Configuration Note

AudioCodes Professional Services – Interoperability Lab

Microsoft® Teams Direct Routing Enterprise Model and DTAG'S DLAN SIP Trunk using AudioCodes Mediant™ SBC

Version 7.2

Deutsche Telekom

Microsoft Teams

Microsoft Partner
Gold Communications

audiocodes

Table of Contents

Notice

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

This document is subject to change without notice.

Date Published: January-17-2022

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes

Abbreviations and Terminology

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

Document Revision Record

LTRT	Description
12595	Initial document release for Version 7.2.
12596	Added changes as requested by DTAG
12597	URL typo
12598	Update Classification Rules due to new Microsoft requirements. Added note about Mutual TLS on SIP Interface. Added Firewall Table as option for increase security.

Documentation Feedback

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

This page is intentionally left blank.

1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (hereafter, referred to as *SBC*) for interworking between DLAN'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 DTAG's DLAN partners who are responsible for installing and configuring DTAG's DLAN 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.204.128 or later
Protocol	▪ SIP/TCP or SIP/TLS (to the DTAG's DLAN SIP Trunk) ▪ SIP/TLS (to the Teams Direct Routing)
Additional Notes	None

2.2 DTAG's DLAN SIP Trunking Version

Table 2-2: DTAG's DLAN Version

Vendor/Service Provider	DTAG's DLAN
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	
Protocol	SIP
Additional Notes	None

2.4 Interoperability Test Topology

Microsoft Teams Direct Routing can be implemented in the *Enterprise* or *Hosting* Models. This Configuration Note describes the Enterprise Model implementation. For implementing Hosting Model refer to the generic document: https://www.audiocodes.com/media/13161/connecting-audiocodes-sbc-to-microsoft-teams-direct-routing-hosting-model-configuration-note.pdf

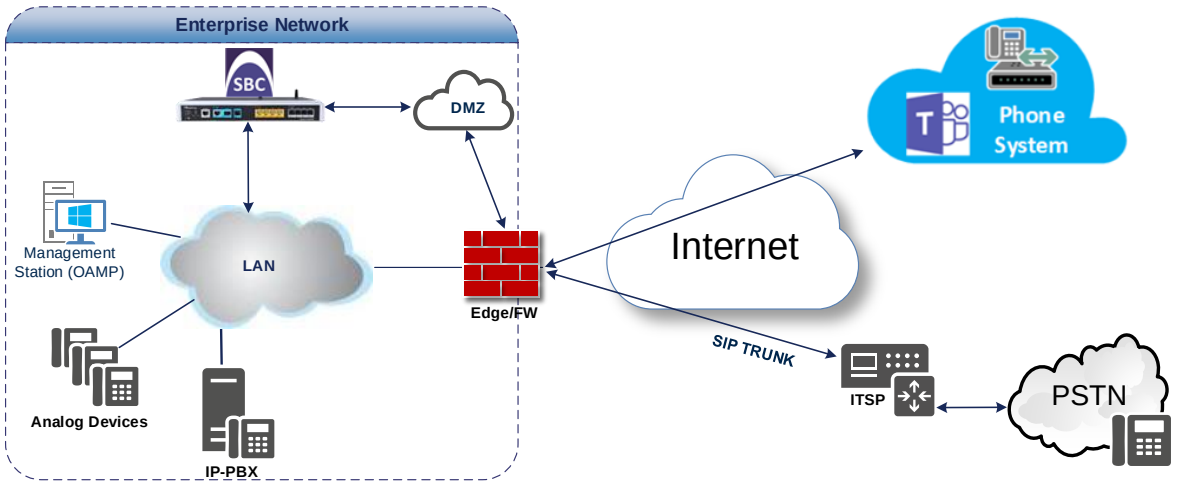
2.4.1 Enterprise Model Implementation

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

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

The figure below illustrates this interoperability test topology:

Figure 2-1: Interoperability Test Topology between SBC and Microsoft Teams Direct Routing Enterprise Model with DTAG's DLAN SIP Trunk



2.4.2 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

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

2.4.3 Infrastructure Prerequisites

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

Table 2-5: Infrastructure Prerequisites

Infrastructure Prerequisite	Details
Certified Session Border Controller (SBC)	See Microsoft's document *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 limitations were observed during interoperability tests performed for AudioCodes SBC interworking between Microsoft Teams Direct Routing and DTAG's DLAN SIP Trunk:

- If the Microsoft Teams Direct Routing sends one of the following error responses:
  - 480 Temporarily Unavailable
  - 503 Service Unavailable
  - 603 Decline

  DTAG's DLAN 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 4.14 on page 56).
- For Incoming calls from the DTAG's DLAN SIP Trunk, the SIP Record-Route Header is represented as **FQDN**. To resolve the IP address for any response, the DNS Query Type should be configured as "SRV" (see Section 4.18.3 on page 88).

3 Configuring Teams Direct Routing

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

3.1 Prerequisites

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

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

3.2 SBC Domain Name in the Teams Enterprise Model

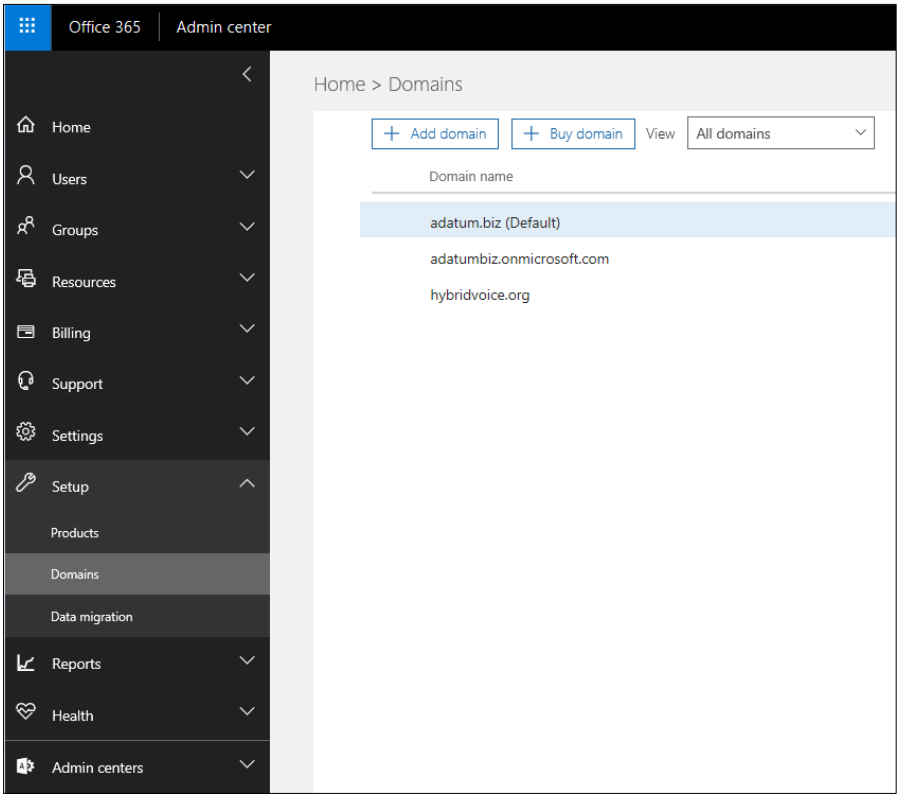
The SBC domain name must be from one of the names registered in 'Domains' of the tenant. You cannot use the ***.onmicrosoft.com** tenant for the domain name. For example, in Figure 2-2, the administrator registered the following DNS names for the tenant:

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 *-Fqdn* ***sbc.aceducation.info*** *-SipSignallingPort* ***5068*** *-ForwardCallHistory $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****"*

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 Microsoft Teams Direct Routing Management Shell after reconfiguration to verify correct values:

- **Get-CsOnlinePSTNGateway**

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

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 Microsoft Teams Direct Routing and the DTAG's DLAN SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

- SBC LAN interface – Enterprise Management
- SBC WAN interface - Both, Teams Direct Routing and DTAG's DLAN SIP Trunking environments

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

Notes:

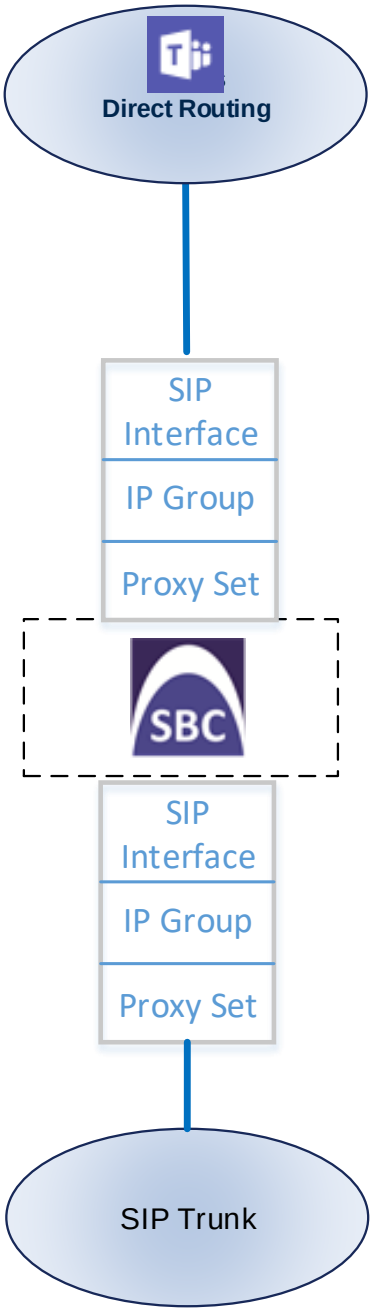
- For implementing Microsoft Teams Direct Routing and DTAG's DLAN SIP Trunk based on the configuration described in this section, AudioCodes SBC must be installed with a License Key that includes the following software features:
  - √ **Microsoft Teams**
  - √ **Security**
  - √ **DSP**
  - √ **RTP**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

  For more information about the License Key, contact your AudioCodes sales representative.
- The scope of this interoperability test and document does **not** cover all security aspects for configuring this topology. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document, which can be found at AudioCodes web site

4.1 SBC Configuration Concept in Teams Direct Routing Enterprise Model

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

Figure 4-1: SBC Configuration Concept

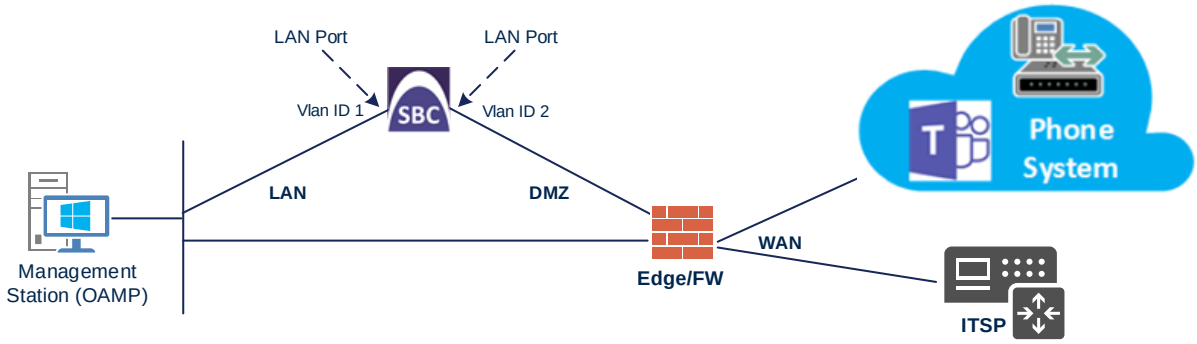


4.2 IP Network Interfaces Configuration

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

- SBC interfaces with the following IP entities:
  - Enterprise Management, located on the LAN
  - DTAG's DLAN SIP Trunk and Microsoft Teams Direct Routing, 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 step describes how to configure VLANs for each of the following interfaces:

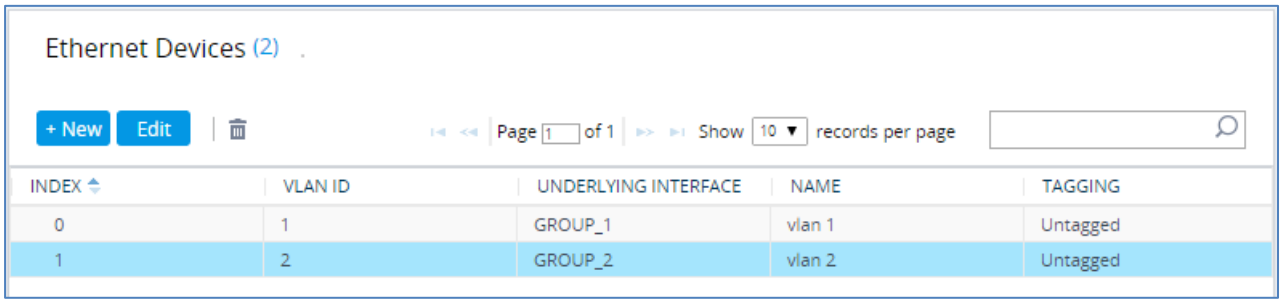
- LAN VoIP (assigned the name "LAN_IF")
- WAN VoIP (assigned the name "WAN_IF")

➢ **To configure the VLANs:**

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

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

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

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

1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Modify the existing LAN network interface:
   a. Select the 'Index' radio button of the **OAMP + Media + Control** table row, and then click **Edit**.
   b. Configure the interface as follows:

Parameter	Value
Name	**LAN_IF** (arbitrary descriptive name)

Ethernet Device	**vlan 1**
IP Address	**10.15.17.77** (LAN IP address of SBC)
Prefix Length	**16** (subnet mask in bits for 255.255.0.0)
Default Gateway	**10.15.0.1**
Primary DNS	**10.15.27.1**

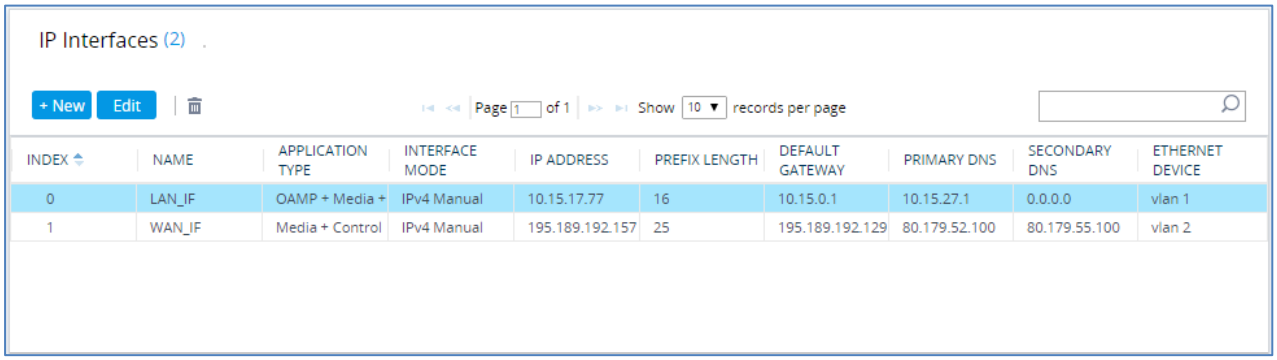
3. Add a network interface for the WAN side:
   a. Click **New**.
   b. Configure the interface as follows:

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

4. Click **Apply**.

The configured IP network interfaces are shown below:

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



4.3 SIP TLS Connection Configuration

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

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

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

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

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

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

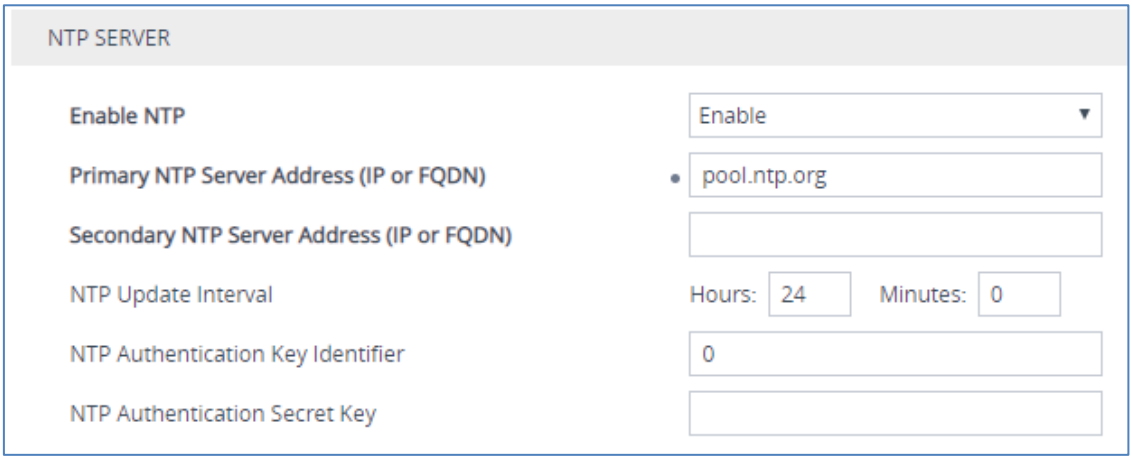
4.3.1 Configure the NTP Server Address

This step describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or another global server) to ensure that the SBC receives the current date and time. This is necessary for validating certificates of remote parties.

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

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

Figure 4-5: Configuring NTP Server Address



3. Click **Apply**.

4.3.2 Create a TLS Context for Microsoft Teams Direct Routing

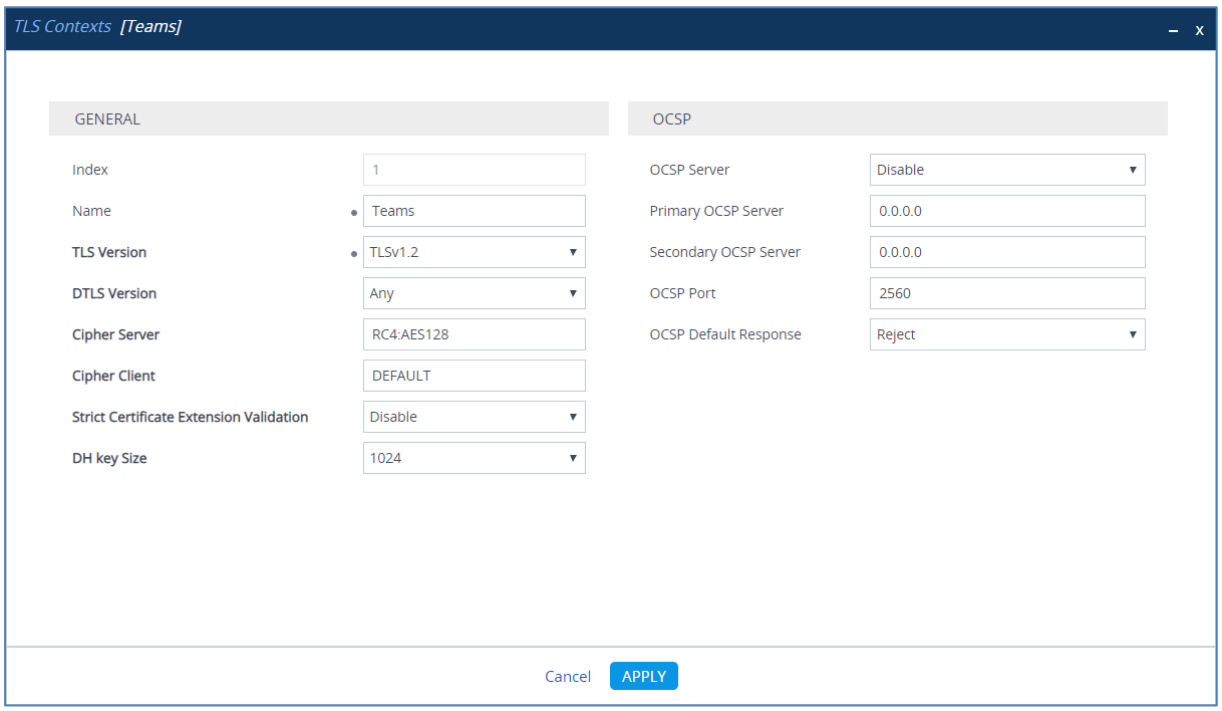
This step describes how to configure TLS Context in the SBC. AudioCodes recommends implementing only TLS to avoid flaws in SSL.

➢ **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 Create a TLS Context for DTAG's DLAN SIP Trunk

This step describes how to configure TLS Context in the SBC for connection with DTAG's DLAN SIP Trunk over TLS.

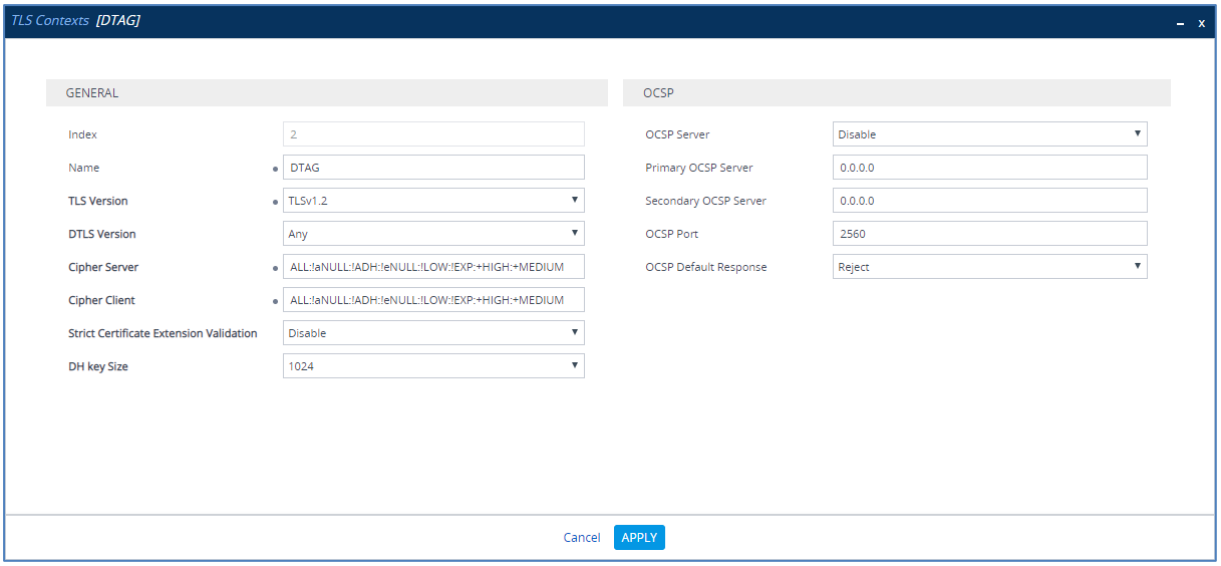
Note: The following configuration step is required **only** if connection to DTAG's DLAN SIP Trunk was made using TLS.

➢ **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	**2**
Name	**DTAG** (arbitrary descriptive name)
TLS Version	**TLSv1.2**
Cipher Server	**ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:+HIGH:+MEDIUM**
Cipher Client	**ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:+HIGH:+MEDIUM**
All other parameters leave unchanged at their default values	

Figure 4-7: Configuring TLS Context for DTAG'S DLAN SIP Trunk



3. Click **Apply**.

4.3.4 Configure a Certificate

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

The procedure involves the following main steps:

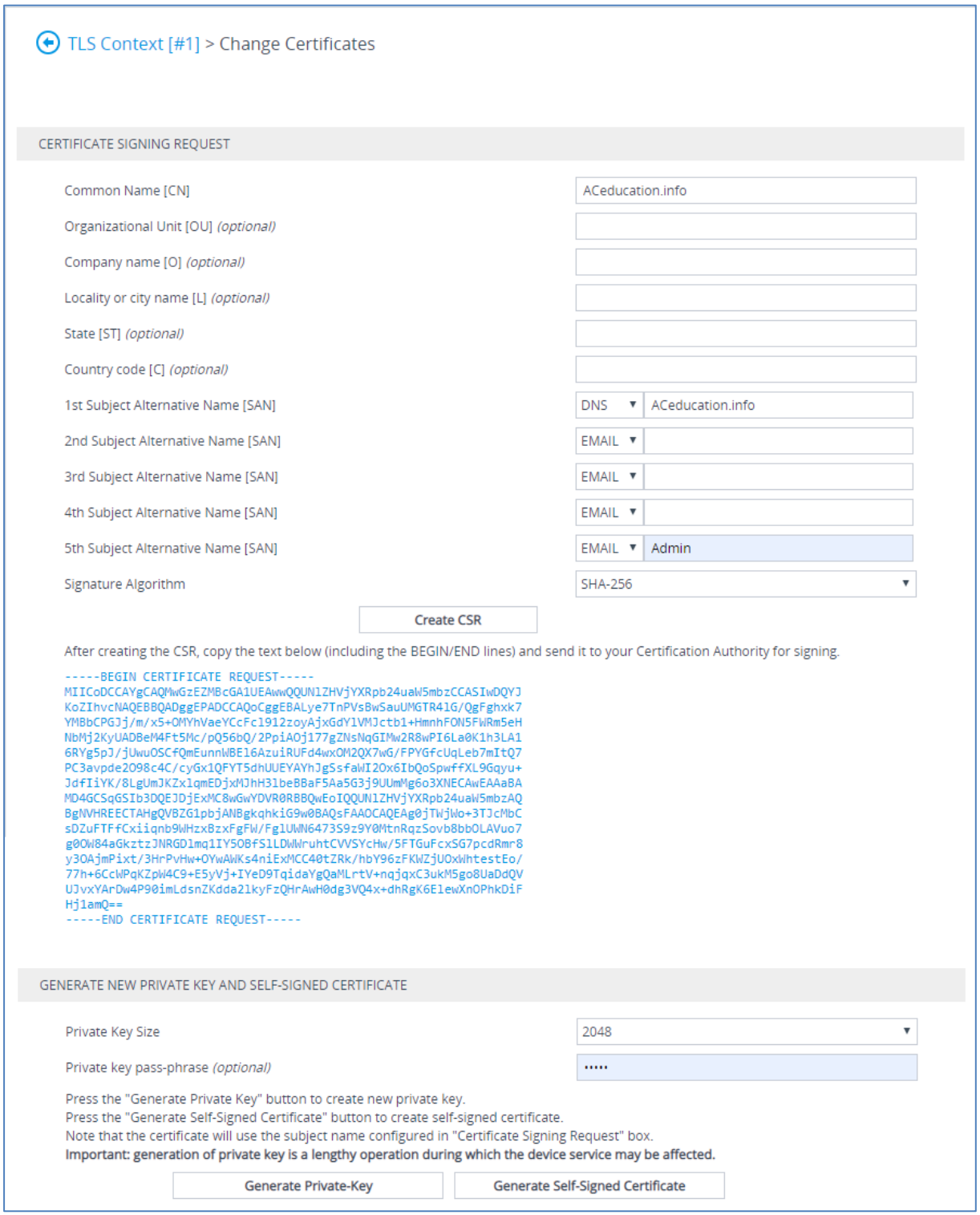
a. Generating a Certificate Signing Request (CSR).
b. Requesting Device Certificate from CA.
c. Obtaining Trusted Root/ Intermediate Certificate from CA.
d. Deploying Device and Trusted Root/ Intermediate Certificates on SBC.

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:

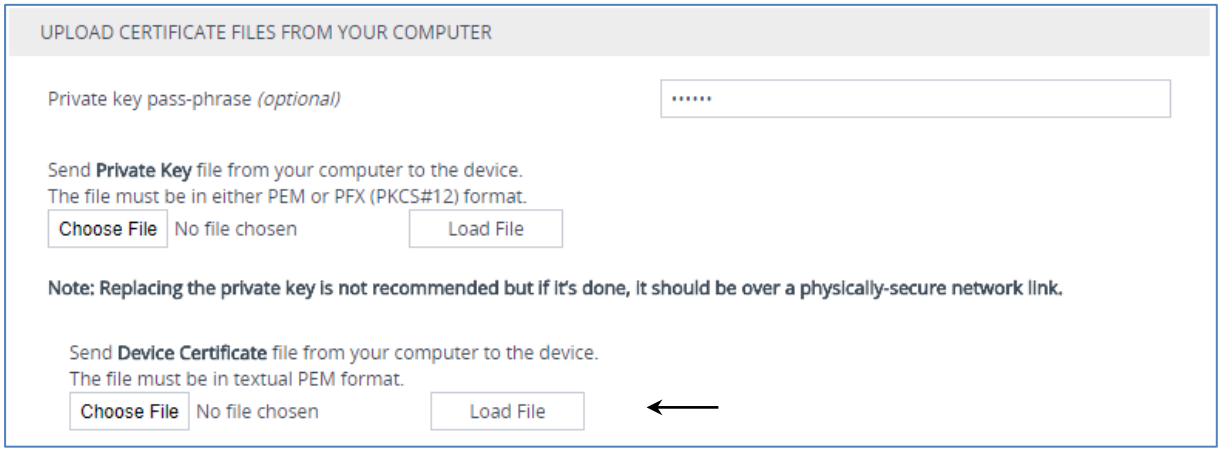
Figure 4-8: Example of Certificate Signing Request – Creating CSR



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:

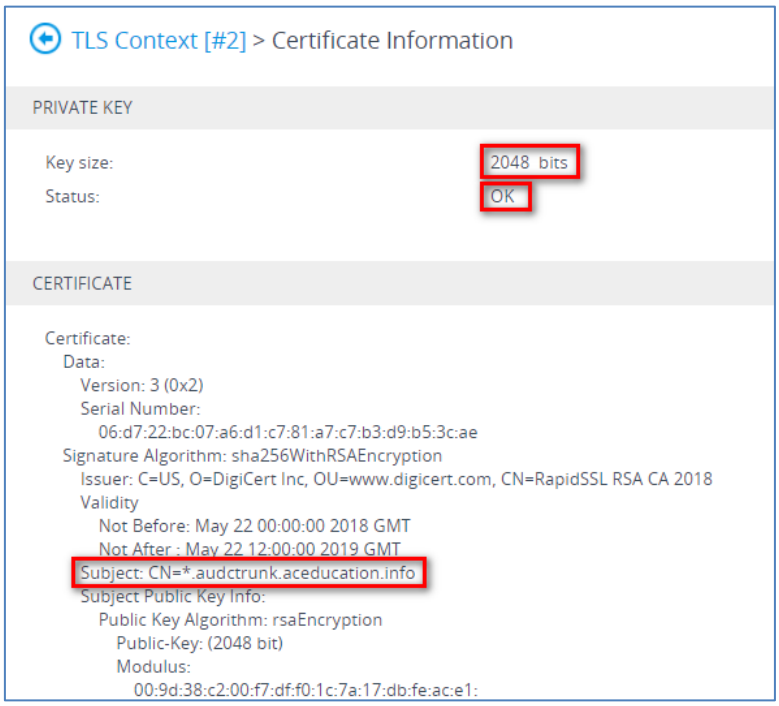
a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
b. Scroll down to the **Upload certificates files from your computer** group, click the **Choose File** button corresponding 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 4-9: 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 4-10: Certificate Information Example

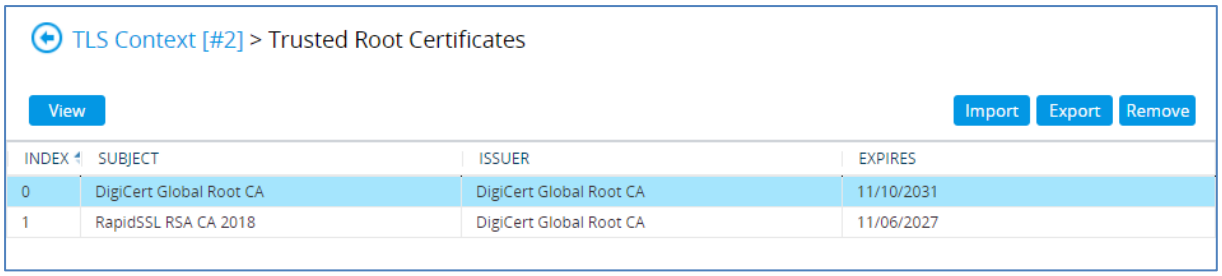


9. In the SBC's Web interface, return to the **TLS Contexts** page.
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Trusted Root Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.

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 4-11: Example of Configured Trusted Root Certificates



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

4.3.5 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.

4.3.6 Deploy Baltimore Trusted Root Certificate

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

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

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

4.4 Configure Media Realms

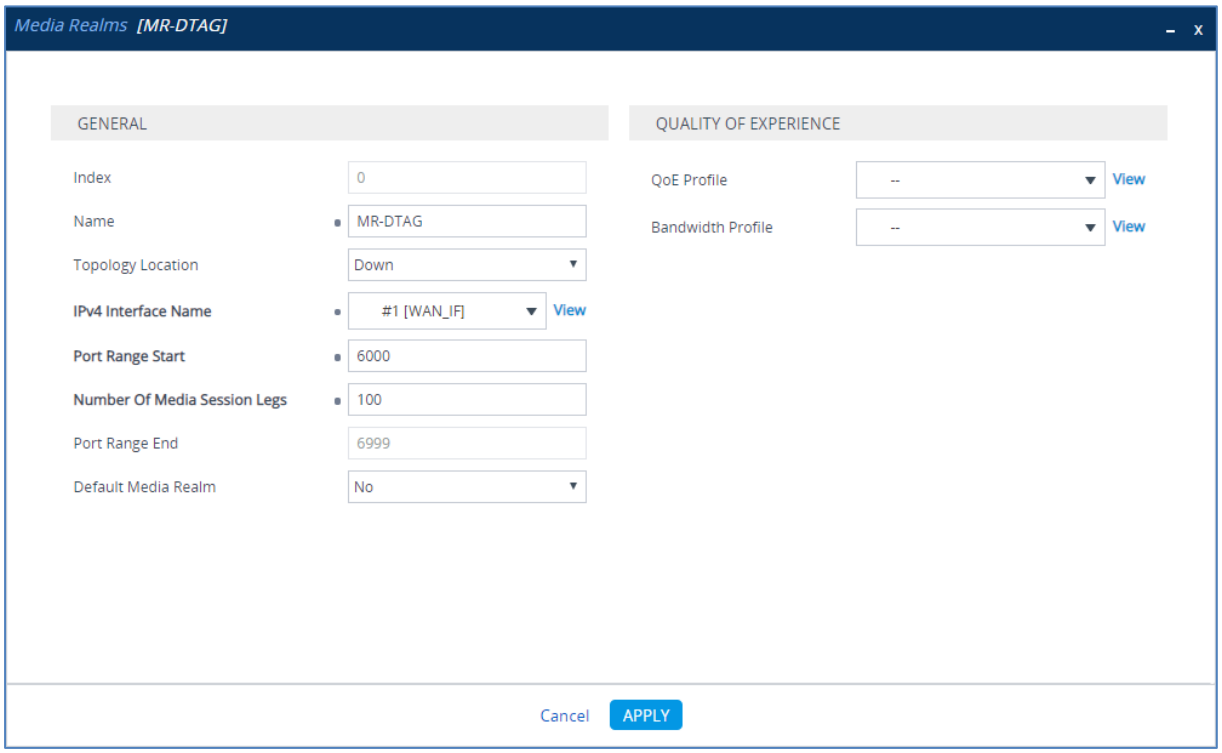
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **To configure Media Realms:**

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

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

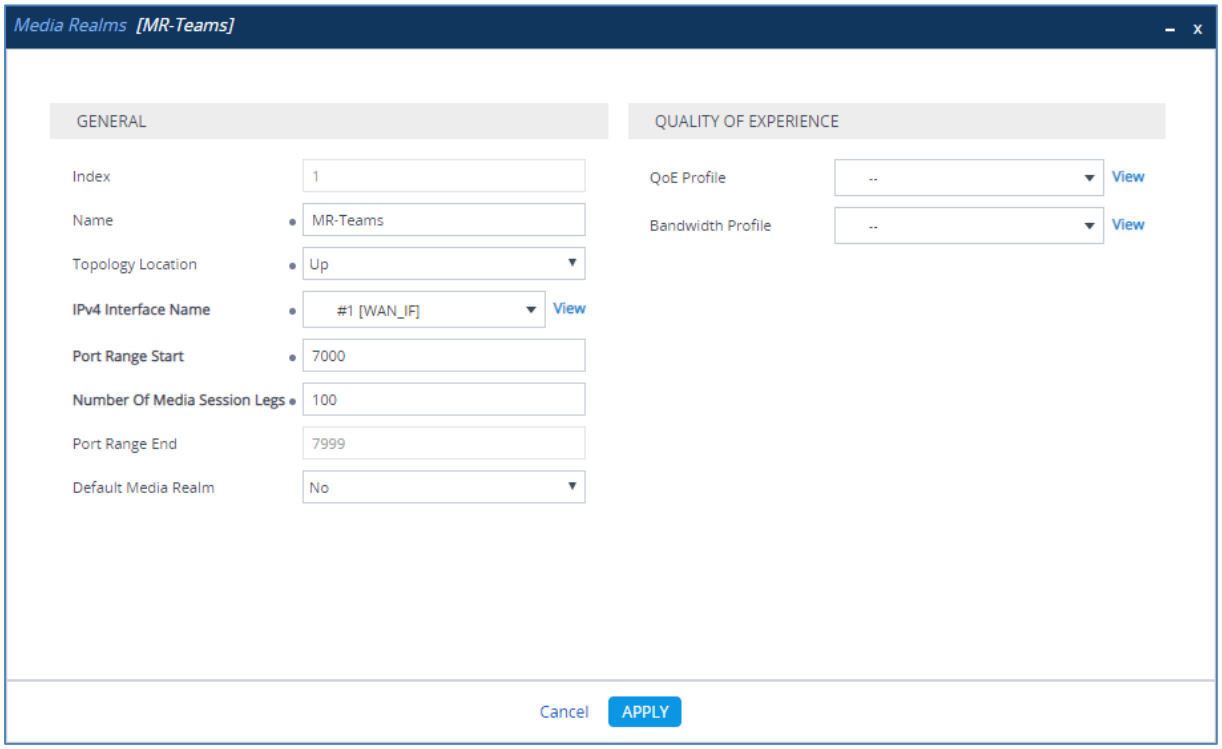
Figure 4-12: Configuring Media Realm for SIP Trunk



3. Configure a Media Realm for the Teams:

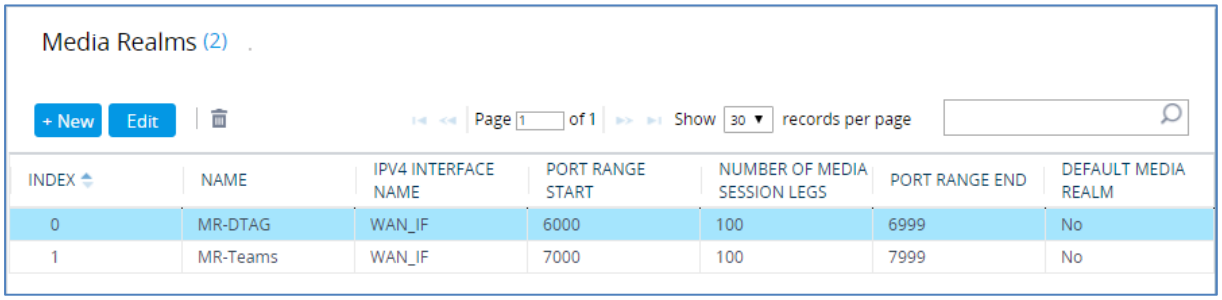
Parameter	Value
Index	**1**
Name	**MR-Teams** (arbitrary name)
Topology Location	**Up**
IPv4 Interface Name	**WAN_IF**
Port Range Start	**7000** (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	**100** (media sessions assigned with port range)

Figure 4-13: Configuring Media Realm for the Teams



The configured Media Realms are shown in the figure below:

Figure 4-14: Configured Media Realms in Media Realm Table



4.5 Configure SIP Signaling Interfaces

This step describes how to configure SIP Interfaces. For the interoperability test topology, internal (towards the SIP Trunk) and external (towards the Microsoft 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 SIP Trunk. You can use the default SIP Interface (Index 0), but modify it as shown below:

Parameter	Value
Index	**0**
Name	**DTAG** (arbitrary descriptive name)
Network Interface	**WAN_IF**
Application Type	**SBC**
TCP Port	**5060** (according to Service Provider requirement)
UDP and TLS Port	**0**
Media Realm	**MR-DTAG**

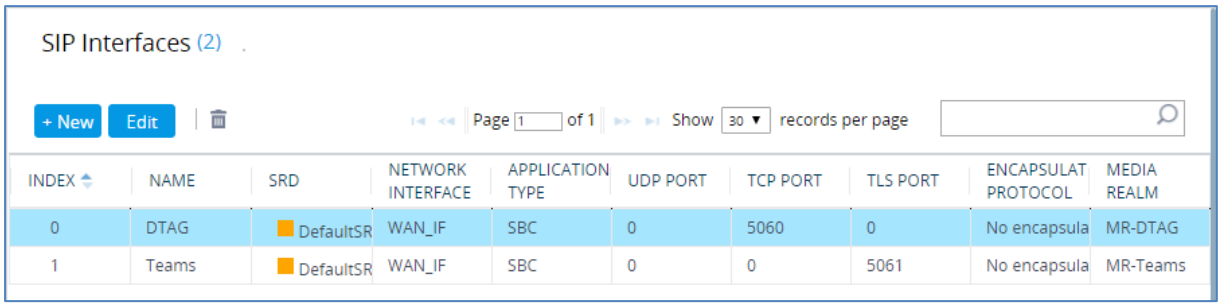
Note: The Direct Routing interface can only use TLS transport for a SIP call. It does not SIP TCP support due to security reasons. The SIP port may be any port of your choice. When pairing the SBC with Office 365, the chosen port is specified in the pairing command.

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**
Pre-classification Manipulation Set ID	**0**
Media Realm	**MR-Teams**

The configured SIP Interfaces are shown in the figure below:

Figure 4-15: Configured SIP Interfaces in SIP Interface Table



Note: For implementing an MTLS connection with the Microsoft Teams network, configure 'TLS Mutual Authentication' to "Enable" for the Teams SIP Interface.

Note: Loading Baltimore Trusted Root Certificates to AudioCodes' SBC is mandatory for implementing an MTLS connection with the Microsoft Teams network. Refer to Section 4.3.6 on page 28.

4.6 Configure Proxy Sets

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

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

- DTAG's DLAN SIP Trunk
- Microsoft Teams Direct Routing

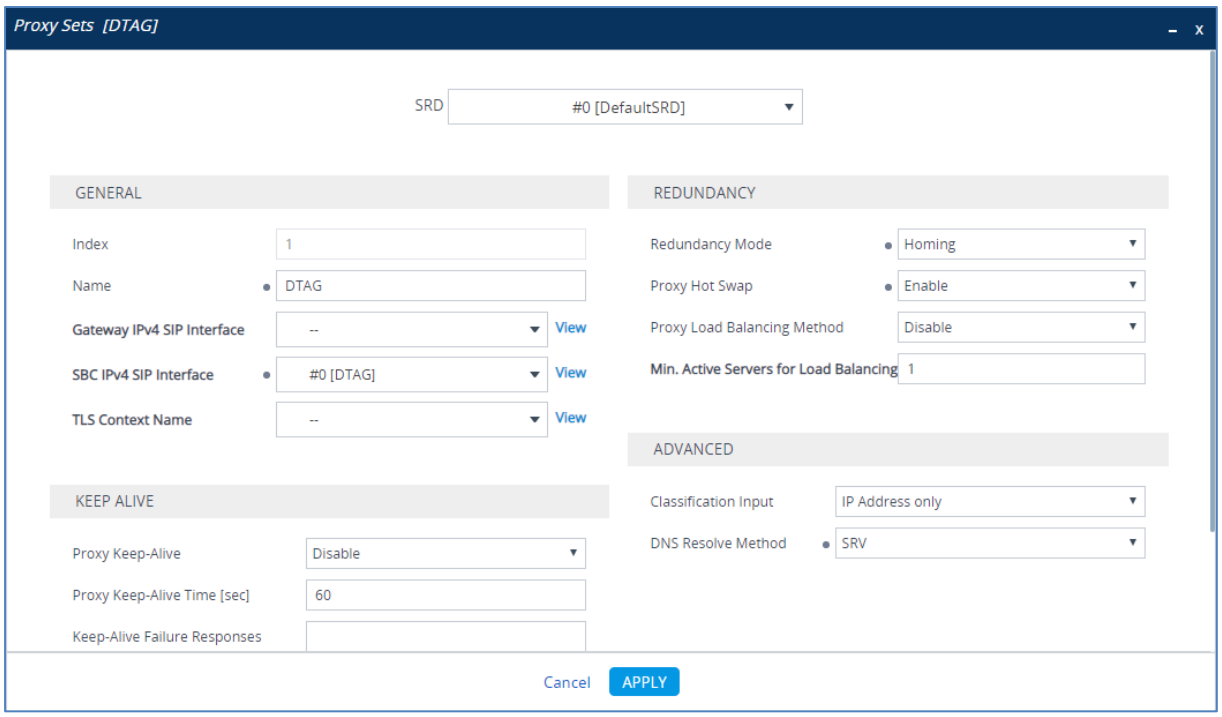
The Proxy Sets will later be applied to the VoIP network by assigning them to IP Groups.

➢ 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 DTAG's DLAN SIP Trunk:

Parameter	Value
Index	**1**
Name	**DTAG**
SBC IPv4 SIP Interface	**DTAG**
Redundancy Mode	**Homing**
Proxy Hot Swap	**Enable**
DNS Resolve Method	**SRV**

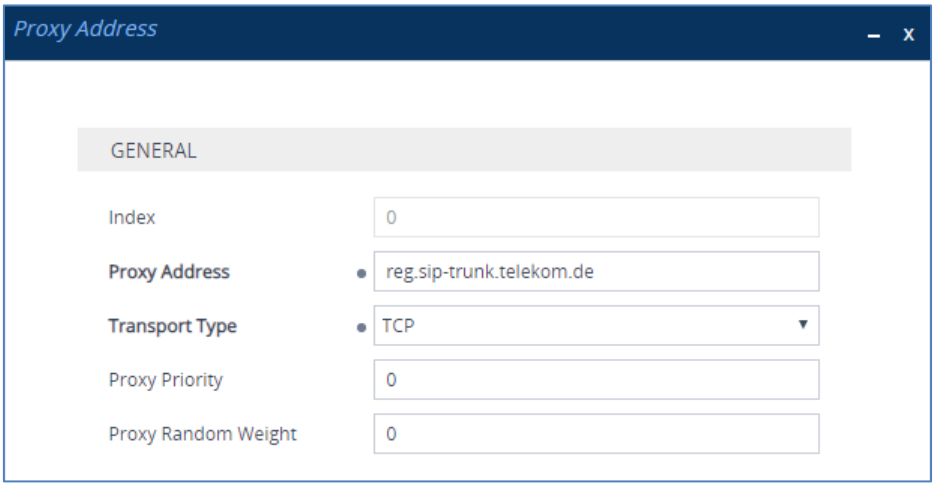
Figure 4-16: Configuring Proxy Set for DTAG's DLAN SIP Trunk



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 4-17: Configuring Proxy Address for DTAG's DLAN SIP Trunk



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

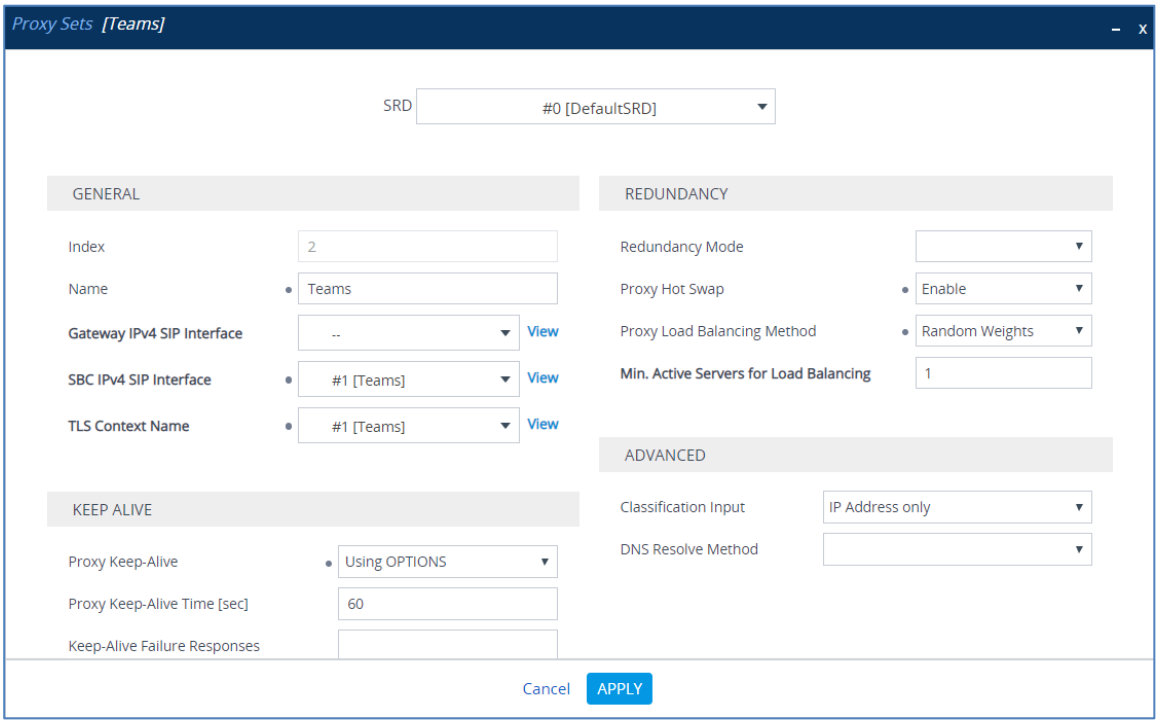
Parameter	Value
Index	**0**
Proxy Address	**reg.sip-trunk.telekom.de** (SIP Trunk FQDN)
Transport Type	**TCP or TLS** (for secure mode only)

d. Click **Apply**.

3. Add a Proxy Set for the Microsoft 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**

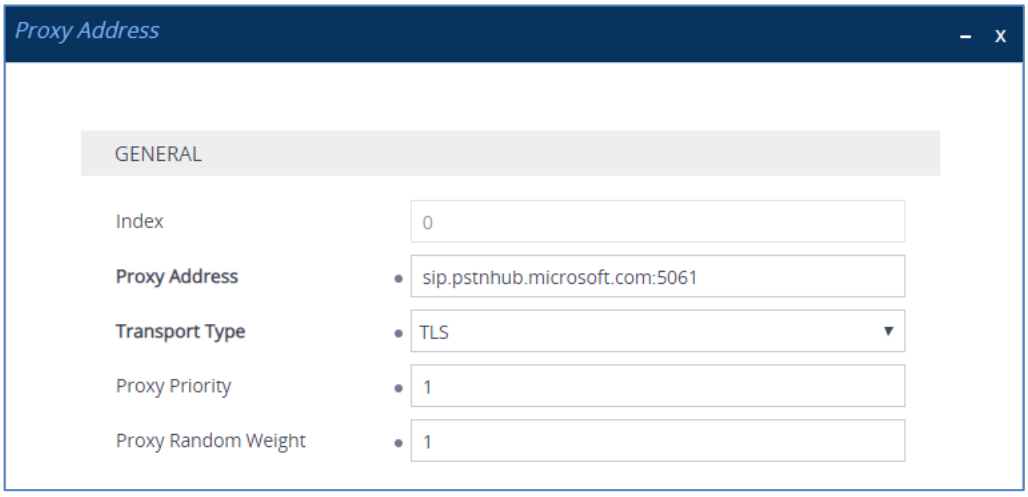
Figure 4-18: Configuring Proxy Set for Microsoft Teams Direct Routing



a. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.

b. Click **New**; the following dialog box appears:

Figure 4-19: Configuring Proxy Address for Microsoft Teams Direct Routing Interface



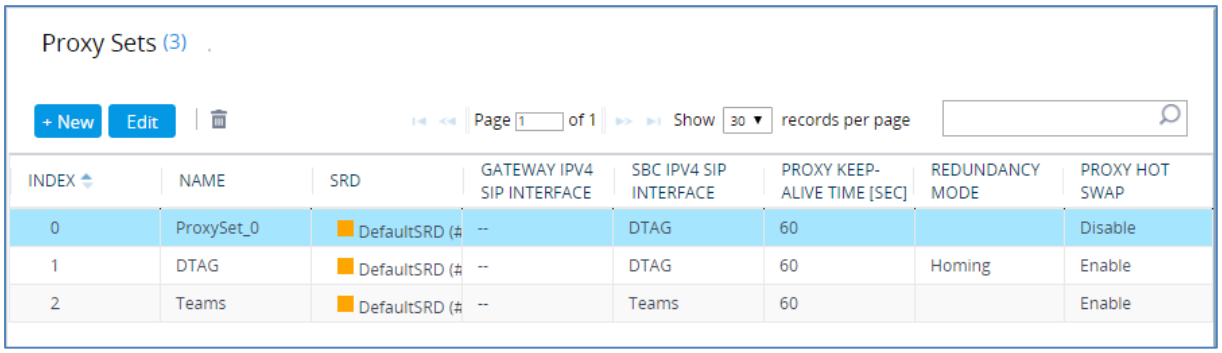
c. Configure the address of the Proxy Set according to the parameters described in the table below.

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 4-20: Configured Proxy Sets in Proxy Sets Table



4.7 Configure Coders

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

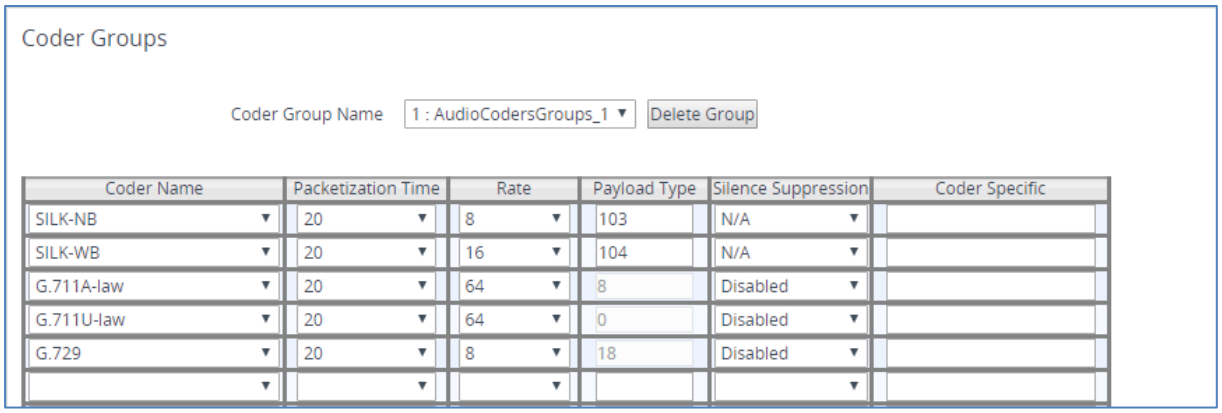
Note that the Coder Group ID for this entity will be assigned to its corresponding IP Profile in the next step.

➢ **To configure coders:**

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

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

Figure 4-21: Configuring Coder Group for Microsoft Teams Direct Routing

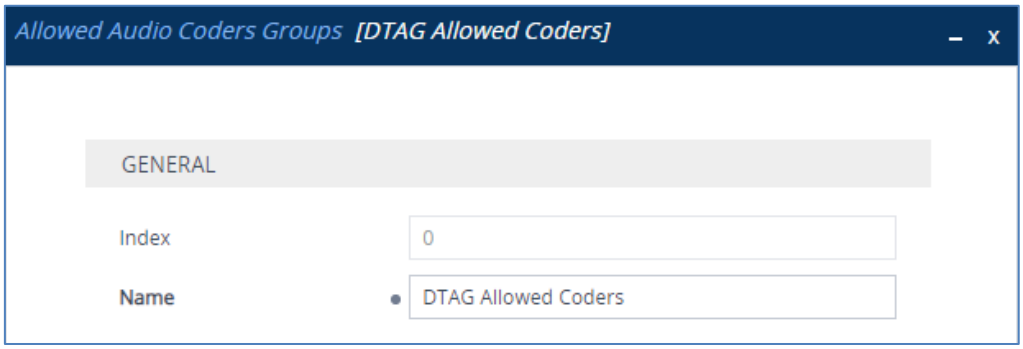


The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the DTAG's DLAN SIP Trunk uses the dedicated coders list whenever possible. Note that this Allowed Coders Group ID will be assigned to the IP Profile belonging to the DTAG's DLAN SIP Trunk in the next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

➢ **To set a preferred coder for the DTAG's DLAN 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 DTAG's DLAN SIP Trunk.

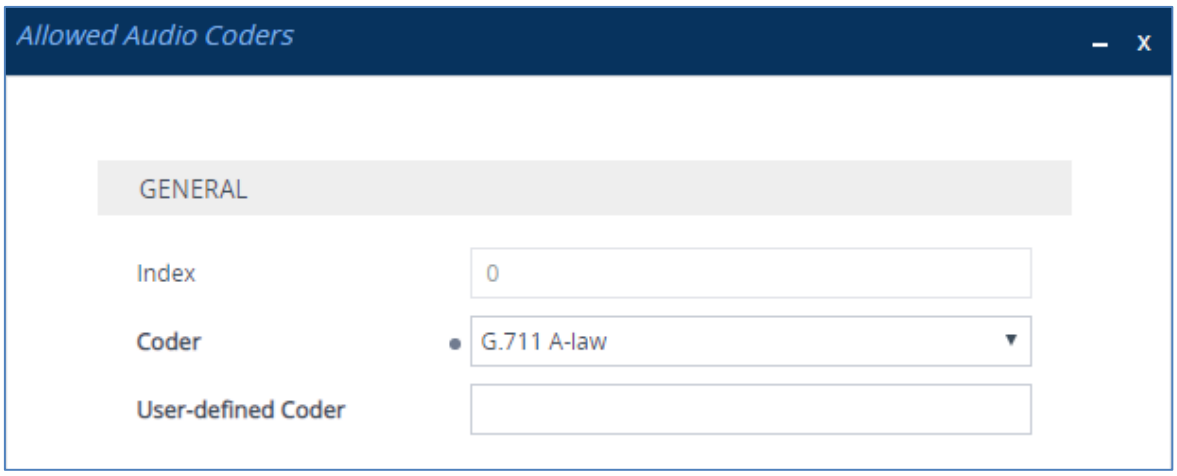
Figure 4-22: Configuring Allowed Coders Group for DTAG's DLAN SIP Trunk



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:

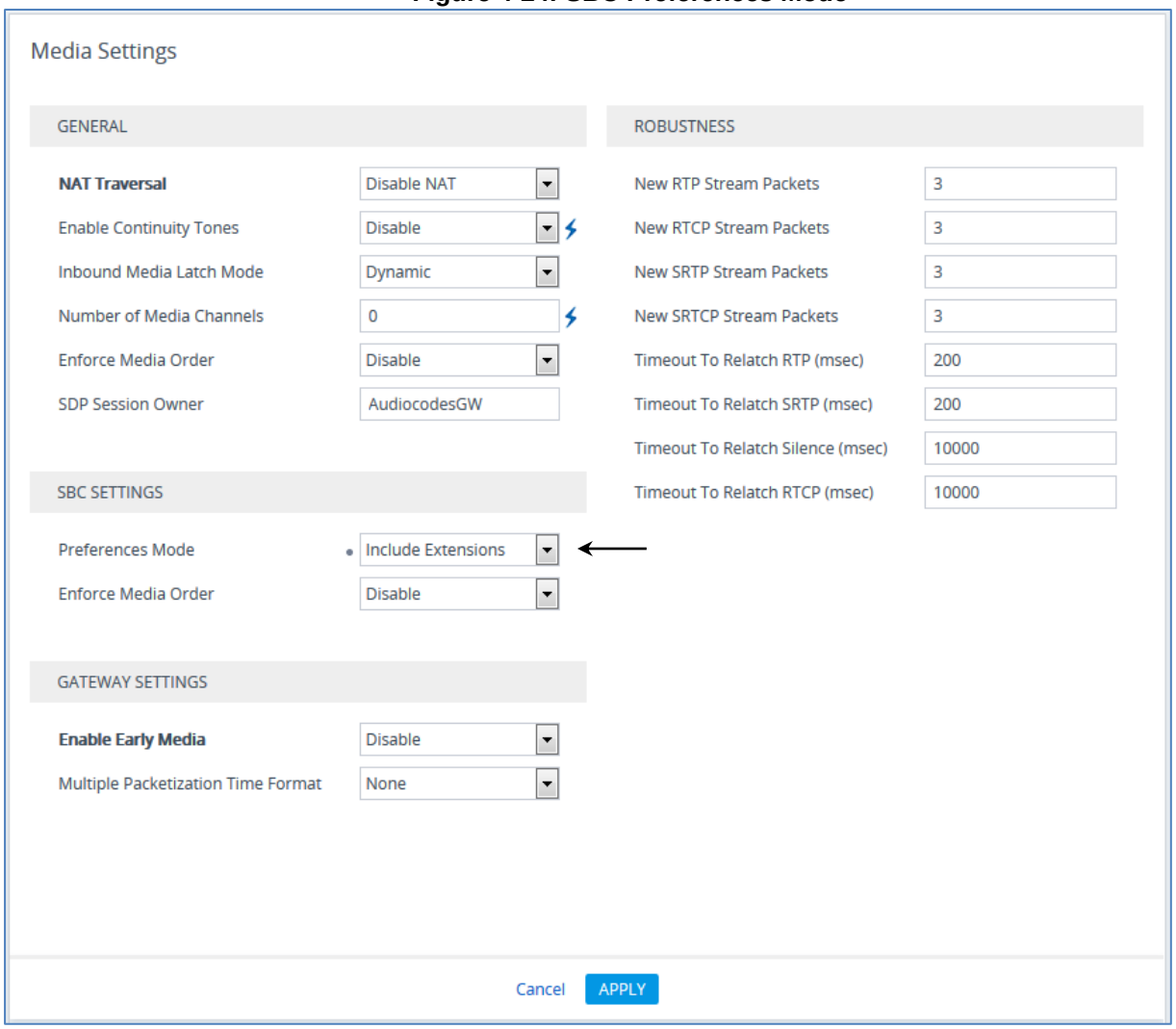
Parameter	Value
Index	**0**
Coder	**G.711 A-law**

Figure 4-23: Configuring Allowed Coders for DTAG's DLAN SIP Trunk



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

Figure 4-24: SBC Preferences Mode



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

4.8 Configure IP Profiles

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

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

- DTAG's DLAN SIP trunk – to operate in non-secure mode using RTP and SIP over TCP or in secure mode using SRTP and SIP over TLS
- Microsoft Teams Direct Routing – to operate in secure mode using SRTP and SIP over TLS

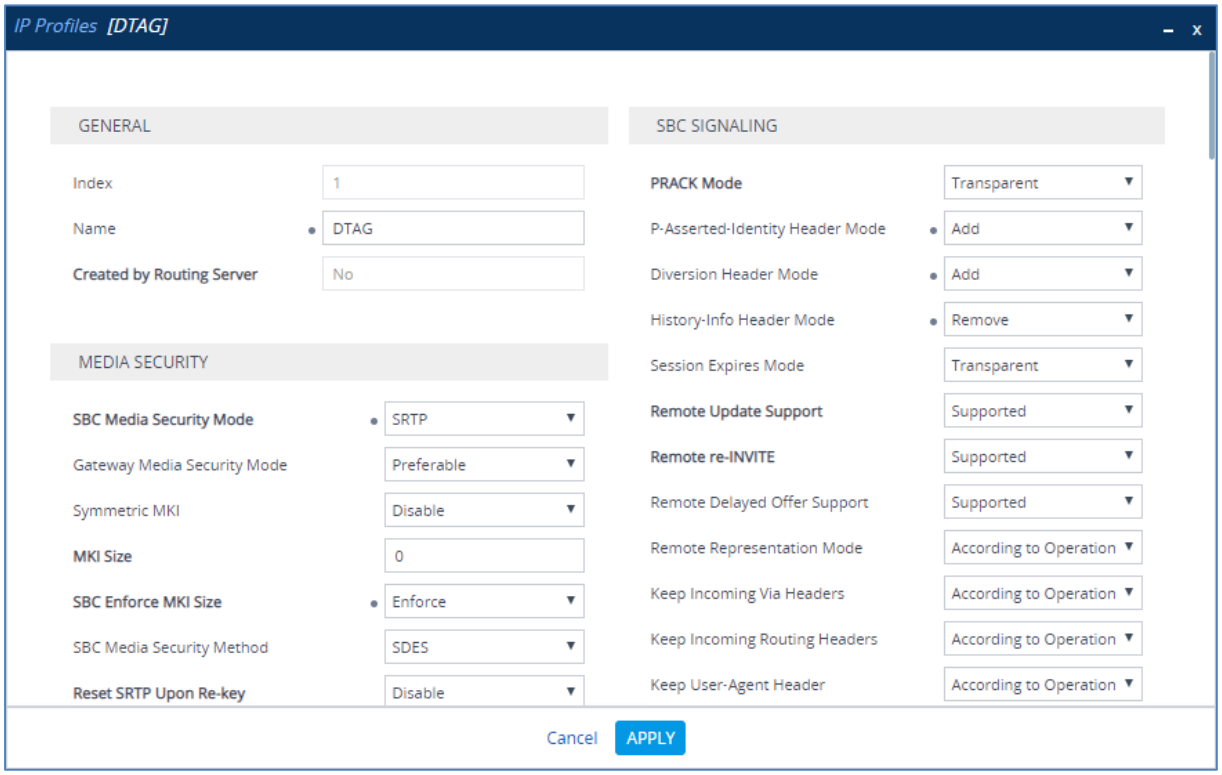
➢ **To configure an IP Profile for the DTAG's DLAN SIP Trunk:**

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	**DTAG**
Media Security	
SBC Media Security Mode	**RTP** or **SRTP** (according to connection)
SBC Enforce MKI Size	**Enforce** (relevant for secure mode only)
SBC Remove Crypto Lifetime in SDP	**Yes** (relevant for secure mode only)
SBC Early Media	
Remote Multiple 18x	**Not Supported**
Remote Early Media Response Type	**183**
Remote Early Media RTP Detection Mode	**By Media**
Remote Can Play Ringback	**No**
SBC Media	
Allowed Audio Coders	**DTAG Allowed Coders**
Use Silence Suppression	**Remove**
RTP Redundancy Mode	**Disable**
RTCP Mode	**Generate Always**
SDP Handle RTCP	**Remove**
Quality of Service	
Signaling DiffServ	**48**
SBC Signaling	
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)
Diversion Header Mode	**Add**
History-Infor Header Mode	**Remove**

SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally**
Play RBT To Transferee	**Yes**

Figure 4-25: Configuring IP Profile for DTAG's DLAN SIP Trunk



3. Click **Apply**.

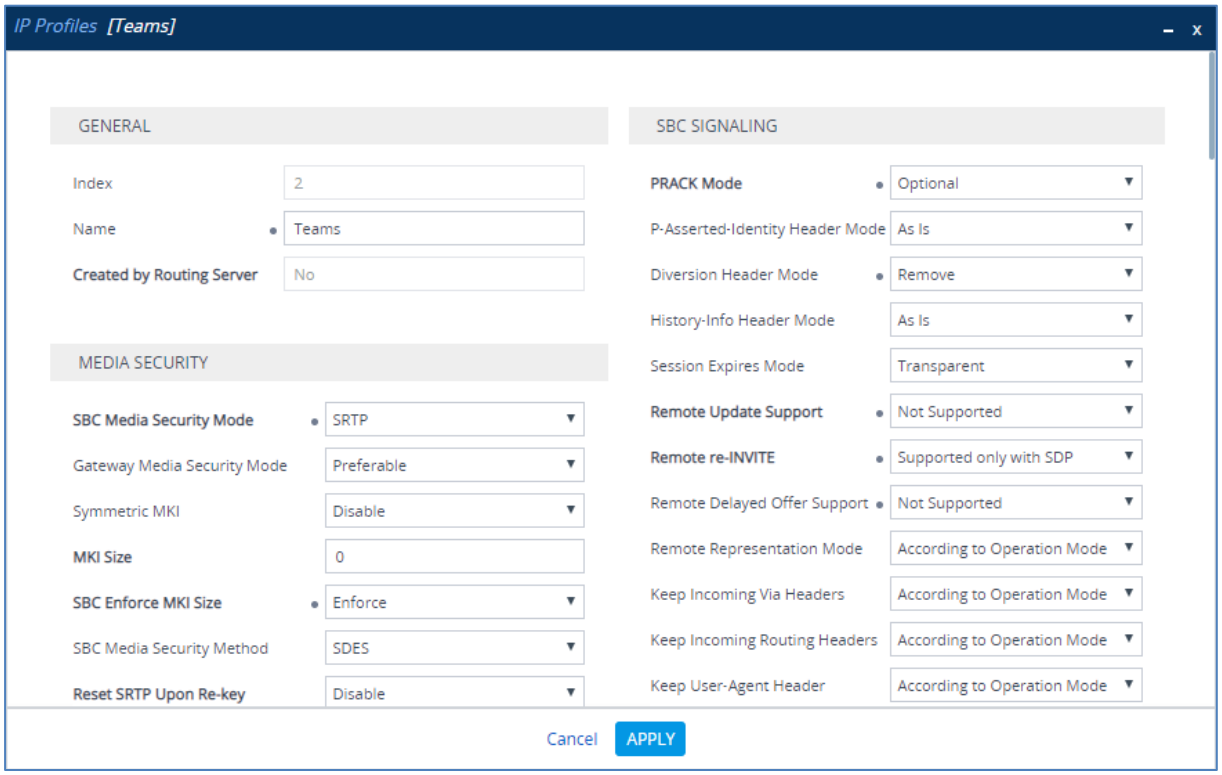
➢ To configure IP Profile for the Microsoft Teams Direct Routing:

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

Parameter	Value
General	
Index	**2**
Name	**Teams** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**SRTP**
SBC Enforce MKI Size	**Enforce**
SBC Early Media	
Remote Early Media RTP Detection Mode	**By Media** (required, as Microsoft Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18x response)

SBC Media	
Extension Coders Group	**AudioCodersGroups_1**
RFC 2833 Mode	**Extend**
ICE Mode	**Lite** (required only when Media Bypass enabled on Microsoft Teams)
Quality of Service	
Signaling DiffServ	**48**
SBC Signaling	
PRACK Mode	**Optional**
Diversion Header Mode	**Remove**
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 4-26: Configuring IP Profile for Microsoft Teams Direct Routing



3. Click **Apply**.

4.9 Configure IP Groups

This step describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the SBC communicates. This can be a server (e.g., IP PBX or 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:

- DTAG's DLAN 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 DTAG's DLAN SIP Trunk:

Parameter	Value
Index	**1**
Name	**DTAG**
Type	**Server**
Proxy Set	**DTAG**
IP Profile	**DTAG**
Media Realm	**MR-DTAG**
SIP Group Name	**sip-trunk.telekom.de** (according to ITSP requirement)

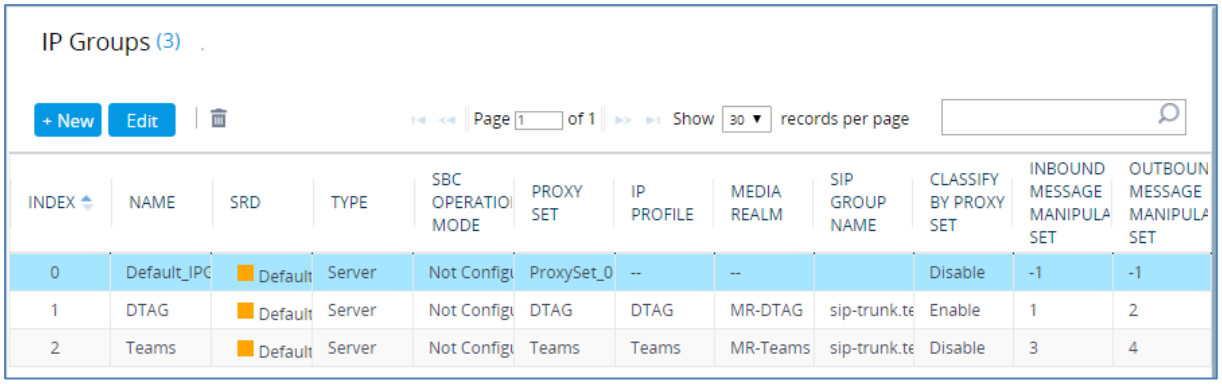
3. Configure an IP Group for the Microsoft Teams Direct Routing:

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

DTLS Context	**Teams**
Proxy Keep-Alive using IP Group settings	**Enable**

The configured IP Groups are shown in the figure below:

Figure 4-27: Configured IP Groups in IP Group Table



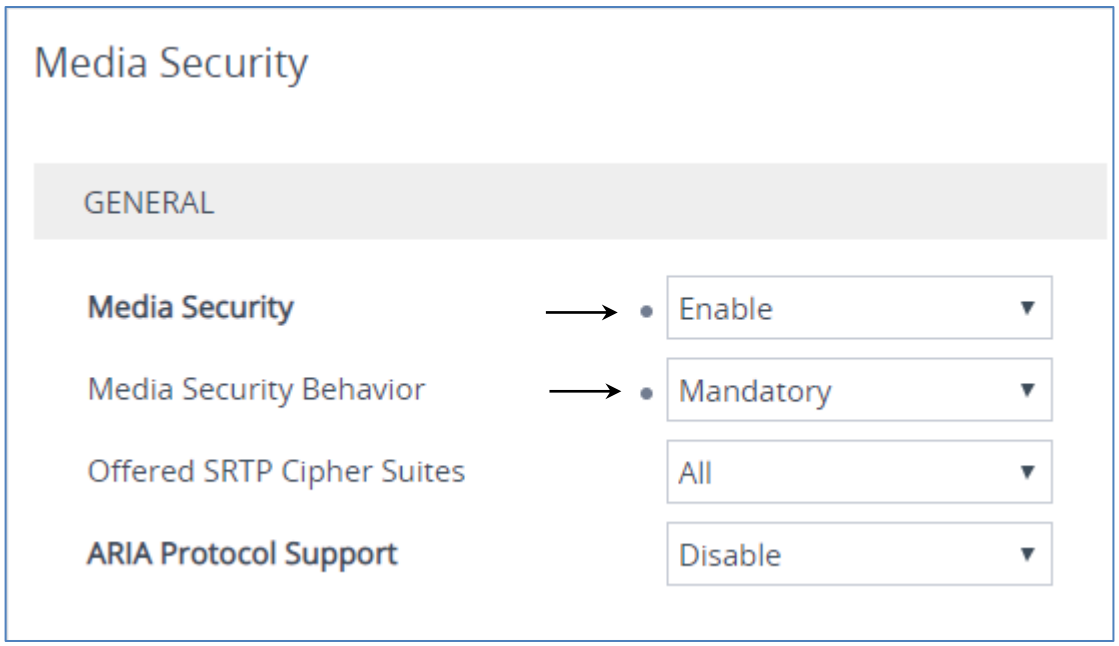
4.10 Configure SRTP

This step 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 4-28: Configuring SRTP



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

4.11 Configuring Message Condition Rules

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

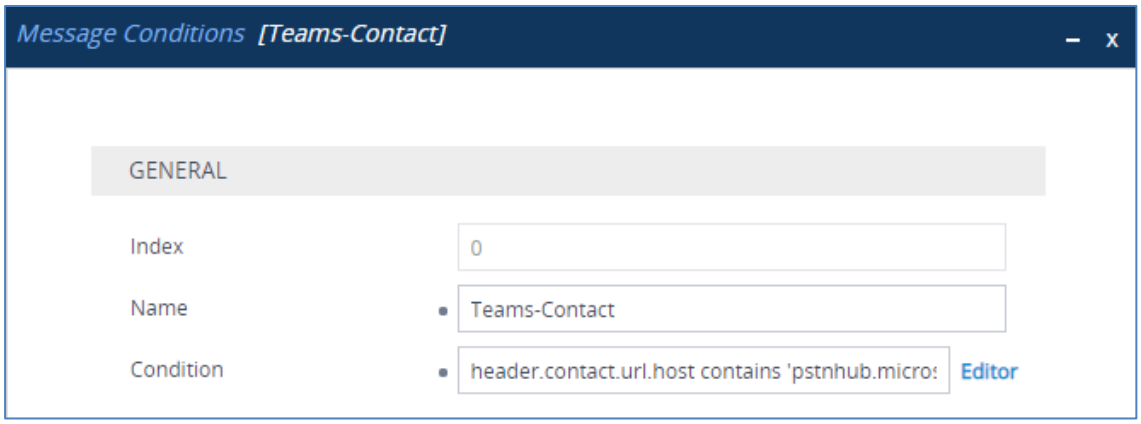
The following condition verifies that the Contact header contains Microsoft Teams FQDN.

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

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

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

Figure 4-29: Configuring Condition Table



3. Click **Apply**.

4.12 Configuring Classification Rules

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

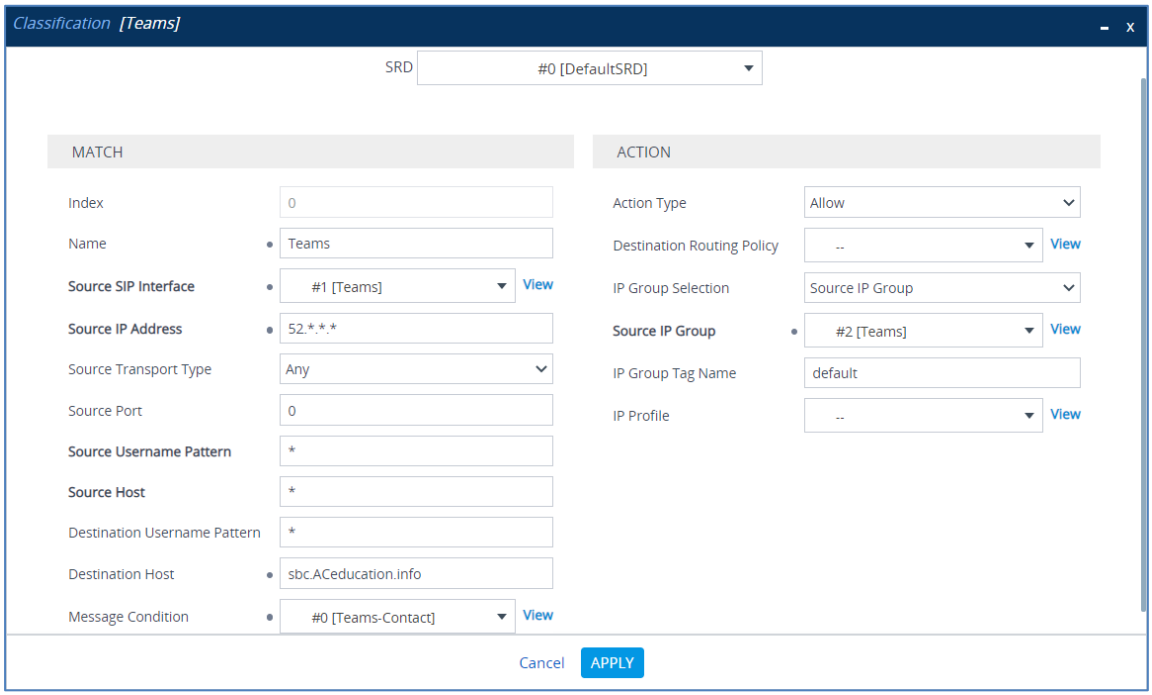
You can also use the Classification table for employing SIP-level access control for successfully classified calls, by configuring Classification rules with whitelist and blacklist settings. If a Classification rule is configured as a whitelist ("Allow"), the device accepts the SIP dialog and processes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

➢ **To configure a Classification 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.*.*.***
Destination Host	**sbc.ACeducation.info**
Message Condition	**Teams-Contact**
Action Type	**Allow**
Source IP Group	**Teams**

Figure 4-30: Configuring Classification Rule



3. Click **Apply**.

4.13 Configure IP-to-IP Call Routing Rules

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups (as configured in Section 4.9 on page 37,) to denote the source and destination of the call.

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

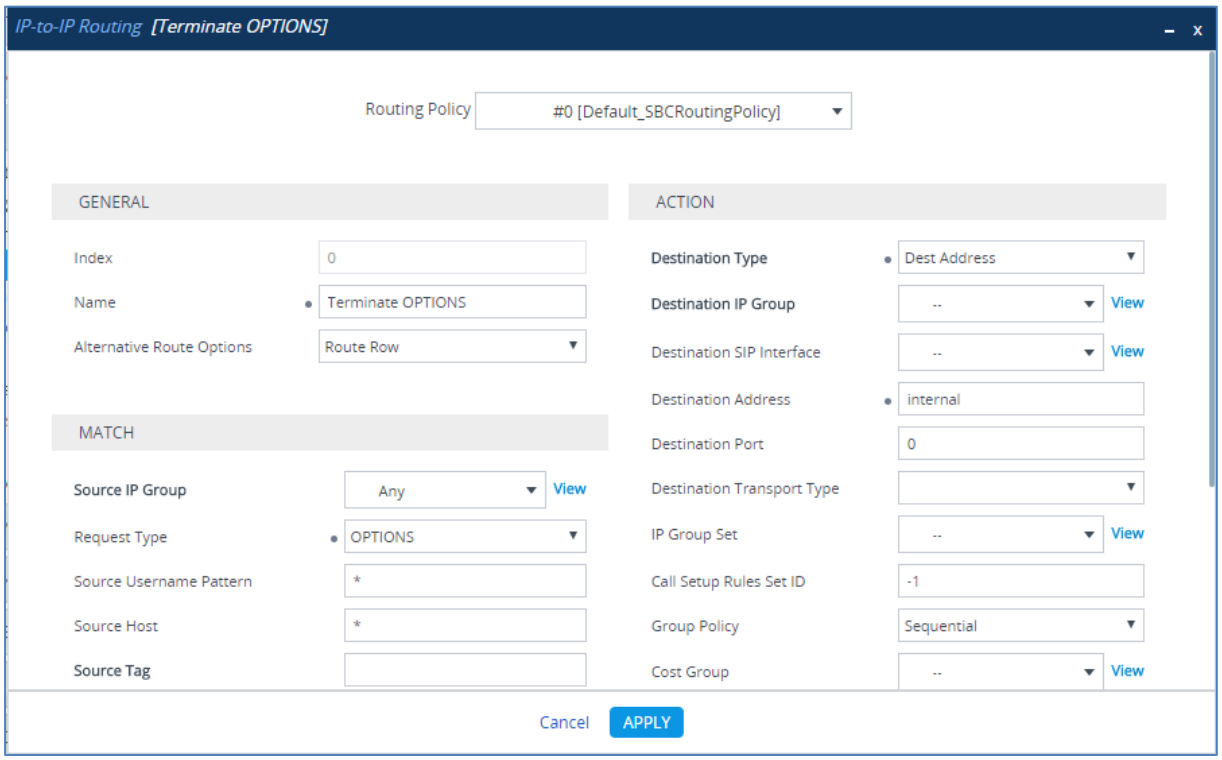
- Terminate SIP OPTIONS messages on the SBC that are received from any entity
- Terminate REFER messages to Teams Direct Routing
- Calls from Teams Direct Routing to DTAG's DLAN SIP Trunk
- Calls from DTAG's DLAN SIP Trunk to Teams Direct Routing

➢ **To configure IP-to-IP routing rules:**

1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure a rule to terminate SIP OPTIONS messages received from the both LAN and DMZ:
   a. Click **New**, and then configure the parameters as follows:

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

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

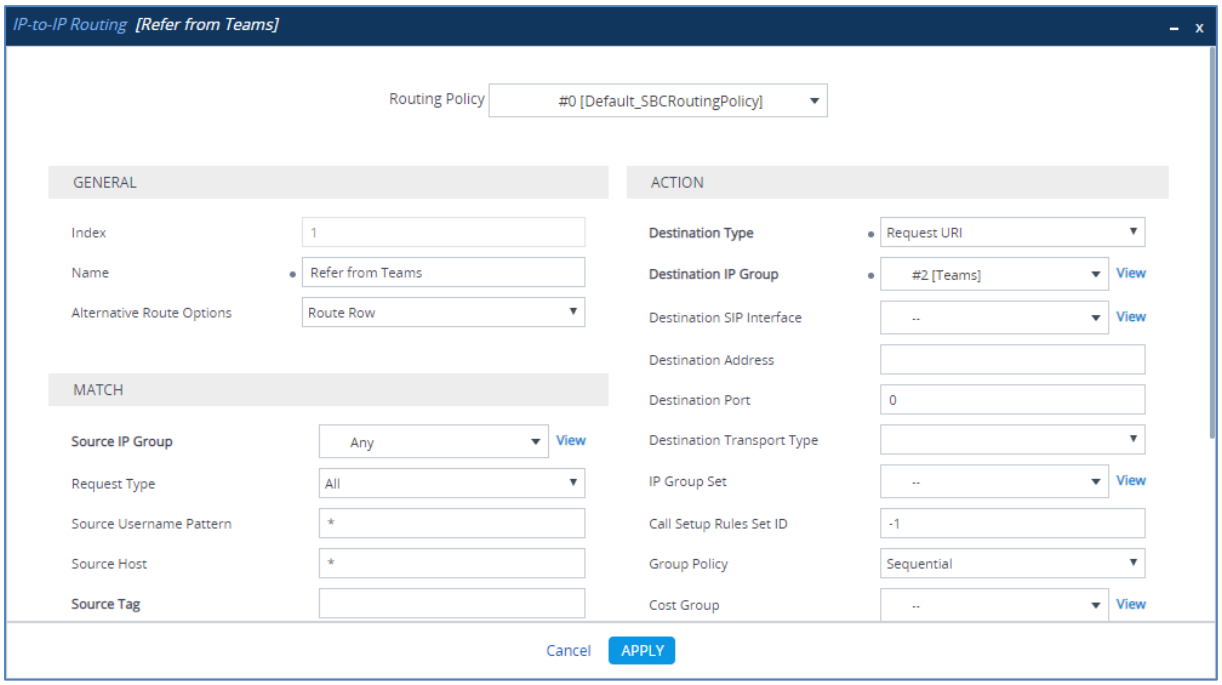


   b. Click **Apply**.

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

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

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

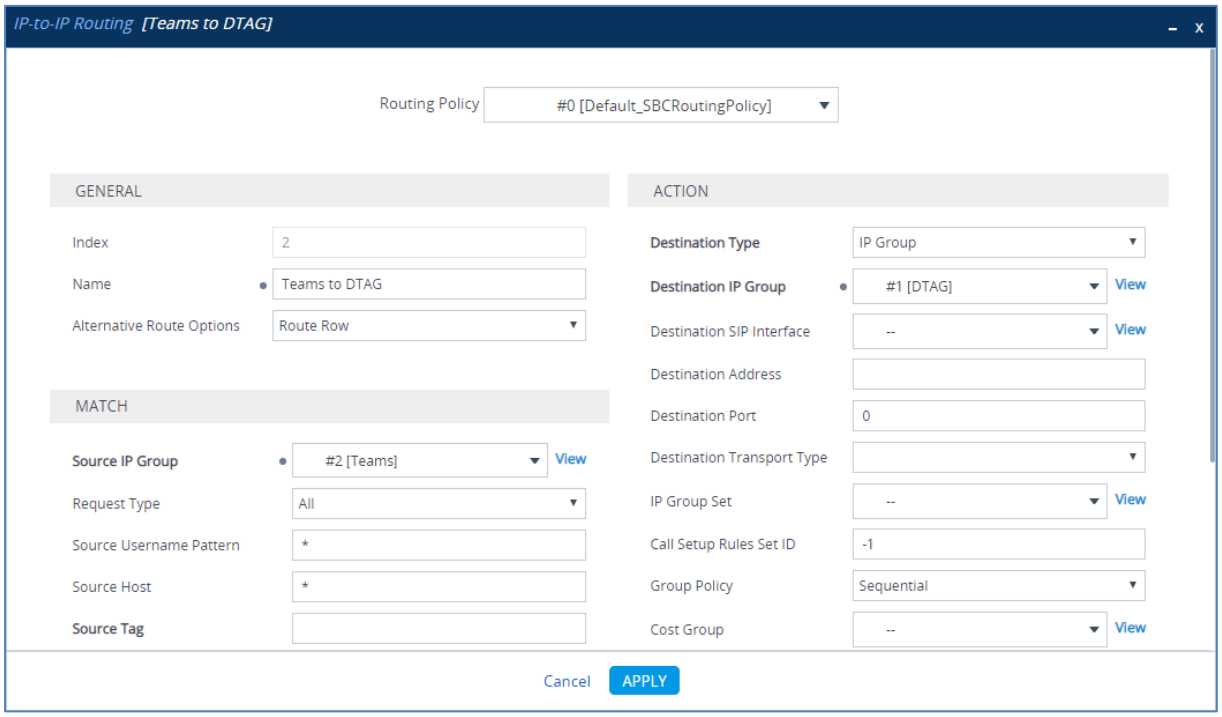


   b. Click **Apply**.

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

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

Figure 4-33: Configuring IP-to-IP Routing Rule for Teams to DTAG's DLAN

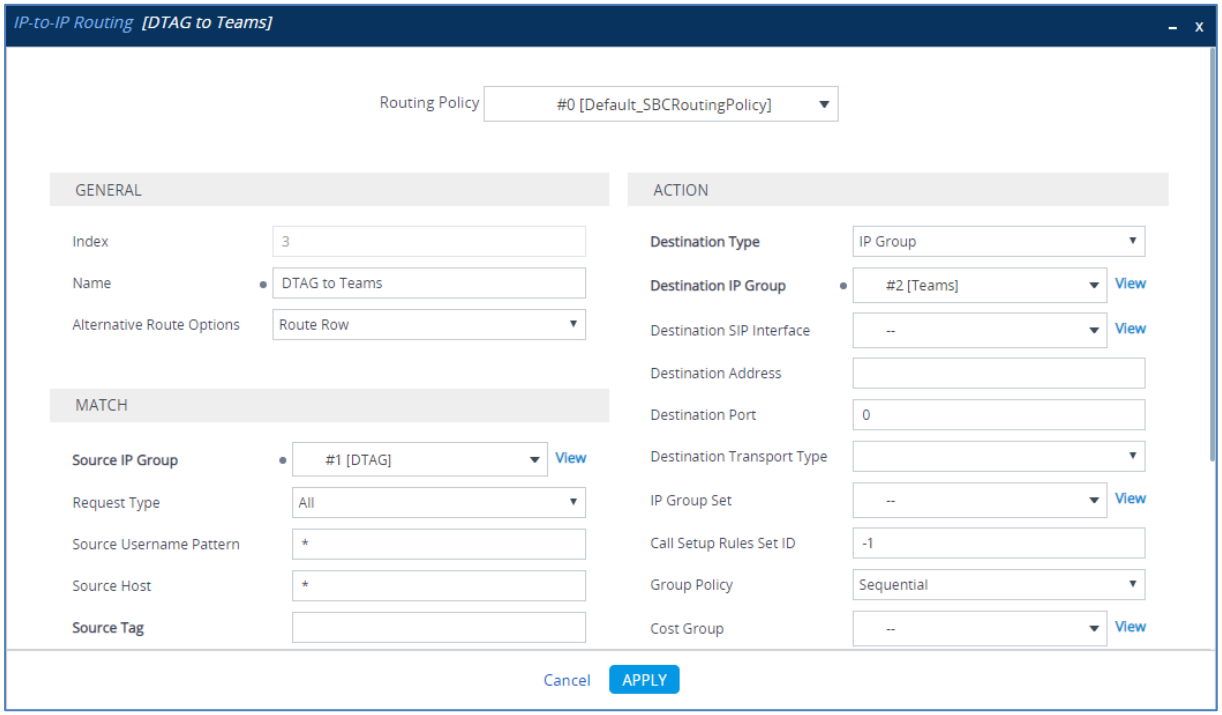


   b. Click **Apply**.

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

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

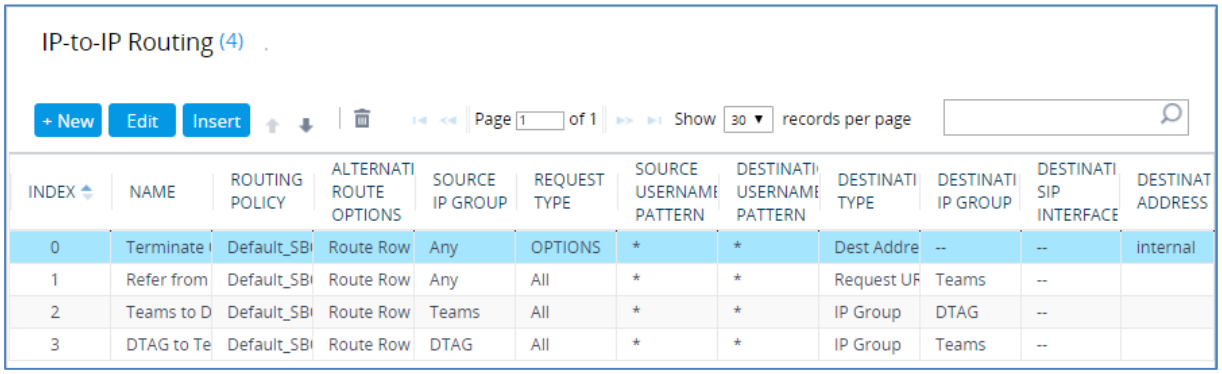
Figure 4-34: Configuring IP-to-IP Routing Rule for DTAG's DLAN to Teams



   b. Click **Apply.**

The configured routing rules are shown in the figure below:

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



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

4.14 Configure Number Manipulation Rules for Special Numbers

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 37) to denote the source and destination of the call.

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

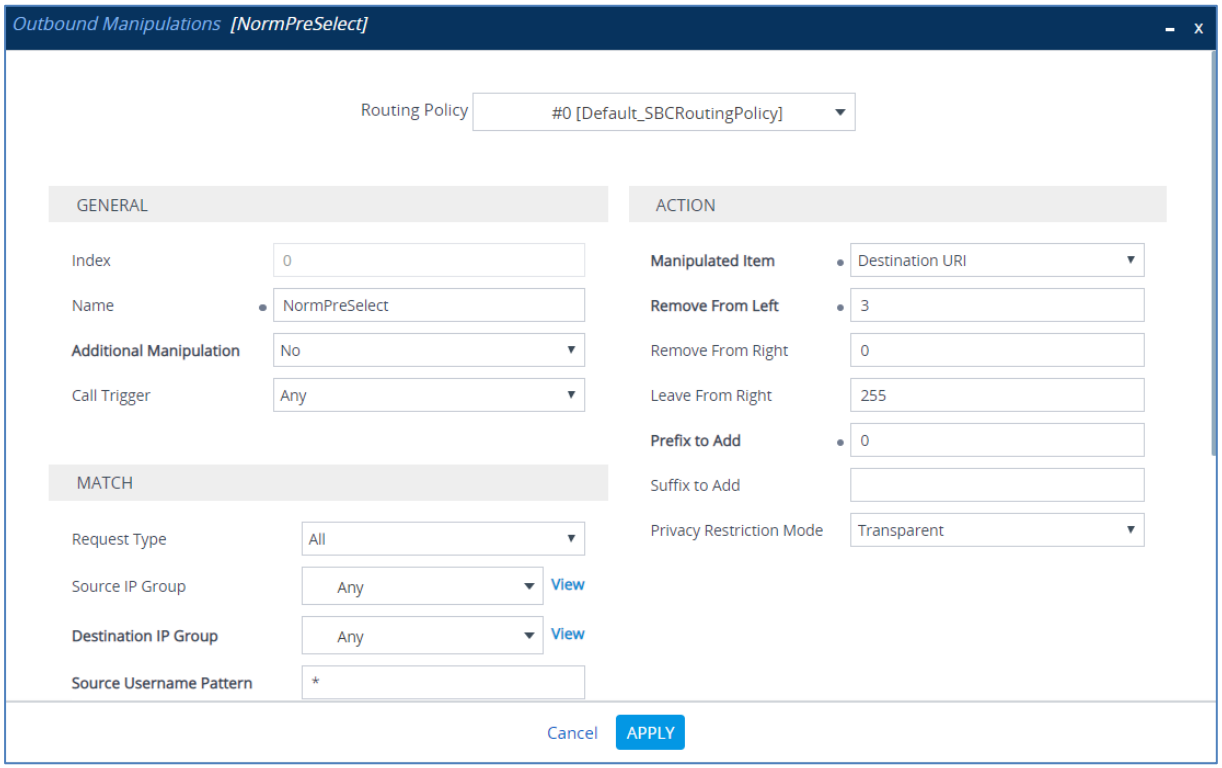
For example, for this interoperability test topology, a manipulation rules were configured for Preselect (a DTAG legal requirement) and Notruf (emergency calls).

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

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

Parameter	Value
Index	**0**
Name	**NormPreSelect**
Destination Username Pattern	**+4910xx**
Manipulated Item	**Destination URI**
Remove From Left	**3**
Prefix to Add	**0**

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

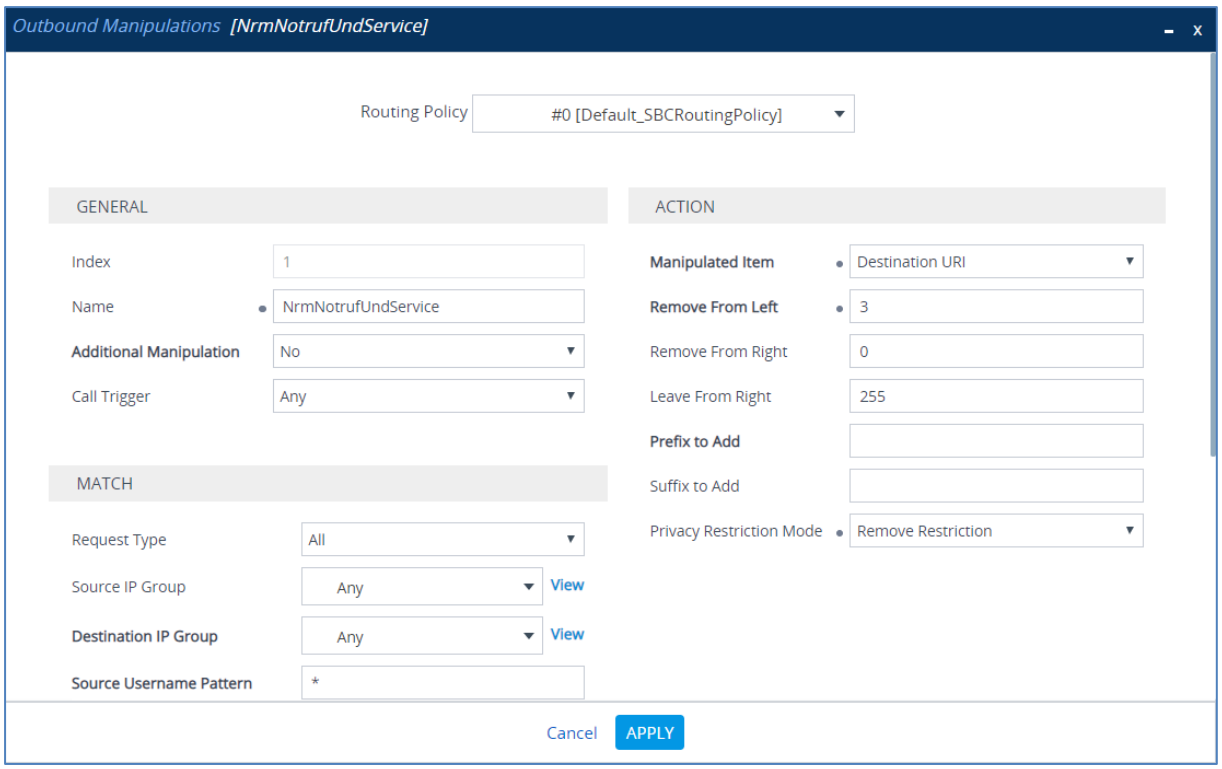


3. Click **Apply**.

4. Click **New**, and then configure the rule for emergency calls as follows:

Parameter	Value
Index	**1**
Name	**NrmNotrufUndService**
Destination Username Pattern	**+4911x**
Manipulated Item	**Destination URI**
Remove From Left	**3**
Privacy Restriction Mode	**Remove Restriction**

Figure 4-37: Configuring IP-to-IP Outbound Manipulation Rule



5. Click **Apply**.

4.15 Configure Message Manipulation Rules

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

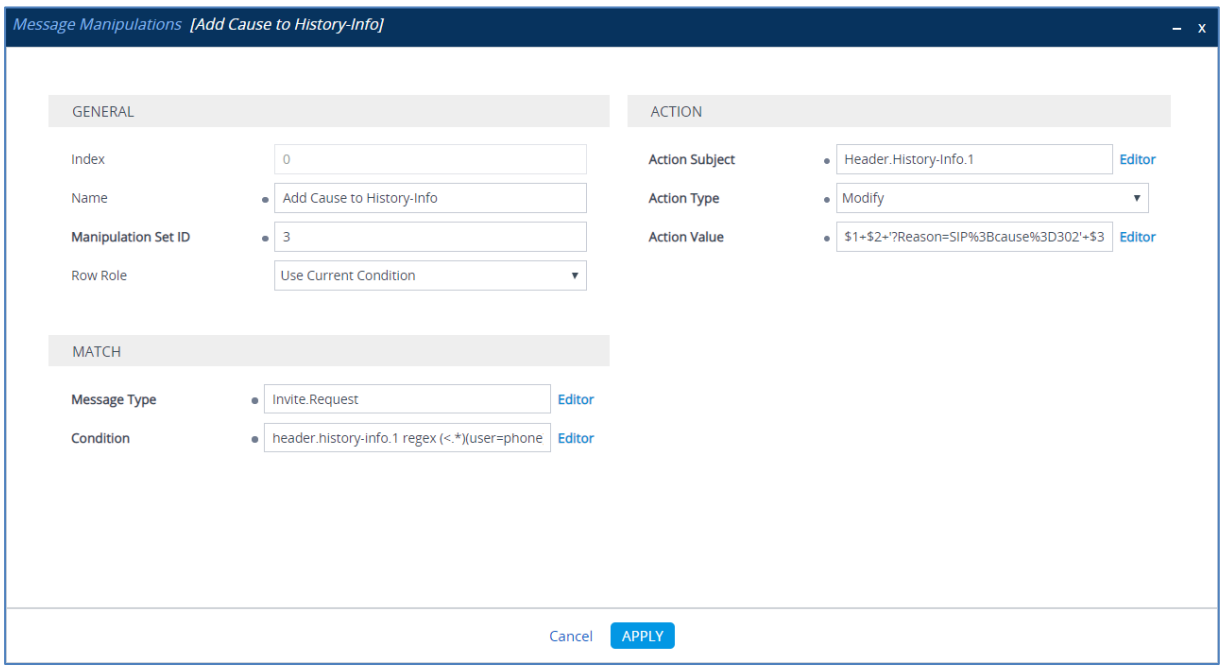
Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

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

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 3). This rule applies to messages received from the Microsoft Teams IP Group in a call forward scenario. This rule adds an Action Value containing the Reason for the History-Info header, which causes the E-SBC to add a Diversion Header towards the SIP Trunk.

Parameter	Value
Index	**0**
Name	**Add Cause to History-Info**
Manipulation Set ID	**3**
Message Type	**Invite.Request**
Condition	**Header.History-Info.1 regex (<.*)(user=phone)(>)(.*)**
Action Subject	**Header.History-Info.1**
Action Type	**Modify**
Action Value	**$1+$2+'?Reason=SIP%3Bcause%3D302'+$3+$4**

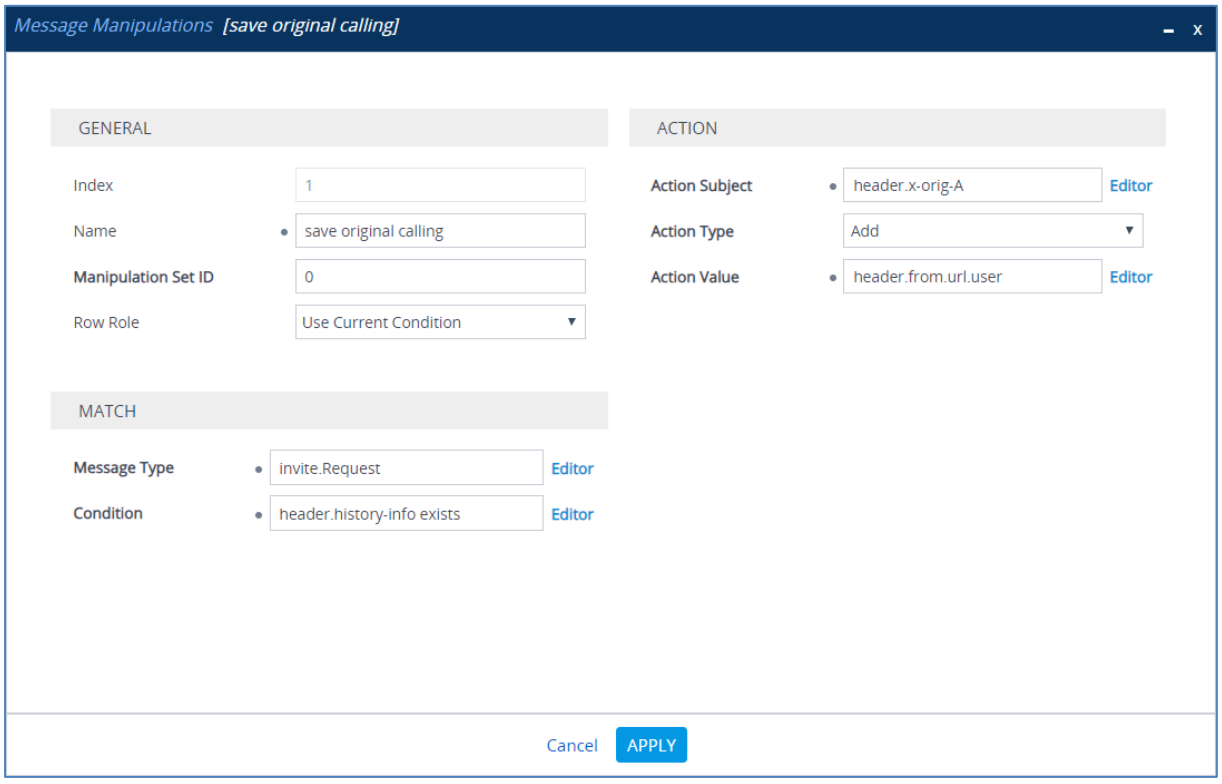
Figure 4-38: Configuring SIP Message Manipulation Rule 0 (for Teams)



3. Configure another manipulation rule (Manipulation Set 0) for Teams. This rule applies to messages received on the Teams SIP Interface. This saves the value of the user part of the SIP From Header into the new header, x-orig-A.

Parameter	Value
Index	**1**
Name	**save original calling**
Manipulation Set ID	**0**
Message Type	**Invite.Request**
Condition	**header.history-info exists**
Action Subject	**header.x-orig-A**
Action Type	**Add**
Action Value	**header.from.url.user**

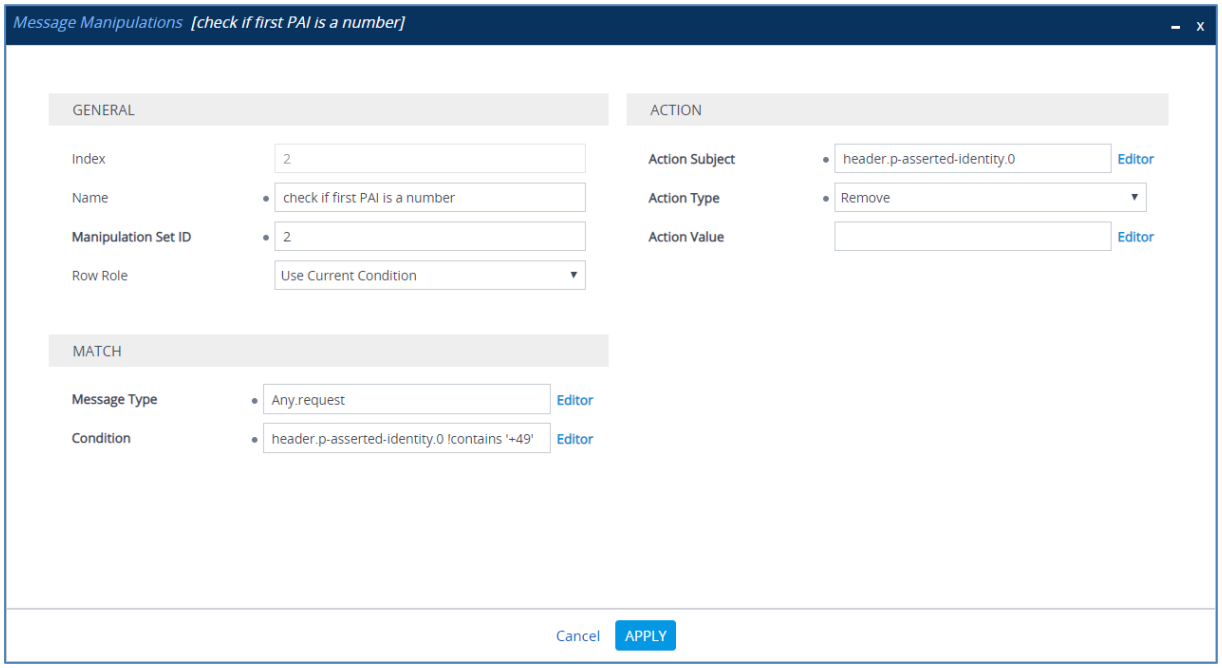
Figure 4-39: Configuring SIP Message Manipulation Rule 1 (for Teams)



4. Configure another manipulation rule (Manipulation Set 2) for DTAG's DLAN SIP Trunk. This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group. This removes Index 0 of the SIP P-Asserted-Identity Header, if it does not contain numbers.

Parameter	Value
Index	**2**
Name	**check if first PAI is a number**
Manipulation Set ID	**2**
Message Type	**Any.Request**
Condition	**header.p-asserted-identity.0 !contains '+49'**
Action Subject	**header.p-asserted-identity.0**
Action Type	**Remove**

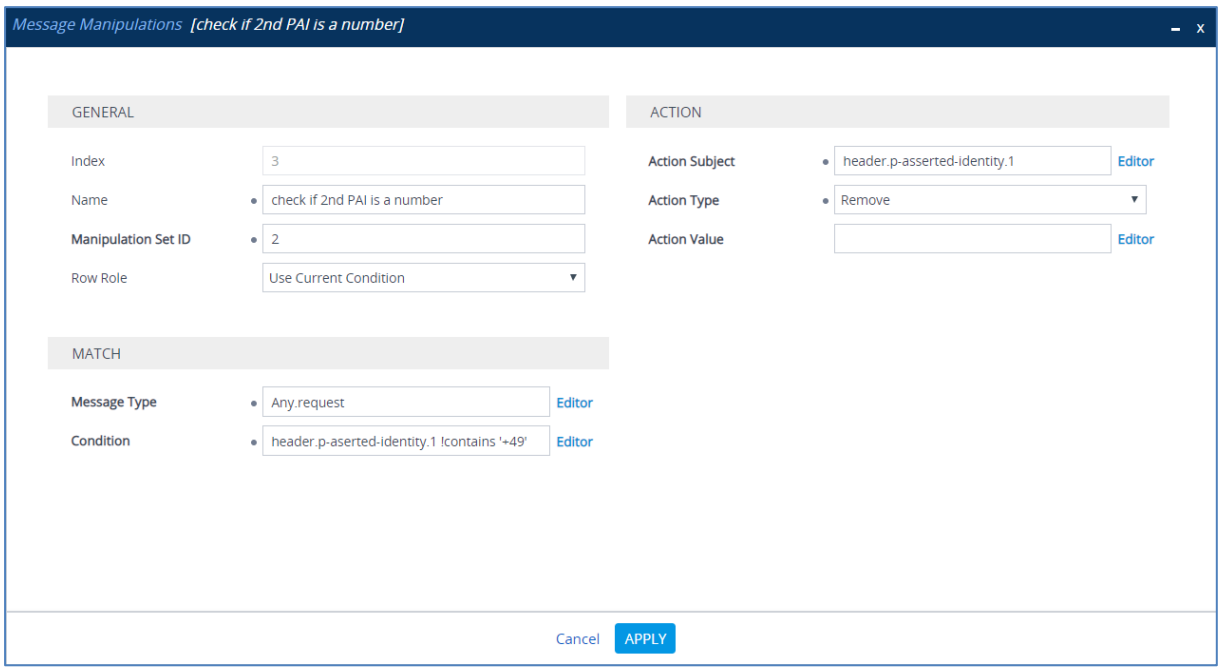
Figure 4-40: Configuring SIP Message Manipulation Rule 2 (for DTAG's DLAN SIP Trunk)



5. Configure another manipulation rule (Manipulation Set 2) for DTAG's DLAN SIP Trunk. This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group. This removes Index 1 of the SIP P-Asserted-Identity Header, if it does not contain numbers.

Parameter	Value
Index	**3**
Name	**check if first PAI is a number**
Manipulation Set ID	**2**
Message Type	**Any.Request**
Condition	**header.p-asserted-identity.1 !contains '+49'**
Action Subject	**header.p-asserted-identity.1**
Action Type	**Remove**

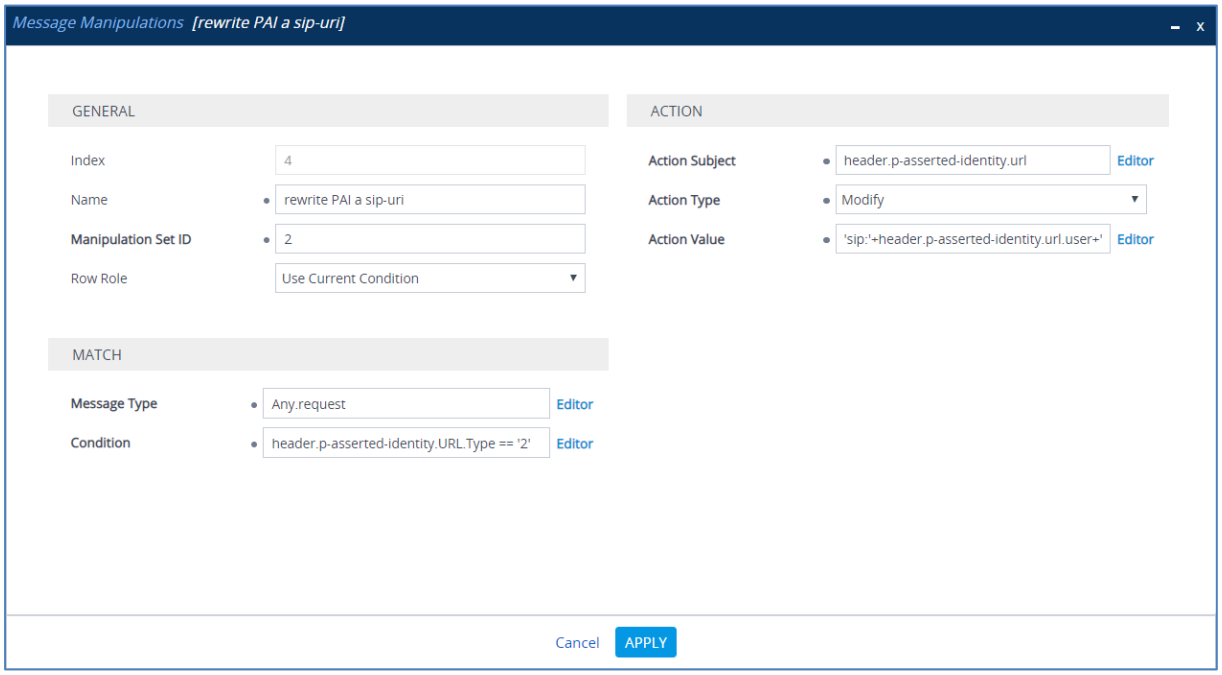
Figure 4-41: Configuring SIP Message Manipulation Rule 3 (for DTAG's DLAN SIP Trunk)



6. Configure another manipulation rule (Manipulation Set 2) for DTAG's DLAN SIP Trunk. This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group. This changes the type of the SIP P-Asserted-Identity Header to the sip-uri.

Parameter	Value
Index	**4**
Name	**rewrite PAI a sip-uri**
Manipulation Set ID	**2**
Message Type	**Any.Request**
Condition	**header.p-asserted-identity.URL.Type == '2'**
Action Subject	**header.p-asserted-identity.url**
Action Type	**Modify**
Action Value	**'sip:'+header.p-asserted-identity.url.user+'@sip-trunk.telekom.de'**

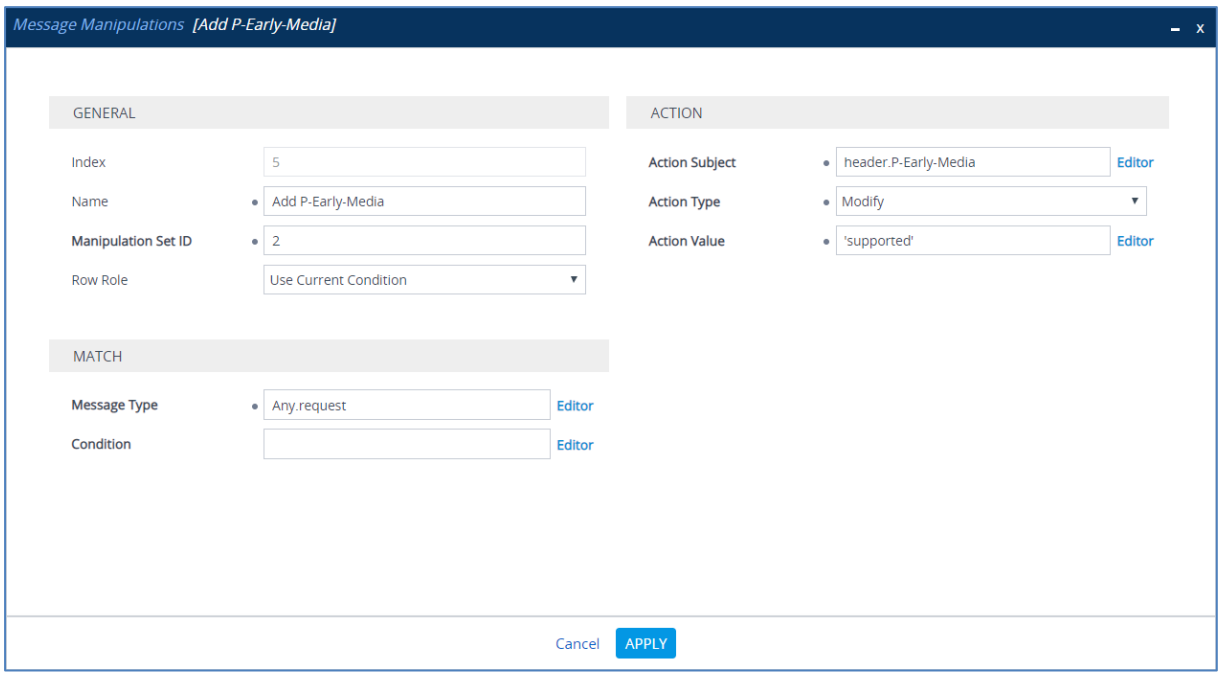
Figure 4-42: Configuring SIP Message Manipulation Rule 4 (for DTAG's DLAN SIP Trunk)



7. Configure another manipulation rule (Manipulation Set 2) for DTAG's DLAN SIP Trunk. This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group. This adds the SIP P-Early-Media Header with the value 'supported'.

Parameter	Value
Index	**5**
Name	**Add P-Early-Media**
Manipulation Set ID	**2**
Message Type	**Any.Request**
Action Subject	**Header.P-Early-Media**
Action Type	**Add**
Action Value	**'supported'**

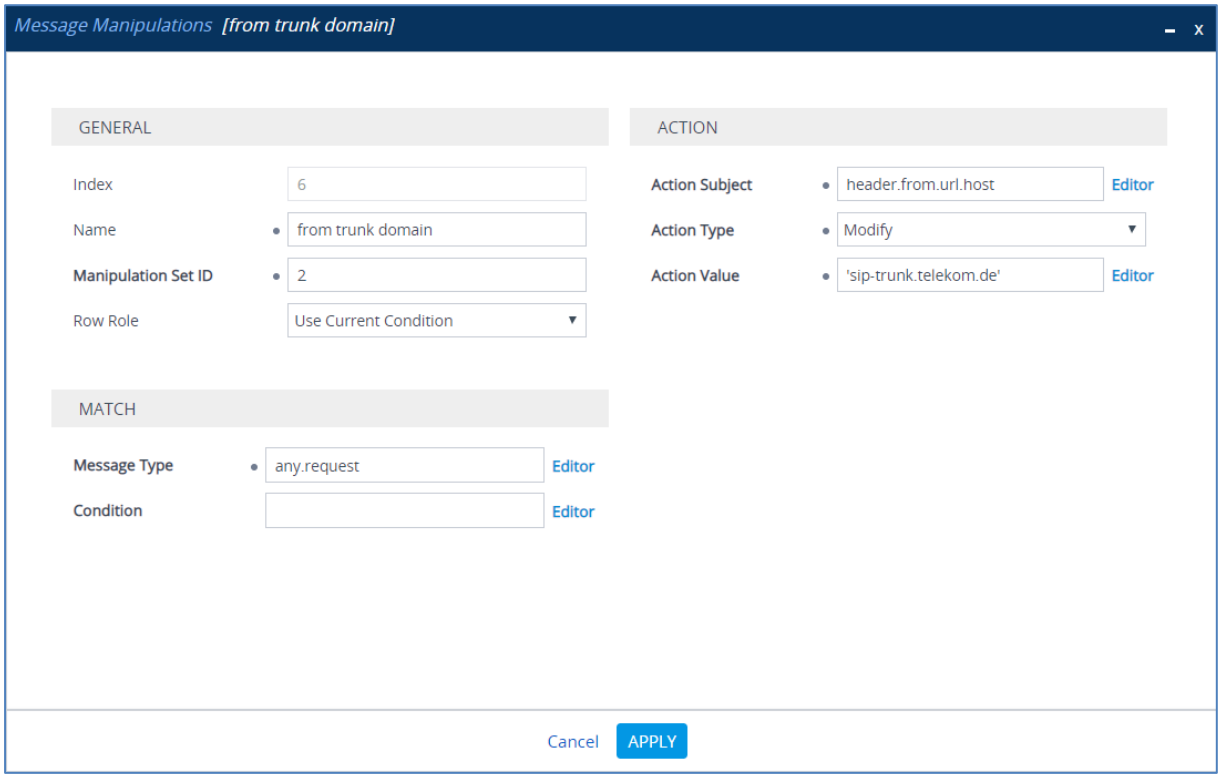
Figure 4-43: Configuring SIP Message Manipulation Rule 5 (for DTAG's DLAN SIP Trunk)



8. Configure another manipulation rule (Manipulation Set 2) for DTAG's DLAN SIP Trunk. This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group. This replaces the host part of the SIP From Header with the value 'sip-trunk.telekom.de'.

Parameter	Value
Index	**6**
Name	**from trunk domain**
Manipulation Set ID	**2**
Message Type	**Any.Request**
Action Subject	**header.from.url.host**
Action Type	**Modify**
Action Value	**'sip-trunk.telekom.de'**

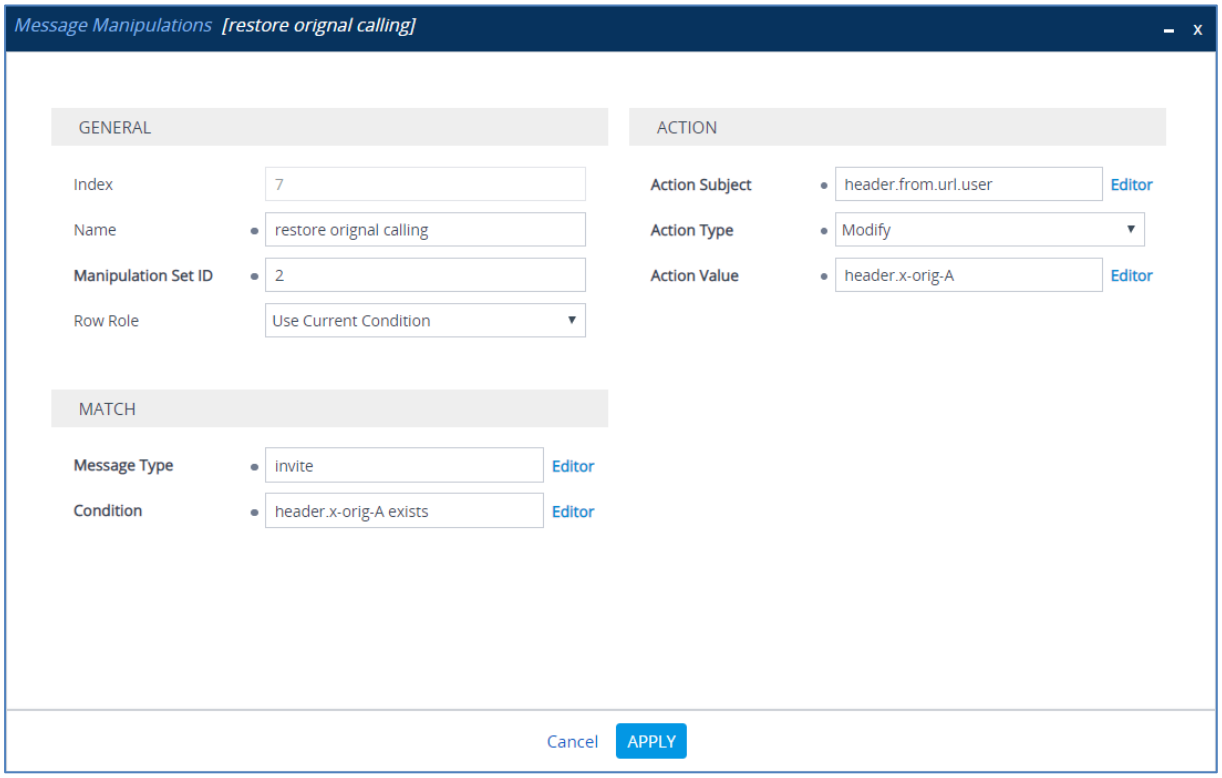
Figure 4-44: Configuring SIP Message Manipulation Rule 6 (for DTAG's DLAN SIP Trunk)



9. Configure another manipulation rule (Manipulation Set 2) for DTAG's DLAN SIP Trunk. This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group. This replaces the user part of the SIP From Header with the saved in the x-orig-A header value.

Parameter	Value
Index	**7**
Name	**restore original calling**
Manipulation Set ID	**2**
Message Type	**Invite**
Condition	**header.x-orig-A exists**
Action Subject	**header.from.url.user**
Action Type	**Modify**
Action Value	**header.x-orig-A**

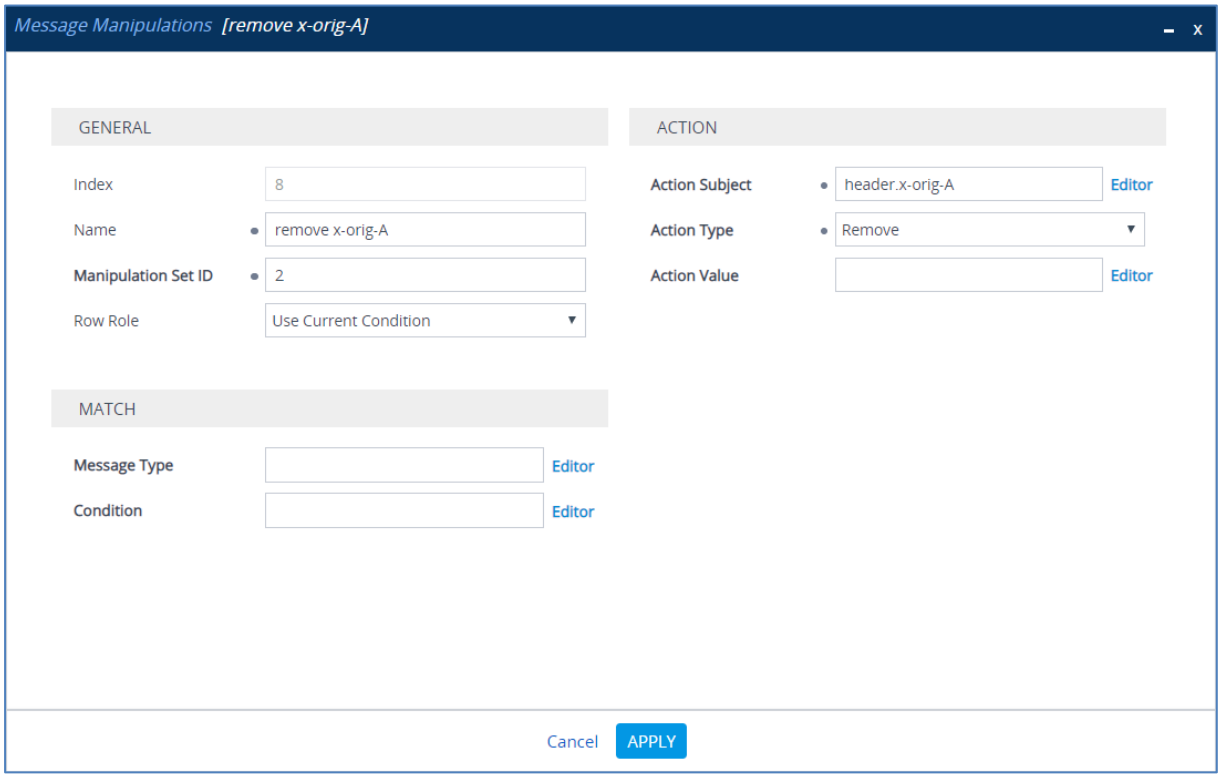
Figure 4-45: Configuring SIP Message Manipulation Rule 7 (for DTAG's DLAN SIP Trunk)



10. Configure another manipulation rule (Manipulation Set 2) for DTAG's DLAN SIP Trunk. This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group. This removes the x-orig-A header.

Parameter	Value
Index	**8**
Name	**remove x-orig-A**
Manipulation Set ID	**2**
Message Type	
Action Subject	**header.x-orig-A**
Action Type	**Remove**

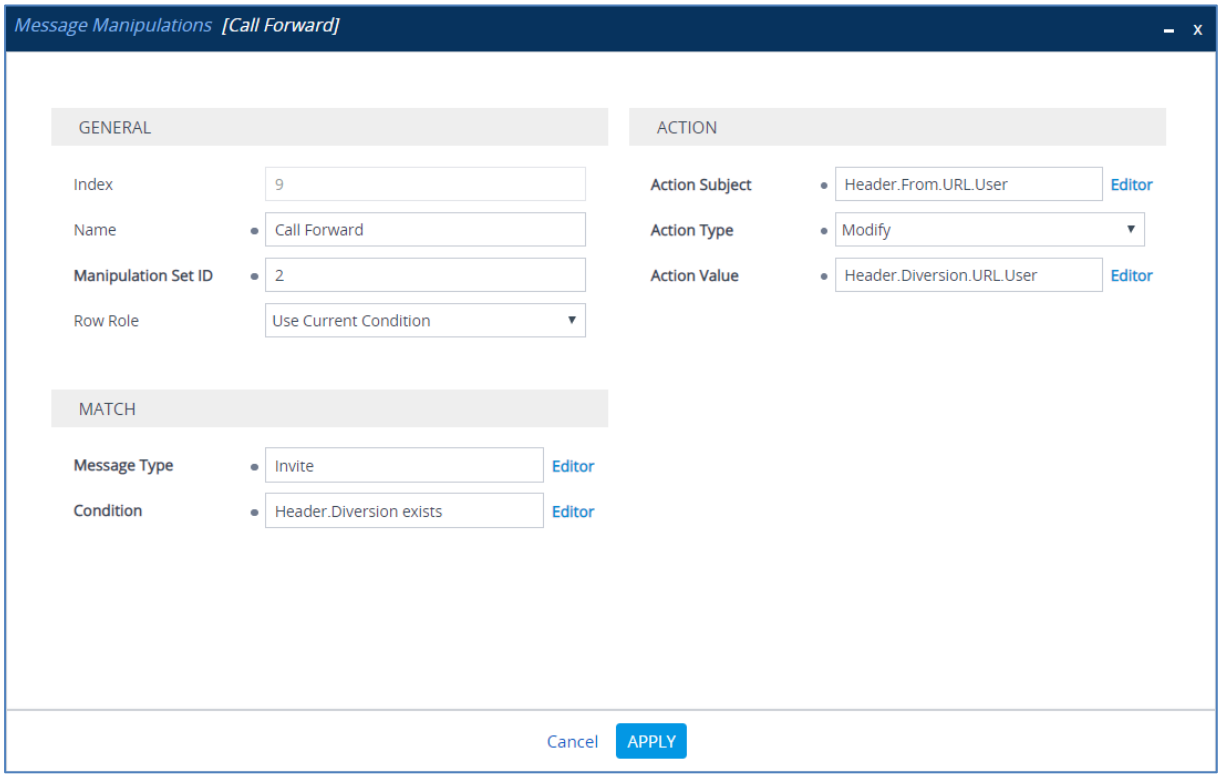
Figure 4-46: Configuring SIP Message Manipulation Rule 8 (for DTAG's DLAN SIP Trunk)



11. Configure another manipulation rule (Manipulation Set 2) for DTAG's DLAN SIP Trunk. This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group in a call forward scenario. This replaces the user part of the SIP From Header with the value from the SIP Diversion Header.

Parameter	Value
Index	**9**
Name	**Call Forward**
Manipulation Set ID	**2**
Message Type	**Invite**
Condition	**Header.Diversion exists**
Action Subject	**Header.From.Url.User**
Action Type	**Modify**
Action Value	**Header.Diversion.Url.User**

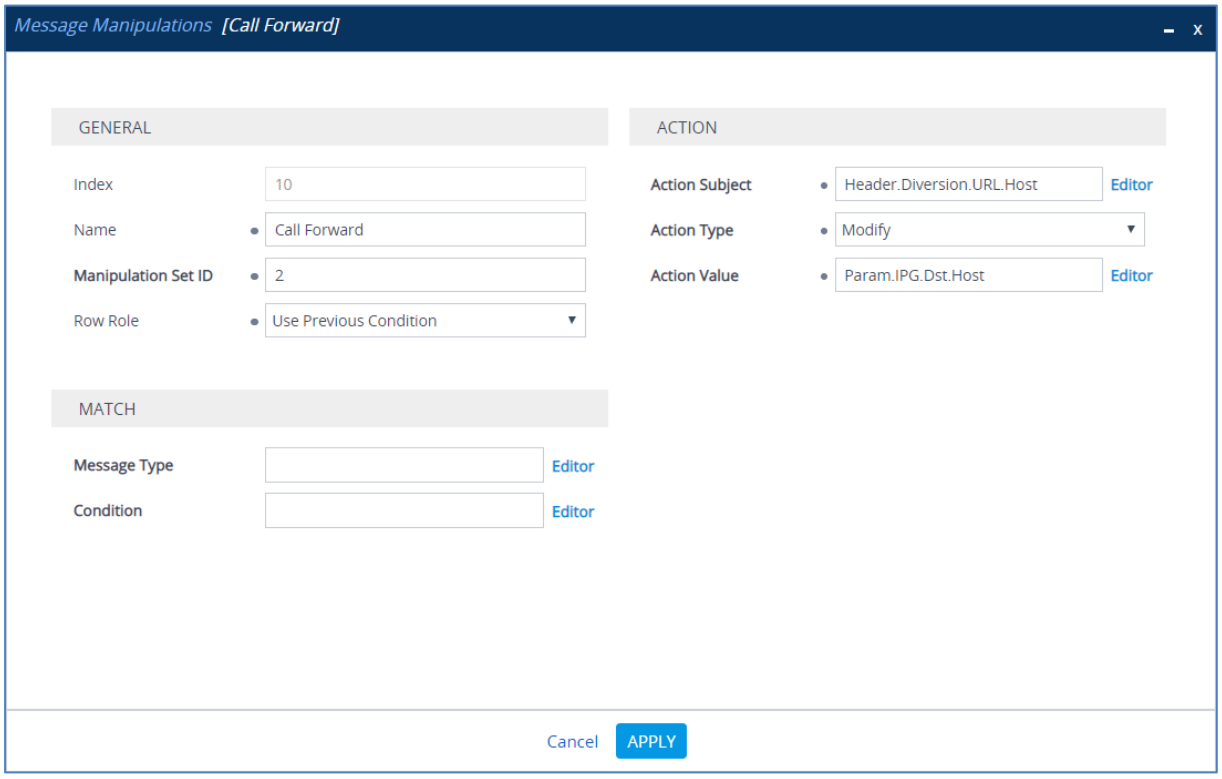
Figure 4-47: Configuring SIP Message Manipulation Rule 9 (for DTAG's DLAN SIP Trunk)



12. If the manipulation rule Index 9 (above) is executed, then the following rule is also executed on the same SIP message. This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group in a call forward scenario. This replaces the host part of the SIP Diversion Header with the value, configured in the SIP trunk IP Group.

Parameter	Value
Index	**10**
Name	**Call Forward**
Manipulation Set ID	**2**
Row Role	**Use Previous Condition**
Condition	
Action Subject	**Header.Diversion.Url.Host**
Action Type	**Modify**
Action Value	**Param.IPG.Dst.Host**

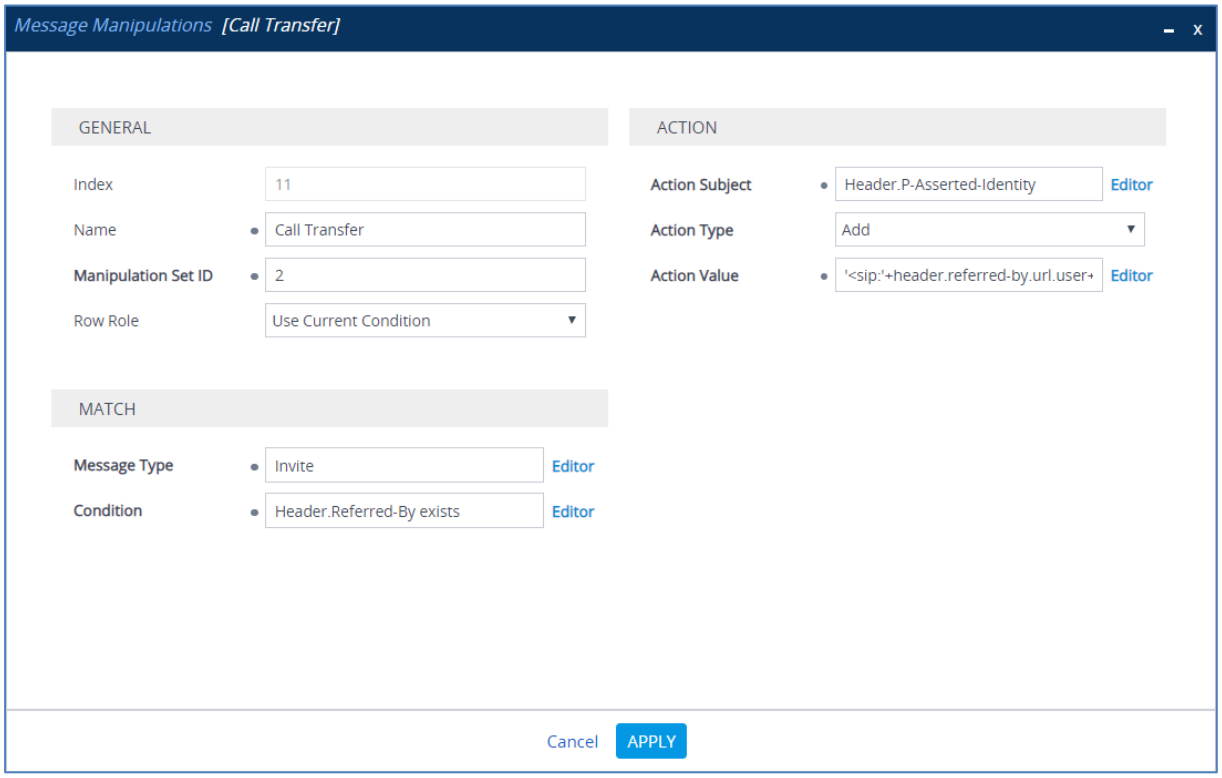
Figure 4-48: Configuring SIP Message Manipulation Rule 10 (for DTAG's DLAN SIP Trunk)



13. Configure another manipulation rule (Manipulation Set 3) for DTAG's DLAN SIP Trunk. This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group in a call transfer scenario. This replaces the user part of the SIP From Header with the value from the SIP Referred-By Header.

Parameter	Value
Index	**11**
Name	**Call Transfer**
Manipulation Set ID	**2**
Message Type	**Invite**
Condition	**Header.Referred-By exists**
Action Subject	**Header.From.Url.User**
Action Type	**Modify**
Action Value	**Header.Referred-By.Url.User**

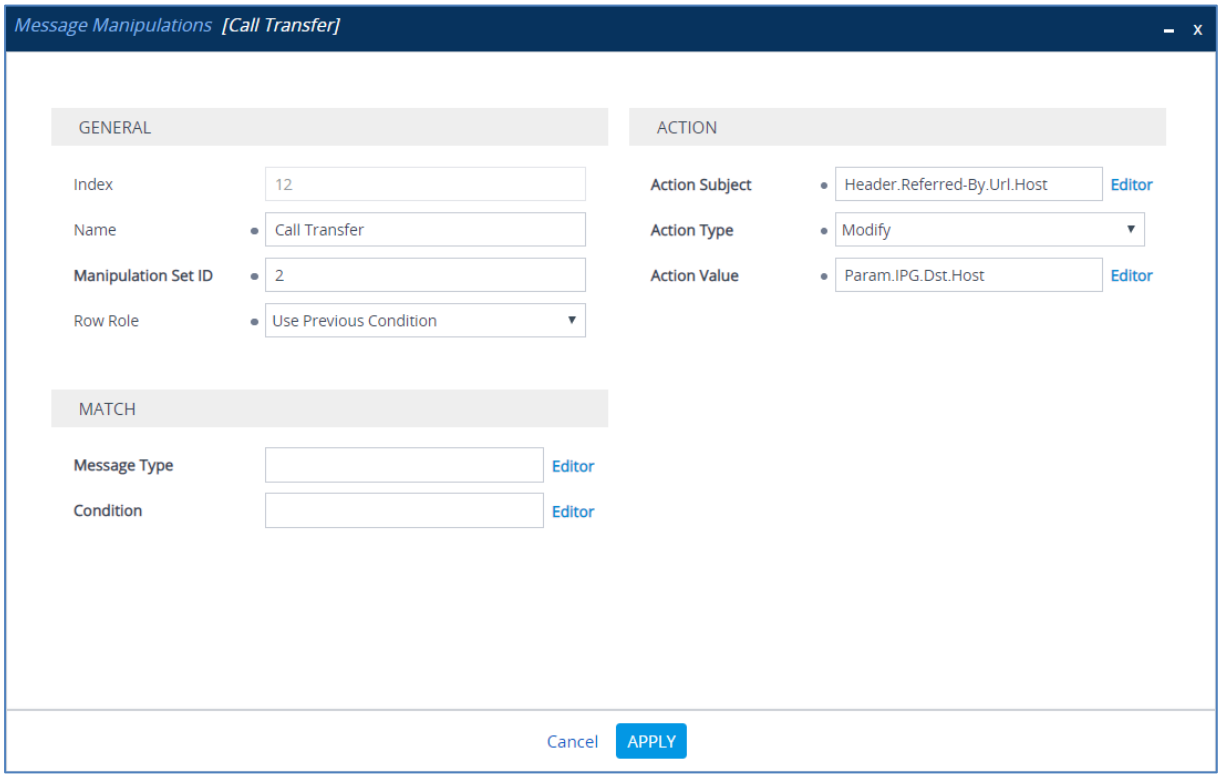
Figure 4-49: Configuring SIP Message Manipulation Rule 11 (for DTAG's DLAN SIP Trunk)



14. If the manipulation rule Index 11 (above) is executed, then the following rule is also executed on the same SIP message. This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group in a call transfer scenario. This replaces the host part of the SIP Referred-By Header with the value, configured in the SIP trunk IP Group.

Parameter	Value
Index	**12**
Name	**Call Transfer**
Manipulation Set ID	**2**
Row Role	**Use Previous Condition**
Condition	
Action Subject	**Header.Referred-By.Url.Host**
Action Type	**Modify**
Action Value	**Param.IPG.Dst.Host**

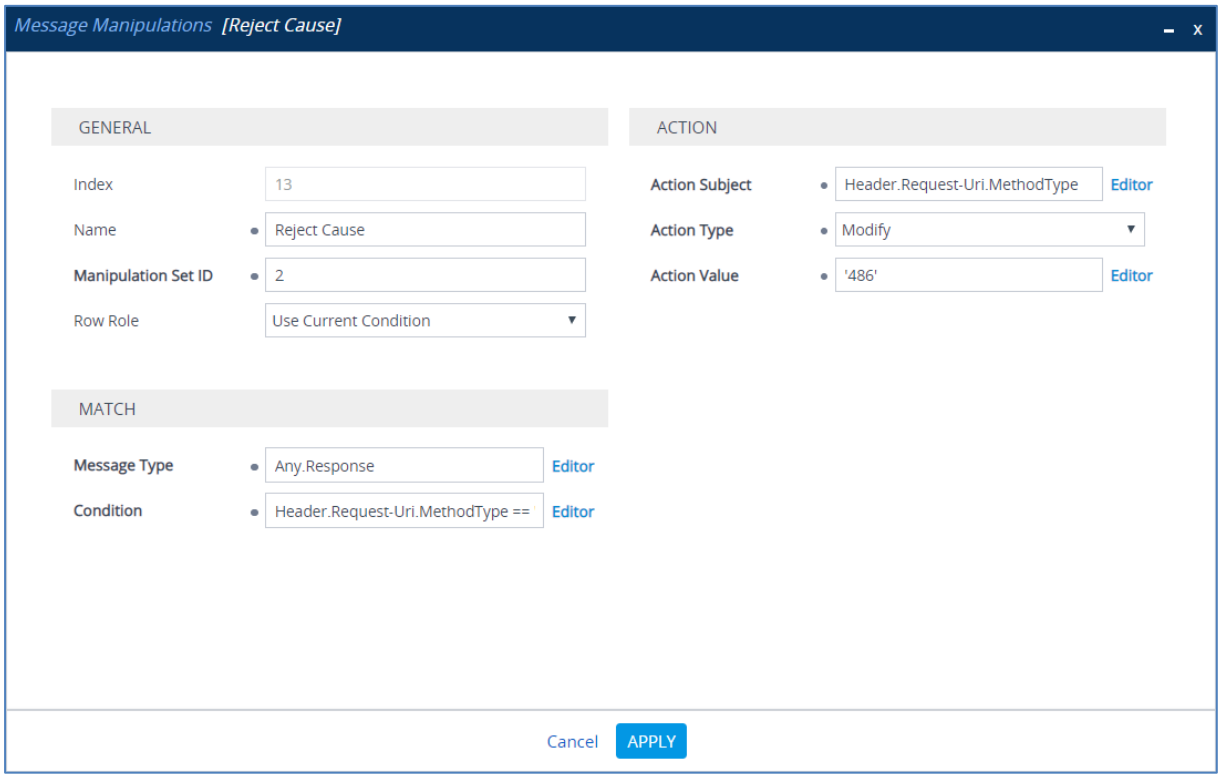
Figure 4-50: Configuring SIP Message Manipulation Rule 12 (for DTAG's DLAN SIP Trunk)



15. Configure another manipulation rule (Manipulation Set 2) for DTAG's DLAN SIP Trunk. This rule is applied to response messages sent to the DTAG's DLAN SIP Trunk IP Group for Rejected Calls initiated by the Teams Direct Routing IP Group. This replaces the method types '480', '503' or '603' with the value '486', because DTAG's DLAN SIP Trunk not recognizes these method types and continue to send Invite messages.

Parameter	Value
Index	**13**
Name	**Reject Cause**
Manipulation Set ID	**2**
Message Type	**Any.Response**
Condition	**Header.Request-Uri.MethodType=='480' OR Header.Request-Uri.MethodType=='503' OR Header.Request-Uri.MethodType=='603'**
Action Subject	**Header.Request-Uri.MethodType**
Action Type	**Modify**
Action Value	**'486'**

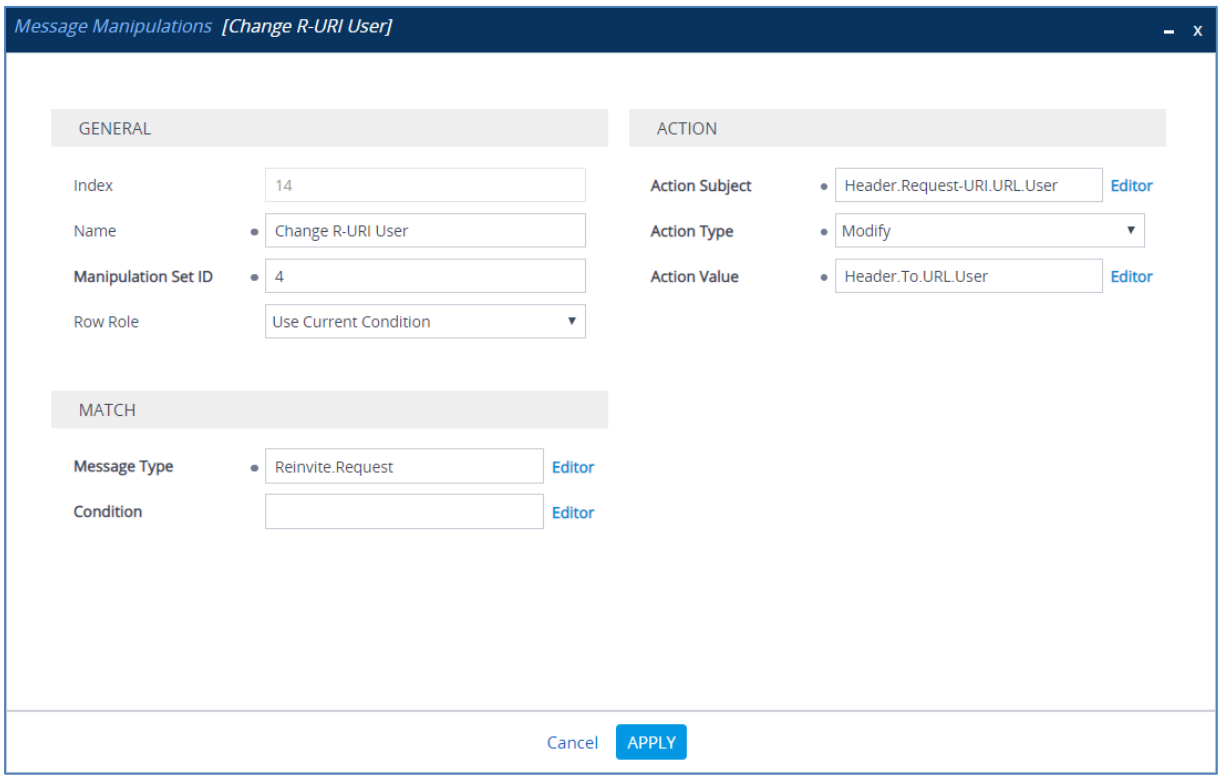
Figure 4-51: Configuring SIP Message Manipulation Rule 13 (for DTAG's DLAN SIP Trunk)



16. Configure another manipulation rule (Manipulation Set 4) for the Teams Direct Routing. This rule is applied to Re-Invite messages sent to the Teams Direct Routing IP Group. This replaces the user part of the SIP Request-URI Header with the value from the SIP To Header.

Parameter	Value
Index	**14**
Name	**Change R-URI User**
Manipulation Set ID	**4**
Message Type	**Reinvite.Request**
Condition	
Action Subject	**Header.Request-URI.URL.User**
Action Type	**Modify**
Action Value	**Header.To.URL.User**

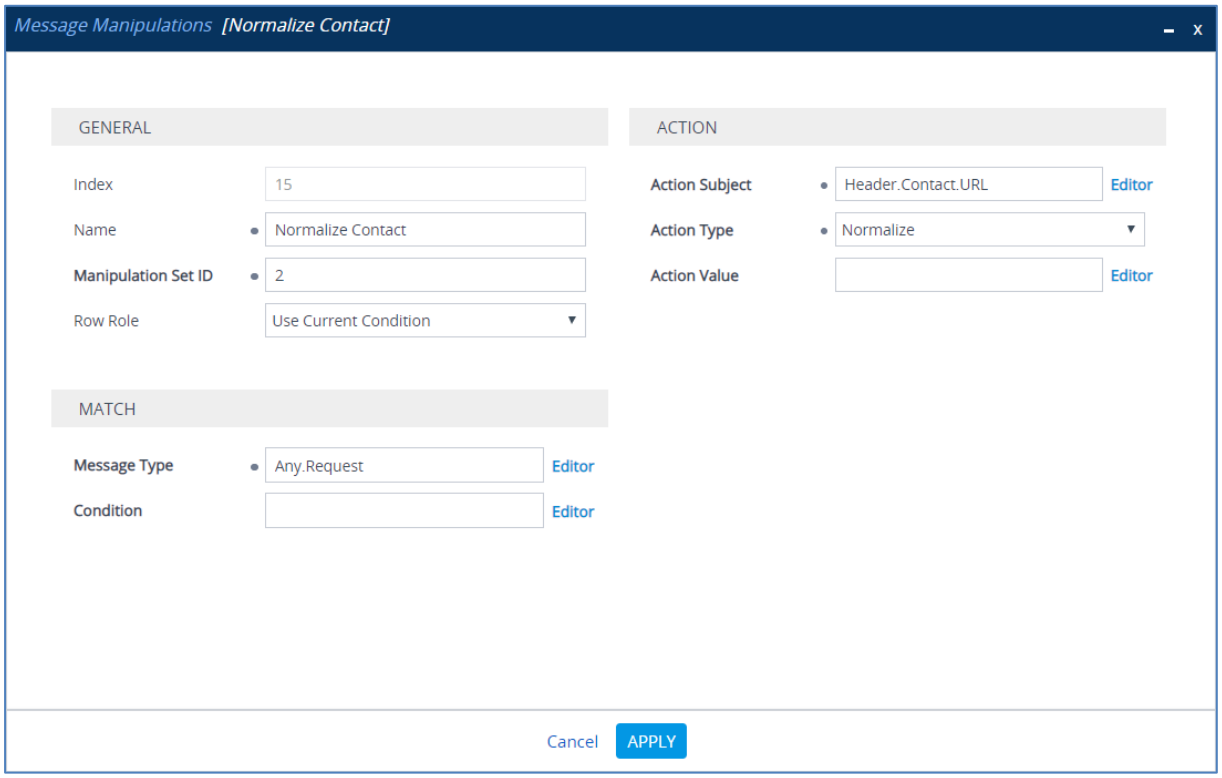
Figure 4-52: Configuring SIP Message Manipulation Rule 14 (for Teams)



17. Configure another manipulation rule (Manipulation Set 2) for DTAG's DLAN SIP Trunk. This rule is applied to all messages sent to the DTAG's DLAN SIP Trunk IP Group. This rule normalizes the SIP Contact Header of each message.

Parameter	Value
Index	**15**
Name	**Normalize Contact**
Manipulation Set ID	**2**
Message Type	**Invite.Request**
Action Subject	**Header.Contact.URL**
Action Type	**Normalize**

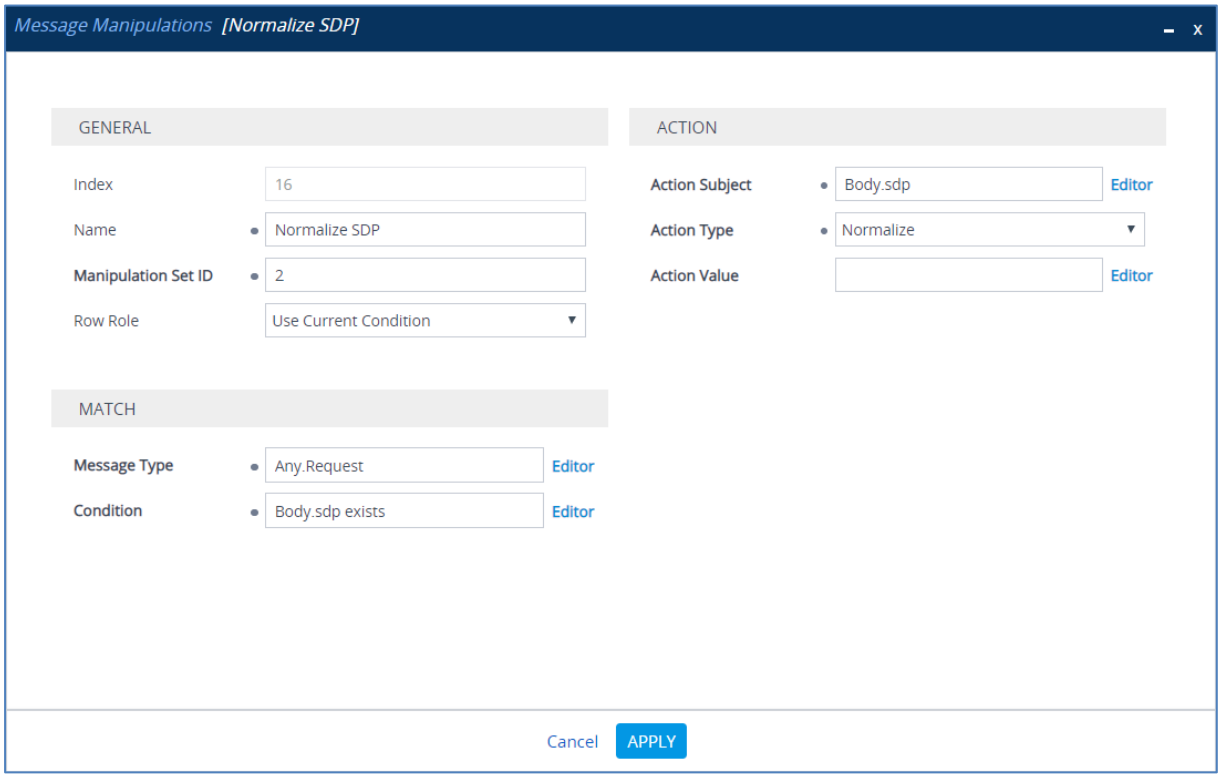
Figure 4-53: Configuring SIP Message Manipulation Rule 15 (for DTAG's DLAN SIP Trunk)



18. Configure another manipulation rule (Manipulation Set 2) for DTAG's DLAN SIP Trunk. This rule is applied to all messages sent to the DTAG's DLAN SIP Trunk IP Group. This rule normalizes the SDP body of each message.

Parameter	Value
Index	**16**
Name	**Normalize SDP**
Manipulation Set ID	**2**
Message Type	**Any.Request**
Condition	**Body.sdp exists**
Action Subject	**Body.sdp**
Action Type	**Normalize**

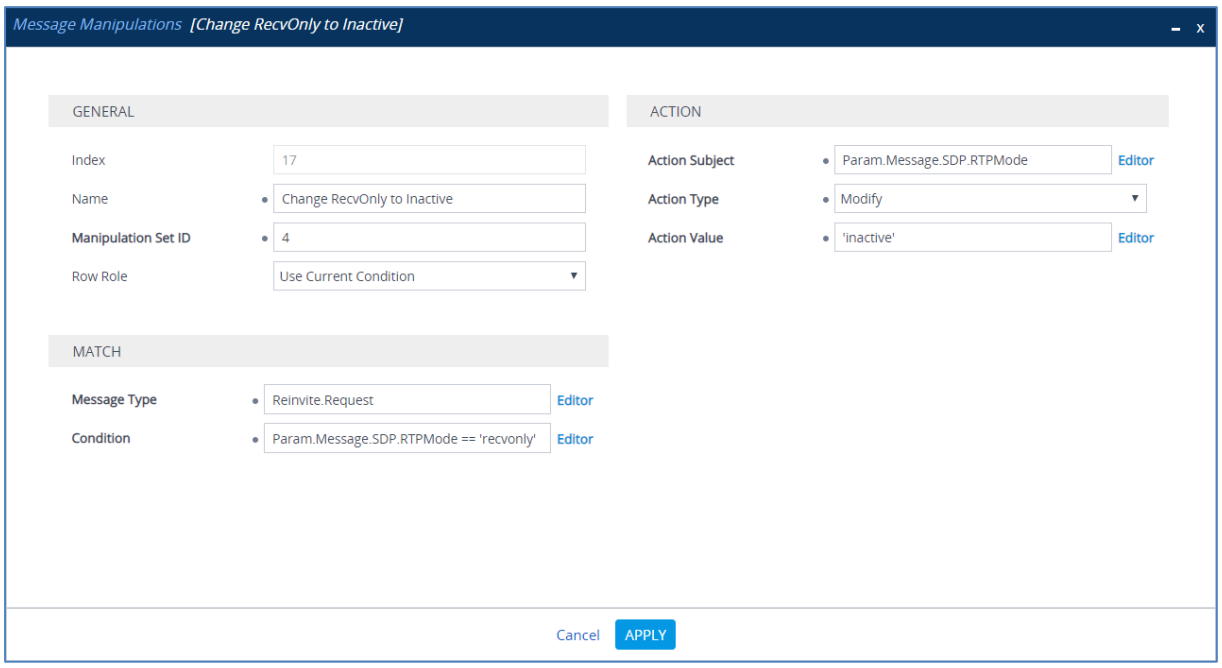
Figure 4-54: Configuring SIP Message Manipulation Rule 16 (for DTAG's DLAN SIP Trunk)



19. Configure another manipulation rule (Manipulation Set 4) for the Teams Direct Routing. This rule is applied to Re-INVITE messages sent to the Teams Direct Routing IP Group. This replaces the SDP RTP mode from 'recvonly' to 'inactive'.

Parameter	Value
Index	**17**
Name	**Change RecvOnly to Inactive**
Manipulation Set ID	**4**
Message Type	**Reinvite.Request**
Condition	**Param.Message.SDP.RTPMode == 'recvonly'**
Action Subject	**Param.Message.SDP.RTPMode**
Action Type	**Modify**
Action Value	**'inactive'**

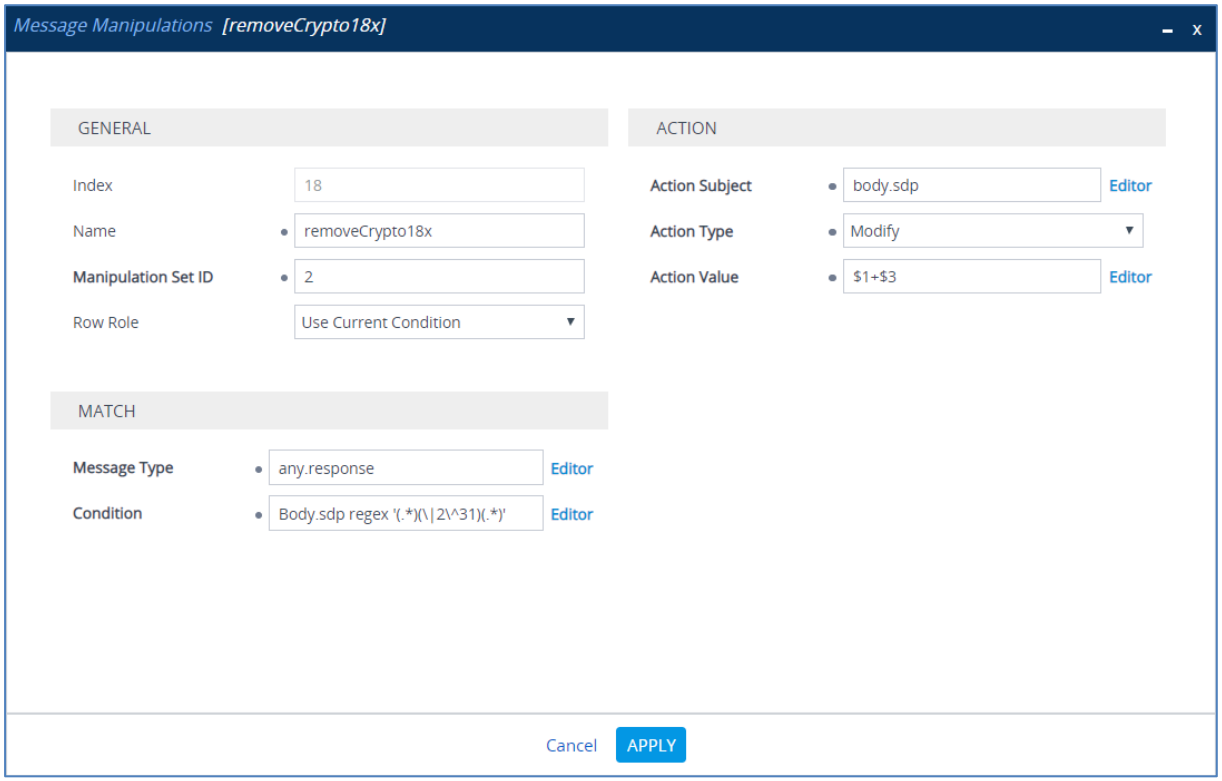
Figure 4-55: Configuring SIP Message Manipulation Rule 17 (for Teams)



20. Configure another manipulation rule (Manipulation Set 2) for DTAG's DLAN SIP Trunk. This rule is applied to all messages sent to the DTAG's DLAN SIP Trunk IP Group. This rule removes the crypto line with '|2^31' from the SDP body of each message.

Parameter	Value
Index	**18**
Name	**removeCrypto18x**
Manipulation Set ID	**2**
Message Type	**Any.Response**
Condition	**Body.sdp regex '(.*)(|2\^31)(.*)'**
Action Subject	**Body.sdp**
Action Type	**Modify**
Action Value	**$1+$3**

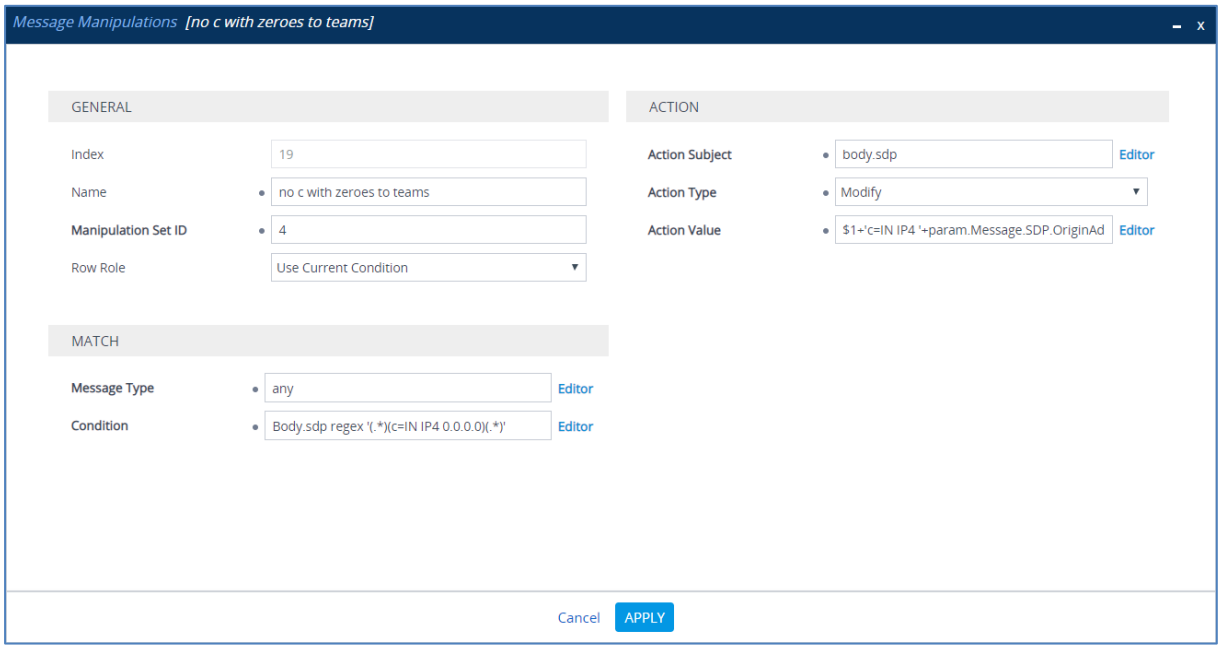
Figure 4-56: Configuring SIP Message Manipulation Rule 18 (for DTAG's DLAN SIP Trunk)



21. Configure another manipulation rule (Manipulation Set 4) for the Teams Direct Routing. This rule is applied to the messages sent to the Teams Direct Routing IP Group. This replaces the SDP RTP address from '0.0.0.0' with the address of the SBC.

Parameter	Value
Index	**19**
Name	**no c with zeroes to teams**
Manipulation Set ID	**4**
Message Type	**Any**
Condition	**Body.sdp regex '(.*)(c=IN IP4 0.0.0.0)(.*)'**
Action Subject	**body.sdp**
Action Type	**Modify**
Action Value	**$1+'c=IN IP4 '+param.Message.SDP.OriginAddress+$3**

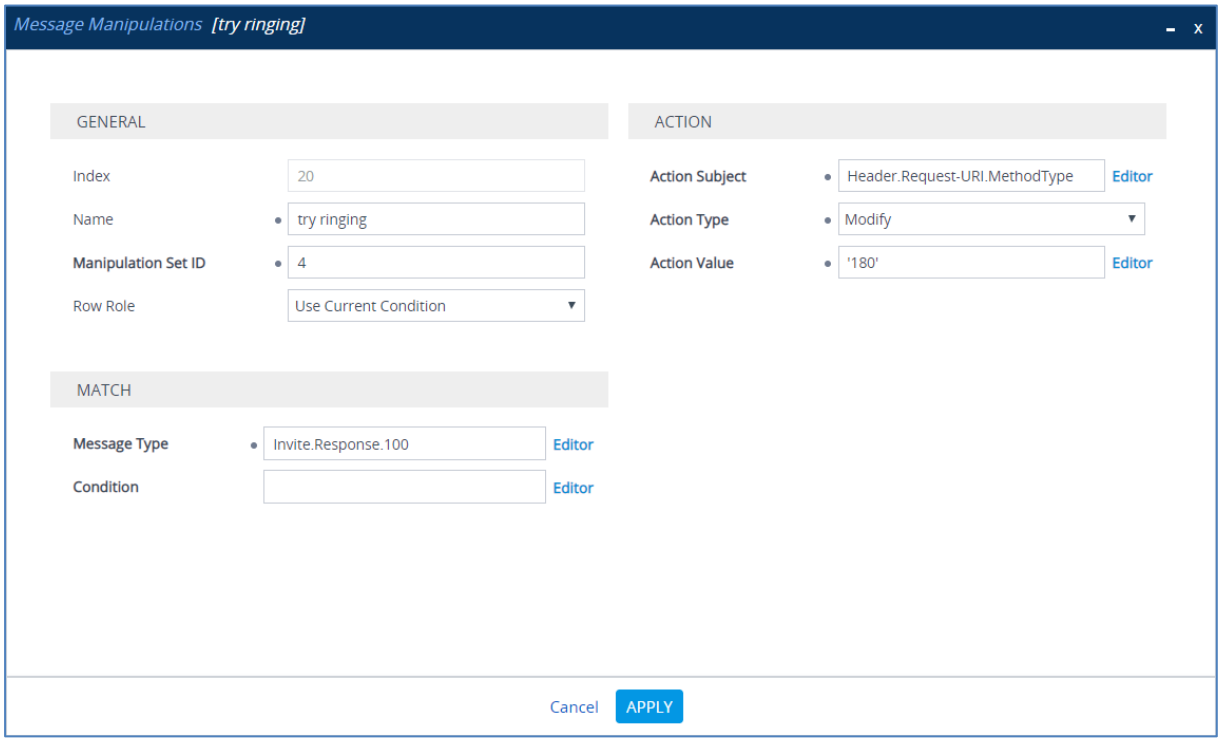
Figure 4-57: Configuring SIP Message Manipulation Rule 19 (for Teams)



22. Configure another manipulation rule (Manipulation Set 4) for the Teams Direct Routing. This rule is applied to the all responses sent to the Teams Direct Routing IP Group. This replaces the method type from '100 Trying' to '180 Ringing'.

Parameter	Value
Index	**20**
Name	**try ringing**
Manipulation Set ID	**4**
Message Type	**Invite.Response.100**
Action Subject	**Header.Request-URI.MethodType**
Action Type	**Modify**
Action Value	**'180'**

Figure 4-58: Configuring SIP Message Manipulation Rule 20 (for Teams)



23. Configure another manipulation rule (Manipulation Set 3). This rule applies to messages received from the Microsoft Teams IP Group. This rule removes the SIP Privacy Header from all messages, except those that don't contain 'anonymous' in the SIP From Header.

Parameter	Value
Index	**21**
Name	**remPrivWhenNotAnon**
Manipulation Set ID	**3**
Message Type	**Any.Request**
Condition	**header.from.url !contains 'anonymous'**
Action Subject	**header.privacy**
Action Type	**Remove**

Figure 4-59: Configuring SIP Message Manipulation Rule 21 (for Teams)

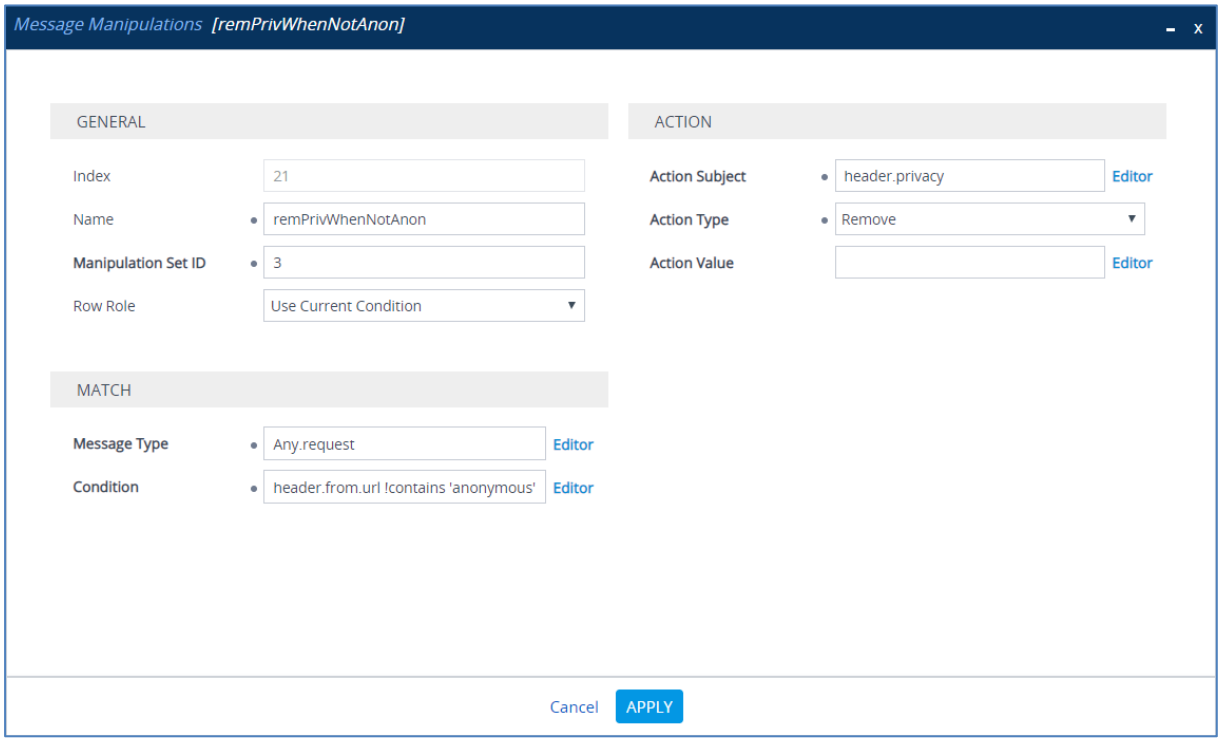


Figure 4-60: Example of Configured SIP Message Manipulation Rules

Message Manipulations (22)

+ New | Edit | Insert | Page 1 of 1 | Show 30 records per page

INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	Add Cause to History-	3	Invite.Request	header.history-info.1	Header.History-Info.1	Modify	$1+$2+'?Reason=SIP%	Use Current Conditio
1	save original calling	0	Invite.Request	header.history-info ex	header.x-orig-A	Add	header.from.url.user	Use Current Conditio
2	check if first PAI is a n	2	Any.request	header.p-asserted-ide	header.p-asserted-ide	Remove		Use Current Conditio
3	check if 2nd PAI is a n	2	Any.request	header.p-asserted-ider	header.p-asserted-ide	Remove		Use Current Conditio
4	rewrite PAI a sip-uri	2	Any.request	header.p-asserted-ide	header.p-asserted-ide	Modify	'sip:'+header.p-assert	Use Current Conditio
5	Add P-Early-Media	2	Any.request		header.P-Early-Media	Modify	'supported'	Use Current Conditio
6	from trunk domain	2	any.request		header.from.url.host	Modify	'sip-trunk.telekom.de	Use Current Conditio
7	restore original calling	2	invite	header.x-orig-A exists	header.from.url.user	Modify	header.x-orig-A	Use Current Conditio
8	remove x-orig-A	2			header.x-orig-A	Remove		Use Current Conditio
9	Call Forward	2	Invite	Header.Diversion exis	Header.From.URL.Use	Modify	Header.Diversion.URL	Use Current Conditio
10	Call Forward	2			Header.Diversion.URL	Modify	Param.IPG.Dst.Host	Use Previous Conditi
11	Call Transfer	2	Invite	Header.Referred-By e	Header.P-Asserted-Id	Add	'<sip:'+header.referre	Use Current Conditio
12	Call Transfer	2			Header.Referred-By.U	Modify	Param.IPG.Dst.Host	Use Previous Conditi
13	Reject Cause	2	Any.Response	Header.Request-Uri.M	Header.Request-Uri.M	Modify	'486'	Use Current Conditio
14	Change R-URI User	4	Reinvite.Request		Header.Request-URI.U	Modify	Header.To.URL.User	Use Current Conditio
15	Normalize Contact	2	Any.Request		Header.Contact.URL	Normalize		Use Current Conditio
16	Normalize SDP	2	Any.Request	Body.sdp exists	Body.sdp	Normalize		Use Current Conditio
17	Change RecvOnly to I	4	Reinvite.Request	Param.Message.SDP.I	Param.Message.SDP.I	Modify	'inactive'	Use Current Conditio
18	removeCrypto18x	2	any.response	Body.sdp regex '(.*)(\r\	body.sdp	Modify	$1+$3	Use Current Conditio

The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set IDs (Manipulation Set IDs 2, 3 and 4) and which are executed for messages sent to and from the DTAG's DLAN SIP Trunk IP Group as well as the Teams Direct Routing IP Group. These rules are specifically required to enable proper interworking between DTAG's DLAN SIP Trunk and Teams Direct Routing. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

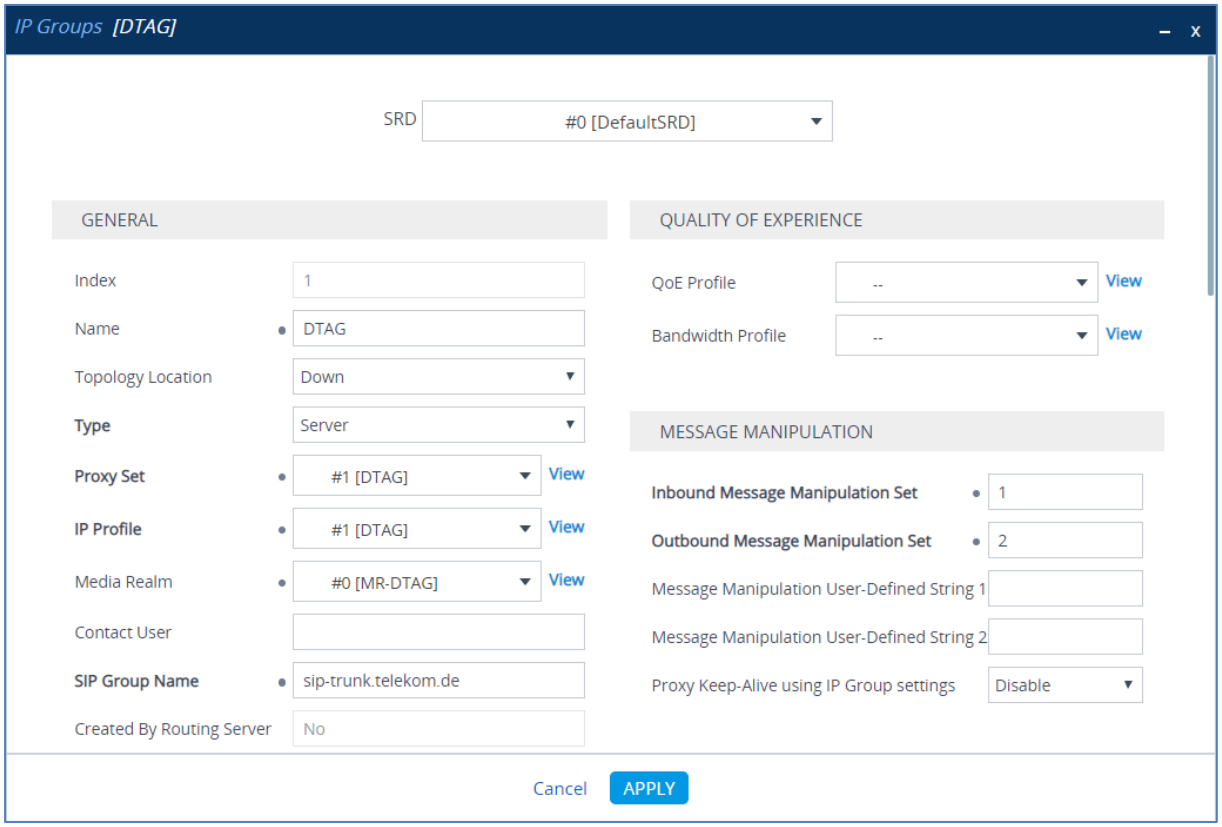
Rule Index	Rule Description	Reason for Introducing Rule
0	This rule applies to messages received from the Microsoft Teams IP Group in a Call Forward scenario. This rule adds an Action Value containing the reason for the History-Info header.	The reason in the History-Info header causes the E-SBC to add a Diversion Header towards the SIP Trunk.
1	This rule applies to messages received on the Teams SIP Interface. This saves the value of the user part of the SIP From Header into the new header, x-orig-A.	The new header, x-orig-A will be used in another message manipulation.
2	This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group. This removes Index 0 of the SIP P-Asserted-Identity Header, if it isn't containing numbers.	According to DTAG requirements.
3	This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group. This removes Index 1 of the SIP P-Asserted-Identity Header, if it doesn't contain numbers.	According to DTAG requirements.
4	This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group. This changes the type of the SIP P-Asserted-Identity Header to the sip-uri.	According to DTAG requirements.
5	This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group. This adds the SIP P-Early-Media Header with the value 'supported'.	According to DTAG requirements.
6	This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group. This replaces the host part of the SIP From Header with the value 'sip-trunk.telekom.de'.	According to DTAG requirements.

Rule Index	Rule Description	Reason for Introducing Rule
7	This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group. This replaces the user part of the SIP From Header with the saved value in the x-orig-A header.	
8	This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group. This removes the x-orig-A header.	This is a proprietary header, which was used temporarily.
9	This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group in a Call Forwarding scenario. This replaces the user part of the SIP From Header with the value from the SIP Diversion Header.	For Call Forward scenarios, DTAG's DLAN SIP Trunk requests from Microsoft Teams, the SIP Diversion header instead of the SIP History-Info header. The SBC mechanism for replacing the History-Info header with the Diversion header requires the reason header in the SIP History-Info header. However, Teams doesn't send the reason in the SIP History-Info header.
10	If the previous manipulation rule (Index 9) is executed, then the following rule is also executed on the same SIP message. This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group in a Call Forwarding scenario. This replaces the host part of the SIP Diversion Header with the value, configured in the SIP Trunk IP Group as Group Name.	
11	This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group in a Call Transfer scenario. This replaces the user part of the SIP From Header with the value from the SIP Referred-By Header.	For Call Transfer scenarios, DTAG's DLAN SIP Trunk requests that the user part of the SIP From Header will be populated with the DDI from the known range and that the host part of the SIP Referred-By header is pre-configured.
12	If the previous manipulation rule (Index 11) is executed, then the following rule is also executed on the same SIP message. This rule applies to messages sent to the DTAG's DLAN SIP Trunk IP Group in a Call Transfer scenario. This replaces the host part of the SIP Referred-By Header with the value, configured in the SIP Trunk IP Group as Group Name.	
13	This rule is applied to response messages sent to the DTAG's DLAN SIP Trunk IP Group for Rejected Calls initiated by the Teams Direct Routing IP Group. This replaces method types '480', '503' or '603' with the value '486'.	DTAG's DLAN SIP Trunk does not recognize these method types and continues to send INVITE messages.
14	This rule is applied to Re-INVITE messages sent to the Teams Direct Routing IP Group. This replaces the user part of the SIP Request-URI Header with the value from the SIP To Header.	According to DTAG requirements.
15	This rule is applied to all messages sent to the DTAG's DLAN SIP Trunk IP Group. This rule normalizes the SIP Contact Header of each message.	According to DTAG requirements.
16	This rule is applied to all messages sent to the DTAG's DLAN SIP Trunk IP Group. This rule normalizes the SDP body of each message.	According to DTAG requirements.
17	This rule is applied to Re-Invite messages sent to the Teams Direct Routing IP Group. This replaces the SDP RTP mode from 'recvonly' to 'inactive'.	Microsoft Teams do not support receive-only RTP mode and accept only inactive RTP mode.

Rule Index	Rule Description	Reason for Introducing Rule
18	This rule is applied to all messages sent to the DTAG's DLAN SIP Trunk IP Group. This rule removes the crypto line with '|2^31' from the SDP body of each message.	According to DTAG requirements.
19	This rule is applied to the messages sent to the Teams Direct Routing IP Group. This replaces the SDP RTP address from '0.0.0.0' by the address of the SBC.	Microsoft Teams do not support 0.0.0.0 as RTP address.
20	This rule is applied to the all responses sent to the Teams Direct Routing IP Group. This replaces the method type from the '100 Trying' to the '180 Ringing'.	According to DTAG requirements.
21	This rule applies to messages received from the Microsoft Teams IP Group. This rule removes the SIP Privacy Header from all messages, except those that don't contain 'anonymous' in the SIP From Header.	According to DTAG requirements.

24. Assign Manipulation Set ID 2 to the DTAG'S DLAN 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 DTAG's DLAN SIP Trunk IP Group, and then click **Edit**.
    c. Set the 'Outbound Message Manipulation Set' field to **2**.

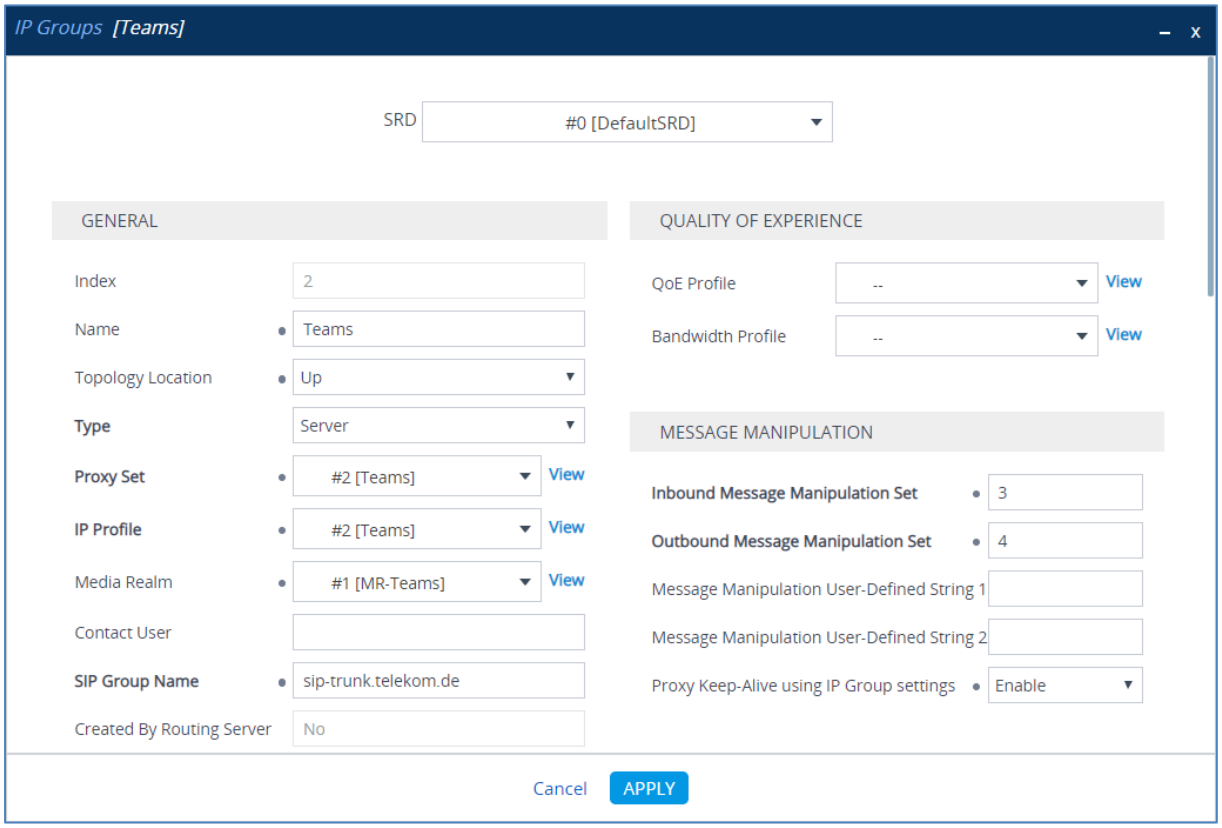
Figure 4-61: Assigning Manipulation Set to the DTAG's DLAN SIP Trunk IP Group



    d. Click **Apply**.

25. Assign Manipulation Set IDs 3 and 4 to 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 Teams Direct Routing IP Group, and then click **Edit**.
    c. Set the 'Inbound Message Manipulation Set' field to **3**.
    d. Set the 'Outbound Message Manipulation Set' field to **4**.

Figure 4-62: Assigning Manipulation Set to Teams Direct Routing IP Group



    e. Click **Apply**.

4.16 Configure Registration Accounts

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

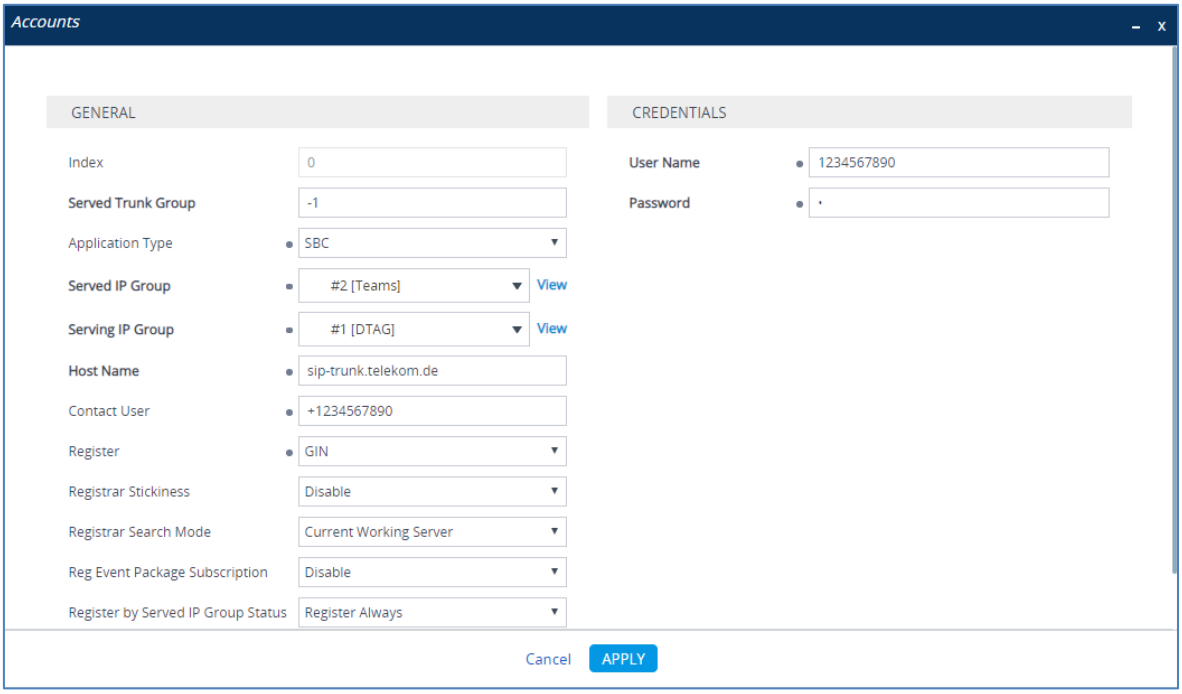
In the interoperability test topology, the Served IP Group is Teams Direct Routing IP Group and the Serving IP Group is DTAG's DLAN SIP Trunk IP Group.

➢ **To configure a registration account:**

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

Parameter	Value
Served IP Group	**Teams**
Application Type	**SBC**
Serving IP Group	**DTAG**
Host Name	As provided by the DTAG'S DLAN SIP Trunk provider
Register	**GIN**
Contact User	**+1234567890** (trunk main line)
Username	As provided by the DTAG'S DLAN SIP Trunk provider
Password	As provided by the DTAG'S DLAN SIP Trunk provider

Figure 4-63: Configuring a SIP Registration Account



4. Click **Apply**.

4.17 Configure Firewall Settings (Optional)

As an extra security, there is option to configure traffic filtering rules (*access list*) for incoming traffic on AudioCodes SBC. For each packet received on the configured network interface, the SBC searches the table from top to bottom until the first matching rule is found. The matched rule can permit (*allow*) or deny (*block*) the packet. Once a rule in the table is located, subsequent rules further down the table are ignored. If the end of the table is reached without a match, the packet is accepted. Please note that the firewall is stateless. The blocking rules will apply to all incoming packets, including UDP or TCP responses.

➢ **To configure a firewall rule:**

1. Open the Firewall table (**Setup** menu > **IP Network** tab > **Security** folder> **Firewall**).
2. Configure the following Access list rules for Teams Direct Rout IP Interface:

Table 4-1: Firewall Table Rules

Index	Source IP	Subnet Prefix	Start Port	End Port	Protocol	Use Specific Interface	Interface ID	Allow Type
0	<Public DNS Server IP> (e.g., 8.8.8.8)	32	0	65535	Any	Enable	WAN_IF	Allow
1	52.112.0.0	14	0	65535	TCP	Enable	WAN_IF	Allow
2	52.120.0.0	14	0	65535	TCP	Enable	WAN_IF	Allow
3	xxx.xxx.xxx.xxx	32	0	65535	UDP	Enable	WAN_IF	Allow
49	0.0.0.0	0	0	65535	Any	Enable	WAN_IF	Block

Note: Be aware, that if in your configuration, connectivity to the DTAG's DLAN SIP Trunk (or other entities) is performed through the same IP Interface as Teams (WAN_IF in our example), you must add rules to allow traffic from these entities. See an example above for index 3.

4.18 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

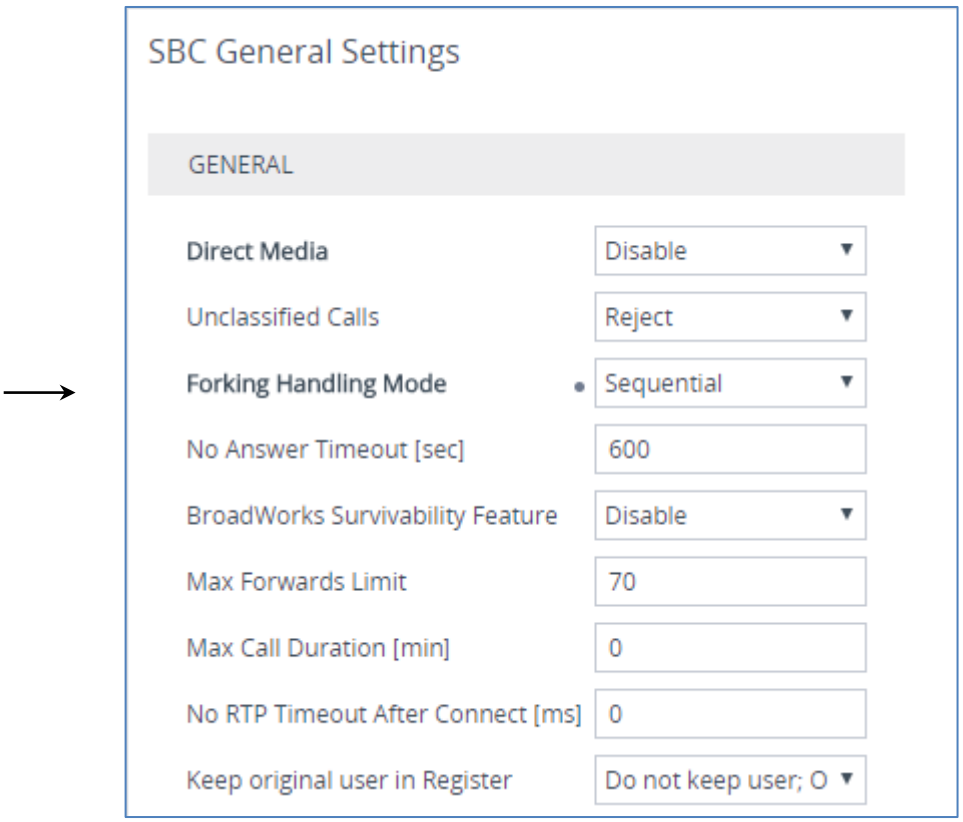
4.18.1 Configure Call Forking Mode

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

➢ **To configure call forking:**

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

Figure 4-64: Configuring Forking Mode



3. Click **Apply**.

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

This step 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.

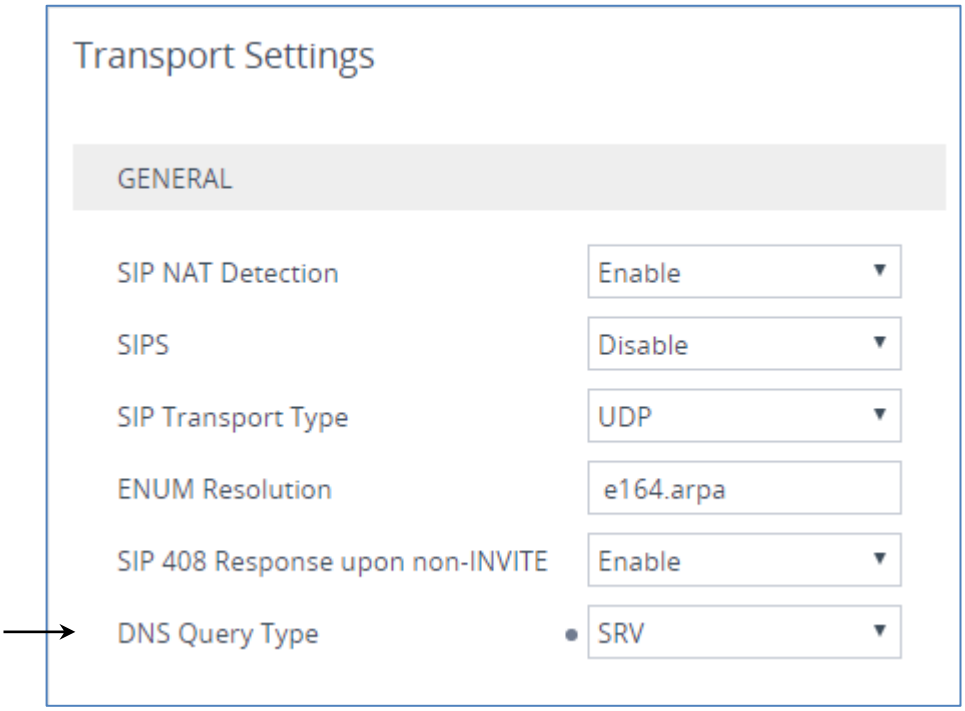
4.18.3 Configure DNS Query Type

This step describes how to configure the SBC's to enable the use of DNS Service Record (SRV) queries to resolve Proxy and Registrar servers and to resolve all domain names that appear in the SIP Contact and Record-Route headers. It is mandatory to set this field for the environment, when the DTAG'S DLAN SIP Trunk address is represented as an FQDN.

➢ **To configure DNS query type:**

1. Open the Transport Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Transport Settings**).
2. Under the General group, from the 'DNS Query Type' drop-down list, select **Enable.**

Figure 4-65: Configuring DNS Query Type



3. Click **Apply**.

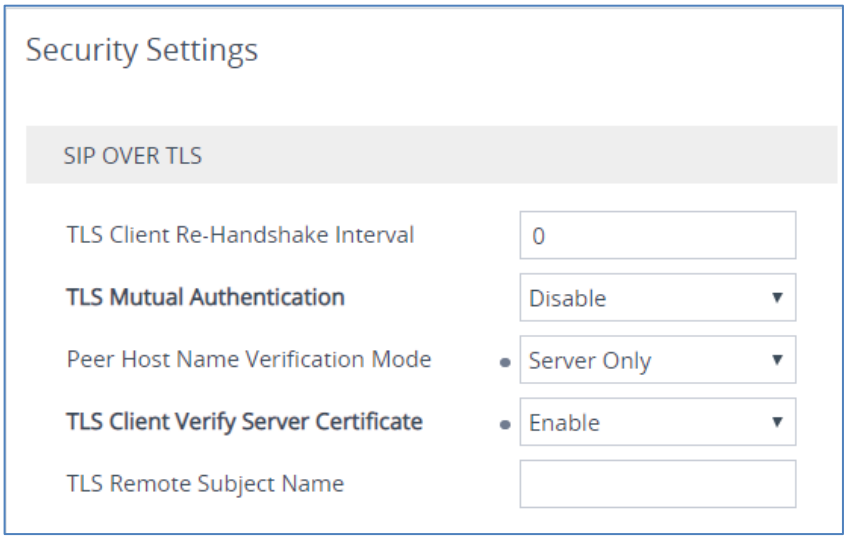
4.18.4 Configure SIP Over TLS parameters for DTAG'S DLAN Connectivity

Note: The following configuration steps are required **only** if connection to the DTAG'S DLAN SIP Trunk done using TLS.

➢ **To configure SIP over TLS parameters for DTAG'S DLAN Connectivity:**

1. Open the Security Settings page (**Setup** menu > **IP Network** tab > **Security** folder > **Security Settings**).
2. Under the SIP Over TLS group, from the 'Peer Host Name Verification Mode' drop-down list, select **Server Only.**
3. From the 'TLS Client Verify Server Certificate' drop-down list, select **Enable.**

Figure 4-66: Configuring SIP Over TLS Settings



4. Click **Apply**.

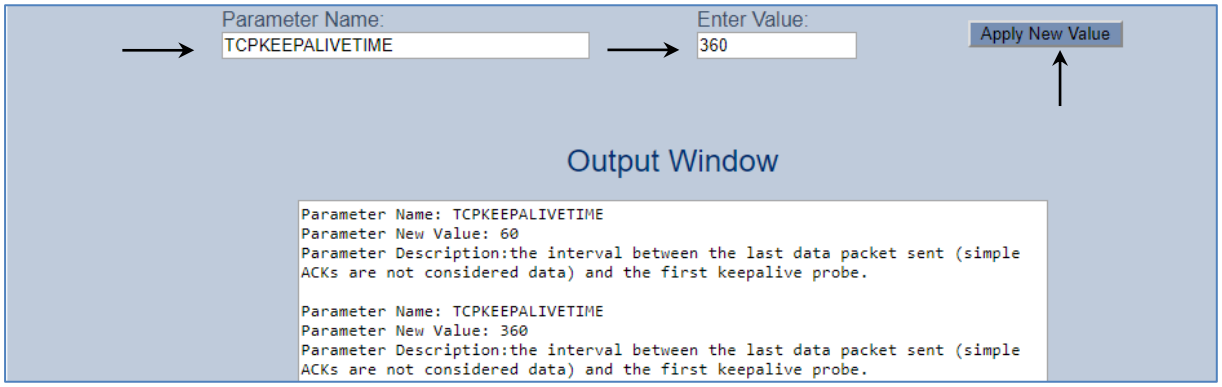
4.18.5 Configure TCP Keep Alive Parameters

This step describes how to configure the SBC's TCP Keep Alive parameters.

➢ **To configure TCP Keep Alive parameters:**

1. Open the Admin page: Append the case-sensitive suffix 'AdminPage' to the device's IP address in your Web browser's URL field (e.g., http://10.15.17.10/AdminPage).
2. In the left pane of the page that opens, click ***ini* Parameters**.

Figure 4-67: Configure TCP keep alive parameters in AdminPage



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

Parameter	Value
TCPKEEPALIVETIME	**360**
TCPKEEPALIVEINTERVAL	**15**
TCPKEEPALIVERETRY	**10**

4. Click the **Apply New Value** button for each field.

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: M500L
;HW Board Type: 69 FK Board Type: 84
;Serial Number: 5961508
;Slot Number: 1
;Software Version: 7.20A.252.062
;DSP Software Version: 5011AE3_R => 710.16
;Ram size: 512M   Flash size: 128M   Core speed: 300Mhz
;Num of DSP Cores: 1
;Num of physical LAN ports: 4
;Profile: NONE
;;;Key features:;Board Type: M500L ;Coders: G723 G729 GSM-FR G727
G722 ;IP Media: VXML ;DATA features: Routing FireWall&VPN WAN BGP
Advanced-Routing Shdsl-Pairs=2 FTTX-WAN ;PSTN Protocols: ISDN
IUA=1 CAS ;DSP Voice features: IpmDetector ;Channel Type: RTP
DspCh=60 ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;E1Trunks=1 ;T1Trunks=1 ;Control Protocols:
MSFT FEU=50 TestCall=5 SIP SBC=10 ;Default features:;Coders: G711
G726;

;-----  HW components -----
;
; Slot # : Module type : # of ports
;----------------------------------------------
;      2 : BRI         : 2
;----------------------------------------------

[SYSTEM Params]

SyslogServerIP = 10.10.10.10
EnableSyslog = 1
NTPServerUTCOffset = 7200
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
AllowWanHttp = 1
AllowWanSSH = 1
NTPServerIP = '0.0.0.0'
SBCWizardFilename = 'templates4.zip'
```

```
[BSP Params]

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

[Analog Params]


[ControlProtocols Params]


[PSTN Params]

V5ProtocolSide = 0

[Voice Engine Params]

FaxBypassPayloadType = 106
ENABLEMEDIASECURITY = 1
PLThresholdLevelsPerMille_0 = 5
PLThresholdLevelsPerMille_1 = 10
PLThresholdLevelsPerMille_2 = 20
PLThresholdLevelsPerMille_3 = 50


[SIP Params]

REGISTRATIONTIME = 360
DISCONNECTONBROKENCONNECTION = 0
PEERHOSTNAMEVERIFICATIONMODE = 1
MEDIASECURITYBEHAVIOUR = 1
GWDEBUGLEVEL = 5
DNSQUERYTYPE = 1
VERIFYSERVERCERTIFICATE = 1
RELIABLECONNECTIONPERSISTENTMODE = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCESMODE = 1
SBCFORKINGHANDLINGMODE = 1
TCPKEEPALIVETIME = 360
TCPKEEPALIVEINTERVAL = 15
TCPKEEPALIVERETRY = 10
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[SNMP Params]


[ 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, 10.15.77.77, 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",
"$1$U2QxbTU2PTpsbm5sbDpQVgAAVlxfXwsMDlMKCwoOFURESkJAREBNT05IT0RHR+
Sxt7bh5OTmsLzs7r216u6joqM=", 1, 0, 5, -1, 15, 60, 200,
"b8abfb918d88d9cf0050dd777cbefcd5", "";
WebUsers 1 = "User",
"$1$o5GRnMLEyZ+Ym5+fn87SiYSDgYLQj93cg4uIidyK9qX2p/ynp6bw+P/6r/Wv97
Pgt7Ls4+7kuuy57ejovOvS1tE=", 1, 0, 5, -1, 15, 60, 50,
"49da902a7b5c3e75fdcb7cee659196fb", "";

[ \WebUsers ]


[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name,
TLSContexts_TLSVersion, TLSContexts_DTLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_RequireStrictCert, TLSContexts_OcspEnable,
TLSContexts_OcspServerPrimary, TLSContexts_OcspServerSecondary,
TLSContexts_OcspServerPort, TLSContexts_OcspDefaultResponse,
TLSContexts_DHKeySize;
TLSContexts 0 = "default", 4, 0,
"ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:+HIGH:+MEDIUM",
"ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:+HIGH:+MEDIUM", 1, 0, 0.0.0.0,
0.0.0.0, 2560, 0, 1024;
TLSContexts 1 = "Teams", 4, 0,
"ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:+HIGH:+MEDIUM",
"ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:+HIGH:+MEDIUM", 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 = "DTAG 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 = "DTAG", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 48,
0, 0, 2, 0, 0, 0, 0, -1, 1, 0, 1, -1, 1, 4, -1, 1, 1, 0, 0, "",
"", 0, 0, "", "DTAG Allowed Coders", "", 0, 1, 0, 0, 0, 0, 0, 8,
300, 400, 1, 2, 0, "", 2, 0, 1, 3, 0, 2, 2, 1, 3, 0, 0, 2, 1, 0,
0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 2, 2, 1, 1,
0, 0, 300, -1, -1, 2, 1, 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,
48, 0, 0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0,
"", "AudioCodersGroups_1", 0, 0, "", "", "", 2, 1, 1, 0, 0, 0, 0,
8, 300, 400, 2, 0, 0, "", 0, 0, 1, 1, 0, 1, 1, 0, 3, 2, 1, 0, 1,
0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 3, 0, 0, 0, 0, 0, 0,
0, 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-DTAG", "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, 1, "";

[ \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 = "DTAG", "WAN_IF", 2, 0, 5060, 0, , 0,
"DefaultSRD", , "default", -1, 0, 500, -1, 0, "MR-DTAG", 0, -1, -
1, -1, 0, 0, , , -1;
SIPInterface 1 = "Teams", "WAN_IF", 2, 0, 0, 5061, , 0,
"DefaultSRD", , "Teams", -1, 1, 0, 0, 0, "MR-Teams", 0, -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, "", "", "DTAG", "", "", 1, 1, 10, -1;
ProxySet 1 = "DTAG", 0, 60, 0, 1, "DefaultSRD", 0, "", 1, 1, "",
"", "DTAG", "", "", 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_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, "", 0, -1, -1, "", "",
"$1$gQ==", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0,
0, "", -1, "", 0, 0, "", 0;
IPGroup 1 = 0, "DTAG", "DTAG", "sip-trunk.telekom.de", "", -1, 0,
"DefaultSRD", "MR-DTAG", 1, "DTAG", -1, 1, 2, 0, 0, "", 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", "sip-trunk.telekom.de", "", -1,
0, "DefaultSRD", "MR-Teams", 0, "Teams", -1, 3, 4, 0, 0, "", 0, -
1, -1, "int-sbc2.audctrunk.aceducation.info", "Admin",
"$1$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "Teams", 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, "reg.sip-trunk.telekom.de", 2, 0, 0;
ProxyIp 1 = "2", 0, "sip.pstnhub.microsoft.com:5061", 2, 1, 1;
ProxyIp 2 = "2", 1, "sip2.pstnhub.microsoft.com:5061", 2, 2, 1;
ProxyIp 3 = "2", 2, "sip3.pstnhub.microsoft.com:5061", 2, 3, 1;

[ \ProxyIp ]


[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroupName, Account_ServingIPGroupName,
Account_Username, Account_Password, Account_HostName,
Account_ContactUser, Account_Register,
Account_RegistrarStickiness, Account_RegistrarSearchMode,
Account_RegEventPackageSubscription, Account_ApplicationType,
Account_RegByServedIPG, Account_UDPPortAssignment;
Account 0 = -1, "Teams", "DTAG", "1234567890", "password", "sip-
trunk.telekom.de", "+1234567890", 2, 0, 0, 0, 2, 0, 0;
```

```
[ \Account ]


[ ConditionTable ]

FORMAT ConditionTable_Index = ConditionTable_Name,
ConditionTable_Condition;
ConditionTable 0 = "Teams-Contact", "Header.Contact.URL.Host
contains 'pstnhub.microsoft.com'";

[ \ConditionTable ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_RoutingPolicyName, IP2IPRouting_SrcIPGroupName,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageConditionName,
IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger,
IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType,
IP2IPRouting_DestIPGroupName, IP2IPRouting_DestSIPInterfaceName,
IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup,
IP2IPRouting_DestTags, IP2IPRouting_SrcTags,
IP2IPRouting_IPGroupSetName, IP2IPRouting_RoutingTagName,
IP2IPRouting_InternalAction;
IP2IPRouting 0 = "Terminate OPTIONS", "Default_SBCRoutingPolicy",
"Any", "*", "*", "*", "*", 6, "", "Any", 0, -1, 1, "", "",
"internal", 0, -1, 0, 0, "", "", "", "", "default", "";
IP2IPRouting 1 = "Refer from Teams", "Default_SBCRoutingPolicy",
"Any", "*", "*", "*", "*", 0, "", "Teams", 2, -1, 2, "Teams", "",
"", 0, -1, 0, 0, "", "", "", "", "default", "";
IP2IPRouting 2 = "Teams to DTAG", "Default_SBCRoutingPolicy",
"Teams", "*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "DTAG", "",
"", 0, -1, 0, 0, "", "", "", "", "default", "";
IP2IPRouting 3 = "DTAG to Teams", "Default_SBCRoutingPolicy",
"DTAG", "*", "*", "*", "*", 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.*.*.*", 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 = "NormPreSelect",
"Default_SBCRoutingPolicy", 0, "Any", "Any", "*", "*", "+4910xx",
"*", "*", "", 0, "Any", 0, 1, 3, 0, 255, "0", "", 0, "", "";
IPOutboundManipulation 1 = "NrmNotrufUndService",
"Default_SBCRoutingPolicy", 0, "Any", "Any", "*", "*", "+4911x",
"*", "*", "", 0, "Any", 0, 1, 3, 0, 255, "", "", 3, "", "";

[ \IPOutboundManipulation ]


[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName,
MessageManipulations_ManSetID, MessageManipulations_MessageType,
MessageManipulations_Condition,
MessageManipulations_ActionSubject,
MessageManipulations_ActionType, MessageManipulations_ActionValue,
MessageManipulations_RowRole;
MessageManipulations 0 = "Add Cause to History-Info", 3,
"Invite.Request", "header.history-info.1 regex
(<.*)(user=phone)(>)(.*)", "Header.History-Info.1", 2,
"$1+$2+'?Reason=SIP%3Bcause%3D302'+$3+$4", 0;
```

```
MessageManipulations 1 = "save original calling", 0,
"Invite.Request", "header.history-info exists", "header.x-orig-A",
0, "header.from.url.user", 0;
MessageManipulations 2 = "check if first PAI is a number", 2,
"Any.request", "header.p-asserted-identity.0 !contains '+49'",
"header.p-asserted-identity.0", 1, "", 0;
MessageManipulations 3 = "check if 2nd PAI is a number", 2,
"Any.request", "header.p-asserted-identity.1 !contains '+49'",
"header.p-asserted-identity.1", 1, "", 0;
MessageManipulations 4 = "rewrite PAI a sip-uri", 2,
"Any.request", "header.p-asserted-identity.URL.Type == '2'",
"header.p-asserted-identity.url", 2, "'sip:'+header.p-asserted-
identity.url.user+'@sip-trunk.telekom.de'", 0;
MessageManipulations 5 = "Add P-Early-Media", 2, "Any.request",
"", "header.P-Early-Media", 2, "'supported'", 0;
MessageManipulations 6 = "from trunk domain", 2, "any.request",
"", "header.from.url.host", 2, "'sip-trunk.telekom.de'", 0;
MessageManipulations 7 = "restore original calling", 2, "invite",
"header.x-orig-A exists", "header.from.url.user", 2, "header.x-
orig-A", 0;
MessageManipulations 8 = "remove x-orig-A", 2, "", "", "header.x-
orig-A", 1, "", 0;
MessageManipulations 9 = "Call Forward", 2, "Invite",
"Header.Diversion exists", "Header.From.URL.User", 2,
"Header.Diversion.URL.User", 0;
MessageManipulations 10 = "Call Forward", 2, "", "",
"Header.Diversion.URL.Host", 2, "Param.IPG.Dst.Host", 1;
MessageManipulations 11 = "Call Transfer", 2, "Invite",
"Header.Referred-By exists", "Header.P-Asserted-Identity", 0,
"'<sip:'+header.referred-by.url.user+'@sip-trunk.telekom.de>'", 0;
MessageManipulations 12 = "Call Transfer", 2, "", "",
"Header.Referred-By.Url.Host", 2, "Param.IPG.Dst.Host", 1;
MessageManipulations 13 = "Reject Cause", 2, "Any.Response",
"Header.Request-Uri.MethodType == '480' OR Header.Request-
Uri.MethodType =='503'  OR Header.Request-Uri.MethodType =='603'",
"Header.Request-Uri.MethodType", 2, "'486'", 0;
MessageManipulations 14 = "Change R-URI User", 4,
"Reinvite.Request", "", "Header.Request-URI.URL.User", 2,
"Header.To.URL.User", 0;
MessageManipulations 15 = "Normalize Contact", 2, "Any.Request",
"", "Header.Contact.URL", 7, "", 0;
MessageManipulations 16 = "Normalize SDP", 2, "Any.Request",
"Body.sdp exists", "Body.sdp", 7, "", 0;
MessageManipulations 17 = "Change RecvOnly to Inactive", 4,
"Reinvite.Request", "Param.Message.SDP.RTPMode == 'recvonly'",
"Param.Message.SDP.RTPMode", 2, "'inactive'", 0;
MessageManipulations 18 = "removeCrypto18x", 2, "any.response",
"Body.sdp regex '(.*)(\|2\^31)(.*)'", "body.sdp", 2, "$1+$3", 0;
MessageManipulations 19 = "no c with zeroes to teams", 4, "any",
"Body.sdp regex '(.*)(c=IN IP4 0.0.0.0)(.*)'", "body.sdp", 2,
"$1+'c=IN IP4 '+param.Message.SDP.OriginAddress+$3", 0;
MessageManipulations 20 = "try ringing", 4, "Invite.Response.100",
"", "Header.Request-URI.MethodType", 2, "'180'", 0;
MessageManipulations 21 = "remPrivWhenNotAnon", 3, "Any.request",
"header.from.url !contains 'anonymous'", "header.privacy", 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 = "DTAG 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, 1, 2, 90, -1, 0, "";
AudioCoders 1 = "AudioCodersGroups_1", 0, 35, 2, 19, 103, 0, "";
AudioCoders 2 = "AudioCodersGroups_1", 1, 36, 2, 43, 104, 0, "";
AudioCoders 3 = "AudioCodersGroups_1", 2, 1, 2, 90, -1, 0, "";
AudioCoders 4 = "AudioCodersGroups_1", 3, 2, 2, 90, -1, 0, "";
AudioCoders 5 = "AudioCodersGroups_1", 4, 3, 2, 19, -1, 0, "";

[ \AudioCoders ]


[ DiffServToVlanPriority ]

FORMAT DiffServToVlanPriority_Index =
DiffServToVlanPriority_DiffServ,
DiffServToVlanPriority_VlanPriority;
DiffServToVlanPriority 0 = 46, 6;
DiffServToVlanPriority 1 = 48, 6;
DiffServToVlanPriority 2 = 26, 4;
DiffServToVlanPriority 3 = 10, 2;

[ \DiffServToVlanPriority ]
```

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-12598