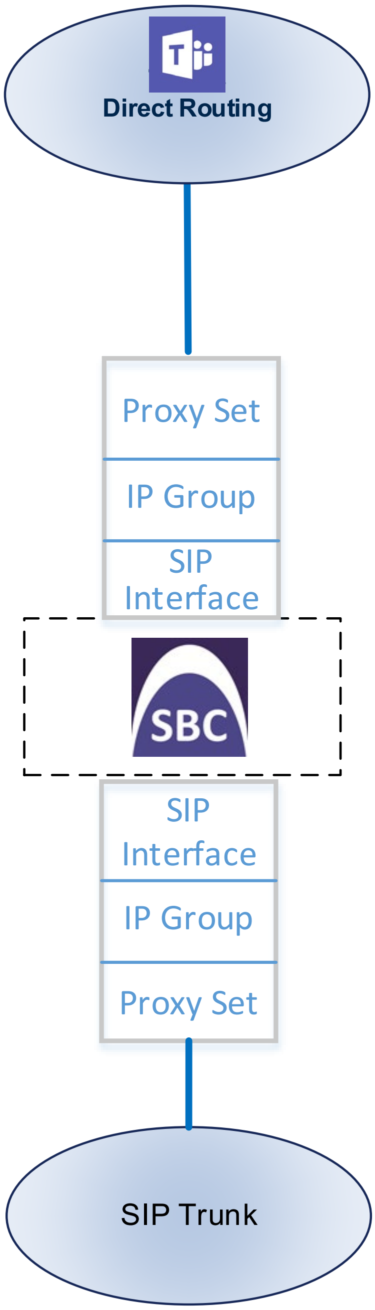
- For implementing Teams Direct Routing and autphone SIP Trunk based on the configuration described in this section, AudioCodes SBC must be installed with a License Key that includes the following software features:
  - √ **Microsoft TEAMS**
  - √ **DSP Channels**
  - √ **Number of SBC sessions** *[Based on requirements]*
  - √ **Transcoding sessions** *[If media transcoding is needed]*

  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

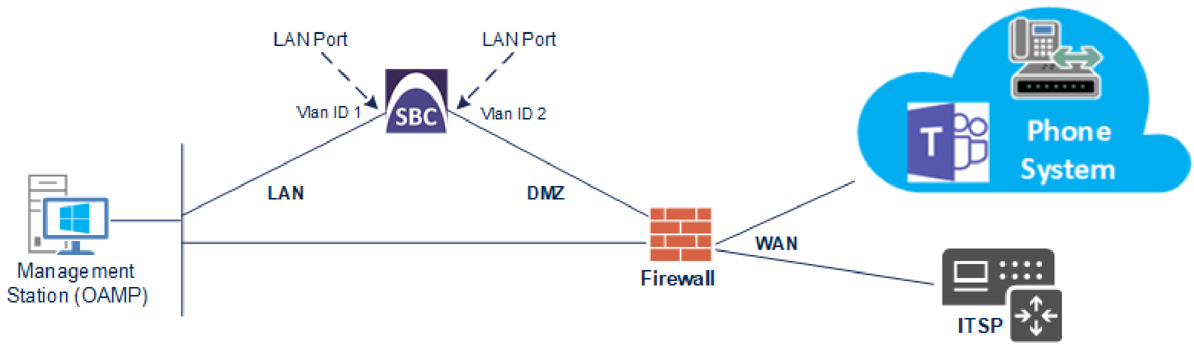


4.2 IP Network Interfaces Configuration

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

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

Figure 4-2: Network Interfaces in Interoperability Test Topology



4.2.1 Configure VLANs

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

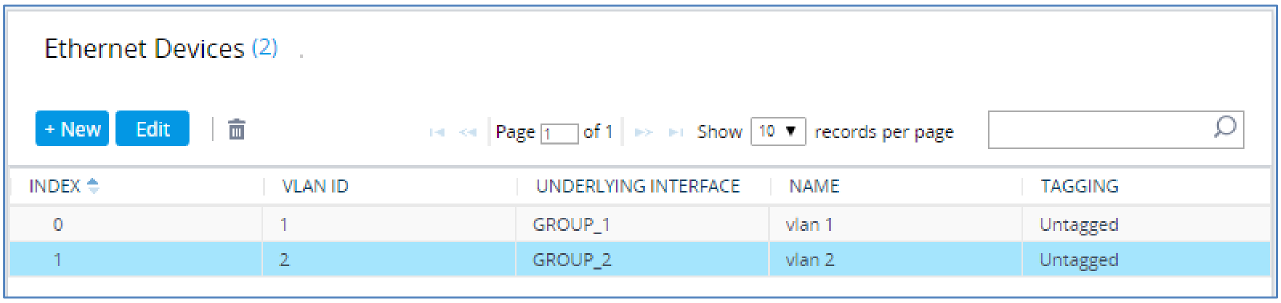
- LAN VoIP (assigned the name "LAN_IF")
- WAN VoIP (assigned the name "WAN_IF")

➢ **To configure the VLANs:**

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



4.2.2 Configure Network Interfaces

This section 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**

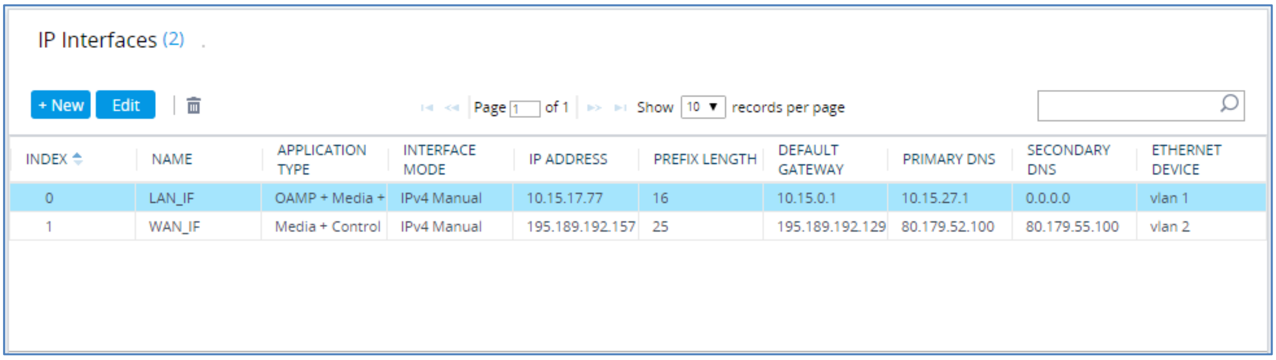
3. Add a network interface for the WAN side:
   a. Click **New**.
   b. Configure the interface as follows:

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



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

- CN: ACeducation.info
- SAN: ACeducation.info

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

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

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

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

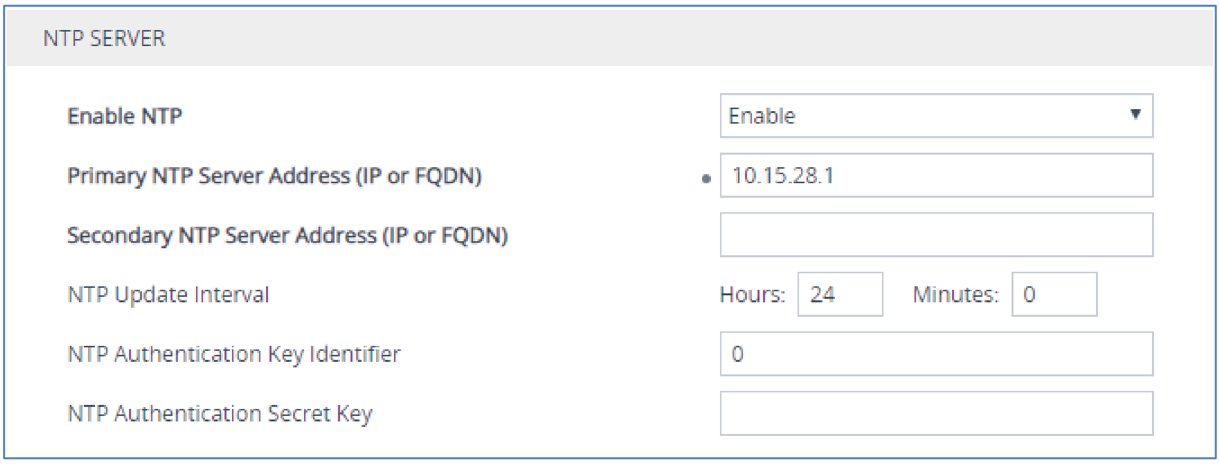
4.3.1 Configure the NTP Server Address

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

➢ **To configure the NTP server address:**

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

Figure 4-5: Configuring NTP Server Address



3. Click **Apply**.

4.3.2 Create a TLS Context for Teams Direct Routing

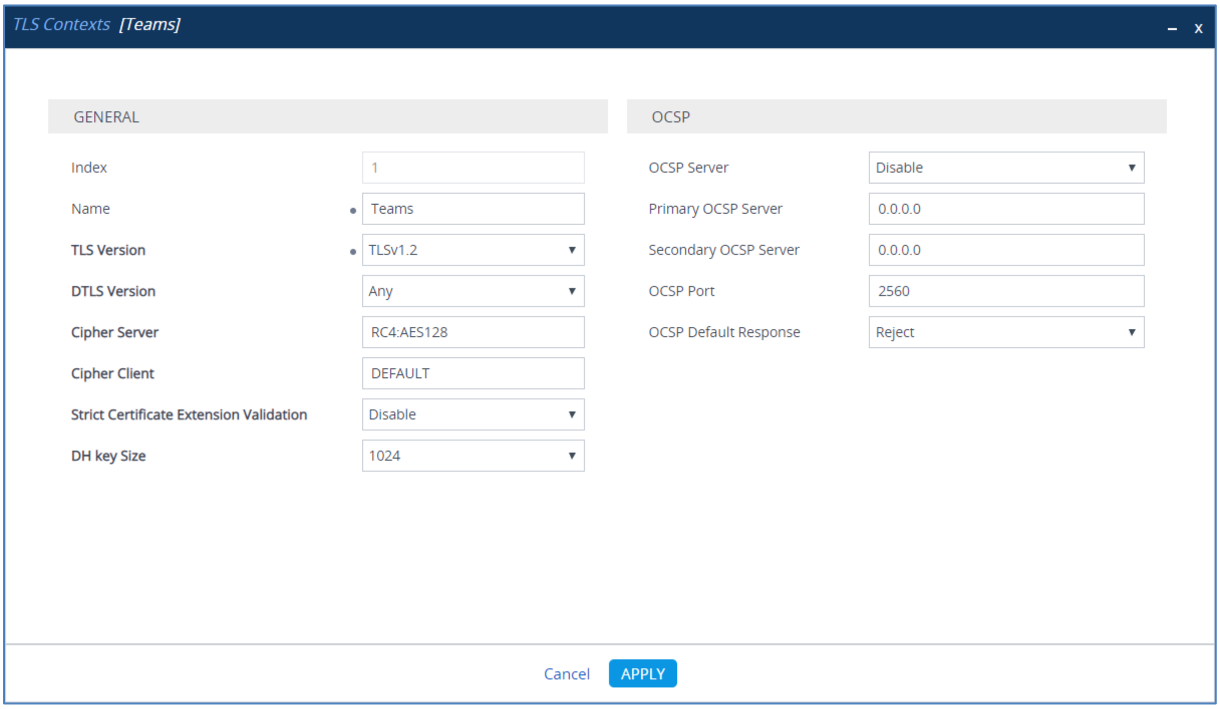
This section describes how to configure TLS Context in the SBC. AudioCodes recommends implementing only TLS to avoid flaws in SSL.

➢ **To configure the TLS version:**

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

Parameter	Value
Index	**1**
Name	**Teams** (arbitrary descriptive name)
TLS Version	**TLSv1.2**
All other parameters leave unchanged at their default values	

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



3. Click **Apply**.

4.3.3 Configure a Certificate

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

The procedure involves the following main steps:

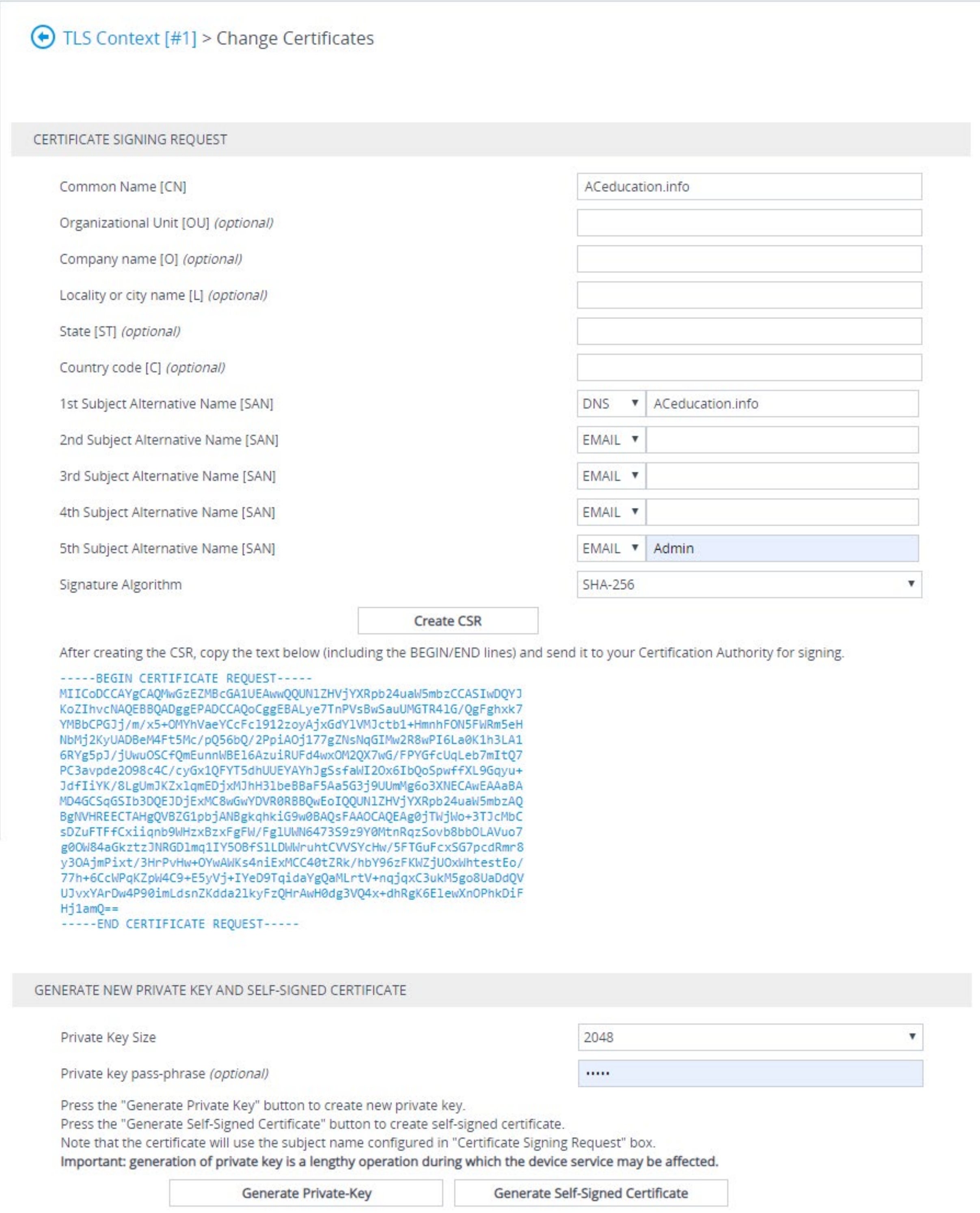
a. Generating a Certificate Signing Request (CSR).
b. Requesting Device Certificate from CA.
c. Obtaining Trusted Root/ Intermediate Certificate from CA.
d. Deploying Device and Trusted Root/ Intermediate Certificates on SBC.

> **Note:** The domain portion of the Common Name [CN] and 1st Subject Alternative Name [SAN] 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. In the '1st Subject Alternative Name [SAN]' field, change the type to 'DNS' and enter the SBC FQDN name (based on example above, **ACeducation.info**).
   c. 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.
   d. To change the key size on TLS Context, go to: **Generate New Private Key and Self-Signed Certificate**, change the 'Private Key Size' to **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.
   e. Fill in the rest of the request fields according to your security provider's instructions.
   f. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 4-7: Example of Certificate Signing Request – Creating CSR

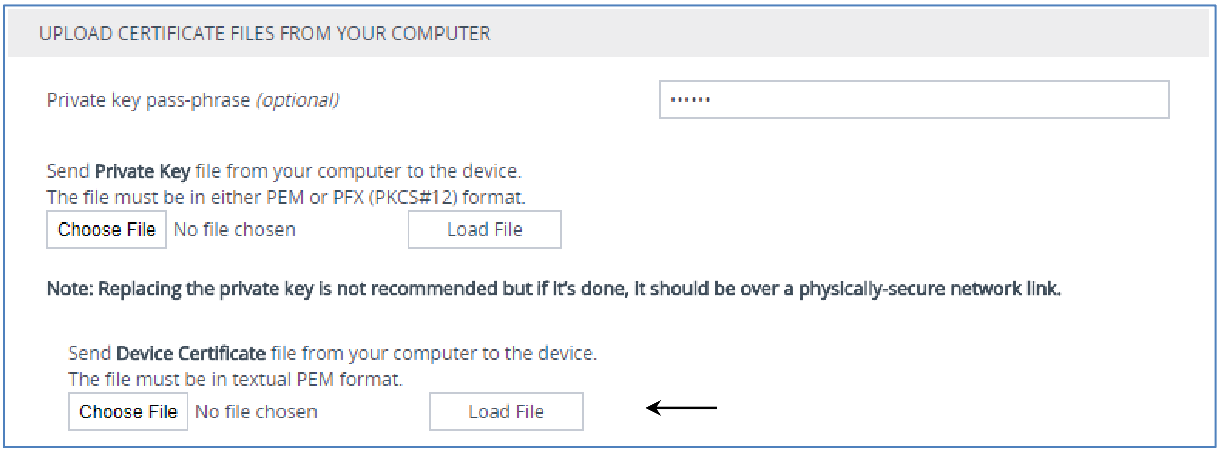


4. Copy the CSR from the line **"----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----"** to a text file (such as Notepad), and then save it to a folder on your computer with the file name, for example *certreq.txt*.
5. Send *certreq.txt* file to the Certified Authority Administrator for signing.
6. After obtaining an SBC signed and Trusted Root/Intermediate Certificate from the CA, in the SBC's Web interface, return to the **TLS Contexts** page and do the following:

a. In the TLS Contexts page, select the required TLS Context index row, 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.

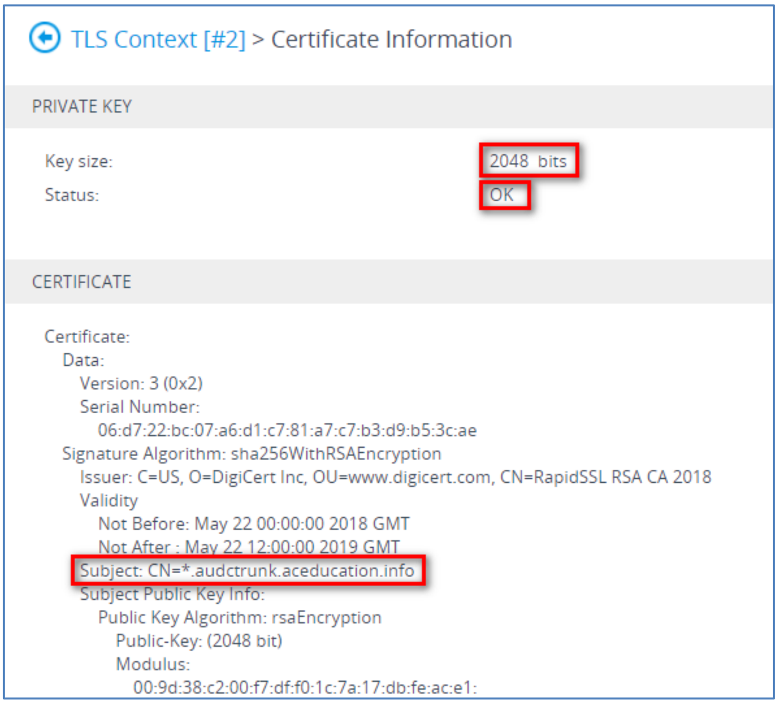
Figure 4-8: Uploading the Certificate Obtained from the Certification Authority



7. Confirm that the certificate was uploaded correctly. A message indicating that the certificate was uploaded successfully is displayed in blue in the lower part of the page.

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

Figure 4-9: Certificate Information Example



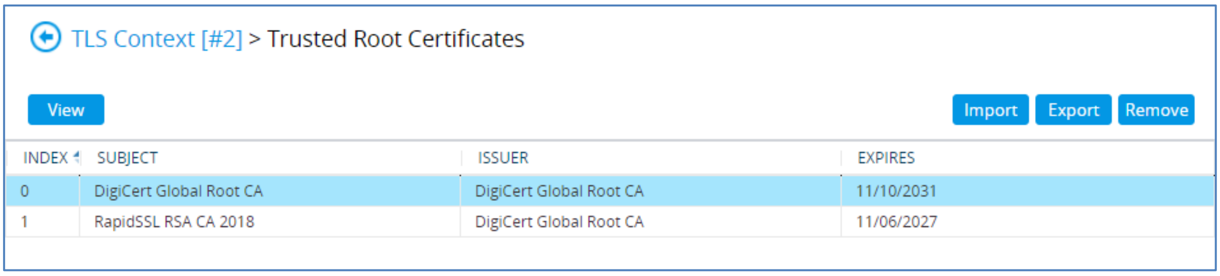
9. In the SBC's Web interface, return to the **TLS Contexts** page.

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



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

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

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

4.4 Configure Media Realms

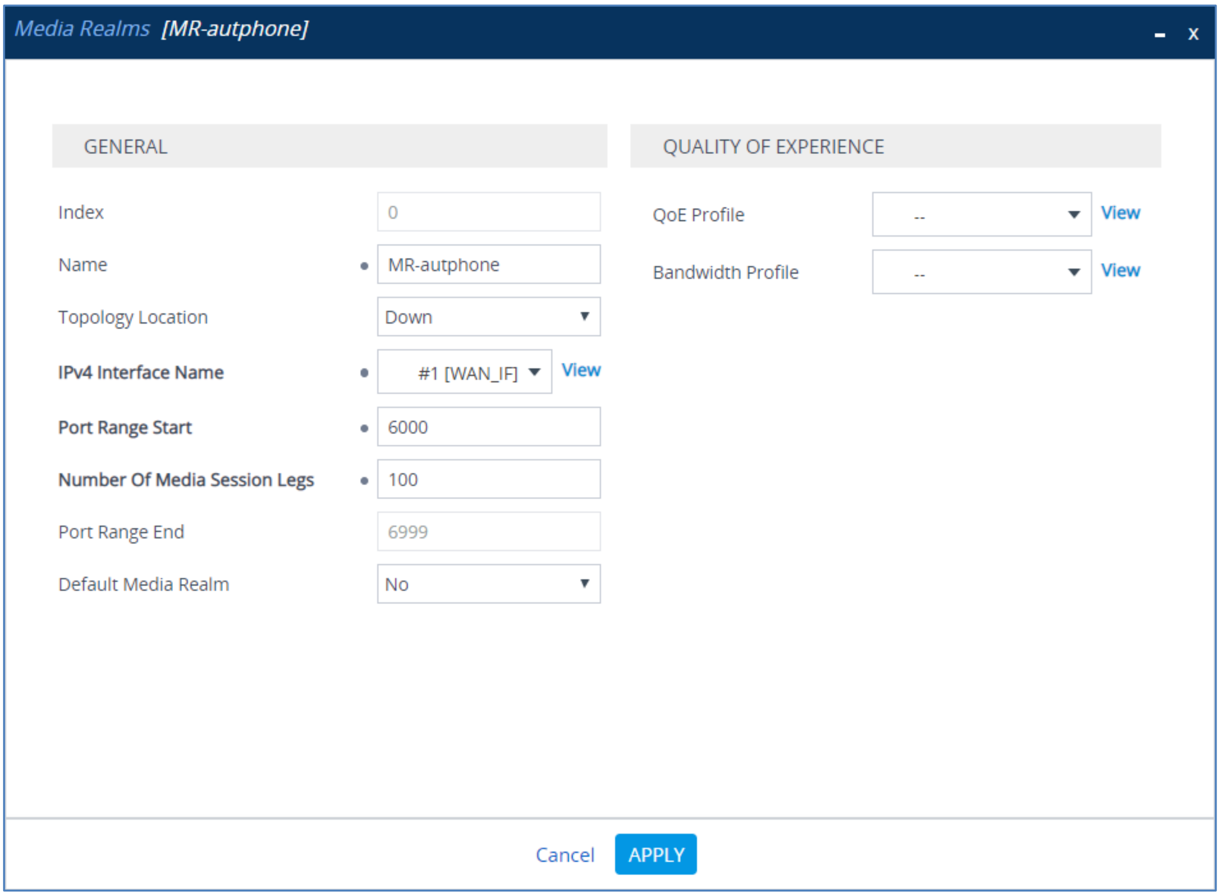
This section describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **To configure Media Realms:**

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

Parameter	Value
Index	**0**
Name	**MR-autphone** (descriptive name)
IPv4 Interface Name	**WAN_IF**
Port Range Start	**6000** (represents lowest UDP port number used for media)
Number of Media Session Legs	**100** (media sessions assigned with port range)

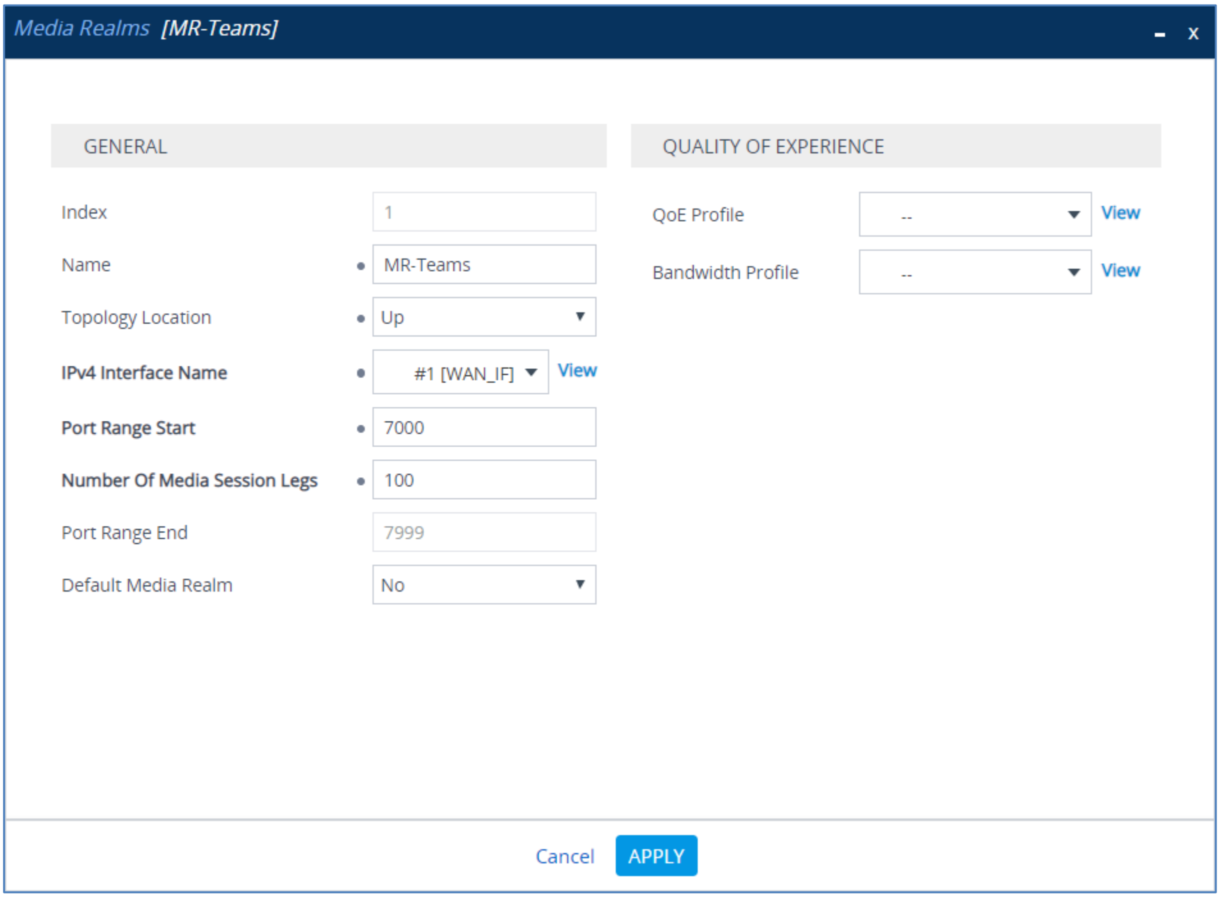
Figure 4-11: Configuring Media Realm for autphone SIP Trunk



3. Configure a Media Realm for WAN traffic:

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

Figure 4-12: Configuring Media Realm for Teams



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-autphone	WAN_IF	6000	100	6999	No
1	MR-Teams	WAN_IF	7000	100	7999	No

4.5 Configure SIP Signaling Interfaces

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

➢ **To configure SIP Interfaces:**

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

Parameter	Value
Index	**0**
Name	**autphone** (arbitrary descriptive name)
Network Interface	**WAN_IF**
Application Type	**SBC**
UDP Port	**55060** (according to Service Provider requirement)
TCP and TLS Port	**0**
Media Realm	**MR-autphone**

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

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** (Recommended to prevent DoS attacks)
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	autphone	DefaultSRD	WAN_IF	SBC	55060	0	0	No encapsulati	MR-autphone
1	Teams	DefaultSRD	WAN_IF	SBC	0	0	5061	No encapsulati	MR-Teams

4.6 Configure Proxy Sets

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

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

- autphone SIP Trunk
- Teams Direct Routing

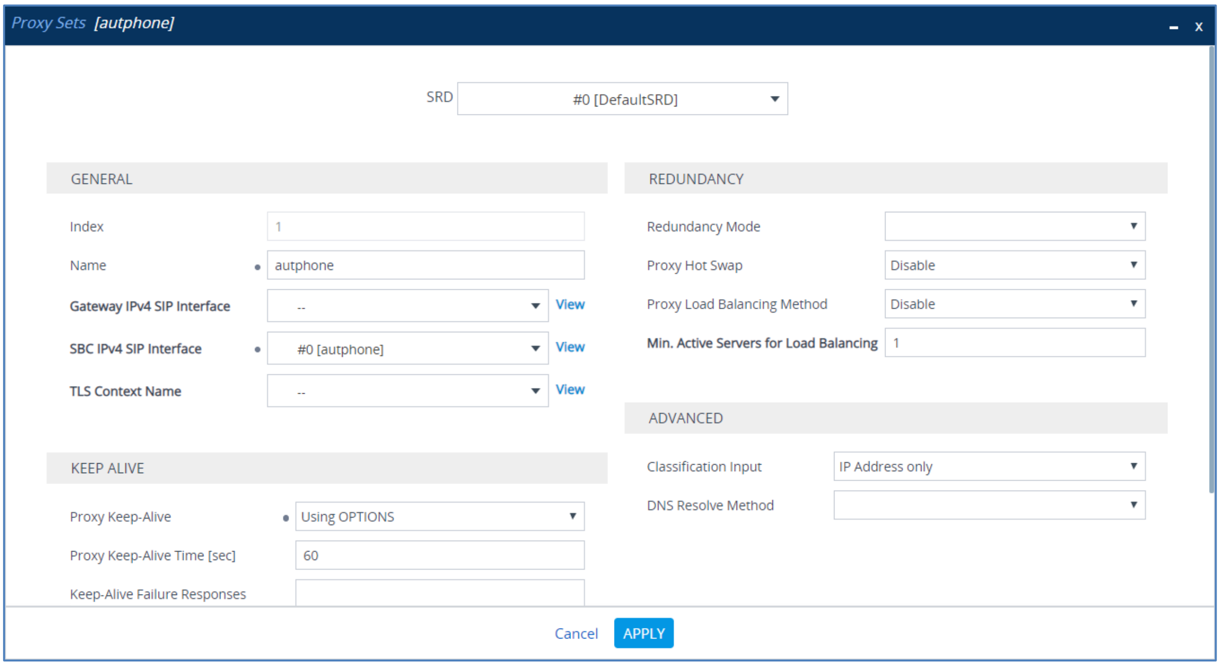
The Proxy Sets will later be applied to the VoIP network by assigning them to IP Groups.

➢ **To configure Proxy Sets:**

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

Parameter	Value
Index	**1**
Name	**autphone**
SBC IPv4 SIP Interface	**autphone**
Proxy Keep-Alive	**Using Options**

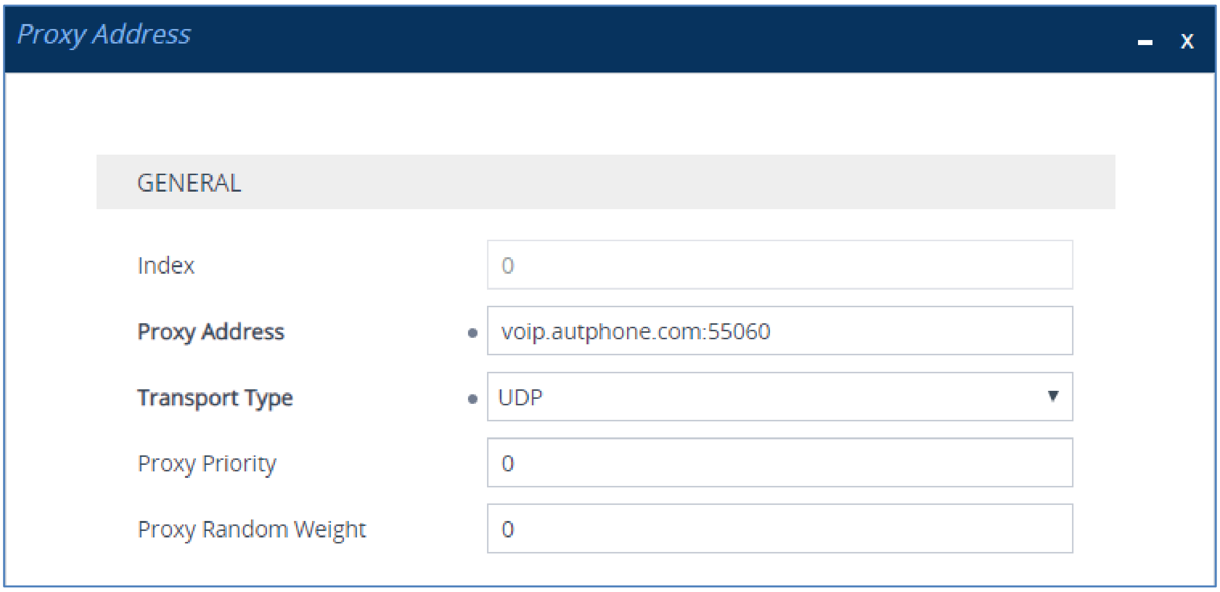
Figure 4-15: Configuring Proxy Set for autphone SIP Trunk



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 autphone SIP Trunk



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

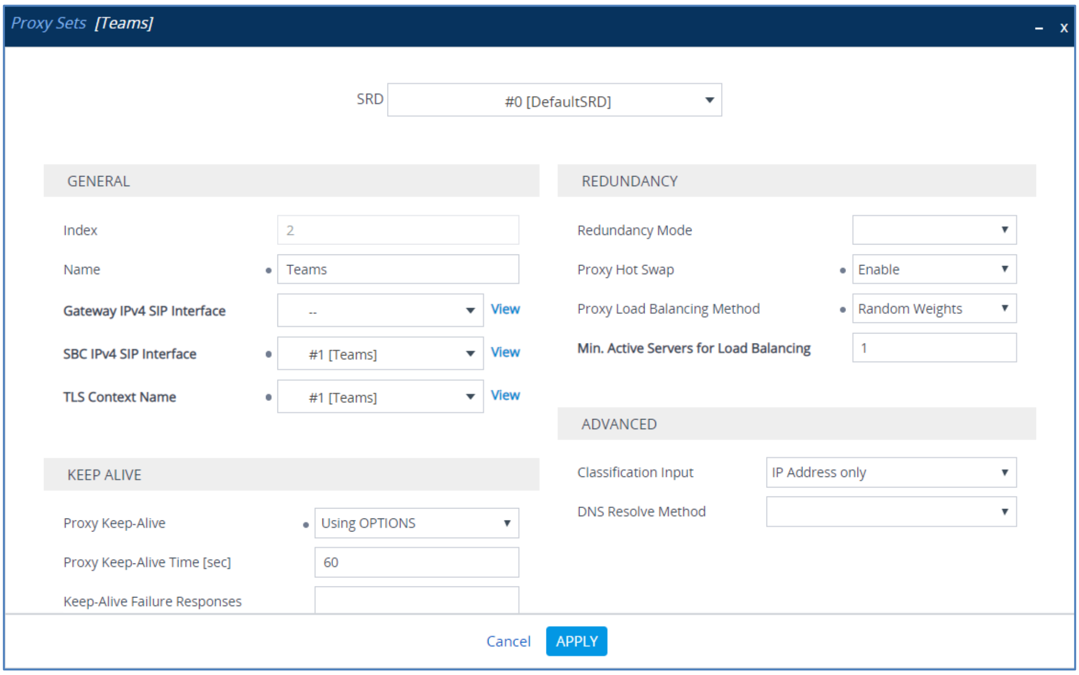
Parameter	Value
Index	**0**
Proxy Address	**voip.autphone.com:55060** (SIP Trunk FQDN)
Transport Type	**UDP**

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**
TLS Context Name	**Teams**
Proxy Keep-Alive	**Using Options**
Proxy Hot Swap	**Enable**
Proxy Load Balancing Method	**Random Weights**

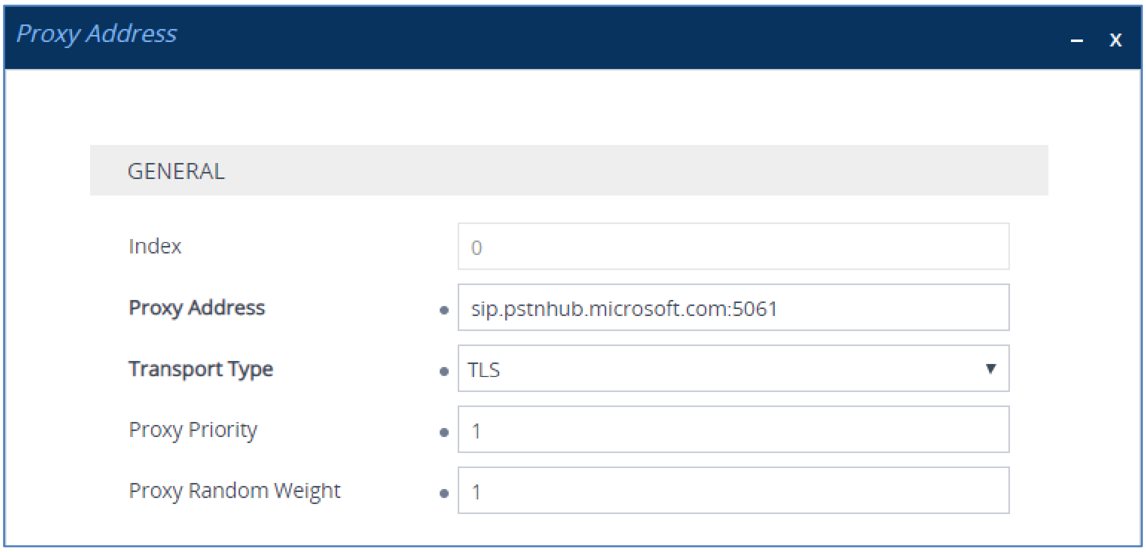
Figure 4-17: Configuring Proxy Set for Teams Direct Routing



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 Teams Direct Routing Interface



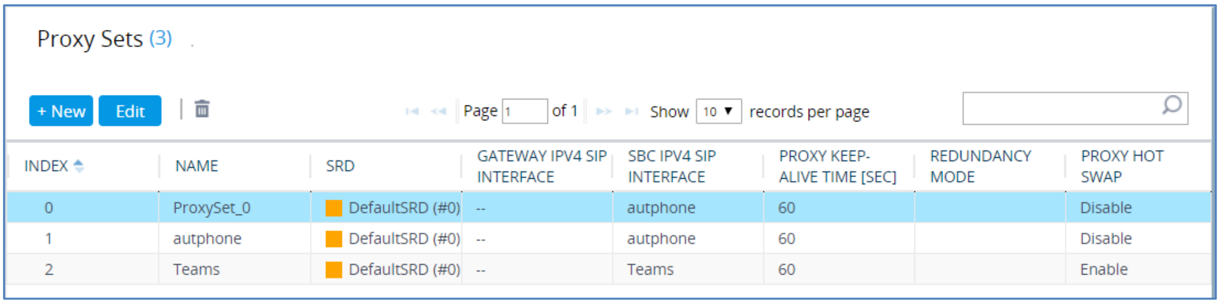
c. Configure the address of the Proxy Set according to the parameters described in the table below.

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

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 (#0)	--	autphone	60		Disable
1	autphone	DefaultSRD (#0)	--	autphone	60		Disable
2	Teams	DefaultSRD (#0)	--	Teams	60		Enable

4.7 Configure Coders

This section describes how to configure coders (termed *Coder Group*). As Teams Direct Routing supports the SILK and G.729 coders while the network connection to autphone 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 autphone SIP Trunk.

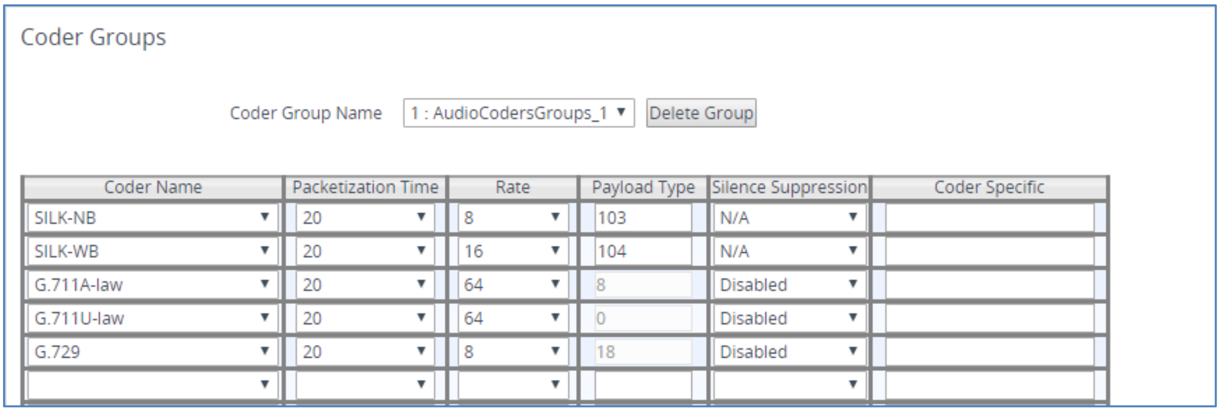
Note that the Coder Group ID for this entity will be assigned to its corresponding IP Profile in the next step.

➢ **To configure coders:**

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

Parameter	Value
Coder Group Name	**AudioCodersGroups_1**
Coder Name	▪ **SILK-NB** ▪ **SILK-WB** ▪ **G.711 A-law** ▪ **G.711 U-law** ▪ **G.729**

Figure 4-20: Configuring Coder Group for Teams Direct Routing

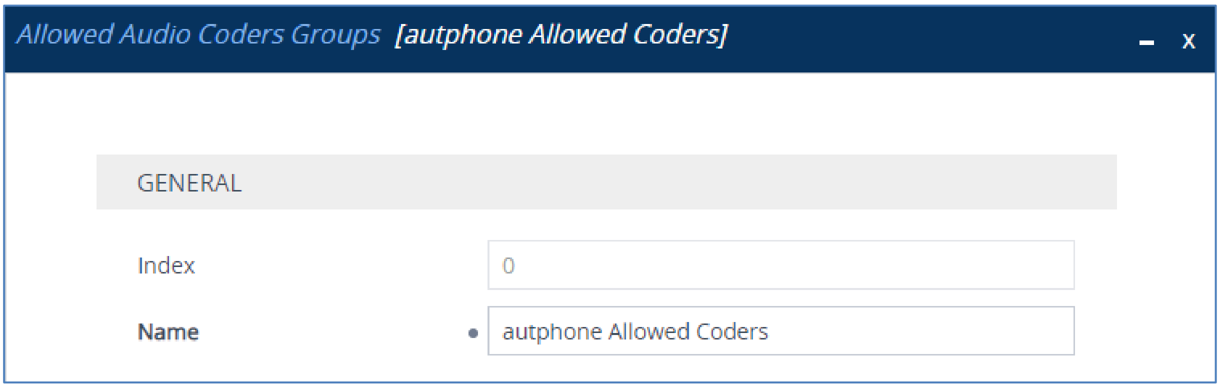


The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the autphone SIP Trunk uses the dedicated coders list whenever possible. Note that this Allowed Coders Group ID will be assigned to the IP Profile belonging to the autphone SIP Trunk in the next step.

➢ **To set a preferred coder for the autphone 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 autphone SIP Trunk.

Figure 4-21: Configuring Allowed Coders Group for autphone SIP Trunk



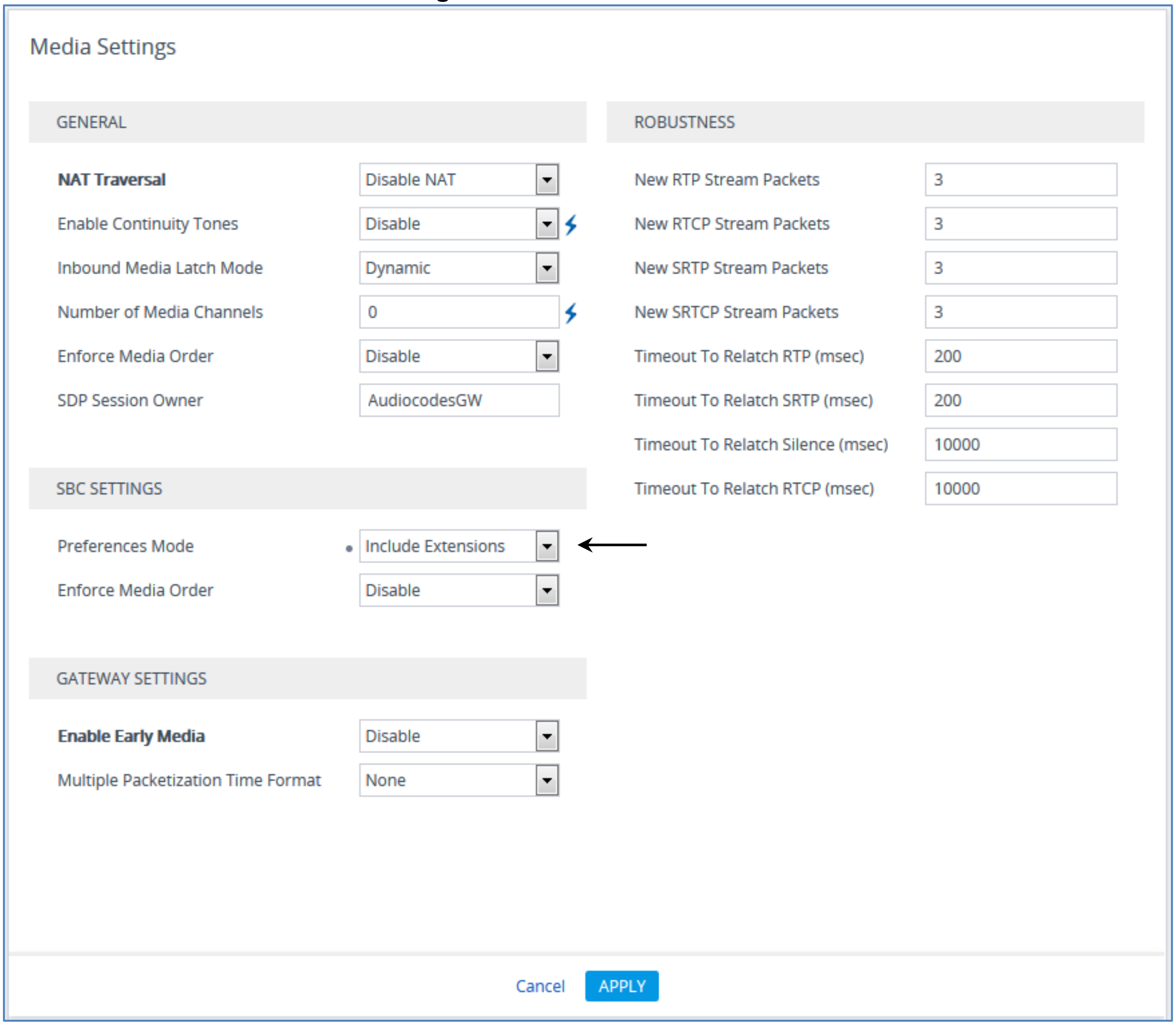
3. Click **Apply.**
4. Select the new row that you configured, and then click the **Allowed Audio Coders** link located below the table; the Allowed Audio Coders table opens.
5. Click **New** and configure an Allowed Coders as follows:

Parameter	Value
Index	**0**
Coder	**G.711 A-law**

Figure 4-22: Configuring Allowed Coders for autphone SIP Trunk

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

Figure 4-23: SBC Preferences Mode



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

4.8 Configure IP Profiles

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

In this interoperability test topology, IP Profiles need to be configured for the following IP entities:

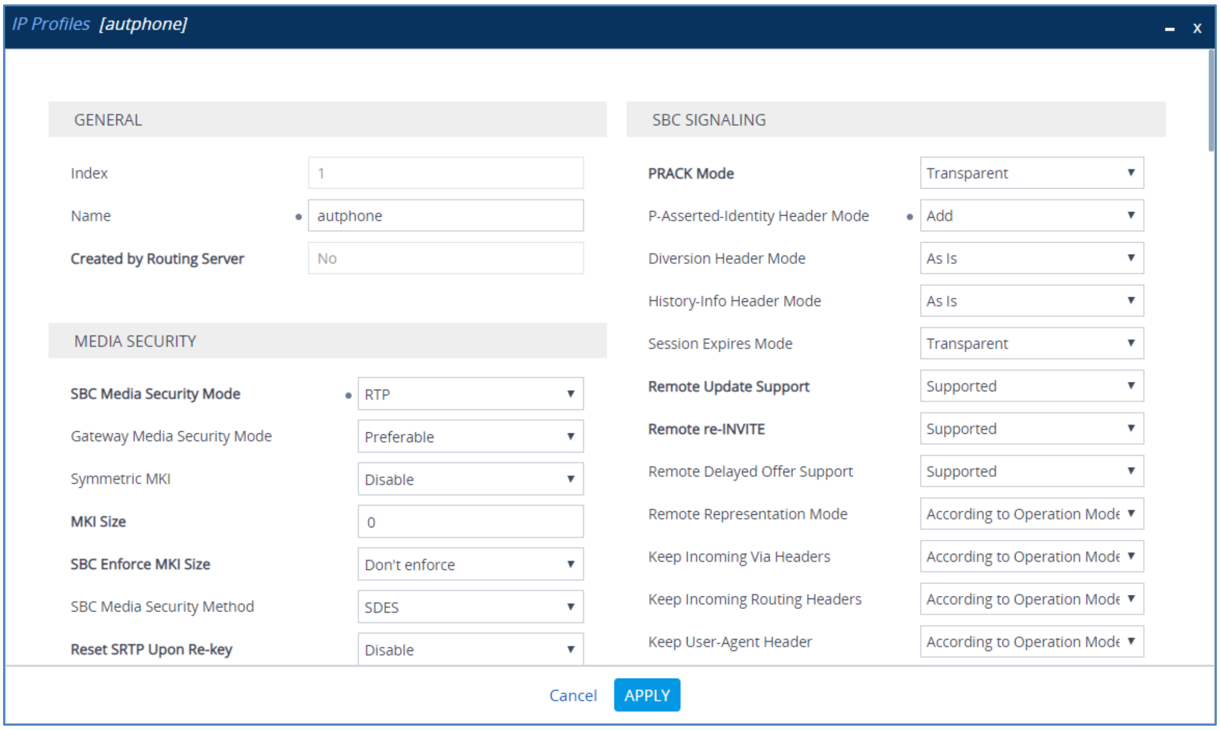
- autphone SIP trunk – to operate in non-secure mode using RTP and SIP over UDP
- Teams Direct Routing – to operate in secure mode using SRTP and SIP over TLS

➢ **To configure an IP Profile for the autphone SIP Trunk:**

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

Parameter	Value
General	
Index	**1**
Name	**autphone**
Media Security	
SBC Media Security Mode	**RTP**
SBC Media	
Allowed Audio Coders	**autphone Allowed Coders**
SBC Signaling	
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)
Session Expires Mode	**Supported**
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 4-24: Configuring IP Profile for autphone SIP Trunk



3. Click **Apply**.

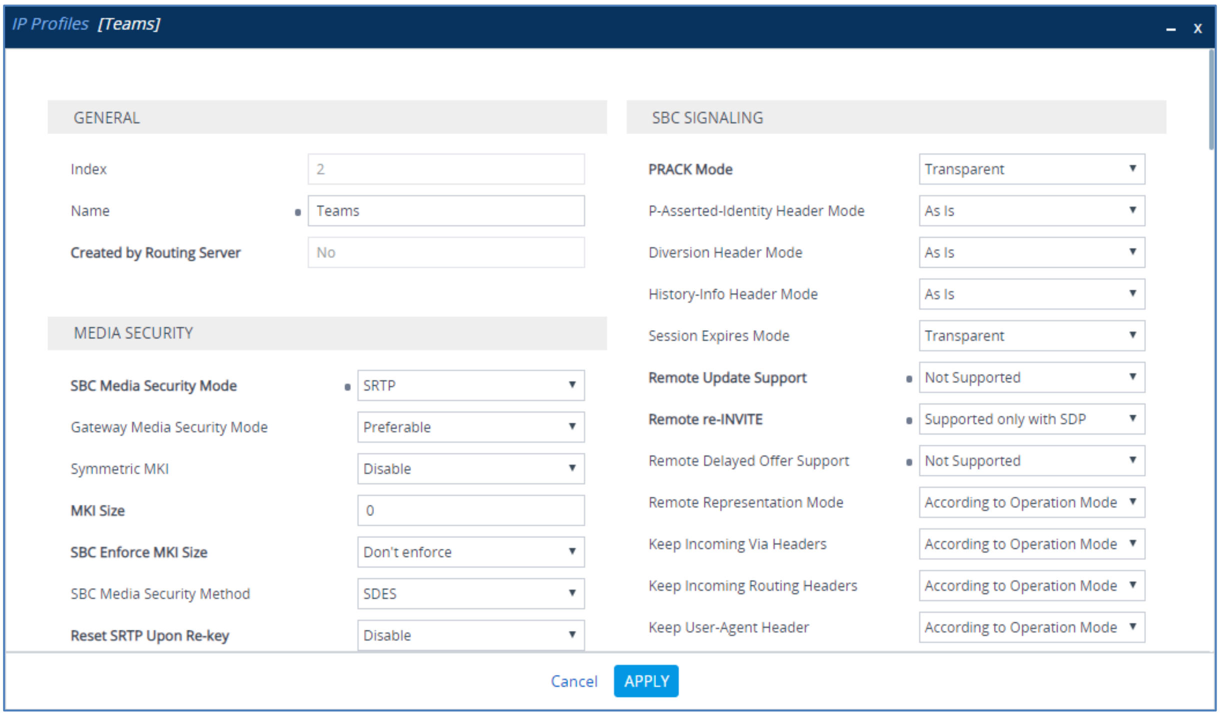
➢ To configure IP Profile for the Teams Direct Routing:

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)
SBC Media	
Extension Coders Group	**AudioCodersGroups_1**
RTCP Mode	**Generate Always** (required, as some ITSPs do not send RTCP packets while in Hold mode, but Microsoft expects them)
ICE Mode	**Lite** (required only when Media Bypass enabled on Teams)

SBC Signaling	
Remote Update Support	**Not Supported**
Remote re-INVITE Support	**Supported Only With SDP**
Remote Delayed Offer Support	**Not Supported**
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally**
Remote 3xx Mode	**Handle Locally**
SBC Hold	
Remote Hold Format	**Inactive** (some SIP Trunk may answer with a=inactive and IP=0.0.0.0 in response to the Re-Invite with Hold request from Teams. Microsoft Media Stack doesn't support this format. So, SBC will replace 0.0.0.0 with its IP address)

Figure 4-25: Configuring IP Profile for Teams Direct Routing



3. Click **Apply**.

4.9 Configure IP Groups

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

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

- autphone 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 autphone SIP Trunk:

Parameter	Value
Index	**1**
Name	**autphone**
Type	**Server**
Proxy Set	**autphone**
IP Profile	**autphone**
Media Realm	**MR-autphone**
SIP Group Name	**voip.autphone.com** (according to ITSP requirement)

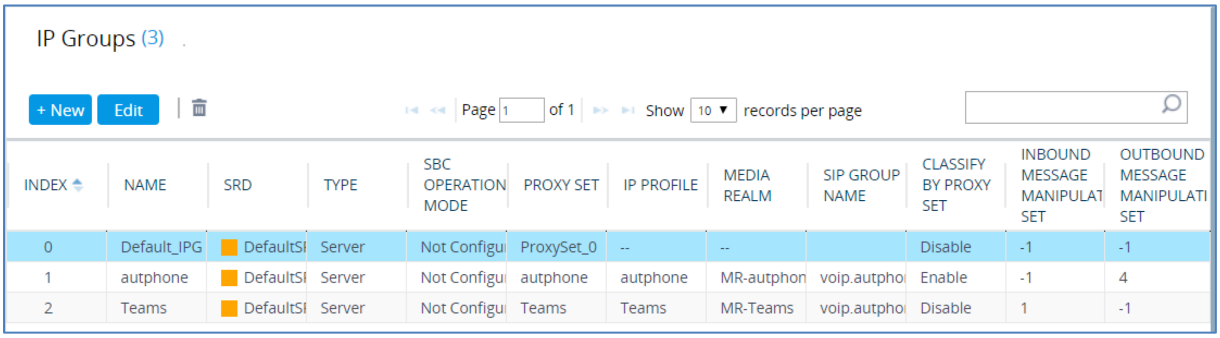
3. Configure an IP Group for the Teams Direct Routing:

Parameter	Value
Index	**2**
Name	**Teams**
Topology Location	**Up**
Type	**Server**
Proxy Set	**Teams**
IP Profile	**Teams**
Media Realm	**MR-Teams**
SIP Group Name	**voip.autphone.com** (according to ITSP requirement)
Classify By Proxy Set	**Disable**
Local Host Name	**< FQDN name of your SBC in the Teams Direct Routing tenant >** (For example, sbc1.customers.ACeducation.info)
Always Use Src Address	**Yes**

Proxy Keep-Alive using IP Group settings	**Enable**

The configured IP Groups are shown in the figure below:

Figure 4-26: 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 MANIPULAT SET	OUTBOUND MESSAGE MANIPULATI SET
0	Default_IPG	DefaultSI	Server	Not Configu	ProxySet_0	--	--		Disable	-1	-1
1	autphone	DefaultSI	Server	Not Configu	autphone	autphone	MR-autphon	voip.autpho	Enable	-1	4
2	Teams	DefaultSI	Server	Not Configu	Teams	Teams	MR-Teams	voip.autpho	Disable	1	-1

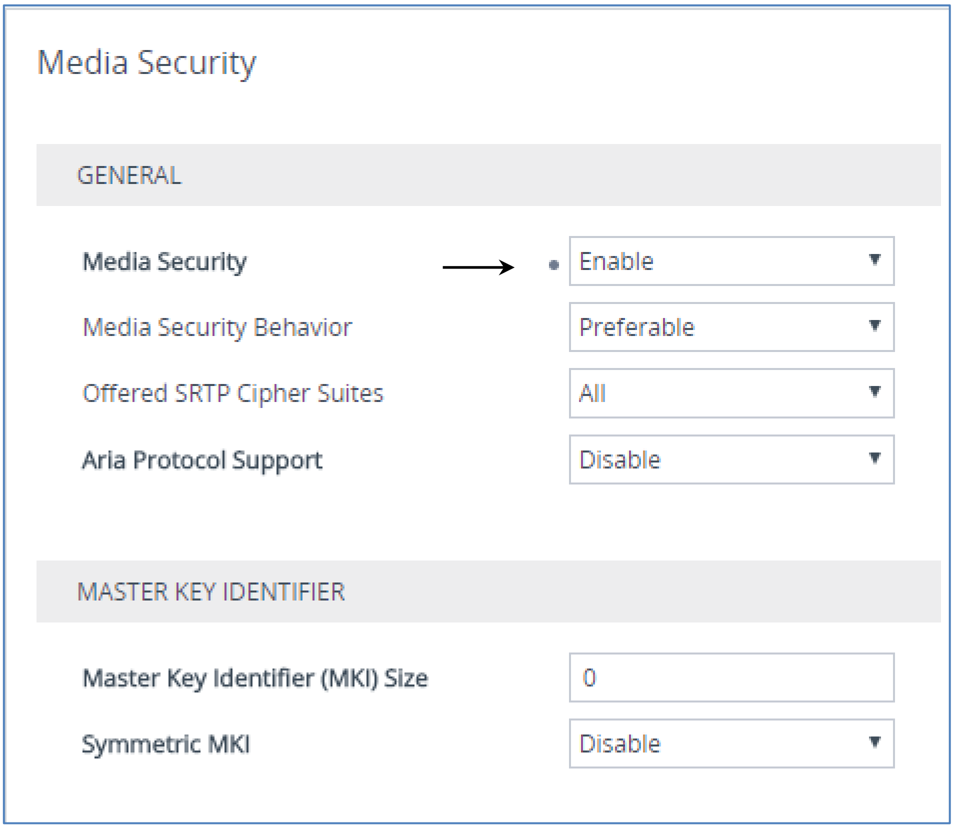
4.10 Configure SRTP

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

➢ **To configure media security:**

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

Figure 4-27: Configuring SRTP



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

4.11 Configuring Message Condition Rules

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

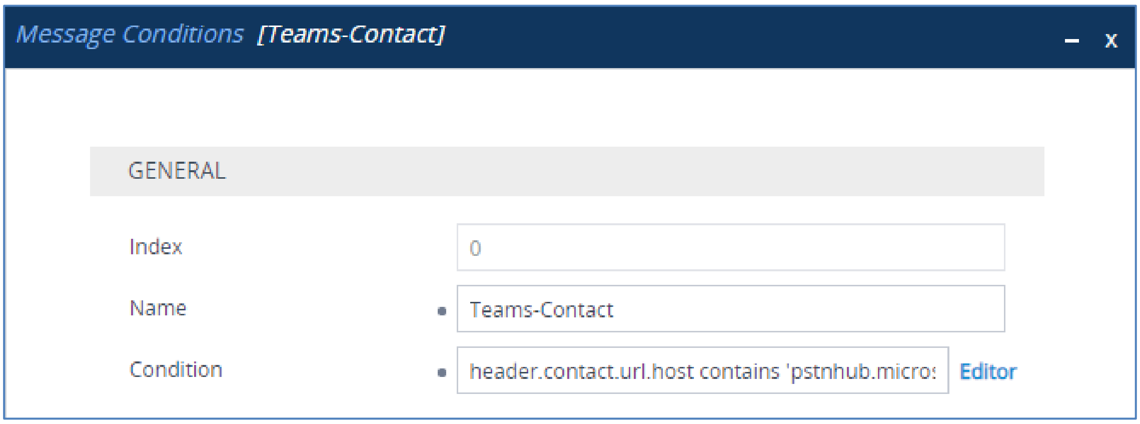
The following condition verifies that the Contact header contains Teams FQDN.

➢ **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 4-28: Configuring Condition Table



3. Click **Apply**.

4.12 Configuring Classification Rules

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

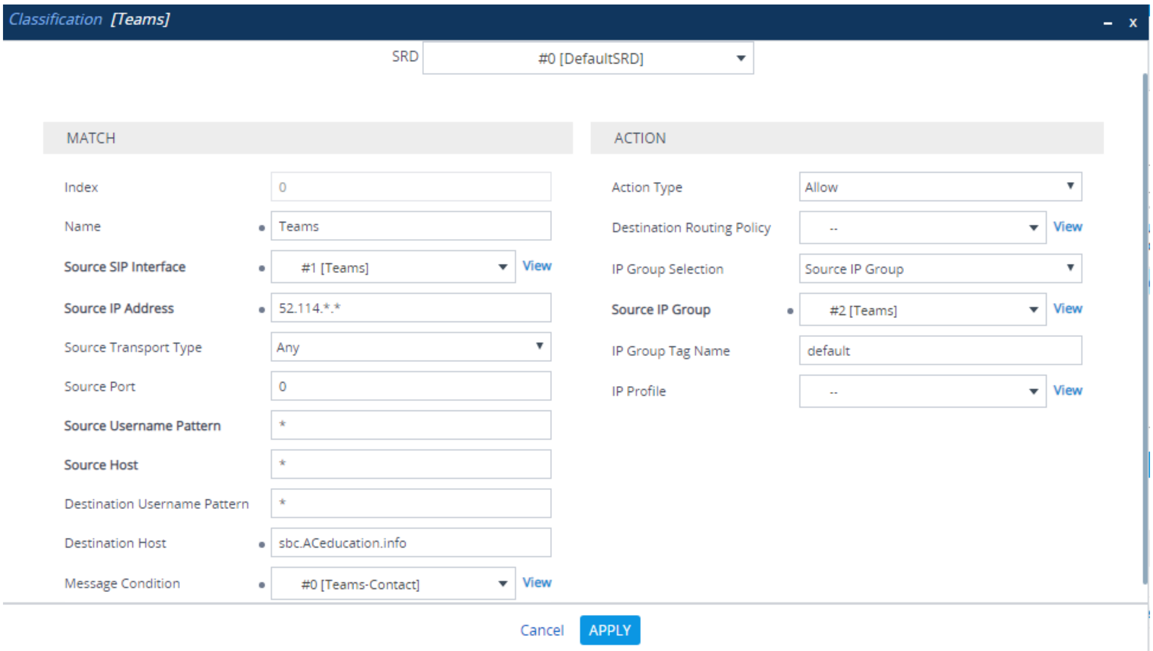
You can also use the Classification table for employing SIP-level access control for successfully classified calls, by configuring Classification rules with whitelist and blacklist settings. If a Classification rule is configured as a whitelist ("Allow"), the device accepts the SIP dialog and processes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

➢ **To configure a Classification rule:**

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

Parameter	Value
Index	**0**
Name	**Teams**
Source SIP Interface	**Teams**
Source IP Address	**52.114.*.***
Destination Host	**sbc.ACeducation.info** (example)
Message Condition	**Teams-Contact**
Action Type	**Allow**
Source IP Group	**Teams**

Figure 4-29: Configuring Classification Rule



3. Click **Apply**.

4.13 Configure IP-to-IP Call Routing Rules

This section describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups (as configured in Section 4.9 on page 38,) 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 autphone SIP Trunk:

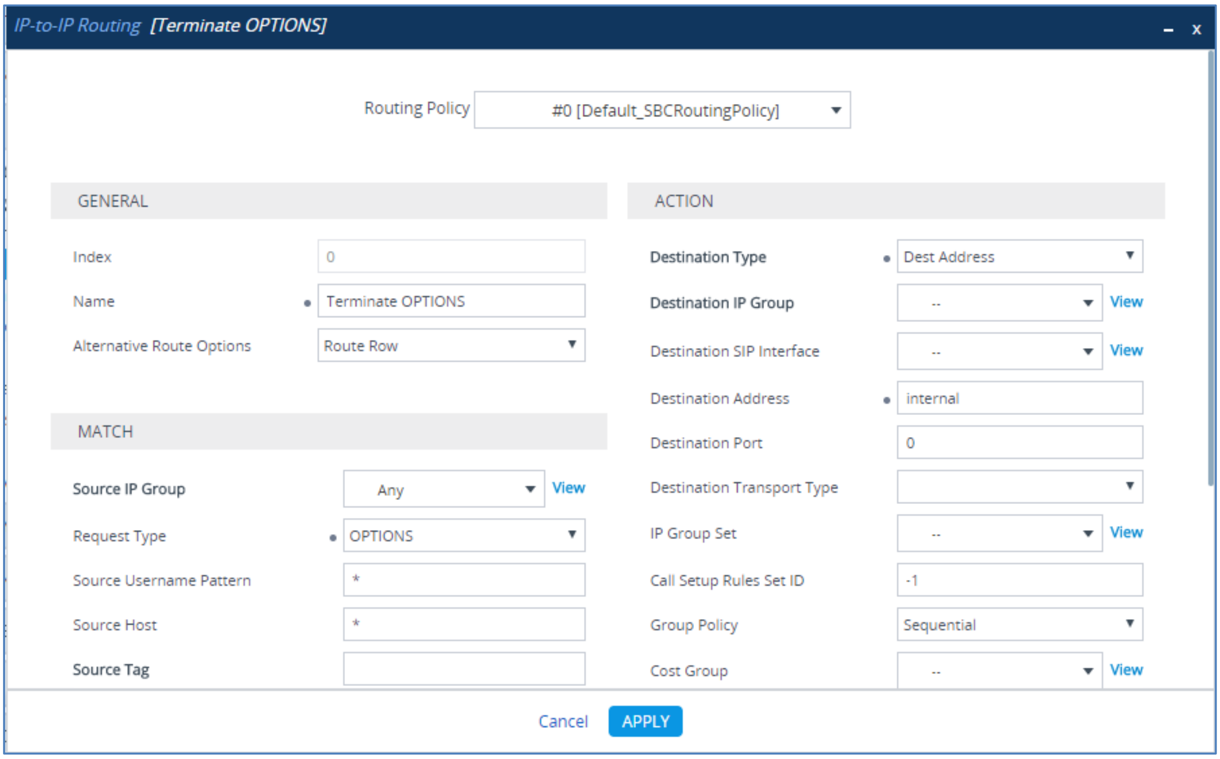
- Terminate SIP OPTIONS messages on the SBC that are received from any entity
- Terminate REFER messages to Teams Direct Routing
- Calls from Teams Direct Routing to autphone SIP Trunk
- Calls from autphone SIP Trunk to Teams Direct Routing

➢ **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 4-30: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS

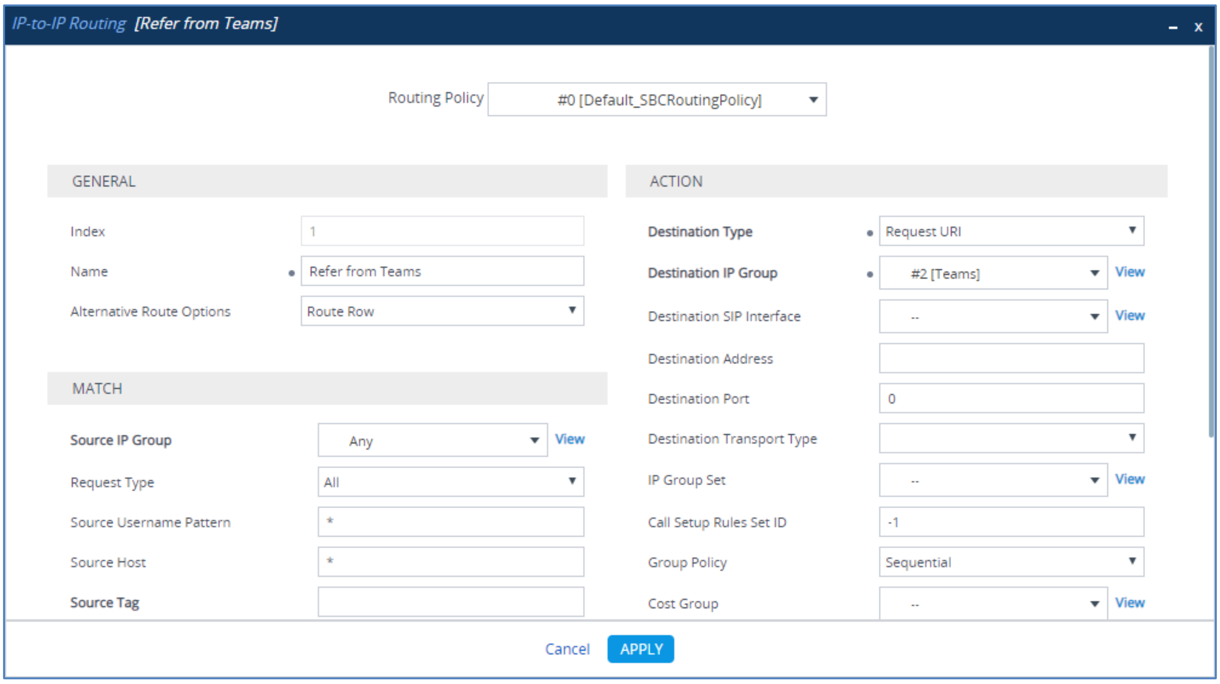


   b. Click **Apply**.

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 4-31: Configuring IP-to-IP Routing Rule for REFER from Teams

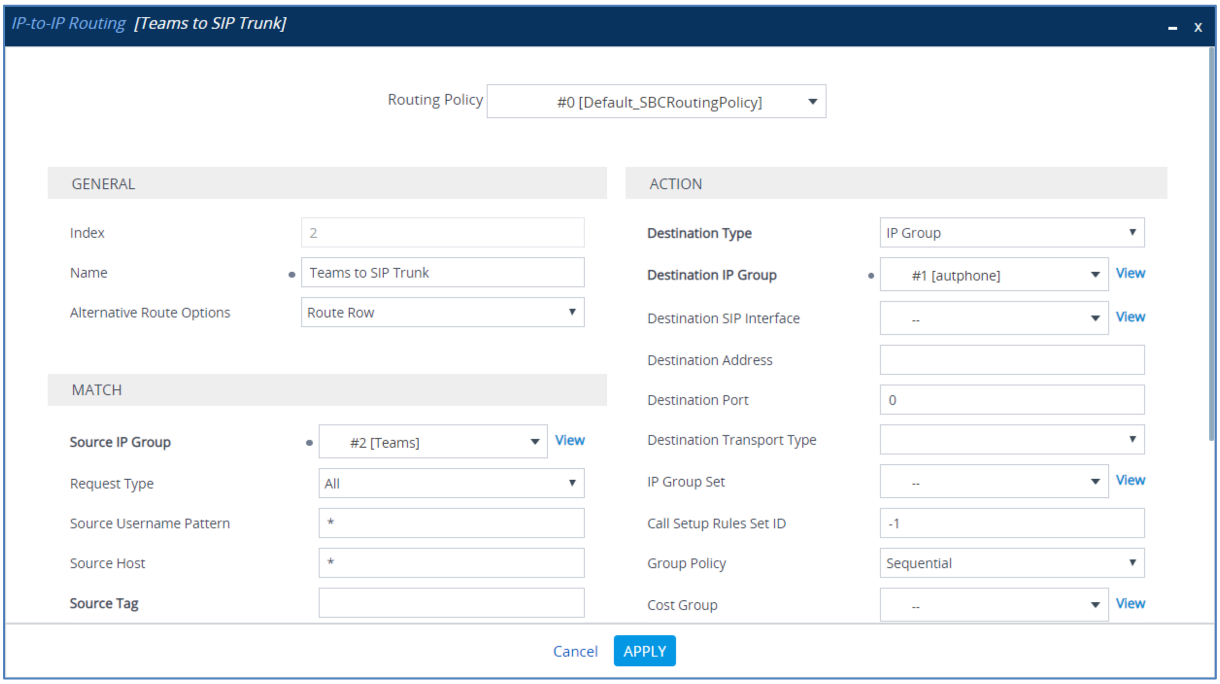


   b. Click **Apply**.

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

Parameter	Value
Index	**2**
Route Name	**Teams to SIP Trunk** (arbitrary descriptive name)
Source IP Group	**Teams**
Destination Type	**IP Group**
Destination IP Group	**autphone**

Figure 4-32: Configuring IP-to-IP Routing Rule for Teams to SIP Trunk

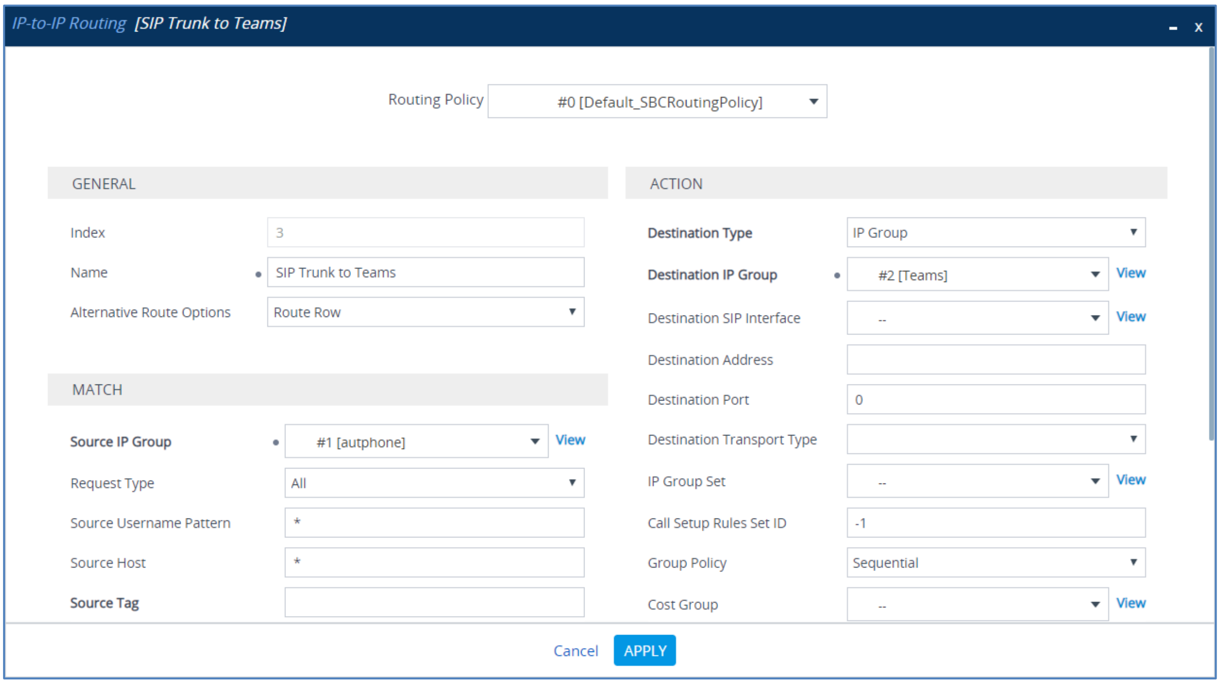


   b. Click **Apply**.

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

Parameter	Value
Index	**3**
Route Name	**SIP Trunk to Teams** (arbitrary descriptive name)
Source IP Group	**autphone**
Destination Type	**IP Group**
Destination IP Group	**Teams**

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



   b. Click **Apply.**

The configured routing rules are shown in the figure below:

Figure 4-34: 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 OF	Default_SBCR	Route Row	Any	OPTIONS	*	*	Dest Address	--	--	internal
1	Refer re-routi	Default_SBCR	Route Row	Any	All	*	*	Request URI	Teams	--	
2	Teams to SIP	Default_SBCR	Route Row	Teams	All	*	*	IP Group	autphone	--	
3	SIP Trunk to T	Default_SBCR	Route Row	autphone	All	*	*	IP Group	Teams	--	

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

4.14 Configure Number Manipulation Rules

This section describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 4.9 on page 38) to denote the source and destination of the call.

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

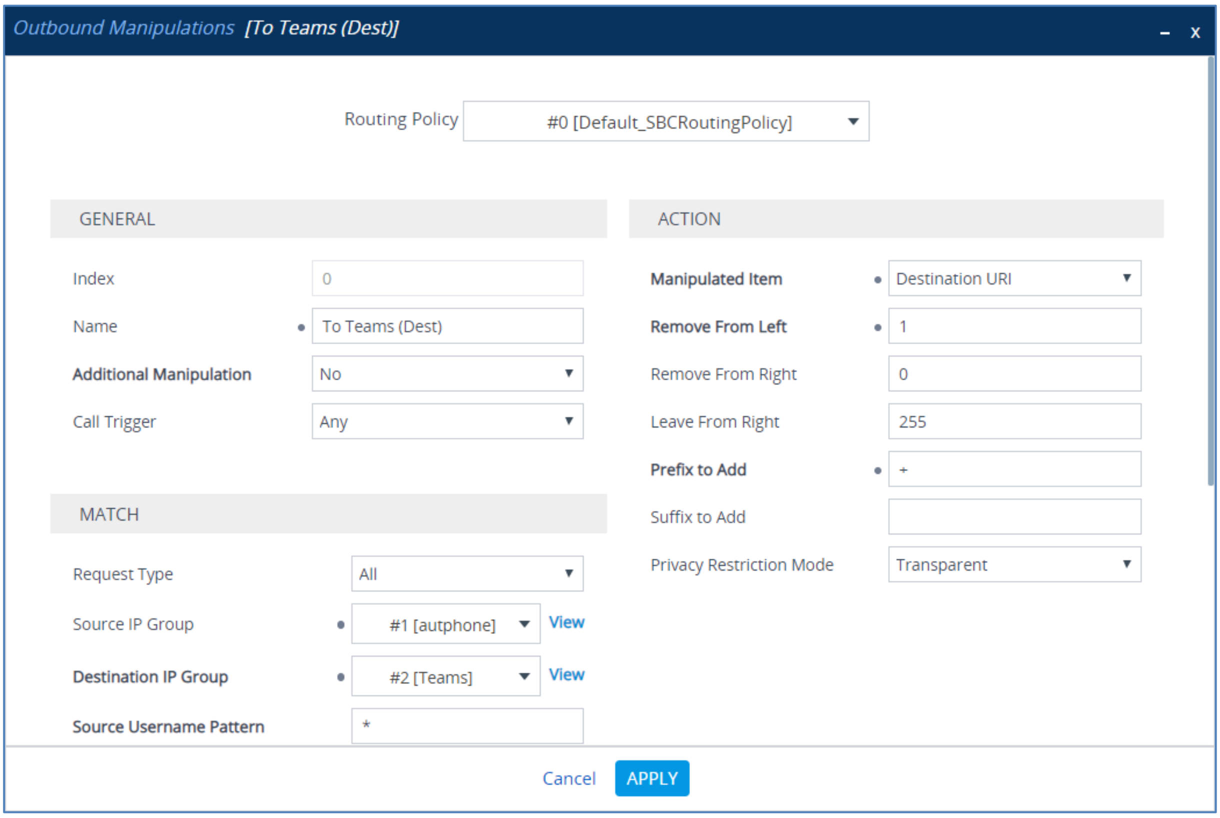
For example, for this interoperability test topology, a manipulation is configured to replace “0” by the “+” (plus sign) to the destination number for calls from the autphone SIP Trunk IP Group to the Teams Direct Routing IP Group for any destination username pattern.

➤ **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	**To Teams (Dest)**
Source IP Group	**autphone**
Destination IP Group	**Teams**
Destination Username Pattern	**0**
Manipulated Item	**Destination URI**
Remove From Left	**1**
Prefix to Add	**+** (plus sign)

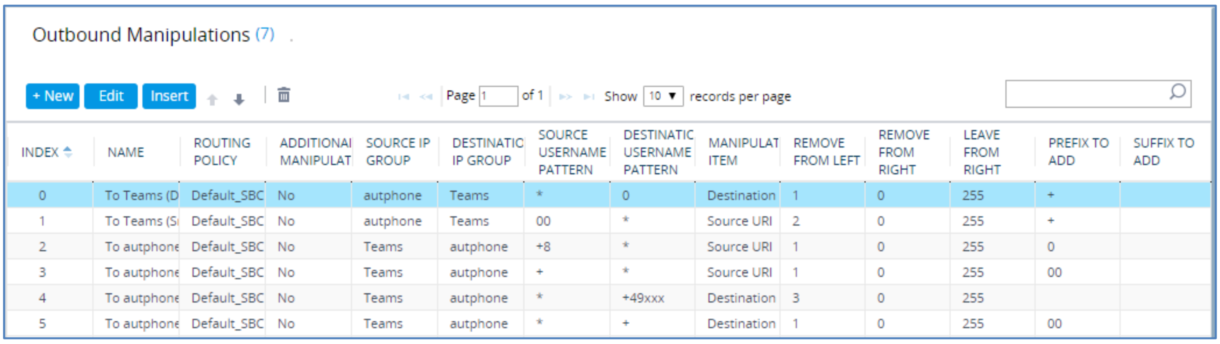
Figure 4-35: Configuring IP-to-IP Outbound Manipulation Rule



3. Click **Apply**.

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between Teams Direct Routing IP Group and autphone SIP Trunk IP Group:

Figure 4-36: Example of Configured IP-to-IP Outbound Manipulation Rules



Outbound Manipulations (7)

INDEX	NAME	ROUTING POLICY	ADDITIONAL MANIPULAT	SOURCE IP GROUP	DESTINATIC IP GROUP	SOURCE USERNAME PATTERN	DESTINATIC USERNAME PATTERN	MANIPULAT ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT	PREFIX TO ADD	SUFFIX TO ADD
0	To Teams (D	Default_SBC	No	autphone	Teams	*	0	Destination	1	0	255	+	
1	To Teams (S	Default_SBC	No	autphone	Teams	00	*	Source URI	2	0	255	+	
2	To autphone	Default_SBC	No	Teams	autphone	+8	*	Source URI	1	0	255	0	
3	To autphone	Default_SBC	No	Teams	autphone	+	*	Source URI	1	0	255	00	
4	To autphone	Default_SBC	No	Teams	autphone	*	+49xxx	Destination	3	0	255		
5	To autphone	Default_SBC	No	Teams	autphone	*	+	Destination	1	0	255	00	

Rule Index	Description
0	Calls from autphone IP Group to Teams IP Group with the prefix destination number "0", remove one digit and add "+" to the prefix of the destination number.
1	Calls from autphone IP Group to Teams IP Group with the prefix source number “00”, remove 2 digits and add "+" to the prefix of the source number.
2	Calls Teams IP Group to autphone IP Group with the prefix source number “+8”, remove one digit and add "0" to the prefix of the source number.

3	Calls Teams IP Group to autphone IP Group with the prefix <u>source</u> number “+”, remove one digit and add "00" to the prefix of the <u>source</u> number.
4	Calls Teams IP Group to autphone IP Group with the prefix <u>destination</u> number “+49” and length 3 digits (Emergency Numbers), remove 3 digits from the <u>destination</u> number.
5	Calls Teams IP Group to autphone IP Group with the prefix <u>destination</u> number “+”, remove one digit and add "00" to the prefix of the <u>destination</u> number.

4.15 Configure Message Manipulation Rules

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

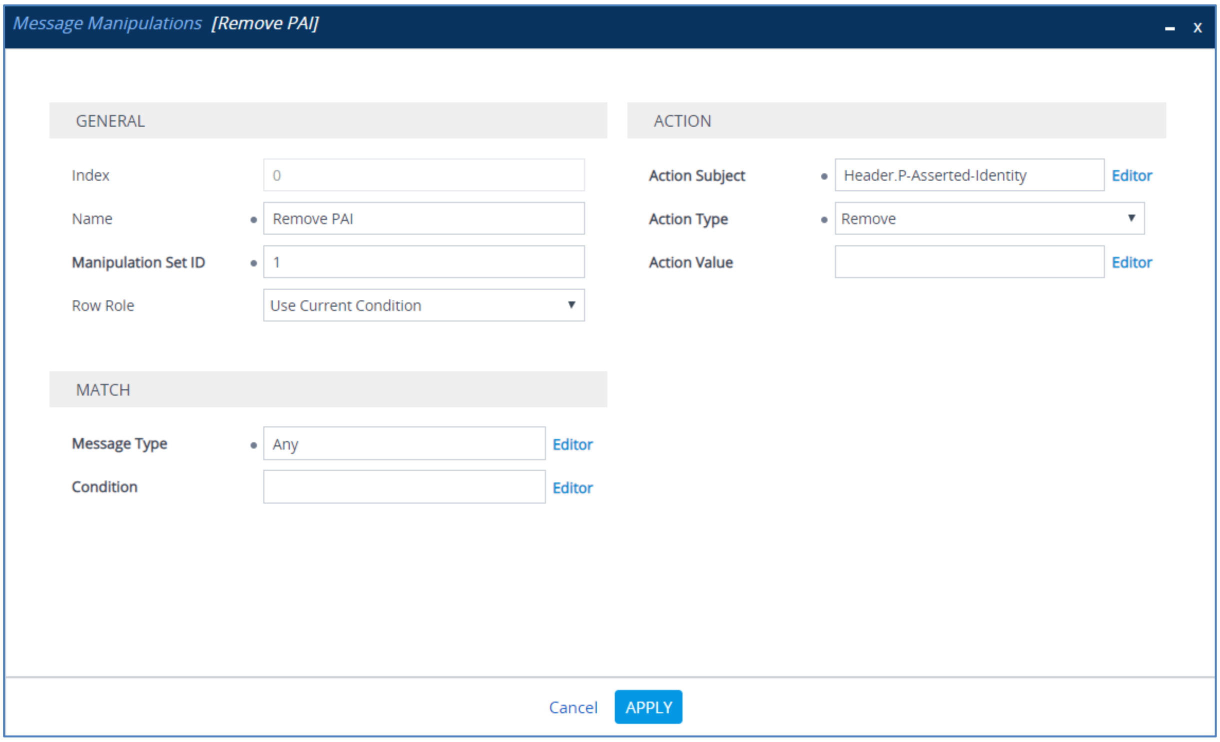
Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

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

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

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

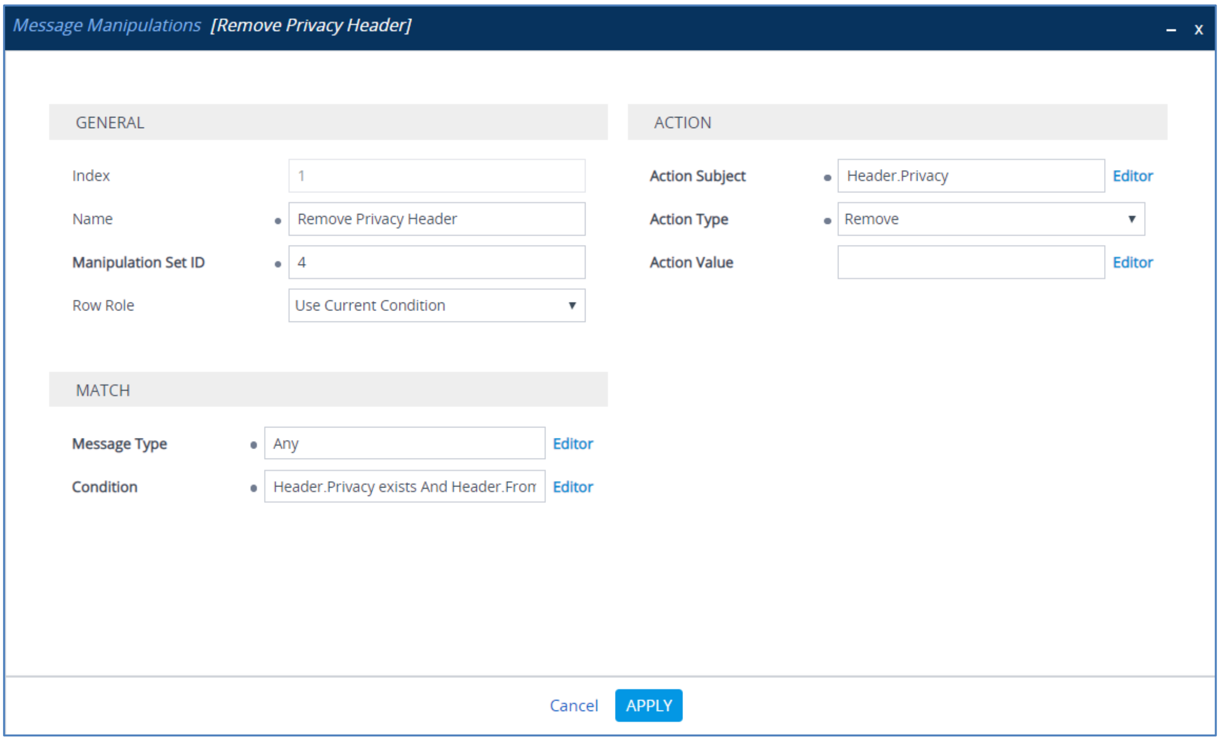
Figure 4-37: Configuring SIP Message Manipulation Rule 0 (for Teams)



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

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

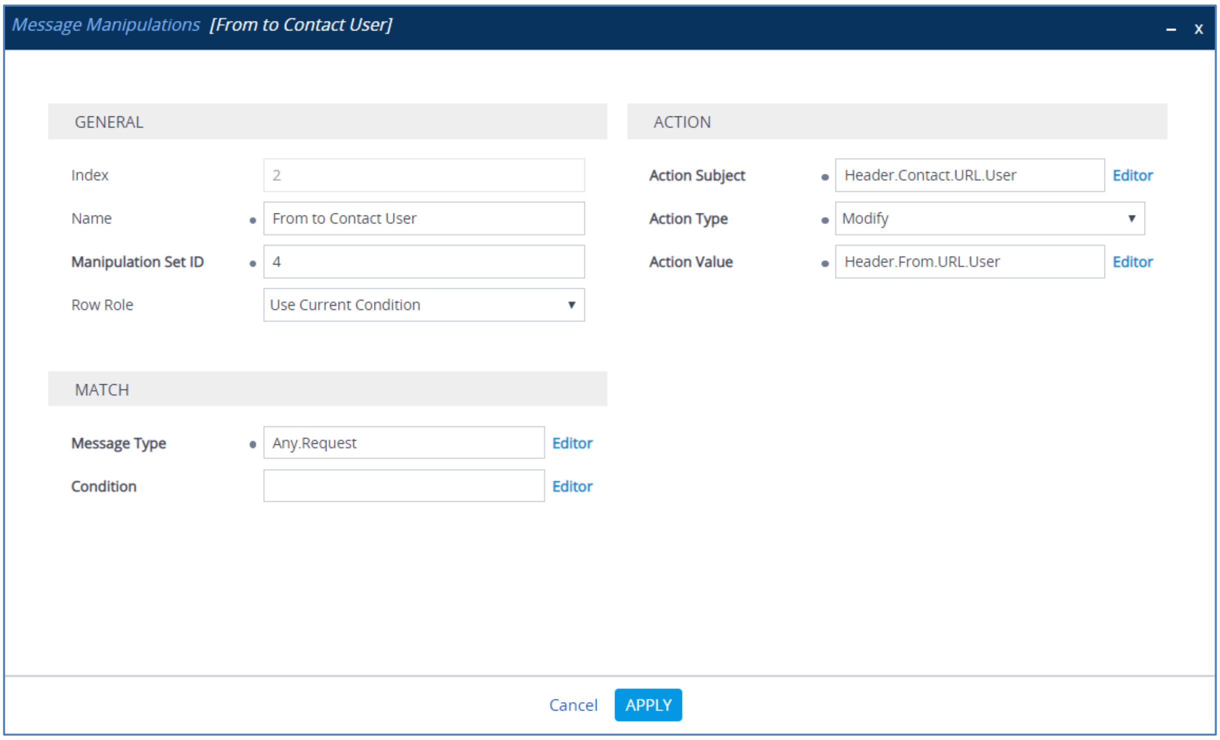
Figure 4-38: Configuring SIP Message Manipulation Rule 1 (for autphone SIP Trunk)



4. Configure another manipulation rule (Manipulation Set 4) for autphone SIP Trunk. This rule applies to all request messages sent to the autphone SIP Trunk IP. This replaces the user part of the SIP Contact Header with the value from the SIP From Header.

Parameter	Value
Index	**2**
Name	**From to Contact User**
Manipulation Set ID	**4**
Message Type	**Any.Request**
Action Subject	**Header.Contact.URL.User**
Action Type	**Modify**
Action Value	**Header.From.URL.User**

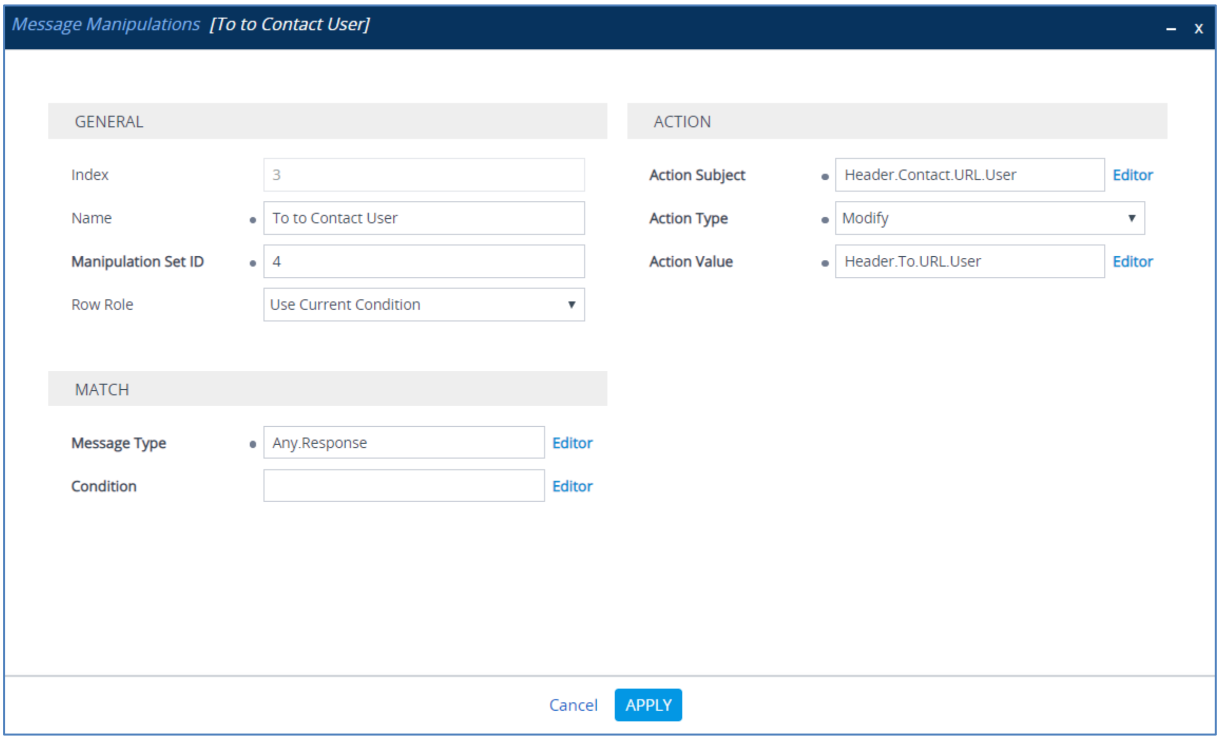
Figure 4-39: Configuring SIP Message Manipulation Rule 2 (for autphone SIP Trunk)



5. Configure another manipulation rule (Manipulation Set 4) for autphone SIP Trunk. This rule applies to all response messages sent to the autphone SIP Trunk IP. This replaces the user part of the SIP Contact Header with the value from the SIP To Header.

Parameter	Value
Index	**3**
Name	**To to Contact User**
Manipulation Set ID	**4**
Message Type	**Any.Response**
Action Subject	**Header.Contact.URL.User**
Action Type	**Modify**
Action Value	**Header.To.URL.User**

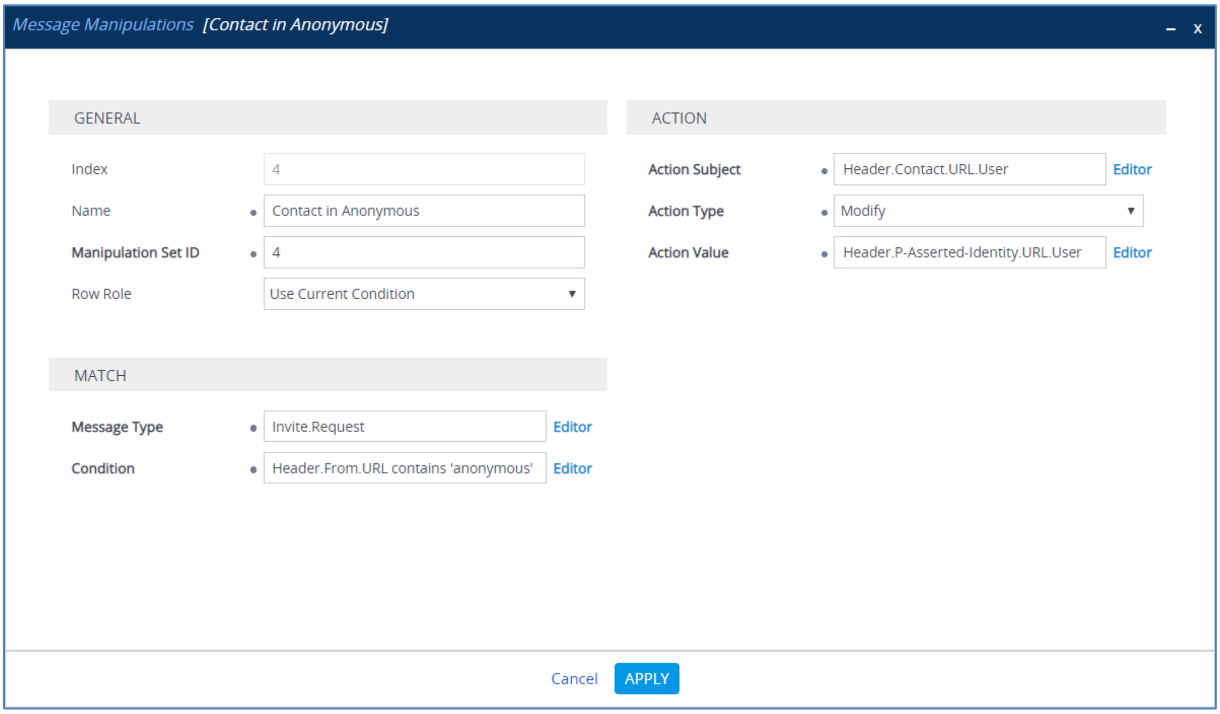
Figure 4-40: Configuring SIP Message Manipulation Rule 3 (for autphone SIP Trunk)



6. Configure another manipulation rule (Manipulation Set 4) for autphone SIP Trunk. This rule applies to all INVITE request messages sent to the autphone SIP Trunk IP in the call with presentation restriction. This replaces the user part of the SIP Contact Header with the value from the SIP P-Asserted-Identity Header.

Parameter	Value
Index	**4**
Name	**Contact in Anonymous**
Manipulation Set ID	**4**
Message Type	**Invite.Request**
Condition	**Header.From.URL contains 'anonymous'**
Action Subject	**Header.Contact.URL.User**
Action Type	**Modify**
Action Value	**Header.P-Asserted-Identity.URL.User**

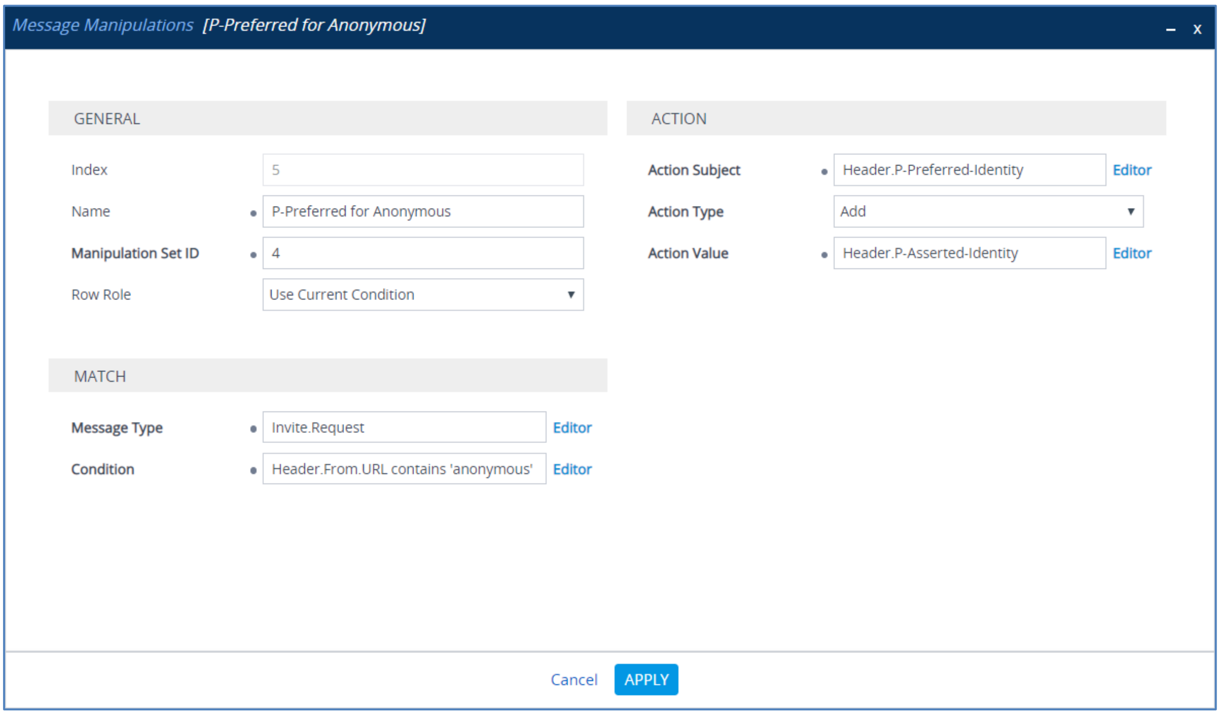
Figure 4-41: Configuring SIP Message Manipulation Rule 4 (for autphone SIP Trunk)



7. Configure another manipulation rule (Manipulation Set 4) for autphone SIP Trunk. This rule applies to all INVITE request messages sent to the autphone SIP Trunk IP in the call with presentation restriction. This replaces the user part of the SIP Contact Header with the value from the SIP P-Asserted-Identity Header.

Parameter	Value
Index	**5**
Name	**P-Preferred for Anonymous**
Manipulation Set ID	**4**
Message Type	**Invite.Request**
Condition	**Header.From.URL contains 'anonymous'**
Action Subject	**Header.P-Preferred-Identity**
Action Type	**Add**
Action Value	**Header.P-Asserted-Identity**

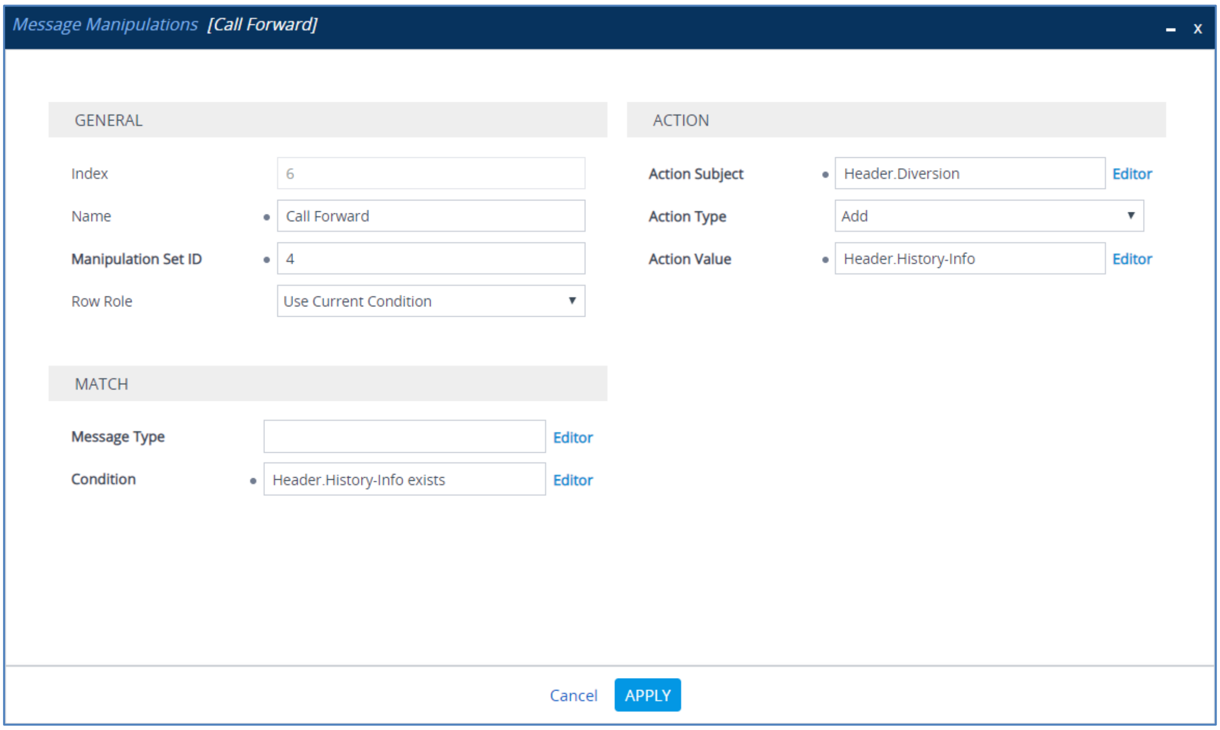
Figure 4-42: Configuring SIP Message Manipulation Rule 5 (for autphone SIP Trunk)



8. Configure another manipulation rule (Manipulation Set 4) for autphone SIP Trunk. This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Forward scenario. This adds the SIP Diversion Header with the value of the SIP History-Info Header, if it exists.

Parameter	Value
Index	**6**
Name	**Call Forward**
Manipulation Set ID	**4**
Condition	**Header.History-Info exists**
Action Subject	**Header.Diversion**
Action Type	**Add**
Action Value	**Header.History-Info**

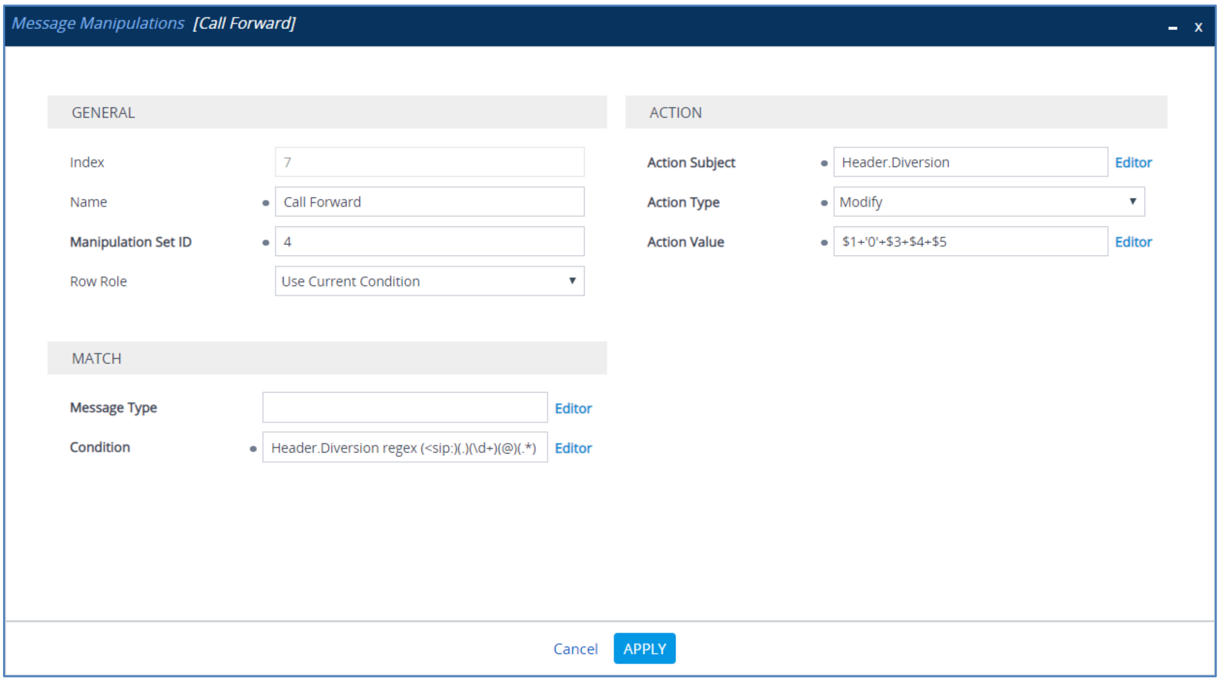
Figure 4-43: Configuring SIP Message Manipulation Rule 6 (for autphone SIP Trunk)



9. Configure another manipulation rule (Manipulation Set 4) for autphone SIP Trunk. This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Forward scenario. This replaces the '+' prefix of the user part of the SIP Diversion Header with the '0'.

Parameter	Value
Index	**7**
Name	**Call Forward**
Manipulation Set ID	**4**
Condition	**Header.Diversion regex (<sip:)(.)(\d+)(@)(.*)**
Action Subject	**Header.Diversion**
Action Type	**Modify**
Action Value	**$1+'0'+$3+$4+$5**

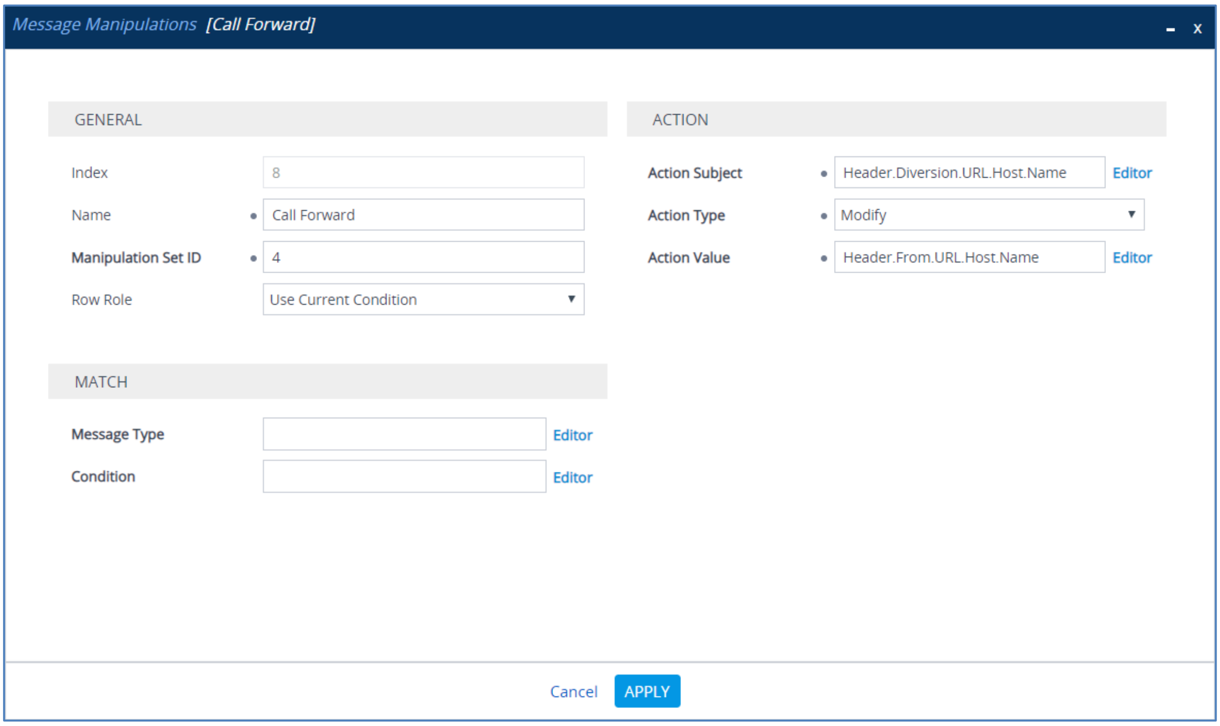
Figure 4-44: Configuring SIP Message Manipulation Rule 7 (for autphone SIP Trunk)



10. Configure another manipulation rule (Manipulation Set 4) for autphone SIP Trunk. This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Forward scenario. This replaces the host part of the SIP Diversion Header with the value from the SIP From Header.

Parameter	Value
Index	**8**
Name	**Call Forward**
Manipulation Set ID	**4**
Action Subject	**Header.Diversion.URL.Host.Name**
Action Type	**Modify**
Action Value	**Header.From.URL.Host.Name**

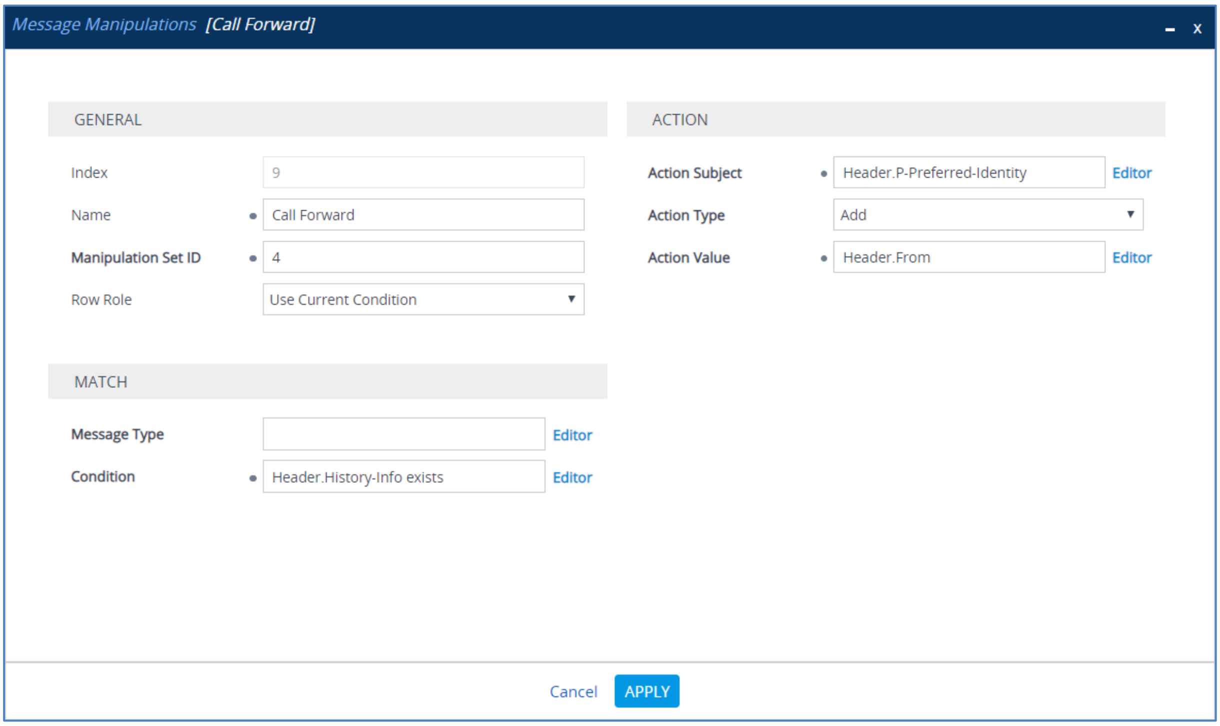
Figure 4-45: Configuring SIP Message Manipulation Rule 8 (for autphone SIP Trunk)



11. Configure another manipulation rule (Manipulation Set 4) for autphone SIP Trunk. This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Forward scenario. This adds the SIP P-Preferred-Identity Header with the value from the SIP From Header.

Parameter	Value
Index	**9**
Name	**Call Forward**
Manipulation Set ID	**4**
Condition	**Header.History-Info exists**
Action Subject	**Header.P-Preferred-Identity**
Action Type	**Add**
Action Value	**Header.From**

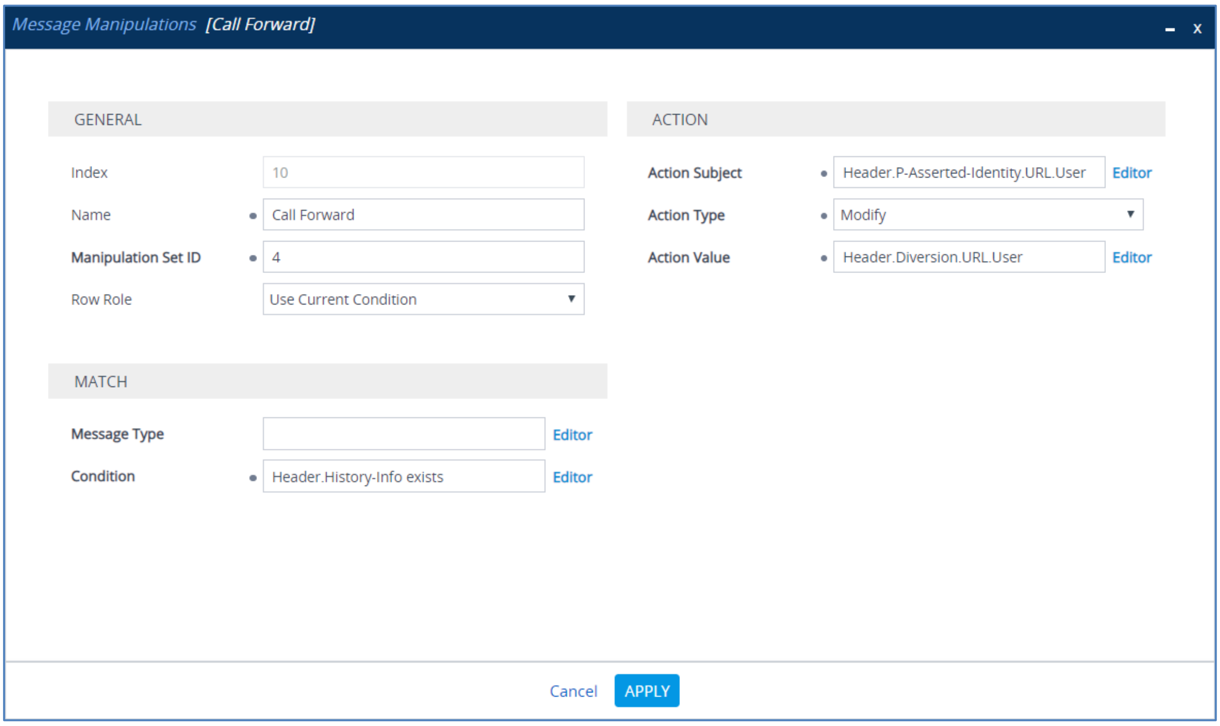
Figure 4-46: Configuring SIP Message Manipulation Rule 9 (for autphone SIP Trunk)



12. Configure another manipulation rule (Manipulation Set 4) for autphone SIP Trunk. This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Forward scenario. This replaces the user part of the SIP P-Asserted-Identity Header with the value from the SIP Diversion Header.

Parameter	Value
Index	**10**
Name	**Call Forward**
Manipulation Set ID	**4**
Condition	**Header.History-Info exists**
Action Subject	**Header.P-Asserted-Identity.URL.User**
Action Type	**Modify**
Action Value	**Header.Diversion.URL.User**

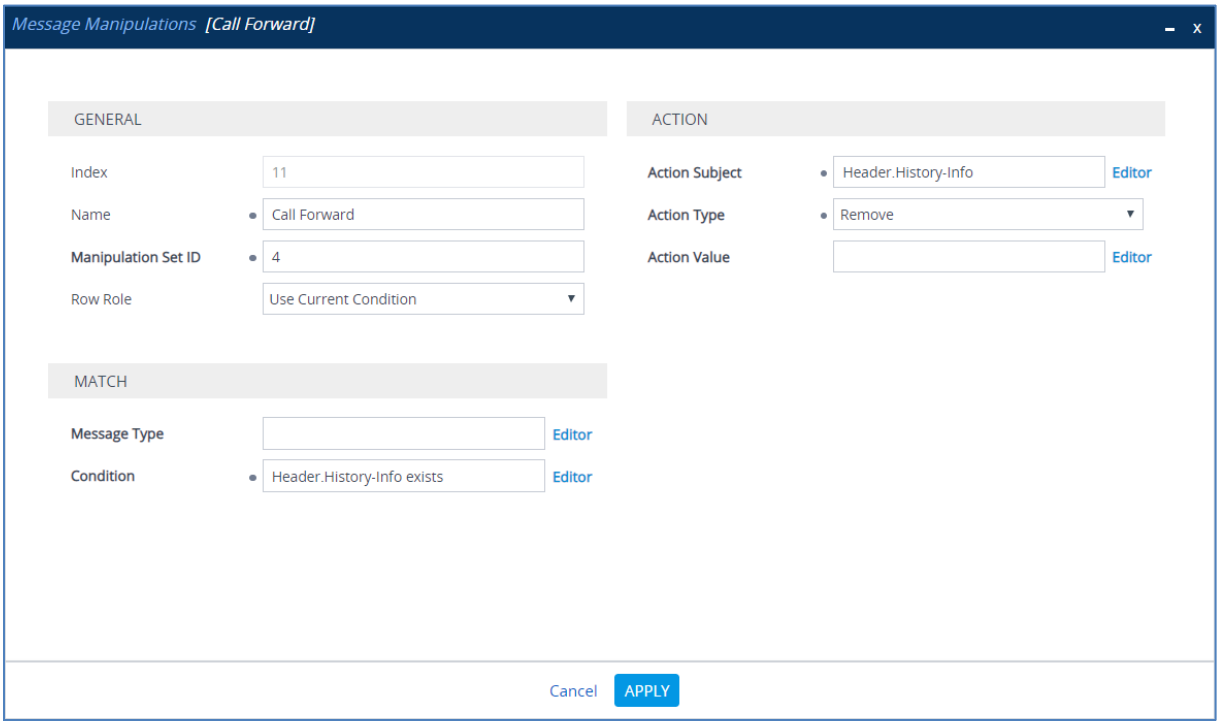
Figure 4-47: Configuring SIP Message Manipulation Rule 10 (for autphone SIP Trunk)



13. Configure another manipulation rule (Manipulation Set 4) for autphone SIP Trunk. This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Forward scenario. This removes the SIP History-Info Header if it exists.

Parameter	Value
Index	**11**
Name	**Call Forward**
Manipulation Set ID	**4**
Condition	**Header.History-Info exists**
Action Subject	**Header.History-Info**
Action Type	**Remove**

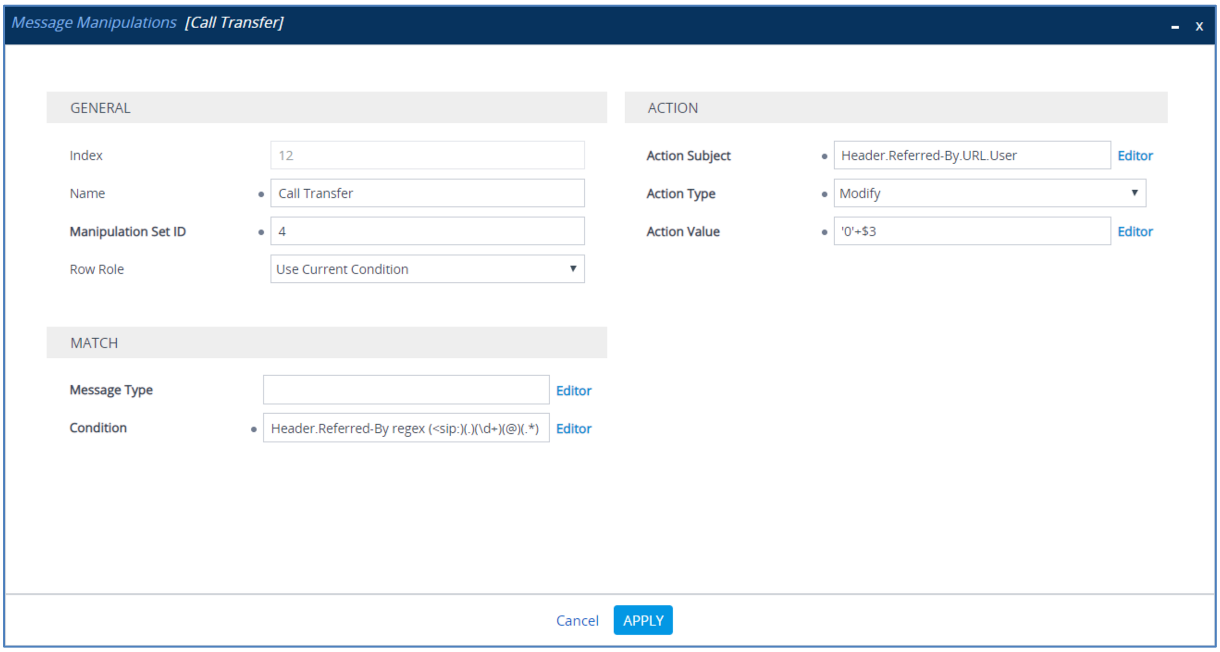
Figure 4-48: Configuring SIP Message Manipulation Rule 11 (for autphone SIP Trunk)



14. Configure another manipulation rule (Manipulation Set 4) for autphone SIP Trunk. This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Transfer scenario. This replaces the '+' prefix of the user part of the SIP Referred-By Header with the '0'.

Parameter	Value
Index	**12**
Name	**Call Transfer**
Manipulation Set ID	**4**
Condition	**Header.Referred-By regex (<sip:)(.)(\d+)(@)(.*)**
Action Subject	**Header.Referred-By.URL.User**
Action Type	**Modify**
Action Value	**'0'+$3**

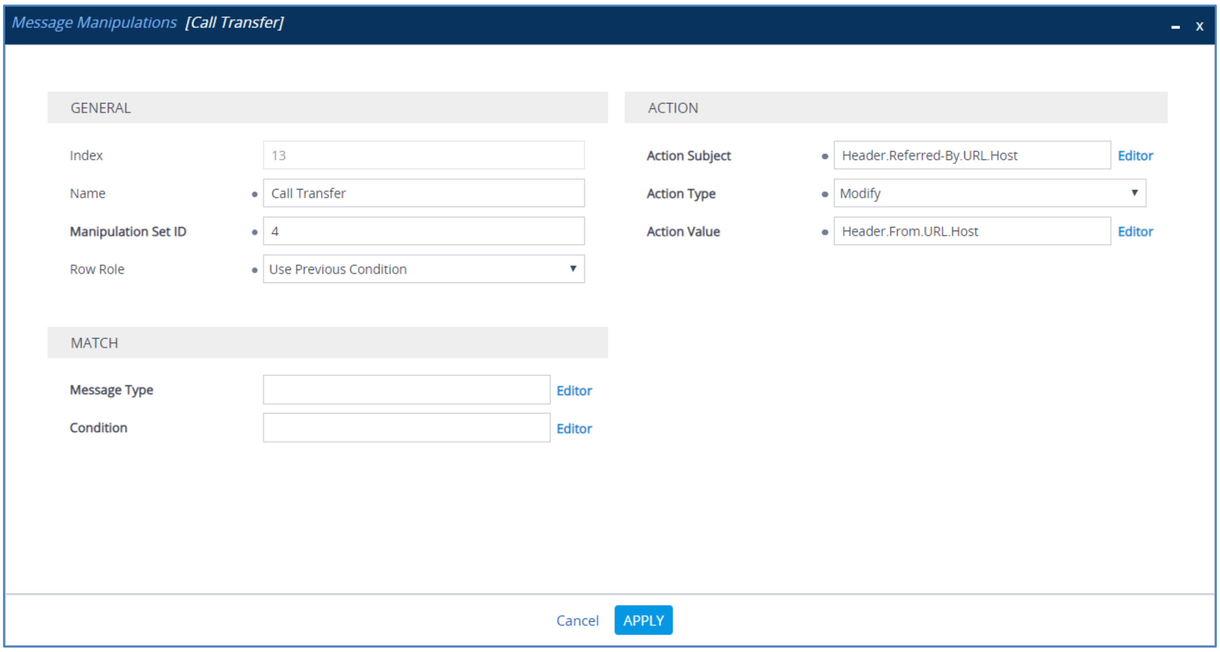
Figure 4-49: Configuring SIP Message Manipulation Rule 12 (for autphone SIP Trunk)



15. If the manipulation rule Index 12 (above) is executed, then the following rule is also executed on the same SIP message. This rule applies to messages sent to the autphone SIP Trunk IP Group in a call transfer scenario. This replaces the host part of the SIP Referred-By Header with the value from the SIP From Header.

Parameter	Value
Index	**13**
Name	**Call Transfer**
Manipulation Set ID	**4**
Row Role	**Use Previous Condition**
Action Subject	**Header.Referred-By.URL.Host**
Action Type	**Modify**
Action Value	**Header.From.URL.Host**

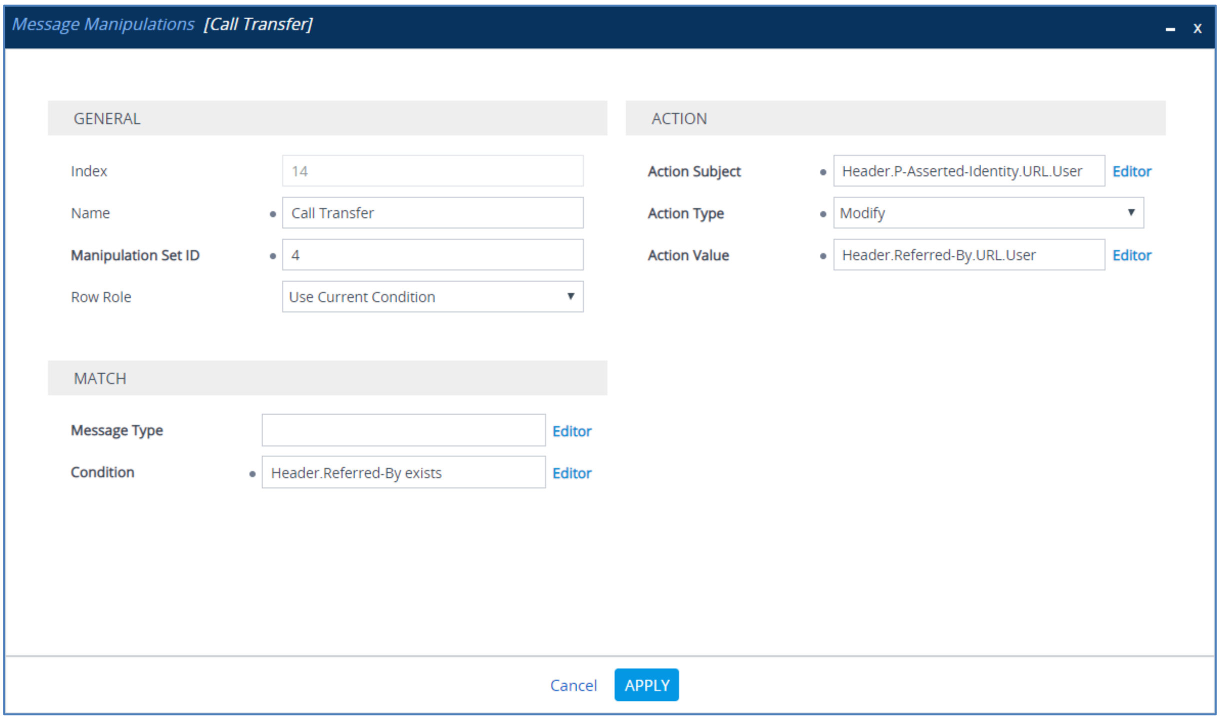
Figure 4-50: Configuring SIP Message Manipulation Rule 13 (for autphone SIP Trunk)



16. Configure another manipulation rule (Manipulation Set 4) for autphone SIP Trunk. This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Transfer scenario. This replaces the user part of the SIP P-Asserted-Identity Header with the value from the SIP Referred-By Header.

Parameter	Value
Index	**14**
Name	**Call Transfer**
Manipulation Set ID	**4**
Condition	**Header.Referred-By exists**
Action Subject	**Header.P-Asserted-Identity.URL.User**
Action Type	**Modify**
Action Value	**Header.Referred-By.URL.User**

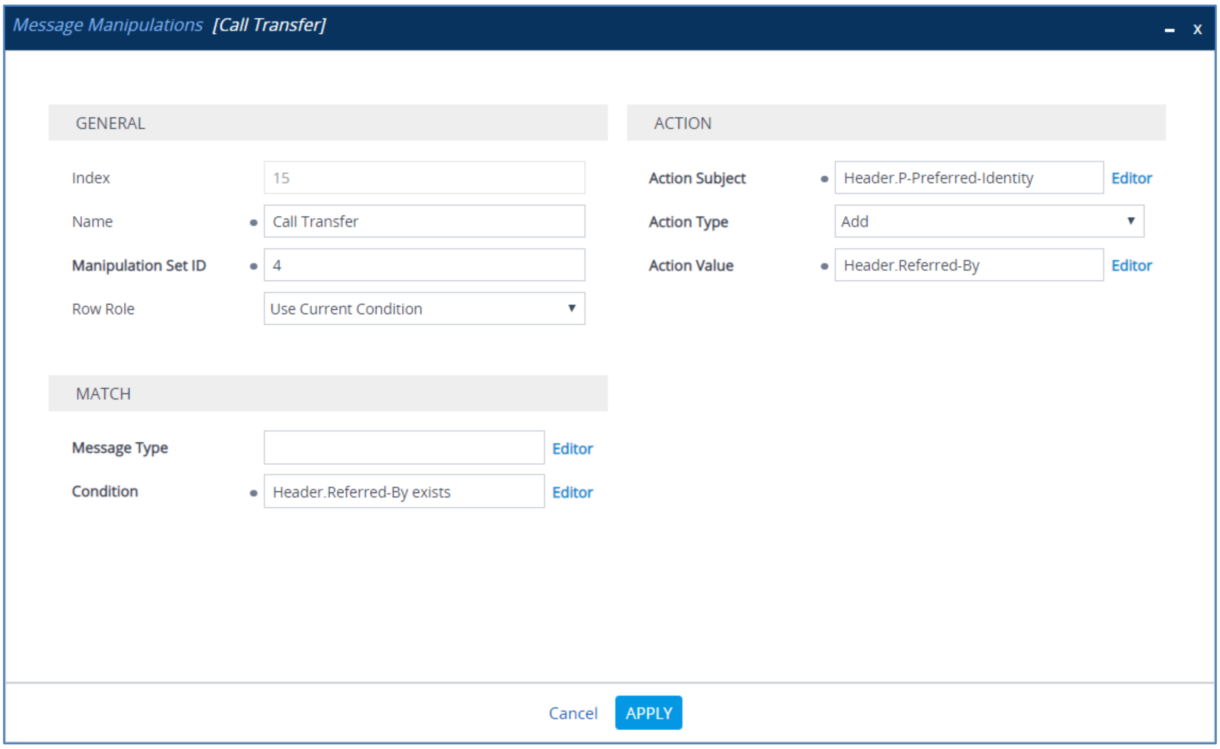
Figure 4-51: Configuring SIP Message Manipulation Rule 14 (for autphone SIP Trunk)



17. Configure another manipulation rule (Manipulation Set 4) for autphone SIP Trunk. This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Transfer scenario. This adds the SIP P-Preferred-Identity Header with the value from the SIP Referred-By Header.

Parameter	Value
Index	**15**
Name	**Call Transfer**
Manipulation Set ID	**4**
Condition	**Header.Referred-By exists**
Action Subject	**Header.P-Preferred-Identity**
Action Type	**Add**
Action Value	**Header.Referred-By**

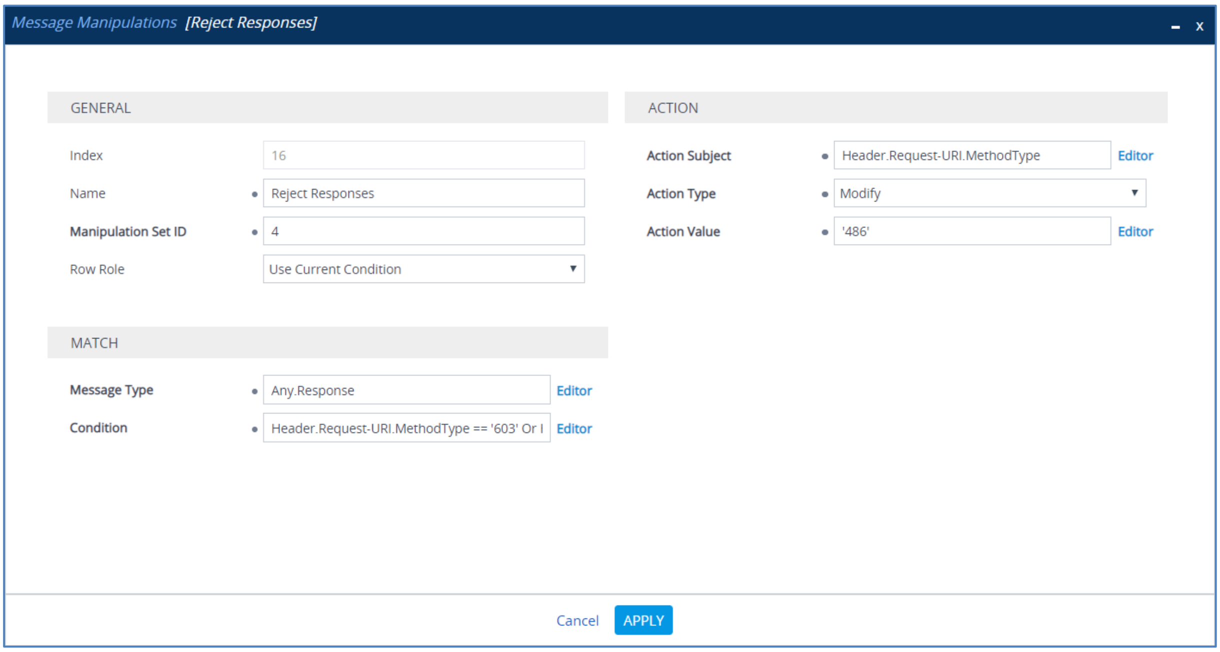
Figure 4-52: Configuring SIP Message Manipulation Rule 15 (for autphone SIP Trunk)



18. Configure another manipulation rule (Manipulation Set 4) for autphone SIP Trunk. This rule is applied to response messages sent to the autphone SIP Trunk IP Group for Rejected Calls initiated by the Teams Direct Routing IP Group. This replaces method types ‘603’, ‘503’ or ‘500’ with the value ‘486’, because autphone SIP Trunk does not recognize these method types.

Parameter	Value
Index	**16**
Name	**Reject Responses**
Manipulation Set ID	**4**
Message Type	**Any.Response**
Condition	**Header.Request-URI.MethodType == '603' Or Header.Request-URI.MethodType == '503' Or Header.Request-URI.MethodType == '500'**
Action Subject	**Header.Request-URI.MethodType**
Action Type	**Modify**
Action Value	**'486'**

Figure 4-53: Configuring SIP Message Manipulation Rule 16 (for autphone SIP Trunk)



19. Configure another manipulation rule (Manipulation Set 4) for autphone SIP Trunk. This rule is applied to response messages sent to the autphone SIP Trunk IP Group for Rejected Calls initiated by the Teams Direct Routing IP Group. This removes the SIP Reason Header.

Parameter	Value
Index	**17**
Name	**Reject Responses**
Manipulation Set ID	**4**
Message Type	**Any.Response**
Action Subject	**Header.Reason**
Action Type	**Remove**

Figure 4-54: Configuring SIP Message Manipulation Rule 17 (for autphone SIP Trunk)

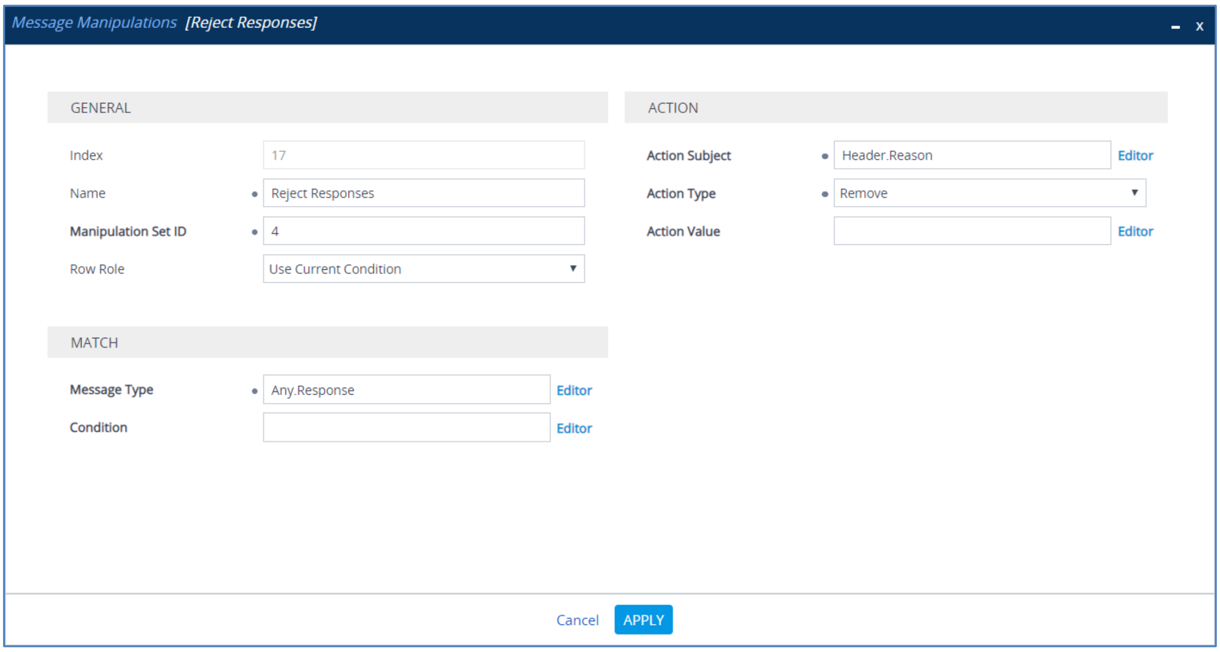
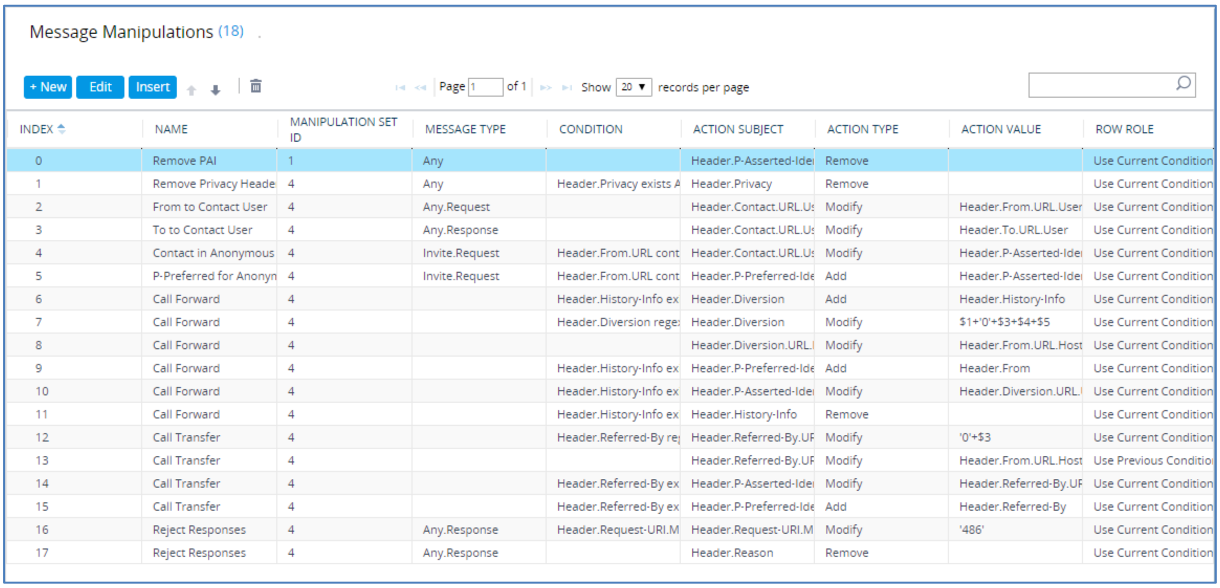


Figure 4-55: Example of Configured SIP Message Manipulation Rules


Message Manipulations (18)

+ New Edit Insert Page 1 of 1 Show 20 records per page

INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	Remove PAI	1	Any		Header.P-Asserted-Ide	Remove		Use Current Condition
1	Remove Privacy Heade	4	Any	Header.Privacy exists A	Header.Privacy	Remove		Use Current Condition
2	From to Contact User	4	Any.Request		Header.Contact.URL.Us	Modify	Header.From.URL.User	Use Current Condition
3	To to Contact User	4	Any.Response		Header.Contact.URL.Us	Modify	Header.To.URL.User	Use Current Condition
4	Contact in Anonymous	4	Invite.Request	Header.From.URL cont	Header.Contact.URL.Us	Modify	Header.P-Asserted-Ide	Use Current Condition
5	P-Preferred for Anonyn	4	Invite.Request	Header.From.URL cont	Header.P-Preferred-Ide	Add	Header.P-Asserted-Ide	Use Current Condition
6	Call Forward	4		Header.History-Info ex	Header.Diversion	Add	Header.History-Info	Use Current Condition
7	Call Forward	4		Header.Diversion rege:	Header.Diversion	Modify	$1+'0'+$3+$4+$5	Use Current Condition
8	Call Forward	4			Header.Diversion.URL.I	Modify	Header.From.URL.Host	Use Current Condition
9	Call Forward	4		Header.History-Info ex	Header.P-Preferred-Ide	Add	Header.From	Use Current Condition
10	Call Forward	4		Header.History-Info ex	Header.P-Asserted-Ide	Modify	Header.Diversion.URL.I	Use Current Condition
11	Call Forward	4		Header.History-Info ex	Header.History-Info	Remove		Use Current Condition
12	Call Transfer	4		Header.Referred-By re	Header.Referred-By.UF	Modify	'0'+$3	Use Current Condition
13	Call Transfer	4			Header.Referred-By.UF	Modify	Header.From.URL.Host	Use Previous Conditio
14	Call Transfer	4		Header.Referred-By ex	Header.P-Asserted-Ide	Modify	Header.Referred-By.UF	Use Current Condition
15	Call Transfer	4		Header.Referred-By ex	Header.P-Preferred-Ide	Add	Header.Referred-By	Use Current Condition
16	Reject Responses	4	Any.Response	Header.Request-URI.M	Header.Request-URI.M	Modify	'486'	Use Current Condition
17	Reject Responses	4	Any.Response		Header.Reason	Remove		Use Current Condition

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

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule applies to messages received from the Teams IP Group. This removes the SIP P-Asserted-Identity Header.	Microsoft Office 365 may be configured to send the PAI header, but we recommend to do this in the SBC for better interoperability.
1	This rule applies to messages sent to the autphone SIP Trunk IP. This removes the SIP Privacy Header in all messages, except for a call with presentation restrictions.	The same as in the previous rule.
2	This rule applies to all request messages sent to the autphone SIP Trunk IP. This replaces the user part of the SIP Contact Header with the value from the SIP From Header.	According to the autphone SIP Trunk requirement.
3	This rule applies to all <u>response</u> messages sent to the autphone SIP Trunk IP. This replaces the user part of the SIP Contact Header with the value from the SIP To Header.	According to the autphone SIP Trunk requirement.
4	This rule applies to all INVITE request messages sent to the autphone SIP Trunk IP in the call with presentation restriction. This replaces the user part of the SIP Contact Header with the value from the SIP P-Asserted-Identity Header.	According to the autphone SIP Trunk requirement.

Rule Index	Rule Description	Reason for Introducing Rule
5	This rule applies to all INVITE request messages sent to the autphone SIP Trunk IP in the call with presentation restriction. This replaces the user part of the SIP Contact Header with the value from the SIP P-Asserted-Identity Header.	According to the autphone SIP Trunk requirement.
6	This rule applies to messages sent to the autphone SIP Trunk IP Group in a call forward scenario. This add the SIP Diversion Header with the value of the SIP History-Info Header, if it exists.	For Call Forward scenarios (A calls B, which forwards the call to C), autphone SIP Trunk requires the following: ▪ Diversion SIP Header with B's number ▪ P-Preferred-Identity SIP Header with A's number ▪ P-Asserted-Identity SIP Header with B's number
7	This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Forward scenario. This replaces the '+' prefix of the user part of the SIP Diversion Header with the '0'.	
8	This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Forward scenario. This replaces the host part of the SIP Diversion Header with value from the SIP From Header.	
9	This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Forward scenario. This adds the SIP P-Preferred-Identity Header with the value from the SIP From Header.	
10	This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Forward scenario. This replaces the user part of the SIP P-Asserted-Identity Header with the value from the SIP Diversion Header.	
11	This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Forward scenario. This removes the SIP History-Info Header, if it exists.	
12	This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Transfer scenario. This replaces the '+' prefix of the user part of the SIP Referred-By Header with the '0'.	For Call Transfer scenarios (A calls B, which transfers the call to C), autphone SIP Trunk requires the following: ▪ Referred-By SIP Header with B's number ▪ P-Preferred-Identity SIP Header with B's number ▪ P-Asserted-Identity SIP Header with B's number
13	This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Transfer scenario. This replaces the host part of the SIP Referred-By Header with the value from the SIP From Header.	
14	This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Transfer scenario. This replaces the user part of the SIP P-Asserted-Identity Header with the value from the SIP Referred-By Header.	
15	This rule applies to messages sent to the autphone SIP Trunk IP Group in a Call Transfer scenario. This adds the SIP P-Preferred-Identity Header with the value from the SIP Referred-By Header.	
16	This rule is applied to response messages sent to the autphone SIP Trunk IP Group for Rejected Calls initiated by the Teams Direct Routing IP Group. This replaces the method types '603', '503' or '500' with the value '486', because autphone SIP Trunk not recognizes these method types.	autphone SIP Trunk does not recognize these method types and continues to send SIP Invite messages.

Rule Index	Rule Description	Reason for Introducing Rule
17	This rule is applied to response messages sent to the autphone SIP Trunk IP Group for Rejected Calls initiated by the Teams Direct Routing IP Group. This remove the SIP Reason Header.	The same as in previous rule.

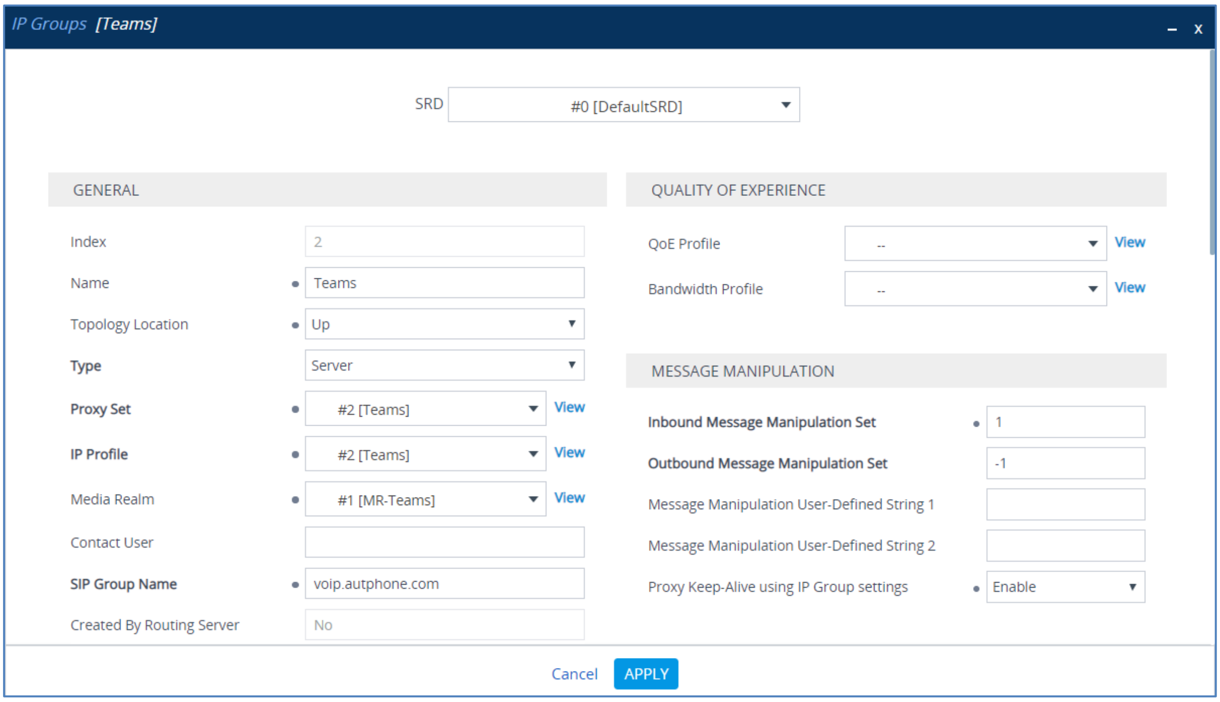
20. Assign Manipulation Set IDs 1 to the Teams Direct Routing IP Group:

a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).

b. Select the row of the Teams Direct Routing IP Group, and then click **Edit**.

c. Set the 'Inbound Message Manipulation Set' field to **1**.

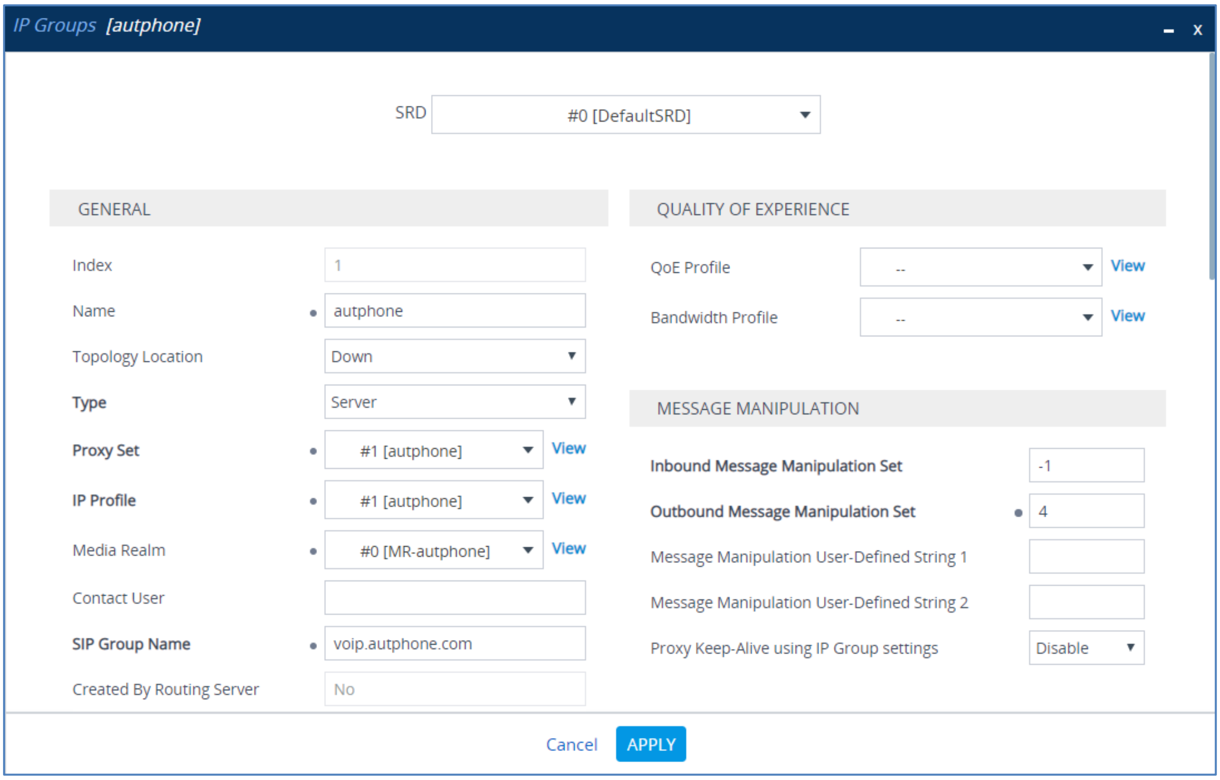
Figure 4-56: Assigning Manipulation Set to the Teams Direct Routing IP Group



d. Click **Apply**.

21. Assign Manipulation Set ID 4 to the autphone 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 autphone SIP trunk IP Group, and then click **Edit**.
    c. Set the 'Outbound Message Manipulation Set' field to **4**.

Figure 4-57: Assigning Manipulation Set 4 to the autphone SIP Trunk IP Group



    d. Click **Apply**.

4.16 Configure Registration Accounts

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

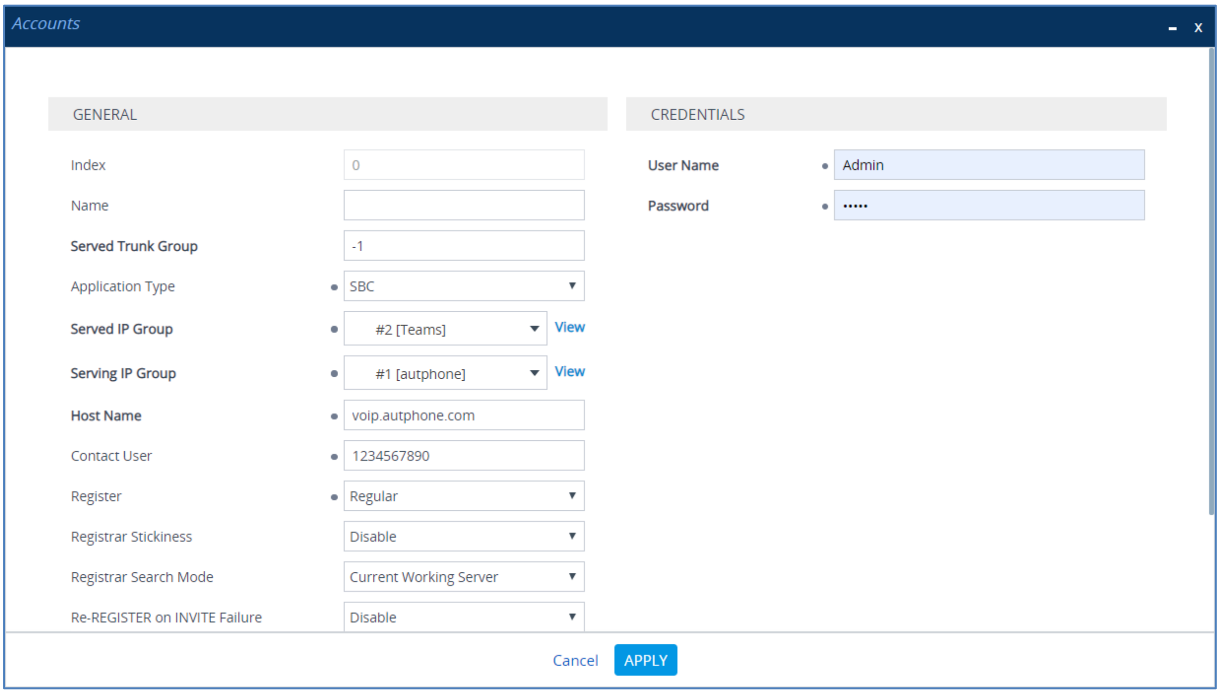
In the interoperability test topology, the Served IP Group is Teams Direct Routing IP Group and the Serving IP Group is autphone SIP Trunk IP Group.

➢ **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
Application Type	**SBC**
Served IP Group	**Teams**
Serving IP Group	**autphone**
Host Name	As provided by the SIP Trunk provider
Register	**Regular**
Contact User	As provided by the SIP Trunk provider
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

Figure 4-58: Configuring a SIP Registration Account



4. Click **Apply**.

4.17 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

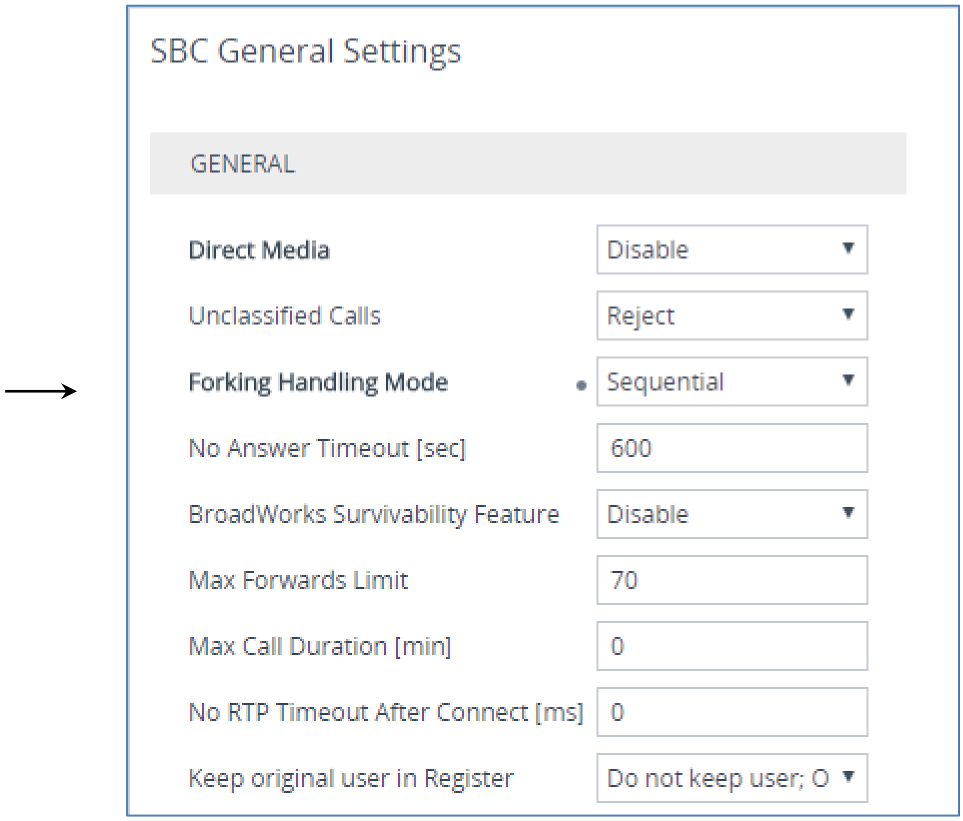
4.17.1 Configure Call Forking Mode

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

➢ **To configure call forking:**

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

Figure 4-59: Configuring Forking Mode



3. Click **Apply**.

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

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

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

➢ **To optimize core allocation for a profile:**

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

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

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 17, 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: M800B
;Board Type: 72
;Serial Number: 5299378
;Slot Number: 1
;Software Version: 7.20A.250.273
;DSP Software Version: 5014AE3_R => 710.11
;Board IP Address: 10.15.77.55
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 512M   Flash size: 64M   Core speed: 500Mhz
;Num of DSP Cores: 3
;Num of physical LAN ports: 4
;Profile: NONE
;;;Key features:;Board Type: M800B ;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 ;DSP Voice
features: RTCP-XR ;DATA features: ;Channel Type: DspCh=30 IPMediaDspCh=30
;HA ;E1Trunks=1 ;T1Trunks=1 ;FXSPorts=4 ;FXOPorts=0 ;BRITrunks=4 ;IP
Media: Conf VXML ;QOE features: VoiceQualityMonitoring MediaEnhancement
;Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
;Control Protocols: MGCP SIP SBC=250 TEAMS MSFT FEU=100 TestCall=100
;Default features:;Coders: G711 G726;

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


[SYSTEM Params]

SyslogServerIP = 10.10.10.10
EnableSyslog = 1
NTPServerUTCOffset = 7200
TLSPkeySize = 2048
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '10.15.28.1'
```

```
SBCWizardFilename = 'templates4.zip'

[BSP Params]

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

[Analog Params]


[ControlProtocols Params]

AdminStateLockControl = 0

[PSTN Params]

V5ProtocolSide = 0

[Voice Engine Params]

BrokenConnectionEventTimeout = 1000
ENABLEMEDIASECURITY = 1
PLThresholdLevelsPerMille_0 = 5
PLThresholdLevelsPerMille_1 = 10
PLThresholdLevelsPerMille_2 = 20
PLThresholdLevelsPerMille_3 = 50
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

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

[SIP Params]

GWDEBUGLEVEL = 5
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCESMODE = 1
MEDIACDRREPORTLEVEL = 1
SBCFORKINGHANDLINGMODE = 1
SBCSESSIONEXPIRES = 1800
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144

[SNMP Params]


[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember;
PhysicalPortsTable 0 = "GE_4_1", 1, 4, "User Port #0", "GROUP_1";
PhysicalPortsTable 1 = "GE_4_2", 1, 4, "User Port #1", "GROUP_1";
PhysicalPortsTable 2 = "GE_4_3", 1, 4, "User Port #2", "GROUP_2";
PhysicalPortsTable 3 = "GE_4_4", 1, 4, "User Port #3", "GROUP_2";
```

```
[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";

[ \EtherGroupTable ]


[ DeviceTable ]

FORMAT 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, 10.15.77.55, 16, 10.15.0.1, "LAN_IF",
10.15.27.1, , "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.157, 24, 195.189.192.129, "WAN_IF",
80.179.52.100, 80.179.55.100, "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",
"$1$bgtdFkgQREJNFRNJHUhDGRtPTuPju+bhteC1ubG4vby9t7fy9fb1oqfyoKmt+KP5/qz9m
ZSTlpyUkpDNzMudz54=", 1, 0, 5, -1, 15, 60, 200,
"e4064f90b5b26631d46fbcdb79f2b7a0", ".fc";
WebUsers 1 = "User",
"$1$Cj46OmhtN3ElJiolcSQnfXh4Ii5+Jn4ZRBQRHR0fHx4bTB9ITE8aVgRQVQUGAAEPXVkCD
w0GWSEgIHN0dHB2LHE=", 1, 0, 5, -1, 15, 60, 50,
"c26a27dd91a886b99de5e81b9a736232", "";

[ \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", 0, 0, "DEFAULT", "DEFAULT", 0, 0, 0.0.0.0,
0.0.0.0, 2560, 0, 1024;
TLSContexts 1 = "Teams", 4, 0, "RC4:AES128", "DEFAULT", 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 = "autphone Allowed Coders";

[ \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_SBCDiversionMode,
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 = "autphone", 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,
"", "autphone Allowed Coders", "", 0, 2, 0, 0, 0, 1, 0, 8, 300, 400, 0,
0, 0, "", 0, 0, 1, 3, 3, 2, 2, 1, 3, 2, 1, 0, 1, 0, 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, "", "", 0, 0, "",
"", "", 0, 1, 0, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0, 0,
1, 0, 3, 2, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 3, 0,
0, 0, 0, 0, 0, 1, 0, 0, 300, -1, -1, 0, 0, 1, 0, 0, 0, 0, -1, -1, -1, -1,
-1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1, 0, 0;

[ \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-autphone", "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_AdditionalUDPPortsMode,
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_CallSetupRulesSetId;
SIPInterface 0 = "autphone", "WAN_IF", 2, 55060, 0, 0, "", 0,
"DefaultSRD", "", "default", -1, 0, 500, -1, 0, "MR-autphone", 0, -1, -1,
-1, 0, 0, "", "", -1;
SIPInterface 1 = "Teams", "WAN_IF", 2, 0, 0, 5061, "", 0, "DefaultSRD",
"", "Teams", -1, 1, 0, -1, 0, "MR-Teams", 1, -1, -1, -1, 0, 1, "", "", -
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, "",
"", "autphone", "", "", 1, 1, 10, -1;
ProxySet 1 = "autphone", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"", "autphone", "", "", 1, 1, 10, -1;
ProxySet 2 = "Teams", 1, 60, 2, 1, "DefaultSRD", 0, "Teams", -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_SBCServerAuthType, IPGroup_OAuthHTTPService,
IPGroup_EnableSBCClientForking, 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_ProxyKeepAliveUsingIPG;
IPGroup 0 = 0, "Default_IPG", "ProxySet_0", "", "", -1, 0, "DefaultSRD",
"", 0, "", -1, -1, -1, 0, 0, "", -1, "", 0, -1, -1, "", "", "$1$gQ==", 0,
"", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0,
"", 0;
IPGroup 1 = 0, "autphone", "autphone", "voip.autphone.com", "", -1, 0,
"DefaultSRD", "MR-autphone", 1, "autphone", -1, -1, 4, 0, 0, "", -1, "",
0, -1, -1, "", "Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "", 0, 0,
"default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, "", 0;
```

```
IPGroup 2 = 0, "Teams", "Teams", "voip.autphone.com", "", -1, 0,
"DefaultSRD", "MR-Teams", 0, "Teams", -1, 1, -1, 0, 0, "", -1, "", 0, -1,
-1, "int-sbc2.audctrunk.aceducation.info", "Admin", "$1$aCkNBwIC", 0, "",
"", 1, "", "", 0, 0, "", 0, 0, -1, 0, 0, 1, "", -1, "", 0, 0, "", 1;

[ \IPGroup ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType, ProxyIp_Priority,
ProxyIp_Weight;
ProxyIp 0 = "1", 0, "voip.autphone.com:55060", 0, 0, 0;
ProxyIp 1 = "2", 0, "sip.pstnhub.microsoft.com:5061", 2, 1, 1;
ProxyIp 2 = "2", 1, "sip2.pstnhub.microsoft.com:5061", 2, 2, 1;
ProxyIp 3 = "2", 2, "sip3.pstnhub.microsoft.com:5061", 2, 3, 1;

[ \ProxyIp ]


[ Account ]

FORMAT Account_Index = Account_AccountName, 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_ReRegisterOnInviteFailure;
Account 0 = "", -1, "Teams", "autphone", "kK7yRmE3fABn56vE",
"$1$suT2jfTX8cz7/vnf1vjXhrg=", "voip.autphone.com", "32217214021", 1, 0,
0, 0, 2, 0, 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 re-routing", "Default_SBCRoutingPolicy", "Any",
"*", "*", "*", "*", 0, "", "Teams", 2, -1, 2, "Teams", "", "", 0, -1, 0,
0, "", "", "", "", "default", "";
IP2IPRouting 2 = "Teams to SIP Trunk", "Default_SBCRoutingPolicy",
"Teams", "*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "autphone", "", "",
0, -1, 0, 0, "", "", "", "", "default", "";
IP2IPRouting 3 = "SIP Trunk to Teams", "Default_SBCRoutingPolicy",
"autphone", "*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "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_IPGroupSelection, Classification_IpGroupTagName;
Classification 0 = "Teams", "Teams-Contact", "DefaultSRD", "Teams",
"52.114.*.*", 0, -1, "*", "*", "*", "int-
sbc2.audctrunk.aceducation.info", 1, "Teams", "", "", 0, "default";

[ \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 = "To Teams (Dest)", "Default_SBCRoutingPolicy",
0, "autphone", "Teams", "*", "*", "0", "*", "*", "", 0, "Any", 0, 1, 1,
0, 255, "+", "", 0, "", "";
```

```
IPOutboundManipulation 1 = "To Teams (Src)", "Default_SBCRoutingPolicy",
0, "autphone", "Teams", "00", "*", "*", "*", "*", "", 0, "Any", 0, 0, 2,
0, 255, "+", "", 0, "", "";
IPOutboundManipulation 2 = "To autphone (Src)",
"Default_SBCRoutingPolicy", 0, "Teams", "autphone", "+8", "*", "*", "*",
"*", "", 0, "Any", 0, 0, 1, 0, 255, "0", "", 0, "", "";
IPOutboundManipulation 3 = "To autphone (Src)",
"Default_SBCRoutingPolicy", 0, "Teams", "autphone", "+", "*", "*", "*",
"*", "", 0, "Any", 0, 0, 1, 0, 255, "00", "", 0, "", "";
IPOutboundManipulation 4 = "To autphone (Emergency)",
"Default_SBCRoutingPolicy", 0, "Teams", "autphone", "*", "*", "+49xxx",
"*", "*", "", 0, "Any", 0, 1, 3, 0, 255, "", "", 0, "", "";
IPOutboundManipulation 5 = "To autphone (Dest)",
"Default_SBCRoutingPolicy", 0, "Teams", "autphone", "*", "*", "+", "*",
"*", "", 0, "Any", 0, 1, 1, 0, 255, "00", "", 0, "", "";

[ \IPOutboundManipulation ]


[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Remove PAI", 1, "Any", "", "Header.P-Asserted-
Identity", 1, "", 0;
MessageManipulations 1 = "Remove Privacy Header", 4, "Any",
"Header.Privacy exists And Header.From.URL !contains 'anonymous'",
"Header.Privacy", 1, "", 0;
MessageManipulations 2 = "From to Contact User", 4, "Any.Request", "",
"Header.Contact.URL.User", 2, "Header.From.URL.User", 0;
MessageManipulations 3 = "To to Contact User", 4, "Any.Response", "",
"Header.Contact.URL.User", 2, "Header.To.URL.User", 0;
MessageManipulations 4 = "Contact in Anonymous", 4, "Invite.Request",
"Header.From.URL contains 'anonymous'", "Header.Contact.URL.User", 2,
"Header.P-Asserted-Identity.URL.User", 0;
MessageManipulations 5 = "P-Preferred for Anonymous", 4,
"Invite.Request", "Header.From.URL contains 'anonymous'", "Header.P-
Preferred-Identity", 0, "Header.P-Asserted-Identity", 0;
MessageManipulations 6 = "Call Forward", 4, "", "Header.History-Info
exists", "Header.Diversion", 0, "Header.History-Info", 0;
MessageManipulations 7 = "Call Forward", 4, "", "Header.Diversion regex
(<sip:)(.)(\d+)(@)(.*)", "Header.Diversion", 2, "$1+'0'+$3+$4+$5", 0;
MessageManipulations 8 = "Call Forward", 4, "", "",
"Header.Diversion.URL.Host.Name", 2, "Header.From.URL.Host.Name", 0;
MessageManipulations 9 = "Call Forward", 4, "", "Header.History-Info
exists", "Header.P-Preferred-Identity", 0, "Header.From", 0;
MessageManipulations 10 = "Call Forward", 4, "", "Header.History-Info
exists", "Header.P-Asserted-Identity.URL.User", 2,
"Header.Diversion.URL.User", 0;
MessageManipulations 11 = "Call Forward", 4, "", "Header.History-Info
exists", "Header.History-Info", 1, "", 0;
MessageManipulations 12 = "Call Transfer", 4, "", "Header.Referred-By
regex (<sip:)(.)(\d+)(@)(.*)", "Header.Referred-By.URL.User", 2,
"'0'+$3", 0;
MessageManipulations 13 = "Call Transfer", 4, "", "", "Header.Referred-
By.URL.Host", 2, "Header.From.URL.Host", 1;
MessageManipulations 14 = "Call Transfer", 4, "", "Header.Referred-By
exists", "Header.P-Asserted-Identity.URL.User", 2, "Header.Referred-
By.URL.User", 0;
```

```
MessageManipulations 15 = "Call Transfer", 4, "", "Header.Referred-By
exists", "Header.P-Preferred-Identity", 0, "Header.Referred-By", 0;
MessageManipulations 16 = "Reject Responses", 4, "Any.Response",
"Header.Request-URI.MethodType == '603' Or Header.Request-URI.MethodType
== '503' Or Header.Request-URI.MethodType == '500'", "Header.Request-
URI.MethodType", 2, "'486'", 0;
MessageManipulations 17 = "Reject Responses", 4, "Any.Response", "",
"Header.Reason", 1, "", 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 = "autphone Allowed Coders", 0, 1, "";

[ \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, 2, 2, 90, -1, 1, "";
AudioCoders 1 = "AudioCodersGroups_0", 1, 1, 2, 90, -1, 1, "";
AudioCoders 2 = "AudioCodersGroups_1", 0, 35, 2, 19, 76, 0, "";
AudioCoders 3 = "AudioCodersGroups_1", 1, 36, 2, 43, 77, 0, "";
AudioCoders 4 = "AudioCodersGroups_1", 2, 1, 2, 90, -1, 0, "";
AudioCoders 5 = "AudioCodersGroups_1", 3, 2, 2, 90, -1, 0, "";
AudioCoders 6 = "AudioCodersGroups_1", 4, 3, 2, 19, -1, 0, "";

[ \AudioCoders ]
```

This page is intentionally left blank.

International Headquarters

1 Hayarden Street,

Airport City

Lod 7019900, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

200 Cottontail Lane

Suite A101E

Somerset NJ 08873

Tel: +1-732-469-0880

Fax: +1-732-469-2298

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

website: https://www.audiocodes.com

Document #: LTRT-33410