Amazon Chime Voice Connector

SIP Trunking Configuration Guide:

Microsoft Teams Direct Routing and AudioCodes Mediant Cloud Edition

November 2019

Document History

Rev. No.	Date	Description
1.0	Nov-26-2019	SIP Trunk Configuration Guide

Table of Contents

Table of Figures

1 Audience

This document is intended for technical staff and Value Added Resellers (VAR) with installation and operational responsibilities. This configuration guide provides steps for configuring SIP trunks using **Microsoft Teams Direct Routing (MS Teams)** and

AudioCodes Mediant Cloud Edition (AudioCodes CE) to connect to **Amazon Chime Voice Connector** for inbound and/or outbound telephony capabilities.

1.1 Amazon Chime Voice Connector

Amazon Chime Voice Connector is a pay-as-you-go service that enables companies to make or receive secure phone calls over the internet or AWS Direct Connect using their existing telephone system or session border controller (SBC). The service has no upfront fees, elastically scales based on demand, supports calling both landline and mobile phone numbers in over 100 countries, and gives customers the option to enable inbound calling, outbound calling, or both.

Amazon Chime Voice Connector uses the industry-standard Session Initiation Protocol (SIP). Amazon Chime Voice Connector does not require dedicated data circuits. A company can use their existing Internet connection or AWS Direct Connect public virtual interface for SIP connectivity to AWS. Voice connectors can be configured in minutes using the AWS Management Console or Amazon Chime API. Amazon Chime Voice Connector offers cost-effective rates for inbound and outbound calls. Calls into Amazon Chime meetings, as well as calls to other Amazon Chime Voice Connector customers are at no additional cost. With Amazon Chime Voice Connector, companies can reduce their voice calling costs without having to replace their on-premises phone system.

2 SIP Trunking Network Components

The network for the SIP trunk reference configuration is illustrated below and is representative of Microsoft Teams Direct Routing and AudioCodes CE configuration.

OnPrem IP PBX is used as a secondary PBX in the topology to perform call failover and call distribution

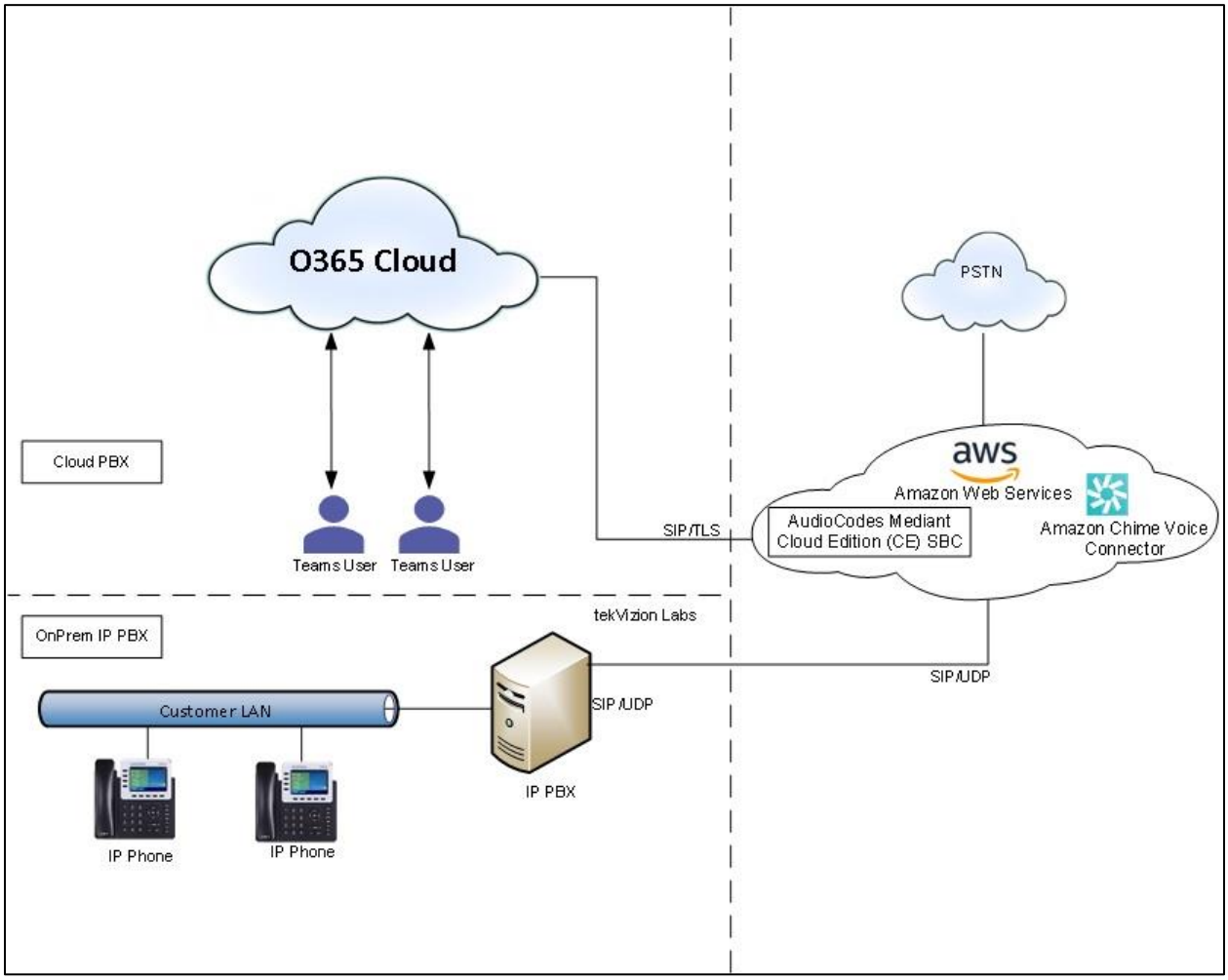

Figure 1: Network Topology

2.1 Hardware Components

- AudioCodes CE running on Amazon Web Service

2.2 Software Requirements

- AudioCodes Mediant Cloud Edition: 7.20A.252.274
- Microsoft Office365 tenant with Required license: E5
- Microsoft Teams Client: 1.2.00.31357

3 Features

3.1 Features Supported

- Calls to and from non-Toll Free number
- Calls to Toll Free number
- Calls to Premium Telephone number
- Calling Party Number Presentation
- Calling Party Number Restriction
- Inbound Calls to an IVR
- International Calls
- Call Authentication
- Anonymous call
- DTMF-RFC 2833
- Long duration calls
- Calls to conference scheduled by Amazon Chime user
- Calls to Amazon Chime Business number
- Call Distribution
- Call Failover

3.2 Features Not Supported

Amazon Chime Voice Connector does not support following features

- Keep Alive SIP OPTIONS
- Keep Alive – Double CRLF

3.3 Features Not Tested

- None

3.4 Caveats and Limitations

- Amazon Chime Voice Connector,
  - does not support SIP NOTIFY or SIP INFO for DTMF
  - does not send SIP session refresher for long duration calls
- When the WAN link is down and a call is in progress, the PSTN call leg is not disconnected automatically after a period of inactivity. The call has to be cleared manually.

4 Configuration

4.1 Configuration Checklist

In this section we present an overview of the steps that are required to configure **MS Teams** and **AudioCodes CE** for SIP Trunking with **Amazon Chime Voice Connector.**

Table 1 – PBX Configuration Steps

Steps	Description	Reference
Step 1	Microsoft Teams Configuration	Section 4.2
Step 2	AudioCodes CE Configuration	Section 4.3

4.2 Microsoft Teams Configuration

This section with screen shots taken from MS Teams used for the interoperability testing, gives a general overview of the PBX configuration. Connect to Microsoft Office365 using Remote PowerShell.

4.2.1 Create Online PSTN Gateway

To pair the SBC with the tenant, use the below command.

```
New-CsOnlinePSTNGateway -Fqdn <SBC FQDN> -SipSignallingPort <SBC SIP Port> -ForwardCallHistory $true –ForwardPai $true -MaxConcurrentSessions <Max Concurrent Sessions the SBC can handle> -Enabled $true
```

After creating Online PSTN Gateway use "Get-CsOnlinePSTNGateway' command to view the online pstn gateway created. Example is shown below.

```
PS C:\Windows\system32> Get-CsOnlinePSTNGateway -Identity sbc

Identity                              : sbc
InboundTeamsNumberTranslationRules    : {}
InboundPstnNumberTranslationRules     : {}
OutboundTeamsNumberTranslationRules   : {}
OutboundPstnNumberTranslationRules    : {}
Fqdn                                  : sbc
SipSignallingPort                     : 5061
FailoverTimeSeconds                   : 10
ForwardCallHistory                    : True
ForwardPai                            : True
SendSipOptions                        : True
MaxConcurrentSessions                 : 100
Enabled                               : True
MediaBypass                           : False
GatewaySiteId                         :
GatewaySiteLbrEnabled                 : False
FailoverResponseCodes                 : 408,503,504
GenerateRingingWhileLocatingUser      : True
PidfLoSupported                       : False
MediaRelayRoutingLocationOverride     :
ProxySbc                              :
BypassMode                            : None
```

Figure 2: Microsoft Teams-OnlinePSTNGateway

MediaBypass is disabled in MS Teams.

4.2.2 Configure Online PSTN Usage

To add a new PSTN Usage, use the below command

```
Set-CsOnlinePstnUsage -identity Global -Usage @{Add="<usage name>"}
```

After creating Online PSTN Usage, use the command" (Get-CsOnlinePstnUsage).usage" to view the online pstn usage created. Example is shown below.

```
PS C:\Windows\system32> (Get-CsOnlinePstnUsage).usage
US and Canada
Test
```

Figure 3: Microsoft Teams-Online PSTN Usage

4.2.3 Configure Online Voice Route

To add a new Online Voice Route, use the below command.

```
New-CsOnlineVoiceRoute -Identity "<Route name>" -NumberPattern ".*" -OnlinePstnGatewayList "<SBCFQDN>" -Priority 1 -OnlinePstnUsages "<PSTN usage name>"}
```

After creating online voice route use "Get-CsOnlineVoiceRoute" command to view the online voice route created. Example is shown below

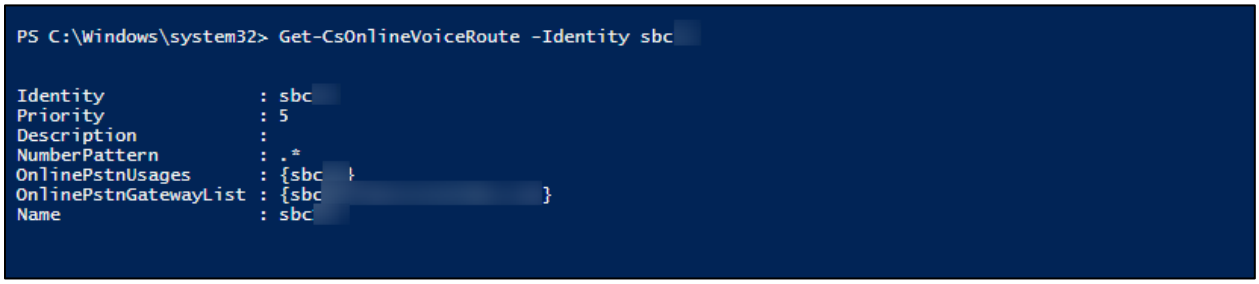

Figure 4: Microsoft Teams-Online Voice Route

4.2.4 Configure Online Voice Routing Policy

To create a new Online Voice Routing Policy, use the below command.

```
New-CsOnlineVoiceRoutingPolicy "<policy name>" -OnlinePstnUsages "<pstn usage name>"
```

After creating online voice routing policy, use "Get-CsOnlineVoiceRoutingPolicy" command to view the online voice routing policy created. Example is shown below.

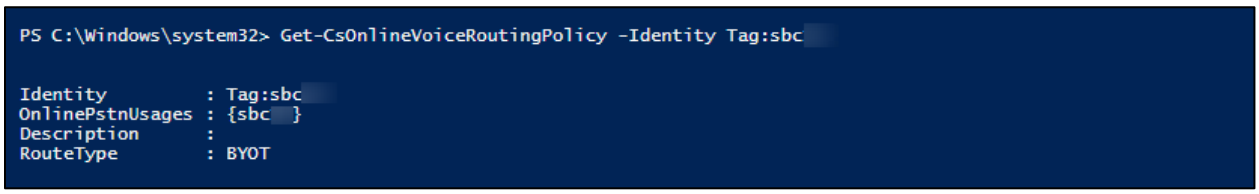

Figure 5: Microsoft Teams-Online Voice Routing Policy

4.2.5 Teams User Configuration

Set the DID to the Teams user using the below command.

```
Set-CsUser -Identity "<User name>" -EnterpriseVoiceEnabled $true -HostedVoiceMail $true -OnPremLineURI <E1.164 phone number with tel: prefixed>
```

Associate Teams user with online voice routing policy using the below command.

```
Grant-CsOnlineVoiceRoutingPolicy -Identity "<User name>" -PolicyName "<policy name>"
```

4.3 AudioCodes CE Configuration

The AudioCodes CE is configured with one trunk pointing to MS Teams Direct Routing and another trunk pointing to Amazon Chime Voice Connector. The steps involved in configuring the IP and Trunks are shown below

4.3.1 Network IP Interface configuration

Navigate to '*SETUP*', '*IP NETWORK'* and expand '*CORE ENTITIES'*. Click '*IP Interfaces*' and the below figure shows the interfaces that are been used.

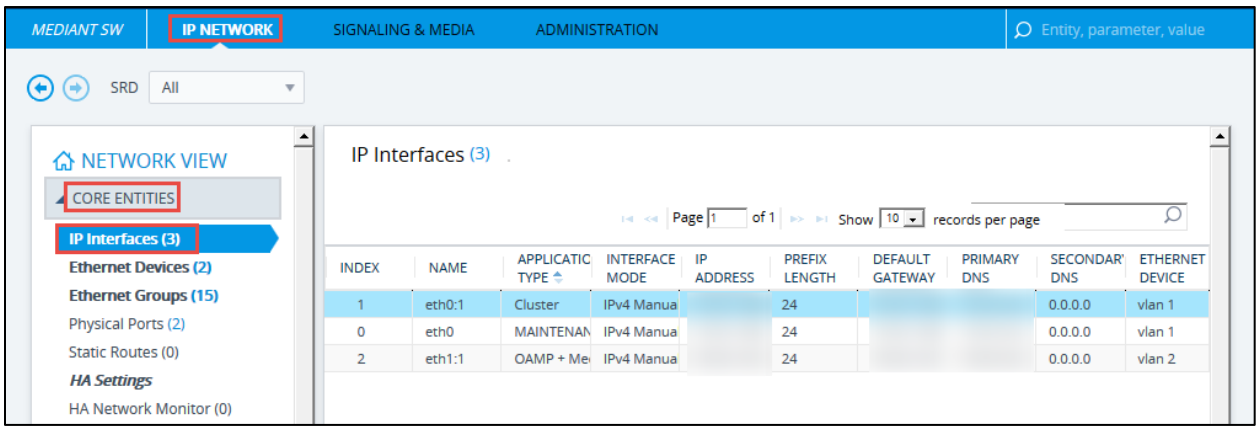

Figure 6: IP Interfaces

4.3.2 Media Realm configuration

Two media realms are created, one is associated to MS Teams and another is associated with Amazon Chime Voice Connector. To configure media realm, navigate to '*SETUP* 'and select '*SIGNALING & MEDIA'*. Expand '*CORE ENTITIES'* and select '*Media Realms'*.

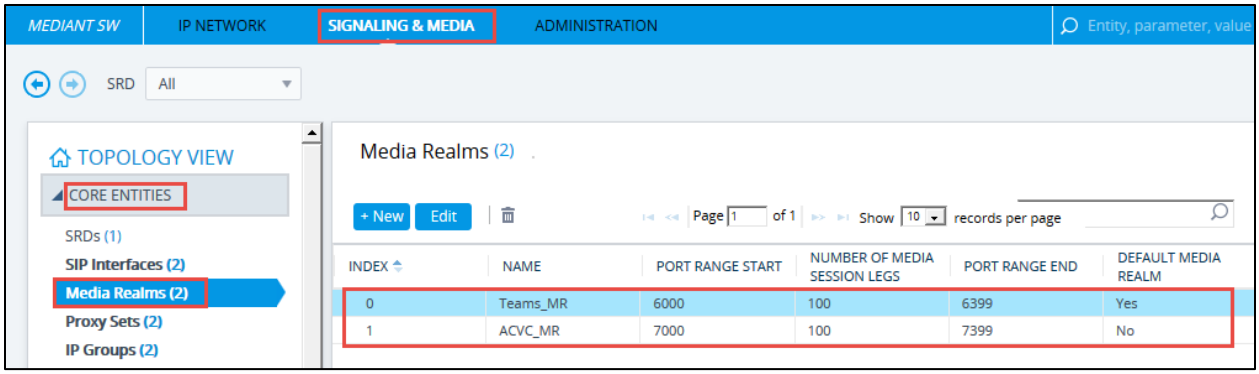

Figure 7: Media Realms Table

Enter the name of the Media Realm, *Port Range Start* value and *Number of Media Session* Legs. Select the appropriate IPv4 Interface Name for MS Teams.

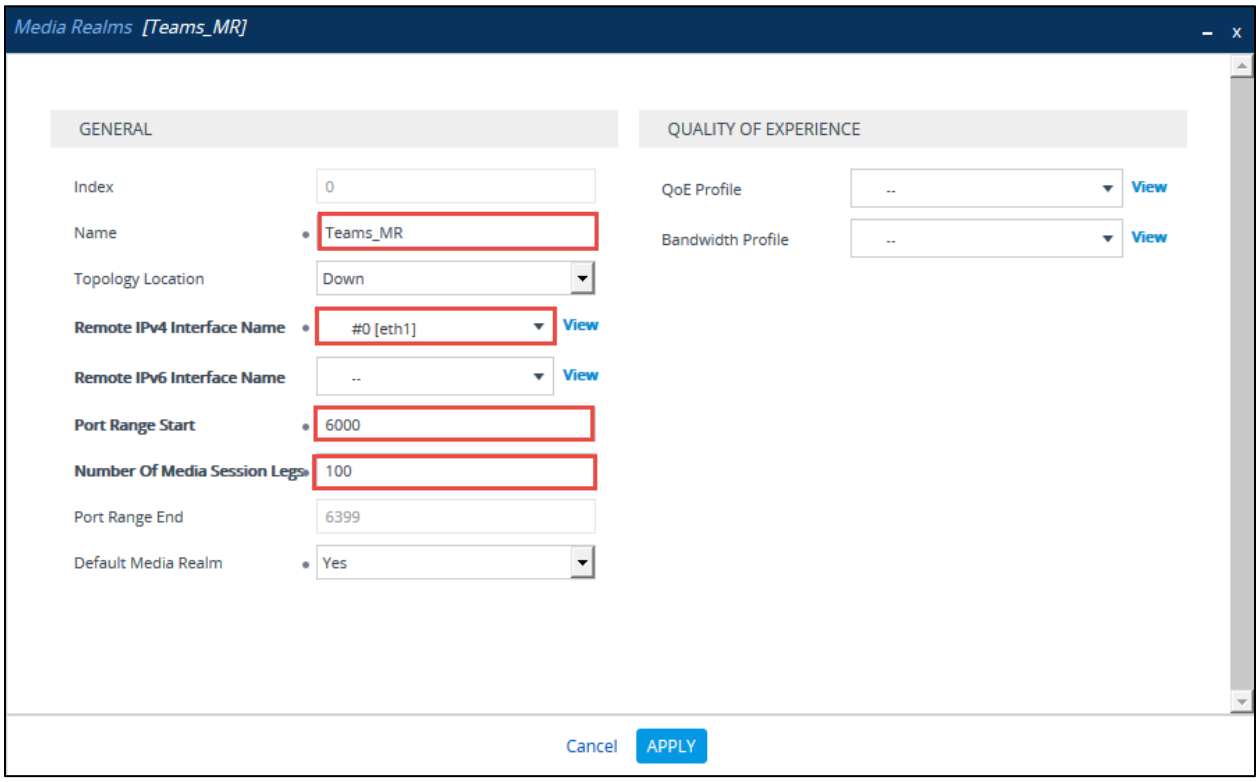

Figure 8: Media Realm for MS Teams

Enter the name of the Media Realm, *Port Range Start* value and *Number of Media Session* Legs. Select the appropriate IPv4 Interface Name for Amazon Chime Voice Connector.

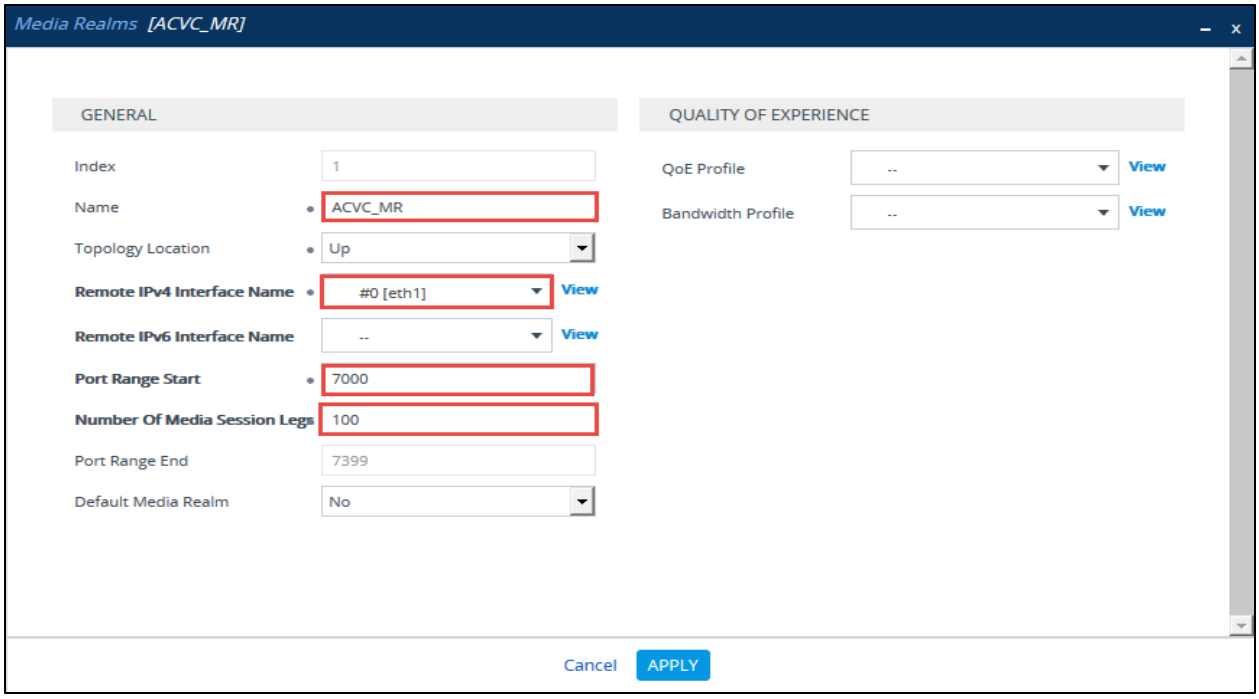

Figure 9: Media Realm for Amazon Chime Voice Connector

4.3.3 SRD configuration

To configure SRD, navigate to '*SETUP*' and select '*SIGNALING & MEDIA*'. Expand '*CORE ENTITIES*' and select *SRDs*.

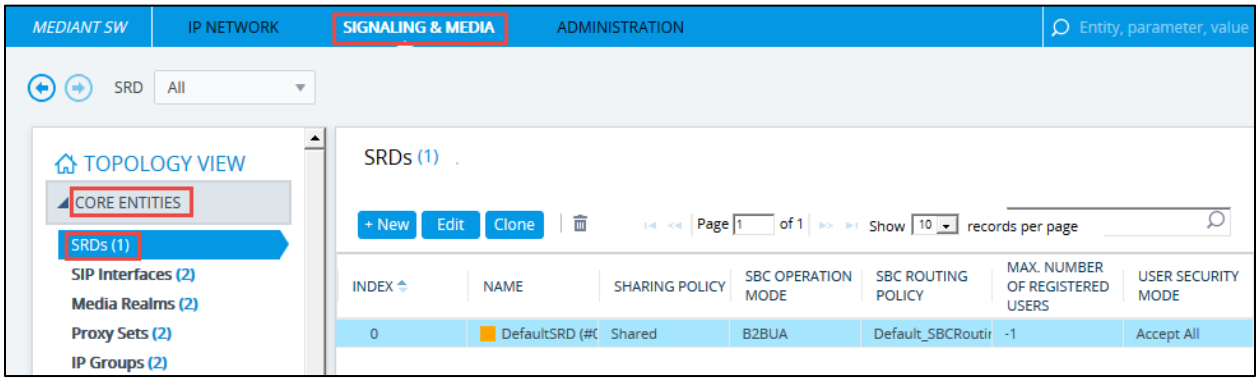

Figure 10: Default SRD

The default SRD configuration is used.

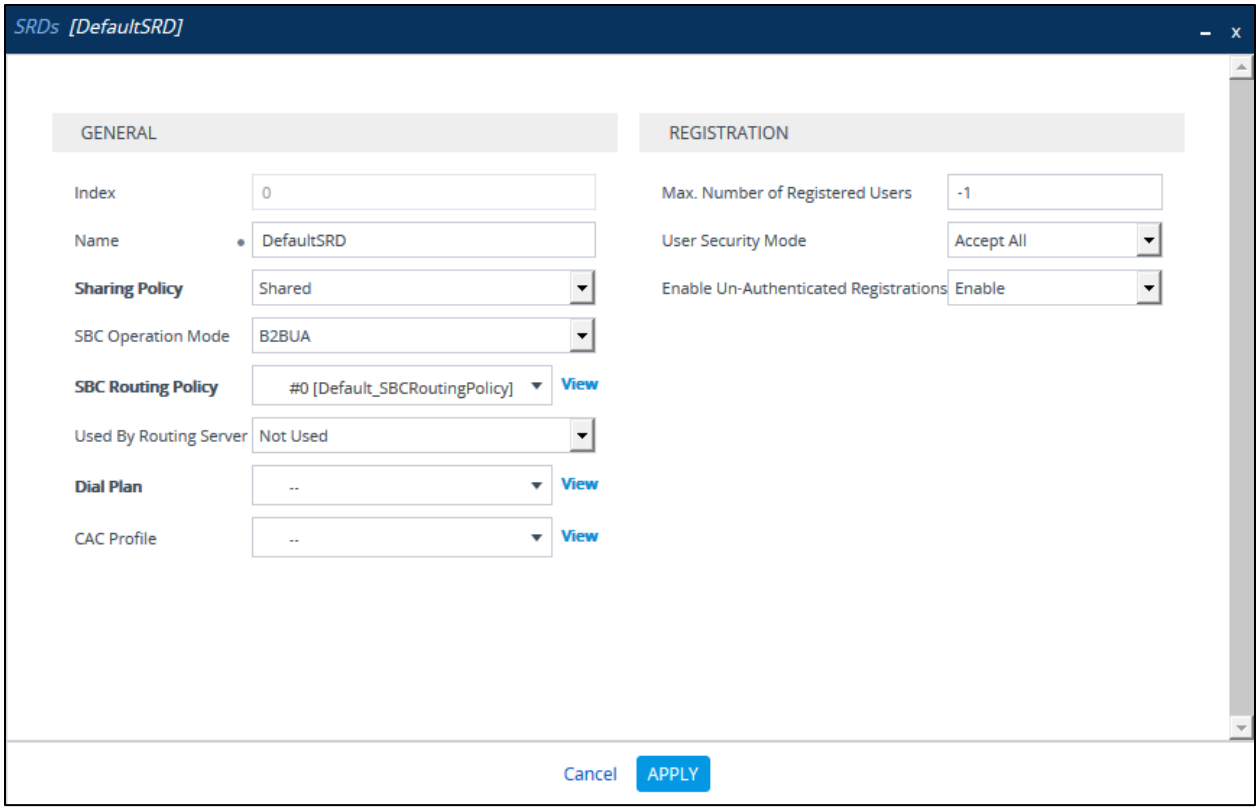

Figure 11: SRD Table Details

4.3.4 SIP Interface configuration

Navigate to '*SETUP*' and select '*SIGNALING & MEDIA*'. Expand '*CORE ENTITIES*' and select '*Sip Interfaces'*. Two SIP Interfaces are created, one is for MS Teams and the other is for Amazon Chime Voice Connector.

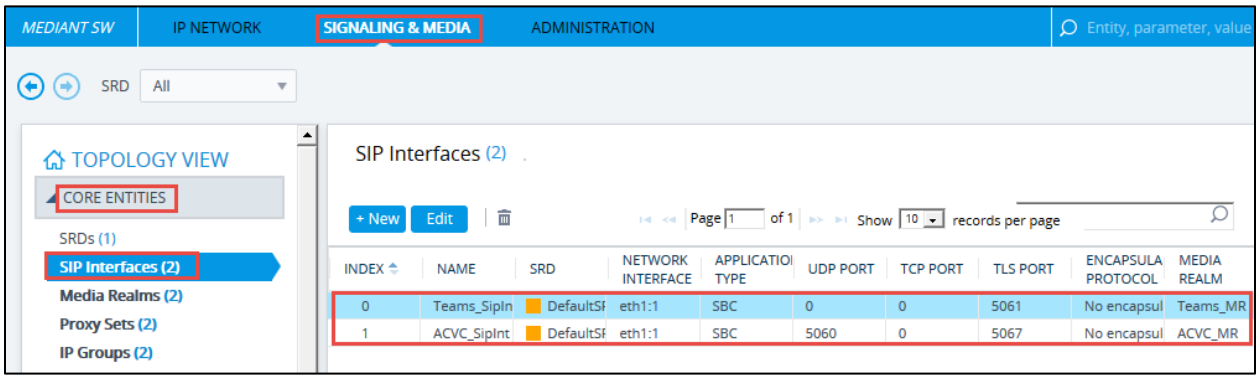

Figure 12: SIP Interfaces

Network Interface, Media Realm, SRD, TLS Context Name, TLS Mutual Authentication and *Port numbers* are associated to MS Teams SIP Interface and the remaining parameters are set to default.

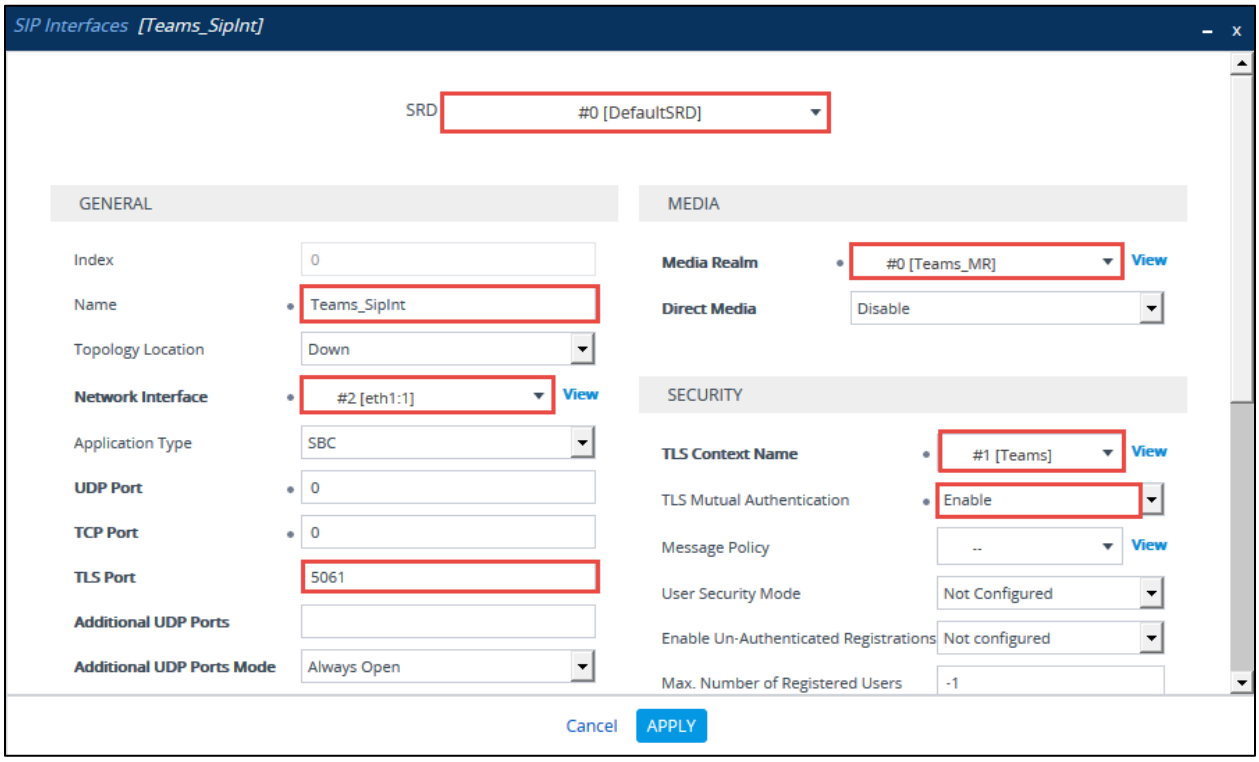

Figure 13: SIP Interface for MS Teams

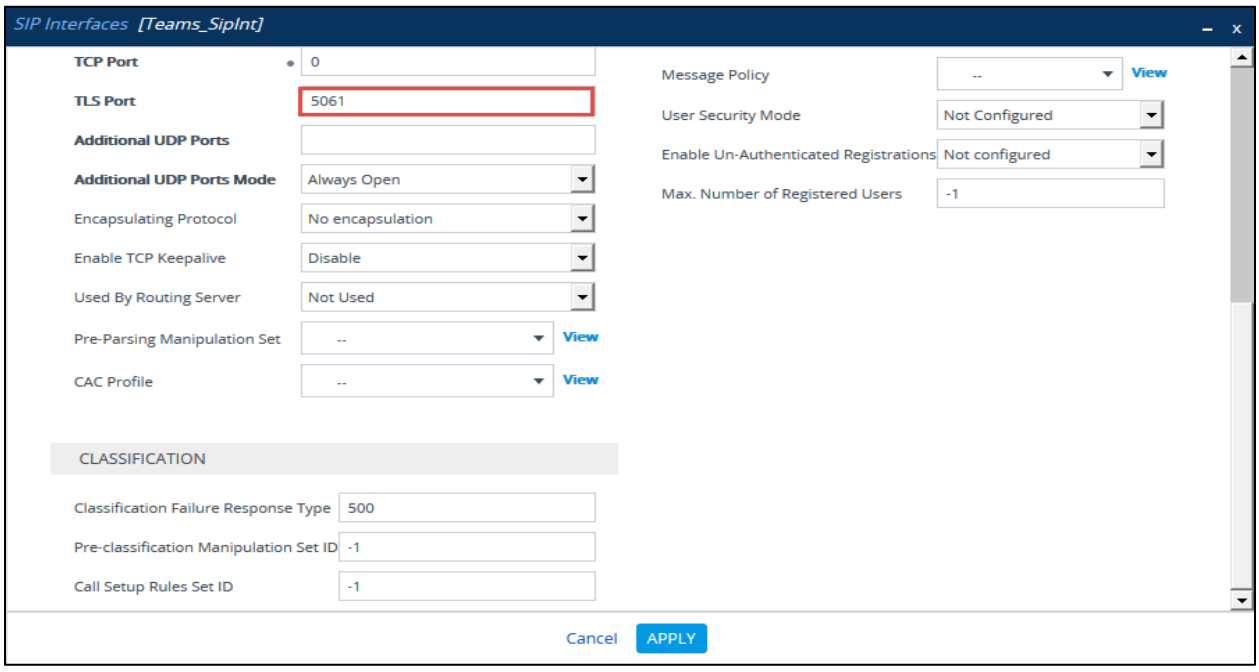

Figure 14: SIP Interface for MS Teams Continuation

Network Interface, Media Realm, SRD and *Port numbers* are associated to Amazon Chime Voice Connector SIP Interface and the remaining parameters are set to default.

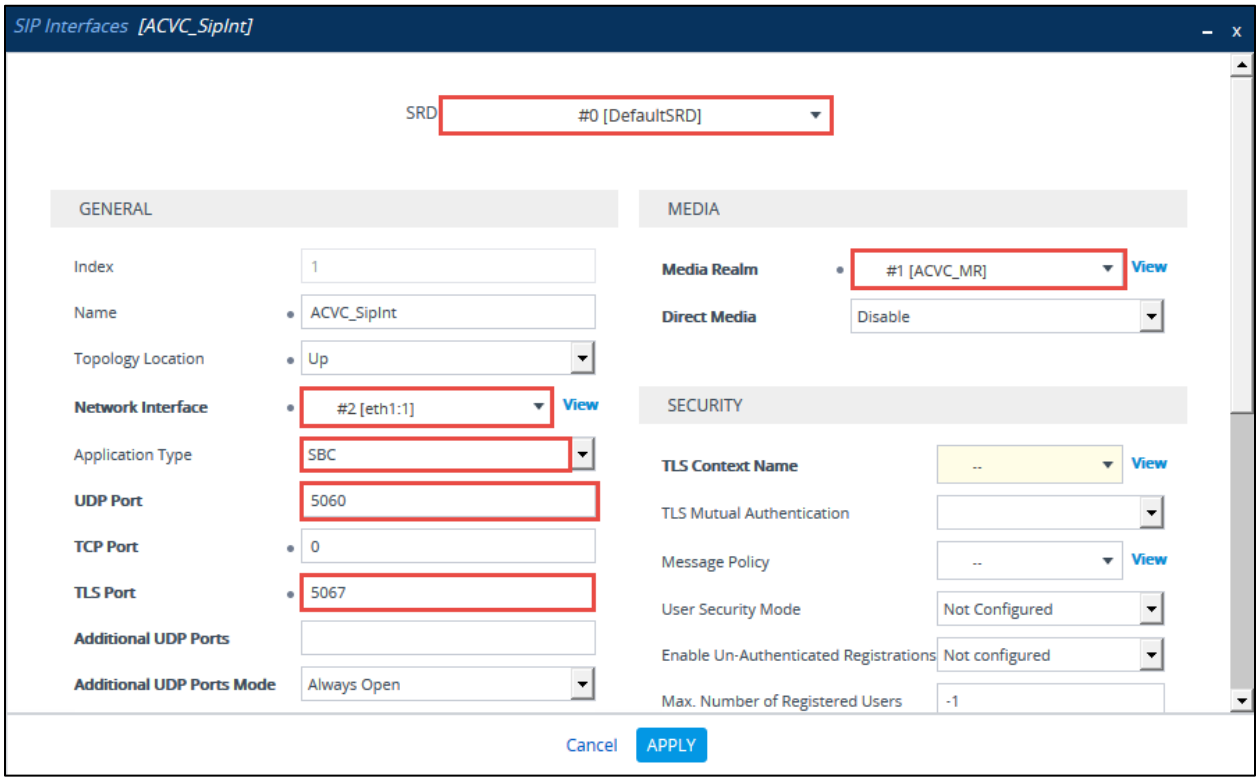

Figure 15: SIP Interface for Amazon Chime Voice Connector

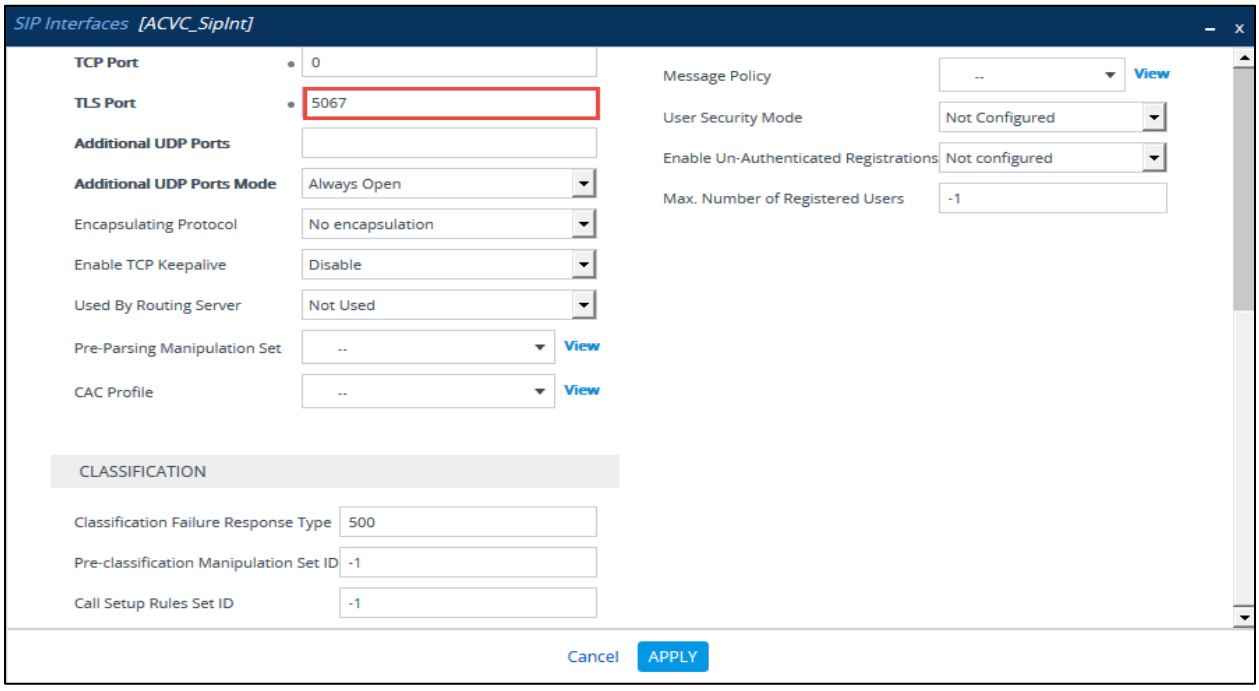

Figure 16: SIP Interface for Amazon Chime Voice Connector Continuation

4.3.5 Proxy Sets configuration

Navigate to '*SETUP*' and select '*SIGNALING & MEDIA*'. Expand '*CORE ENTITIES*' and select '*Proxy Sets*'. Destination address or FQDN is configured in Proxy Sets. Two Proxy Sets are created, one for MS Teams and other for Amazon Chime Voice Connector.

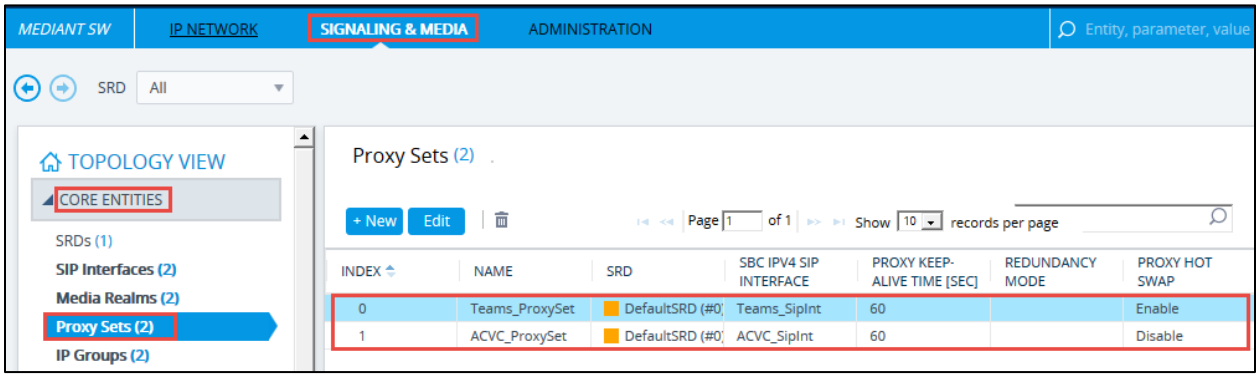

Figure 17: Proxy Sets table

Select *SBC IPv4 SIP Interface, TLS Context Name* and enable *Proxy Keep-Alive* for MS Teams Proxy Set.

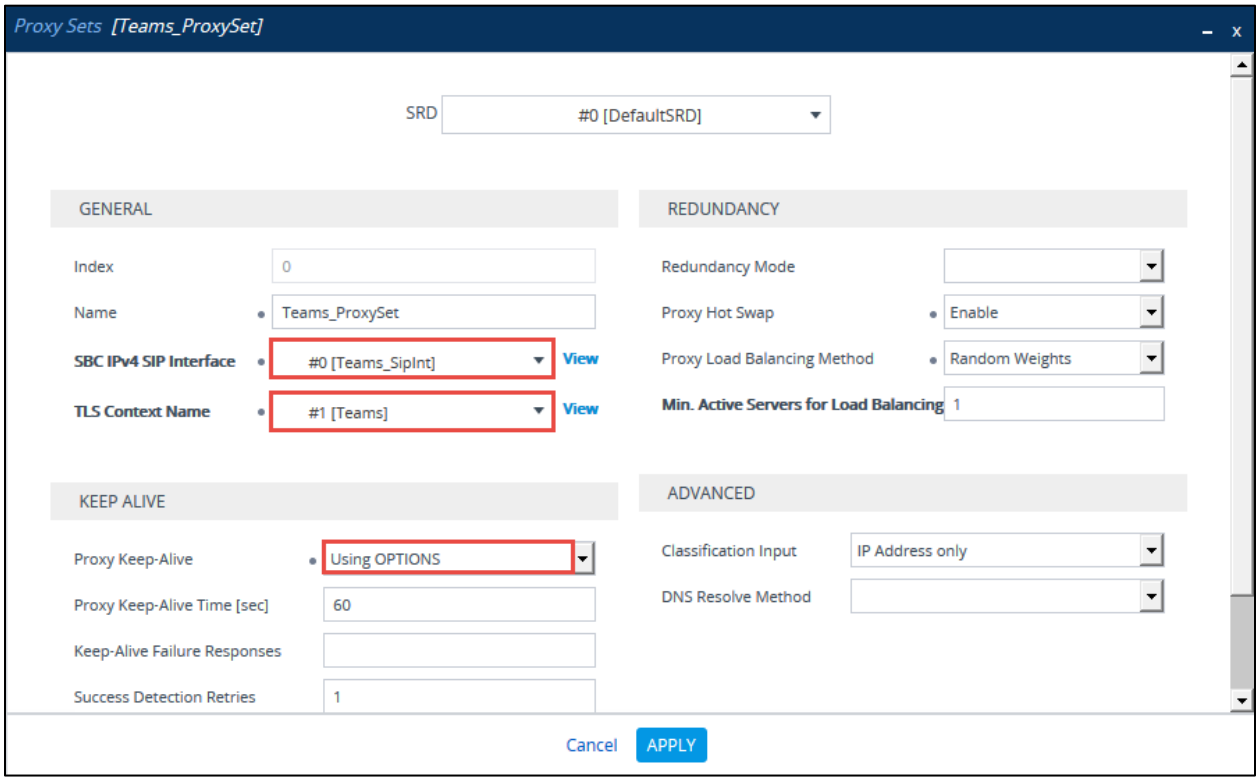

Figure 18: Proxy Set table for MS Teams

Click on '*Proxy Address 0 items*' link in bottom to add *Proxy Address* and *Transport Type*. The Proxy address added for MS Teams is below

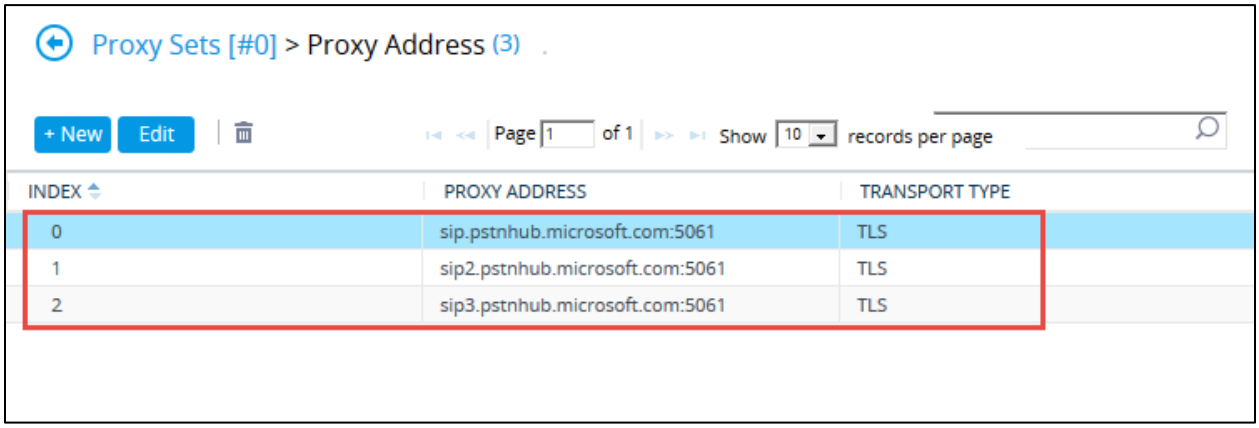

Figure 19: Proxy Address for MS Teams

Select *SBC IPv4 SIP Interface* and enable *Proxy Keep-Alive* for Amazon Chime Voice Connector Proxy Set.

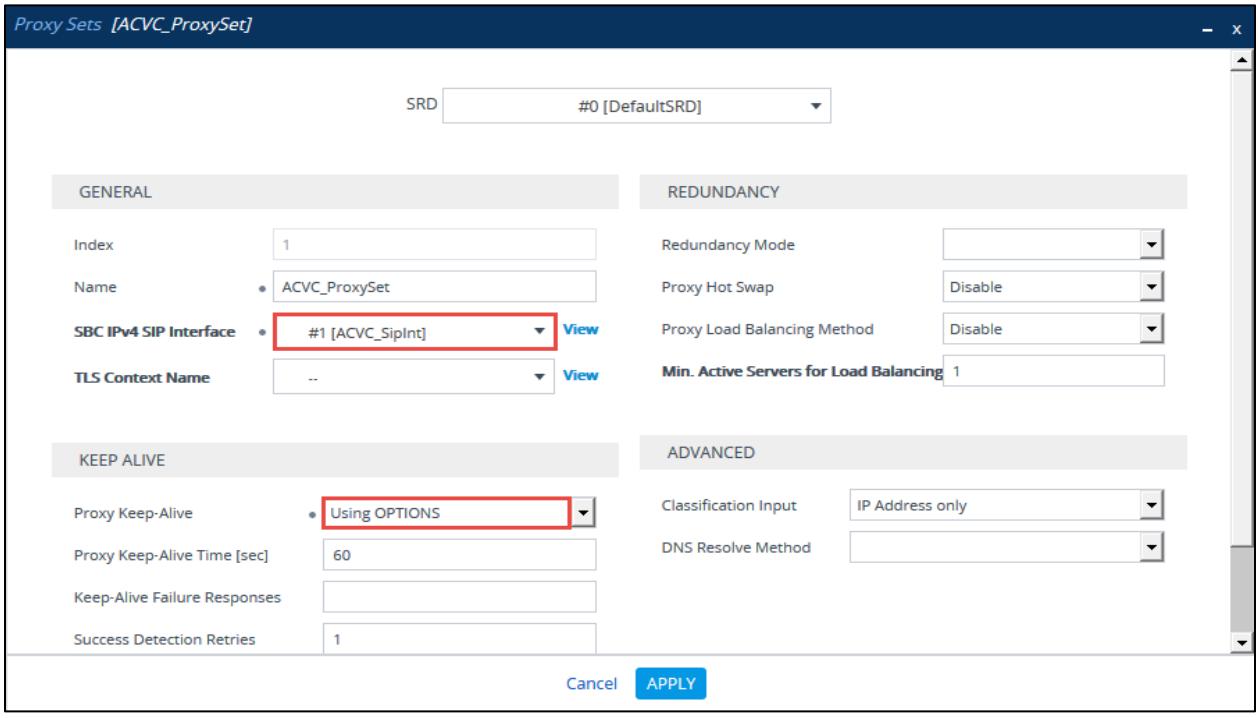

Figure 20: Proxy Set table for Amazon Chime Voice Connector

Click on '*Proxy Address 0 items*' link in bottom to add Proxy Address and Transport Type.

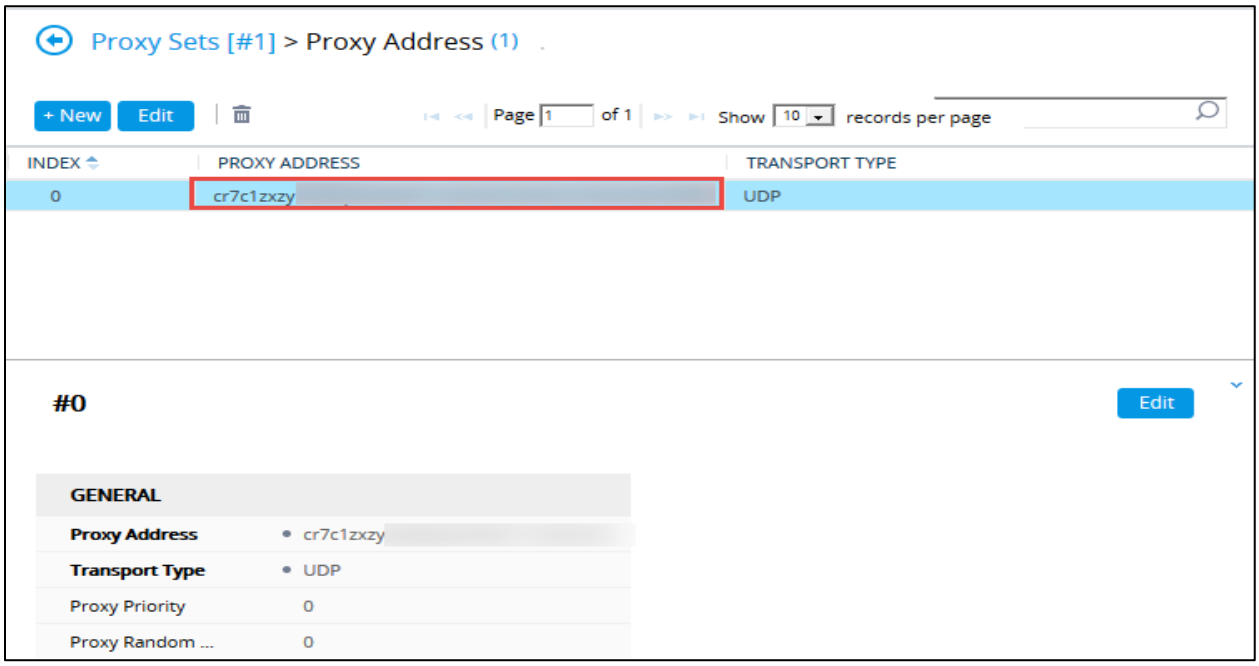

Figure 21: Proxy Address for Amazon Chime Voice Connector

4.3.6 IP Group Table configuration

Navigate to '*SETUP*' and select '*SIGNALING & MEDIA*'. Expand '*CORE ENTITIES*' and select '*IP Groups*'. IP Groups are configured for denoting source and destination in IP-to-IP routing rules. IP Groups created for MS Teams and AudioCodes CE.

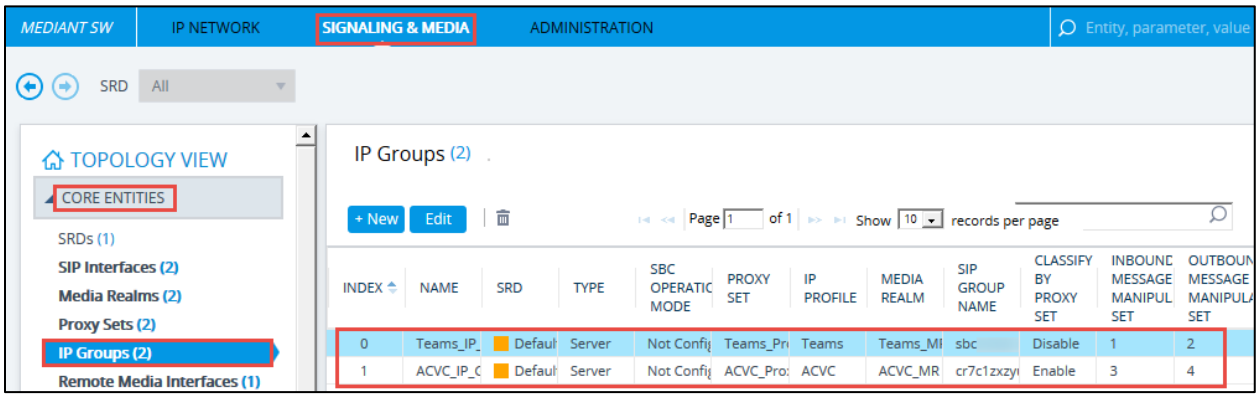

Figure 22: IP Group Table

Enter the name of the IP Groups for MS Teams and associate *Proxy Set, IP Profile, Media Realm* and the remaining parameters are set to default.

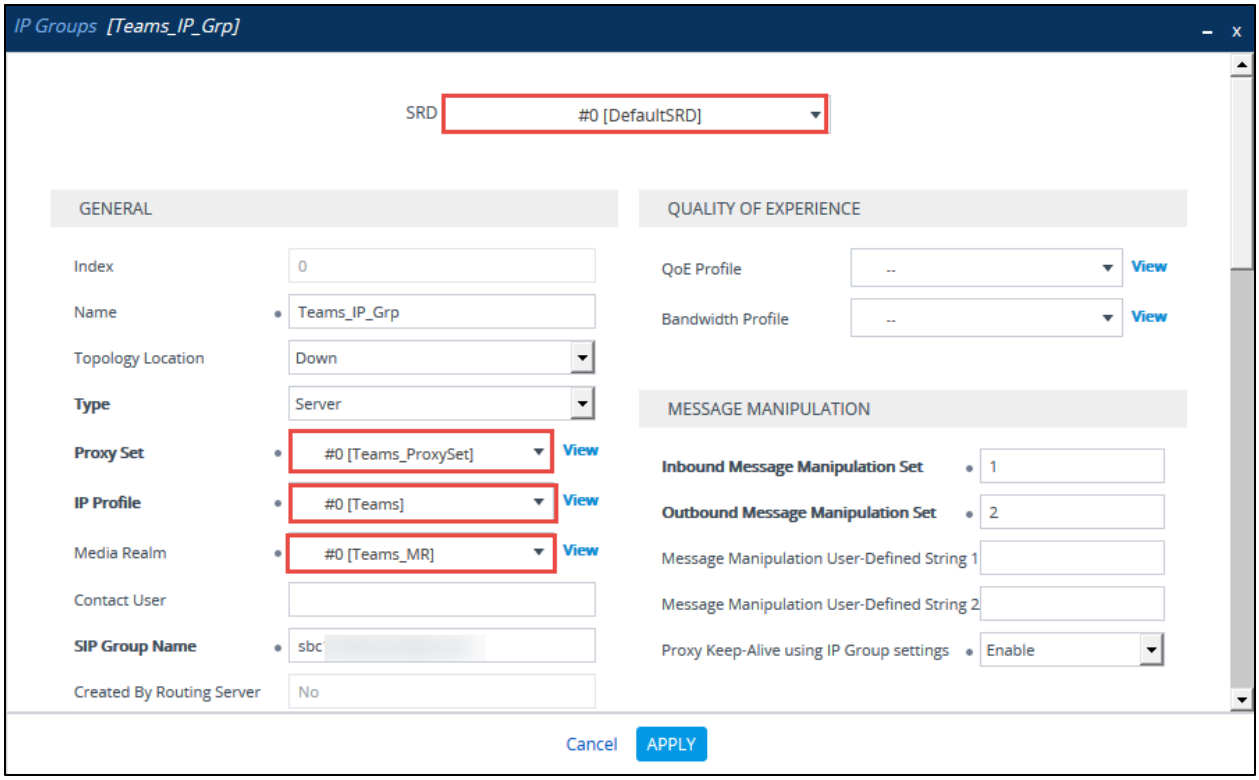

Figure 23: IP Group Table for MS Teams

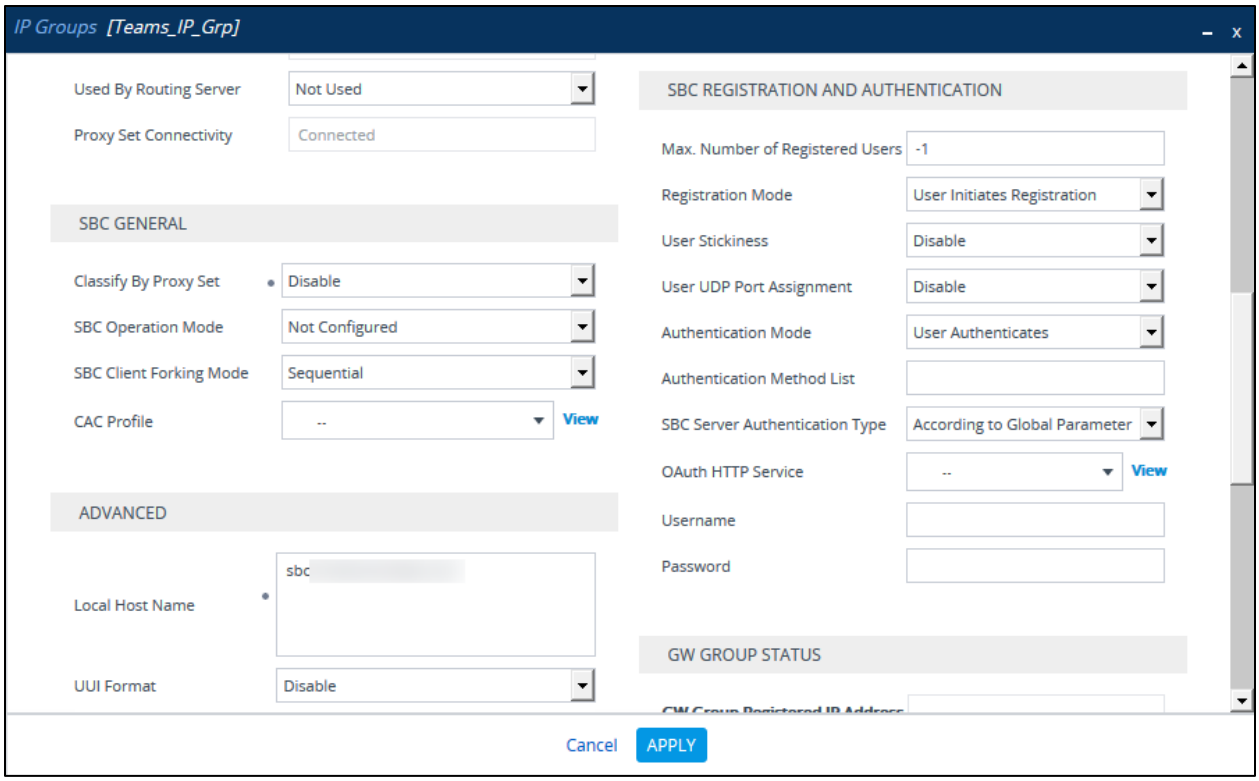

Figure 24: IP Group table for MS Teams

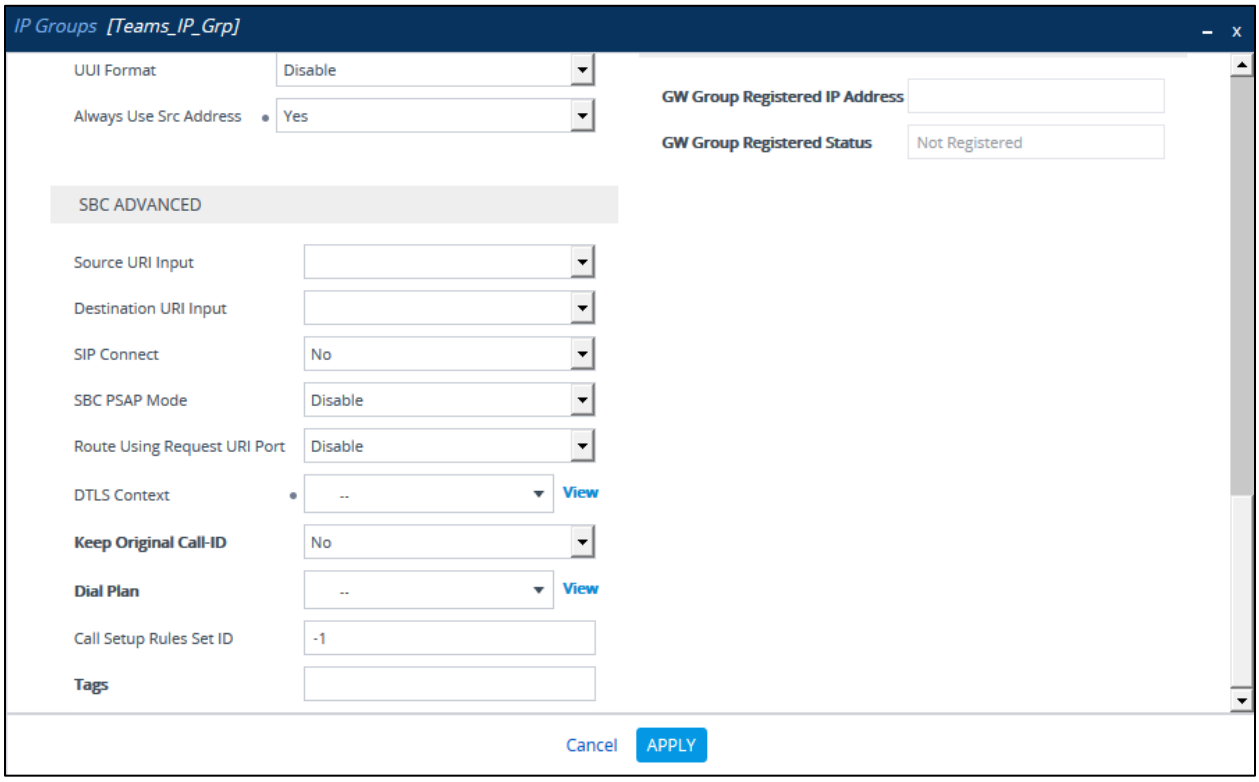

Figure 25: IP Group table for MS Teams Continuation

Enter the name of the IP Groups for Amazon Chime Voice Connector and associate *Proxy Set, IP Profile, Media Realm* and the remaining parameters are set to default.

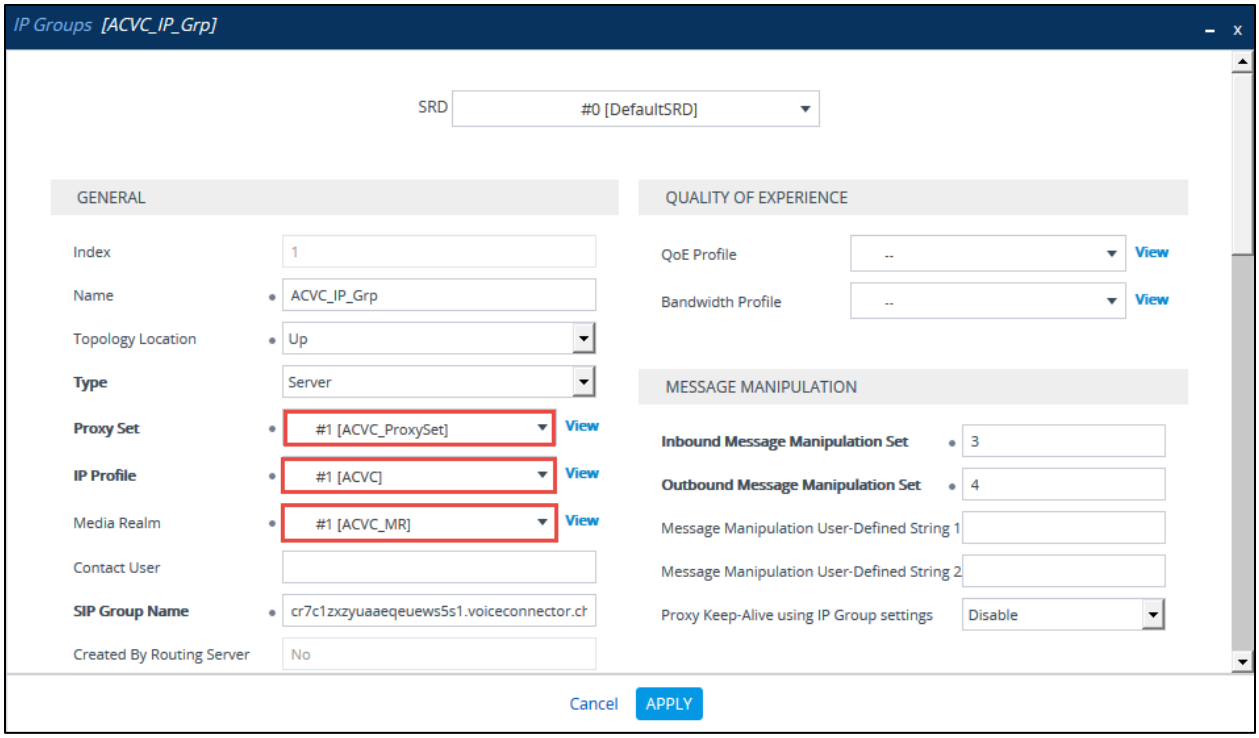

Figure 26: IP Group table for Amazon Chime Voice Connector

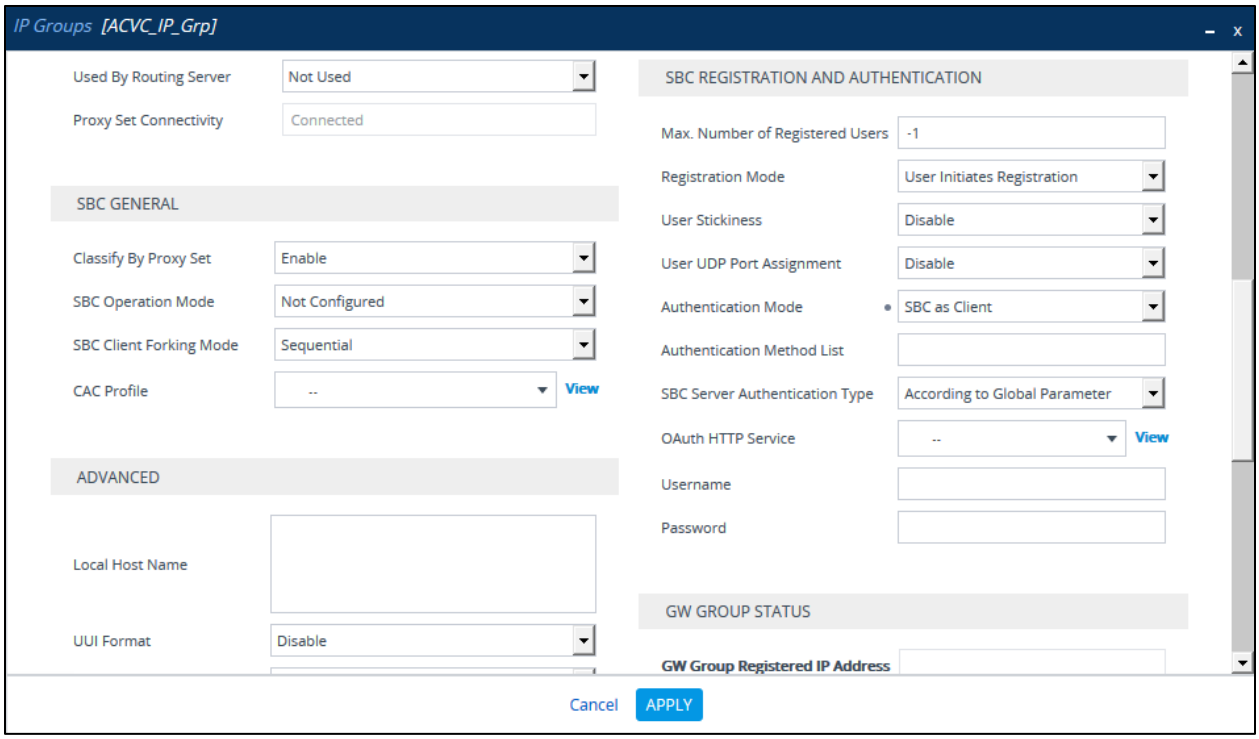

Figure 27: IP Group table for Amazon Chime Voice Connector Continuation

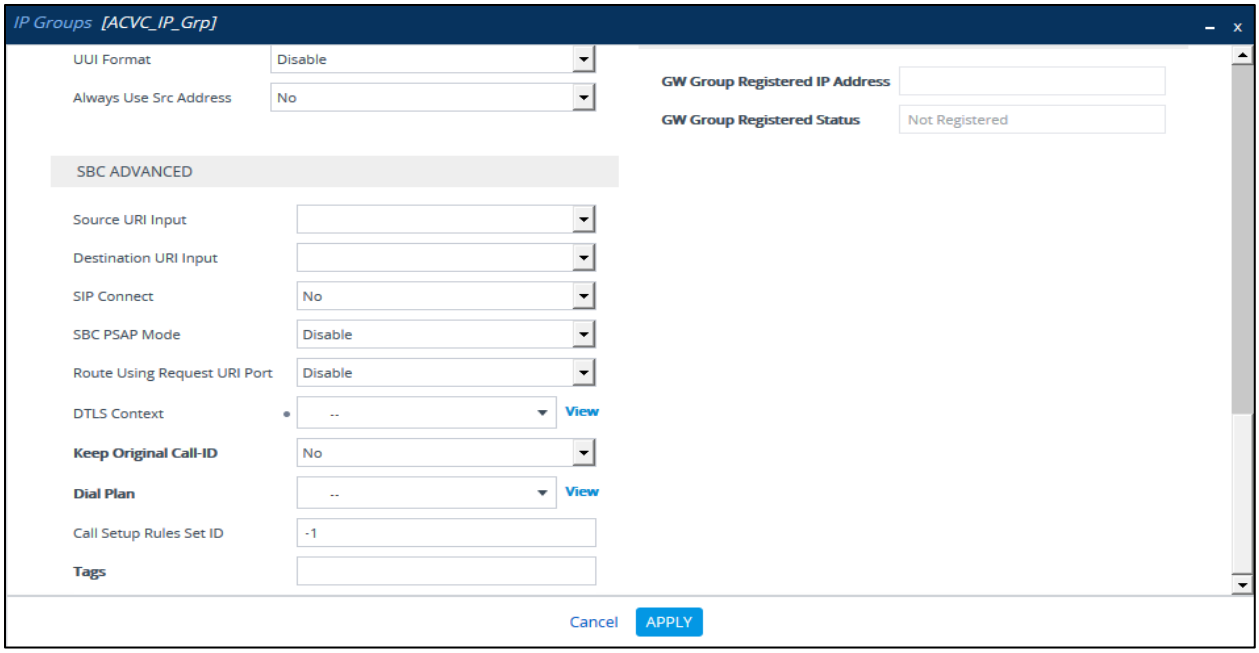

Figure 28: IP Group table for Amazon Chime Voice Connector Continuation

4.3.7 Coder Groups configuration

Navigate to '*SETUP*' and select '*SIGNALING & MEDIA*'. Expand '*CODERS & PROFILES*' and select '*Coder Groups*'. G711 U-law is configured in Coder Groups.

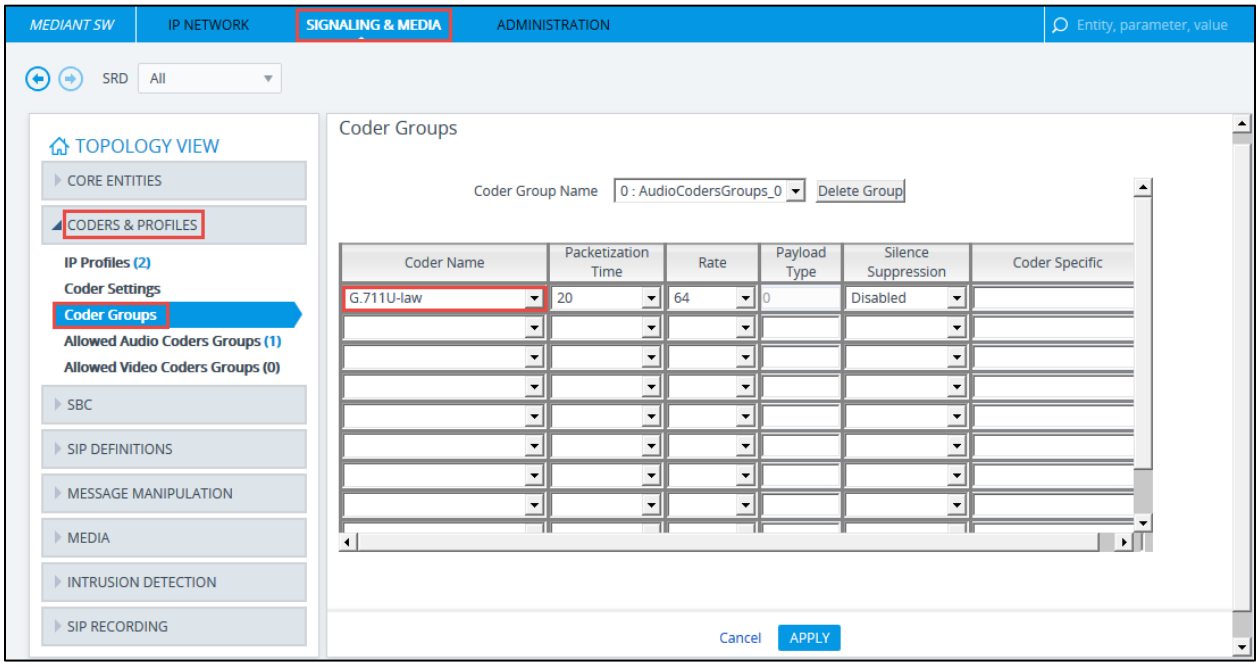

Figure 29: Coder Groups

Navigate to '*SETUP', 'SIGNALING & MEDIA', 'CODERS & PROFILES'* and select '*Allowed Audio Coders Groups*'. Click on '*New*' button to create Allowed Audio

Coders Group and then Click on 'Allowed Audio Coders 0 items' link and click 'New' to add the coders.

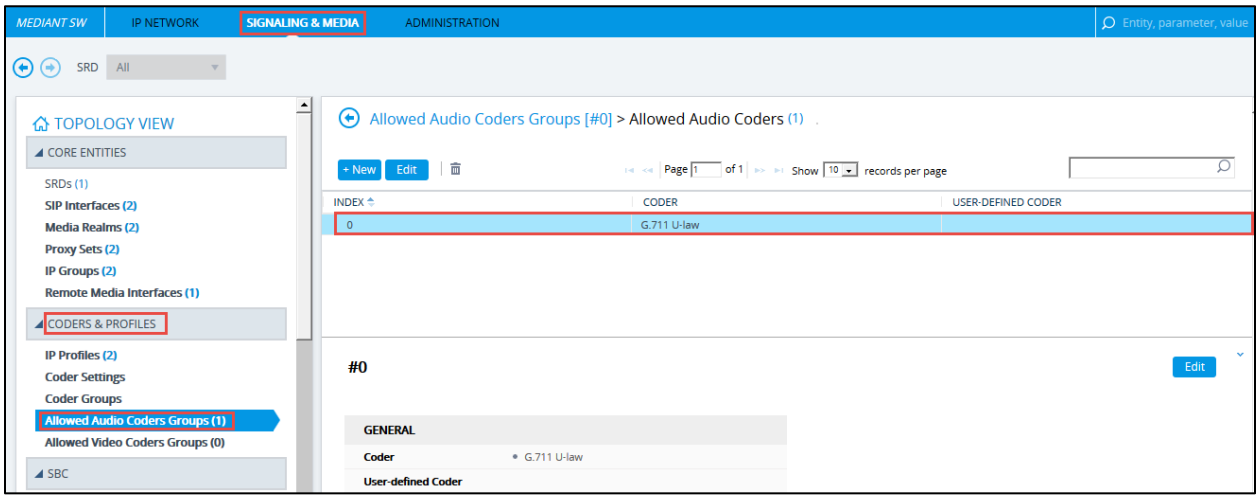

Figure 30: Allowed Audio Coders

4.3.8 IP Profile configuration

Navigate to '*SETUP*' and select '*SIGNALING & MEDIA*'. Expand '*CODERS & PROFILES'* and select '*IP Profiles'*. Two IP Profiles are created, one for MS Teams and other for Amazon Chime Voice Connector.

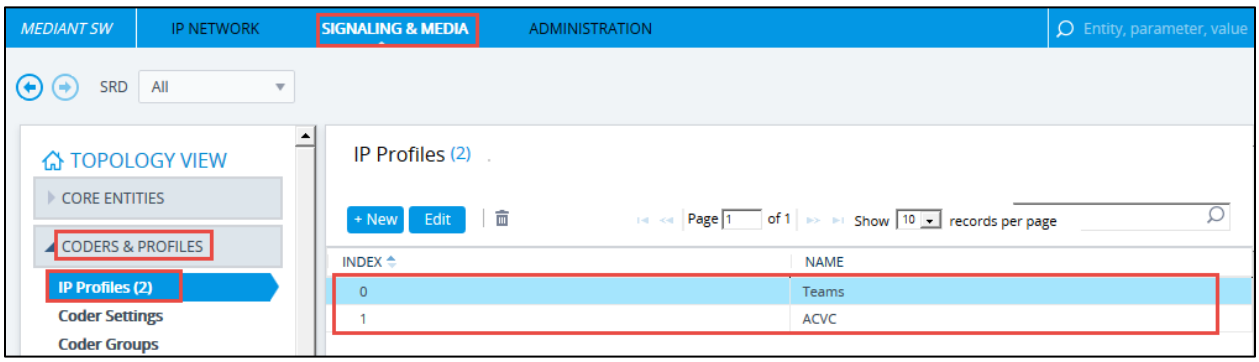

Figure 31: IP Profiles

In the IP Profile for MS Teams, select Session Expire Mode as '*Supported*', Remote re-INVITE as *Supported only with SDP*, Remote Delayed Offer Support as *Not Supported,* SBC Media Security Mode as *SRTP* and Remote Early Media RTP Detection Mode as '*By Media*'. *Extension Coder Group* and *Allowed Audio Coders* are associated appropriately.

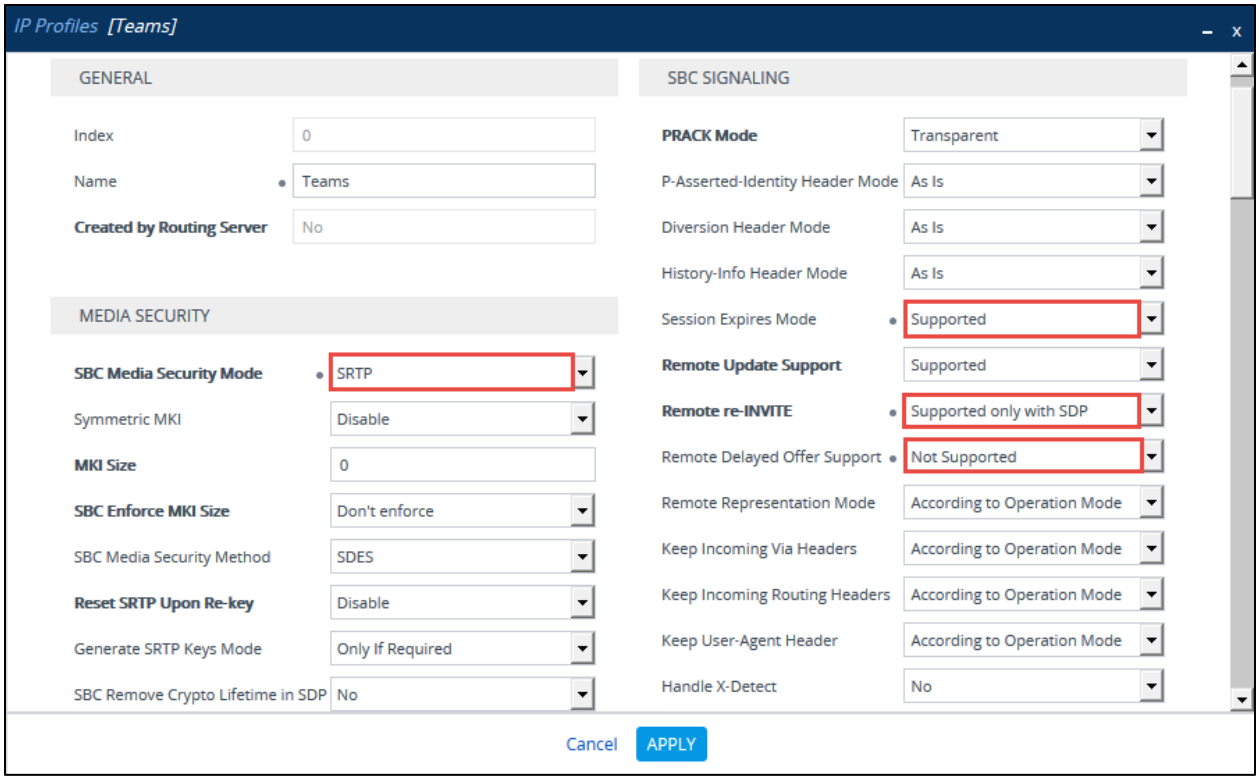

Figure 32: IP Profile for MS Teams

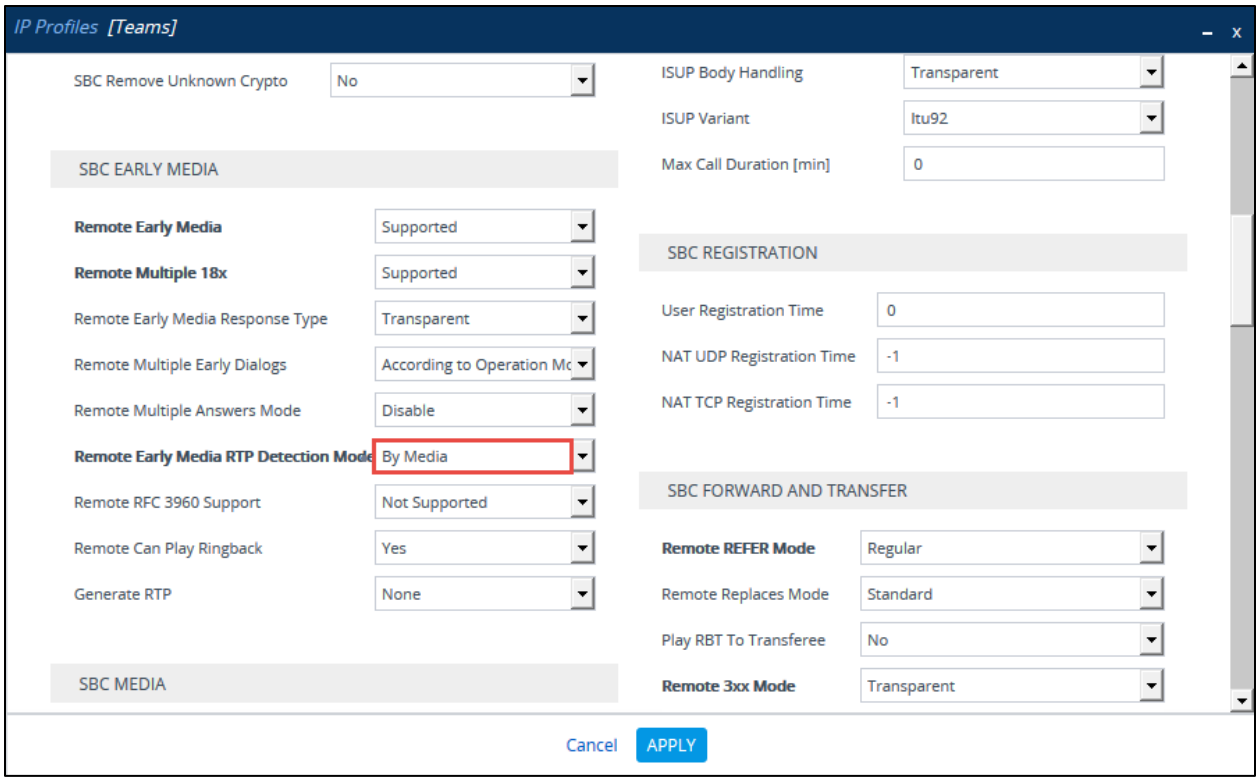

Figure 33: IP Profile for MS Teams Continuation

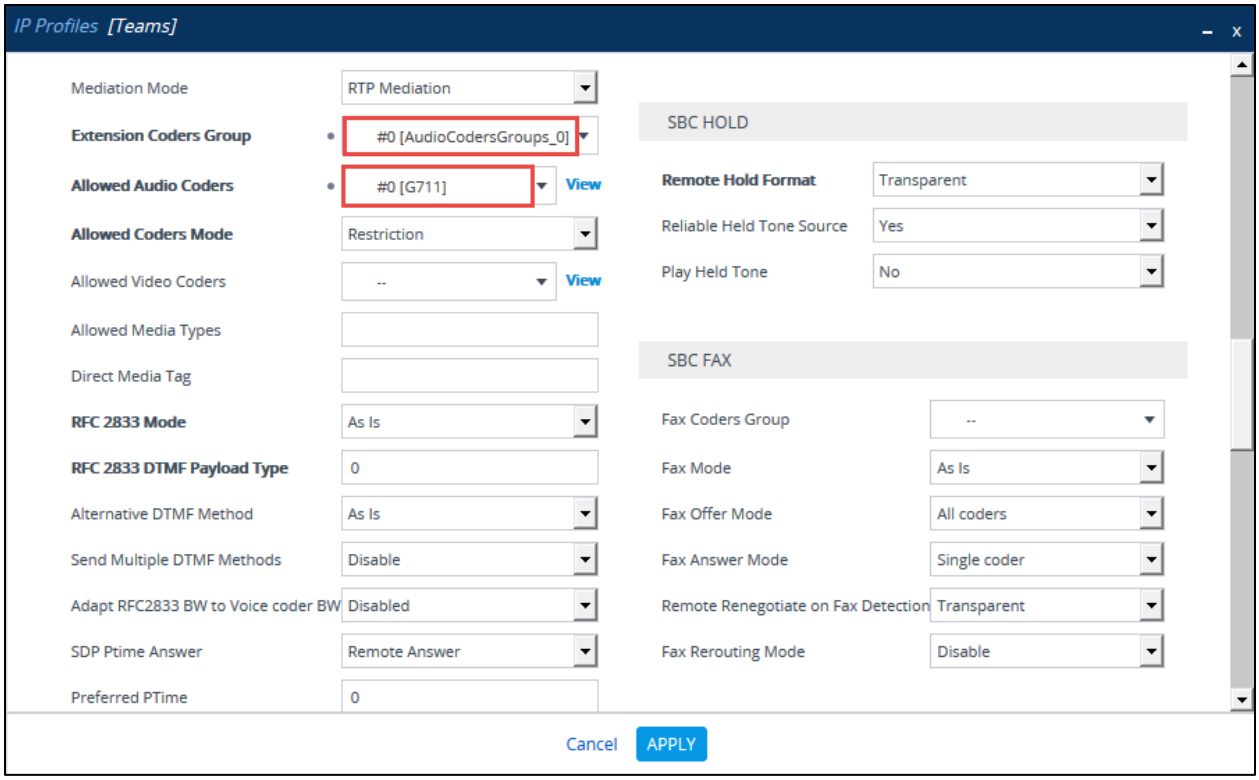

Figure 34: IP Profile for MS Teams Continuation

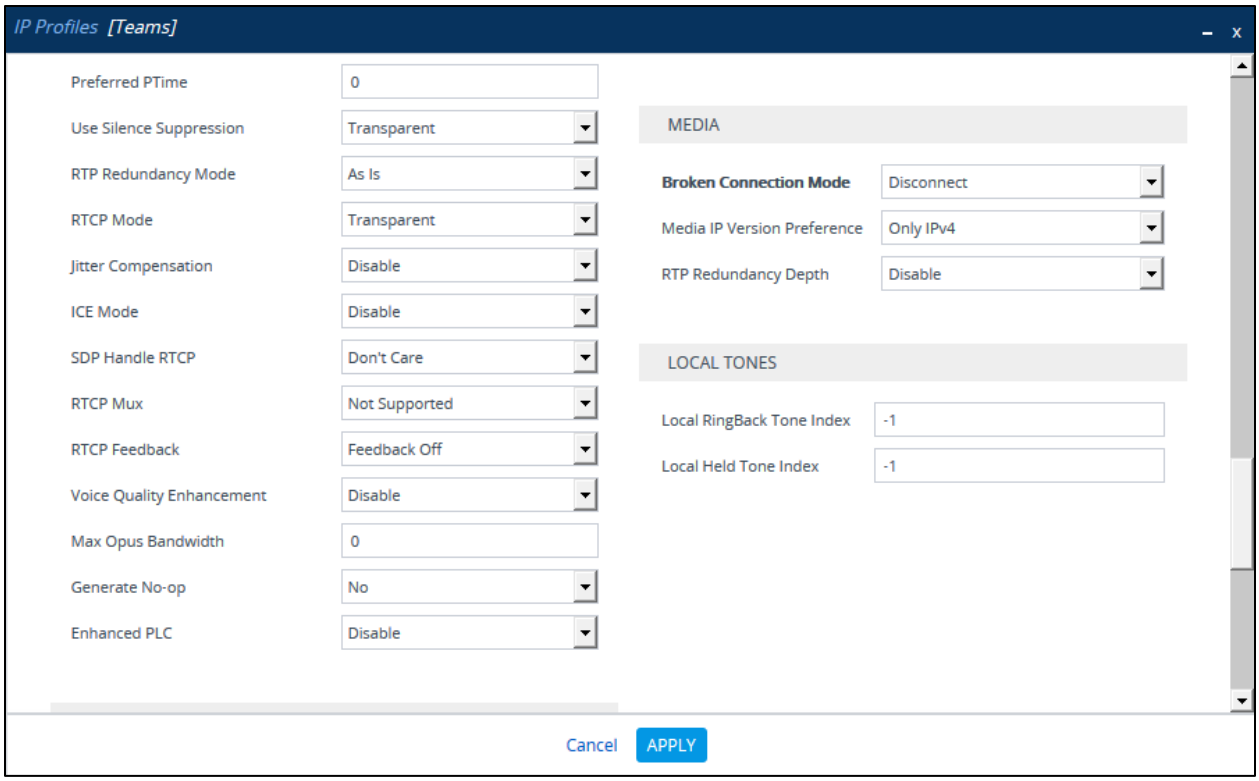

Figure 35: IP Profile for MS Teams Continuation

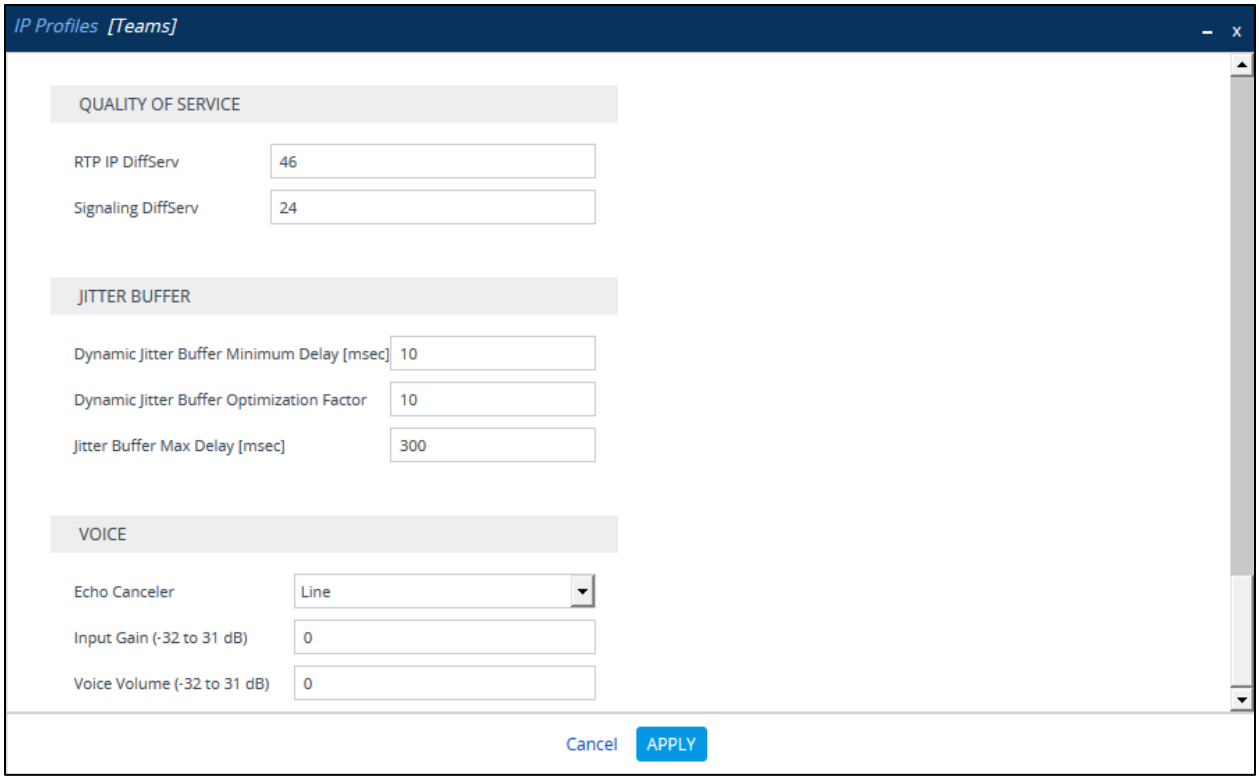

Figure 36: IP Profile for MS Teams Continuation

In the IP profile for Amazon Chime Voice Connector, select Remote Multiple 18x *as 'Not Supported',* SBC Media Security Mode *as 'RTP', Session* Expires Mode as *'Not Supported'* and Remote Update Support as '*Not Supported*'. *Extension Coder Group* and *Allowed Audio Coders* are associated appropriately.

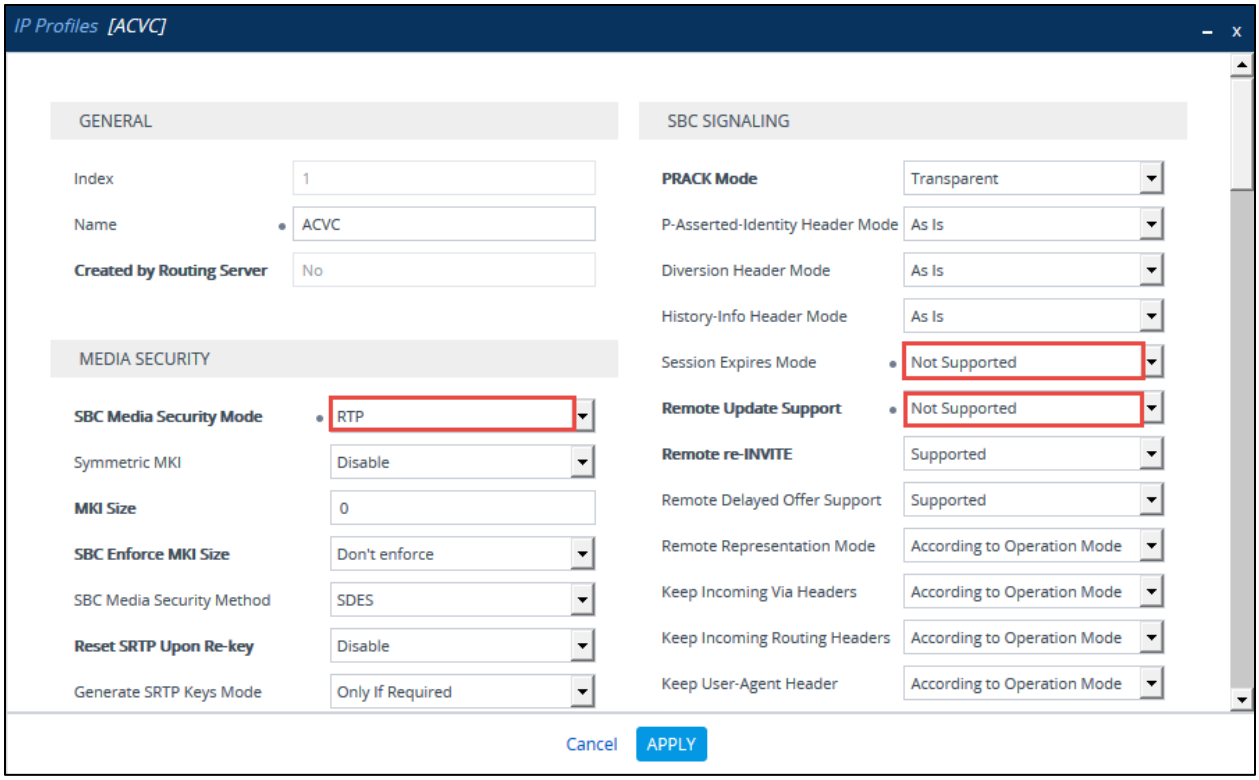

Figure 37: IP Profile for Amazon Chime Voice Connector

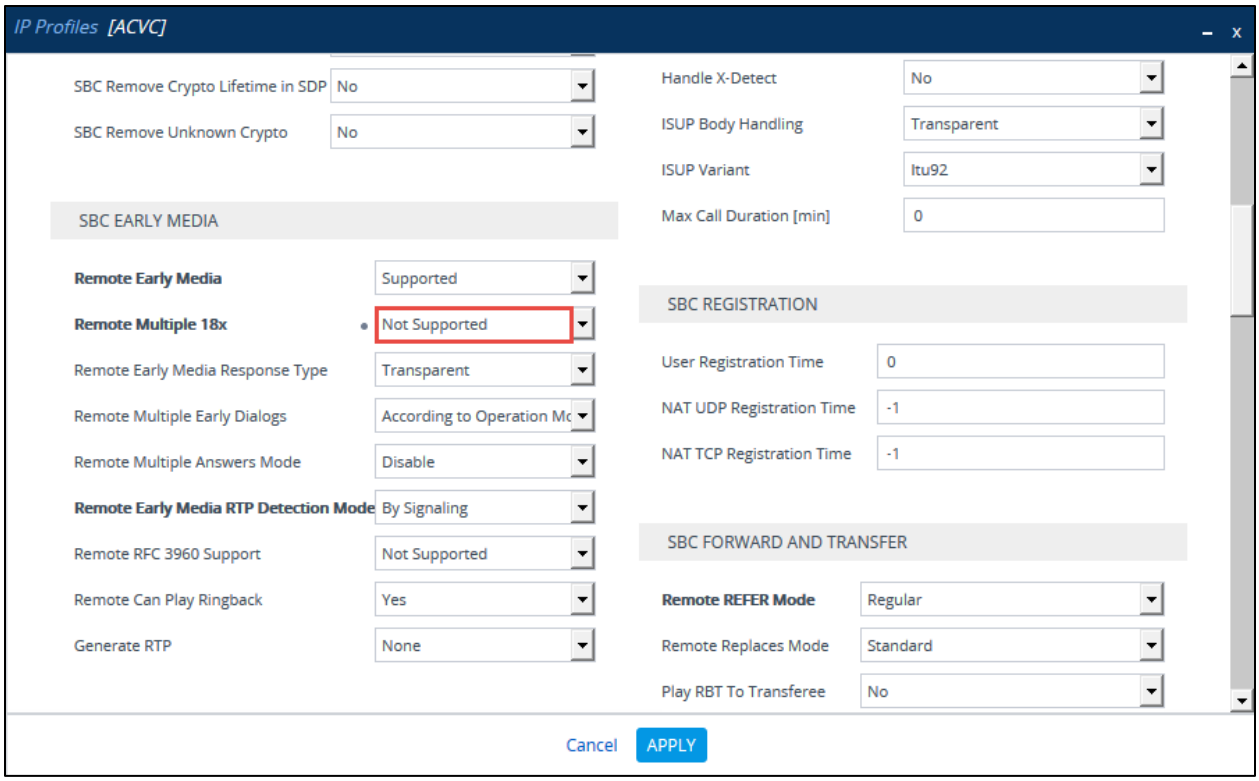

Figure 38: IP Profile for Amazon Chime Voice Connector Continuation

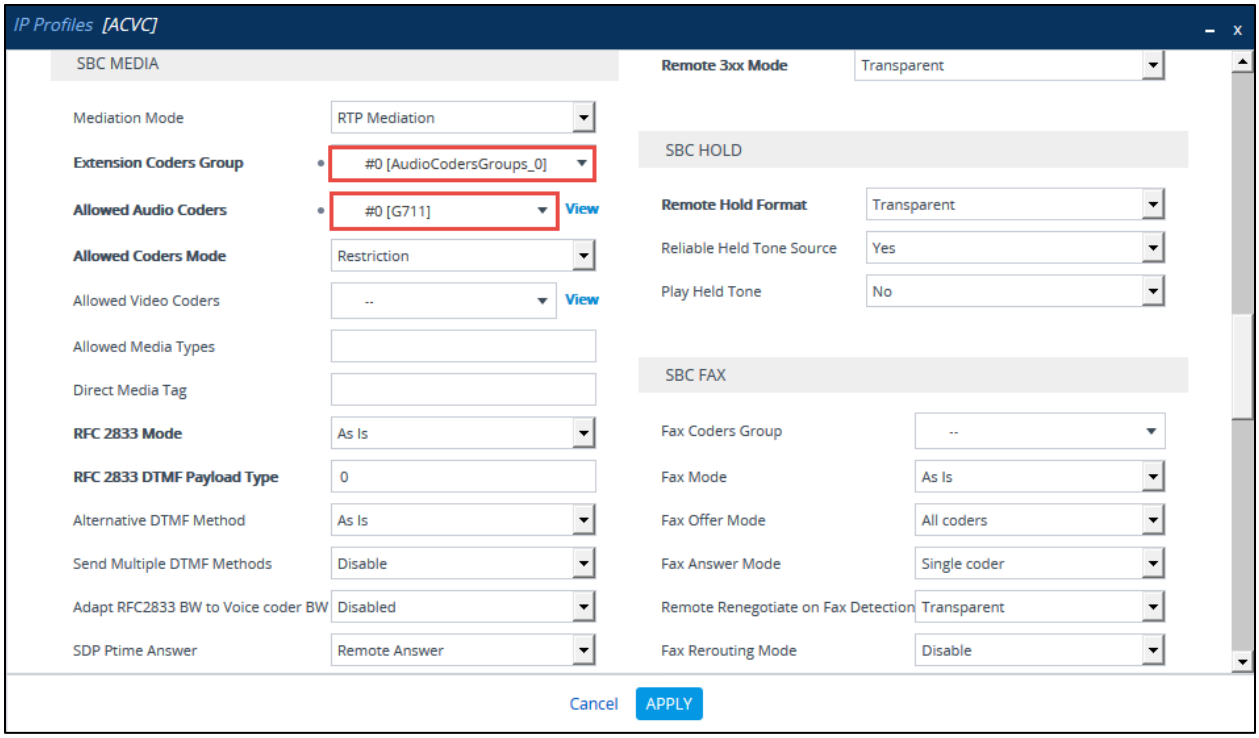

Figure 39: IP Profile for Amazon Chime Voice Connector Continuation

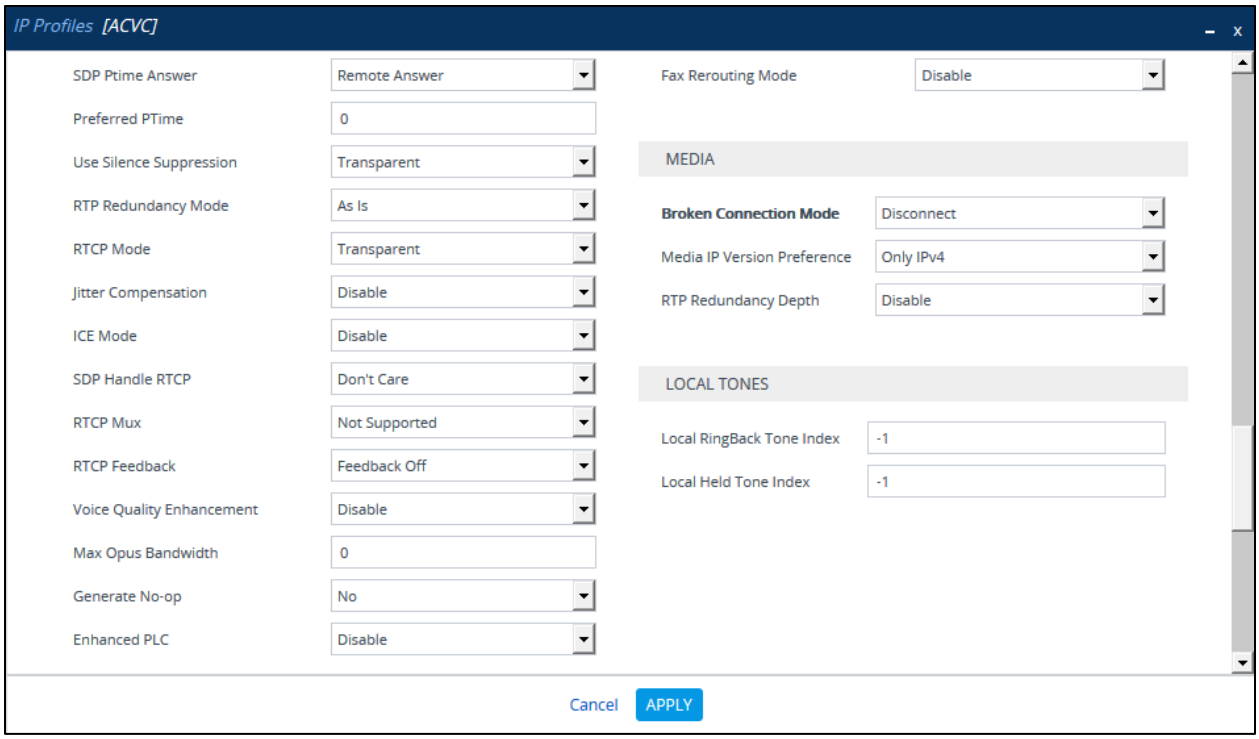

Figure 40: IP Profile for Amazon Chime Voice Connector Continuation

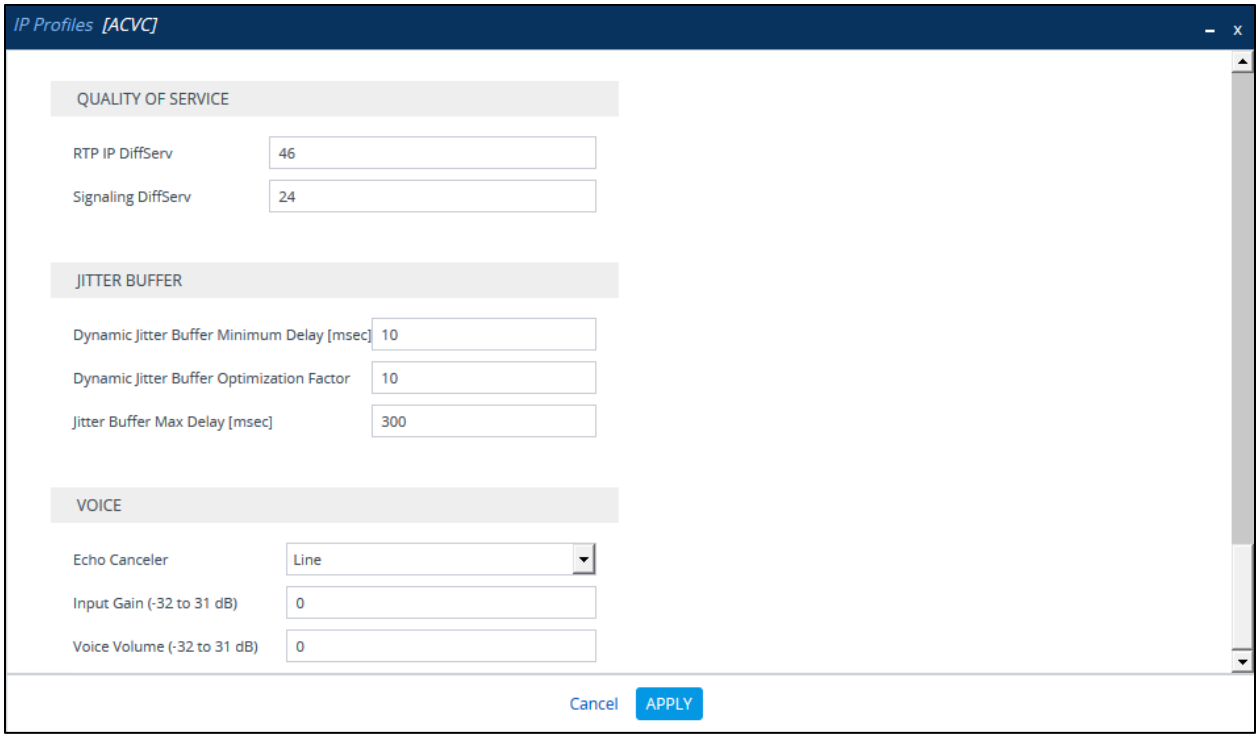

Figure 41: IP Profile for Amazon Chime Voice Connector Continuation

4.3.9 IP-to-IP Routing

Navigate to '*SETUP*' and select '*SIGNALING & MEDIA*'. Expand '*SBC*' and select '*IP-to-IP Routing'*. Routing rules are defined for forwarding SIP messages based on IP Groups from source to destination.

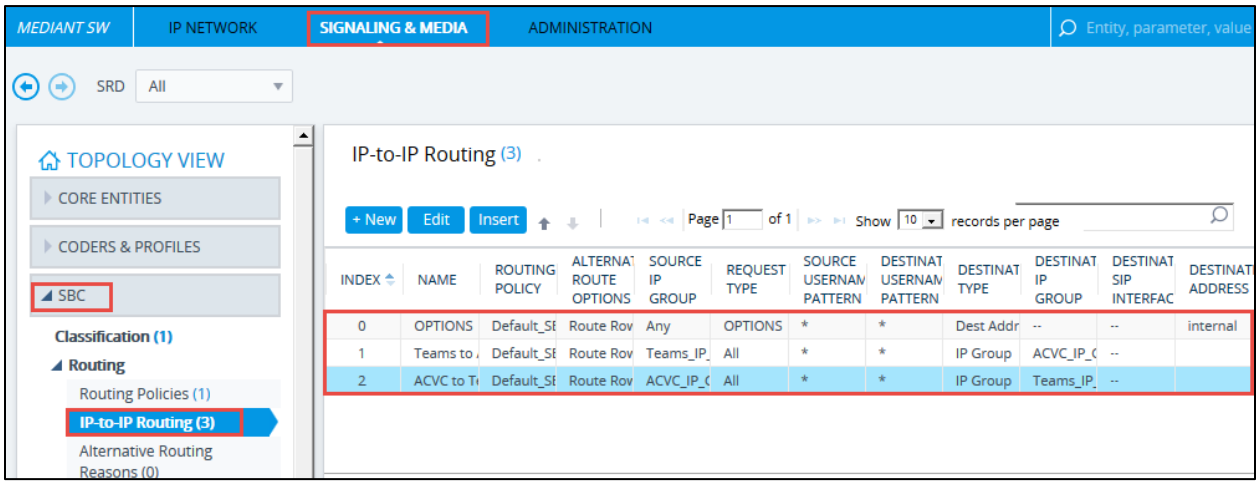

Figure 42: IP-to-IP Routing

IP to IP routing for OPTIONS message

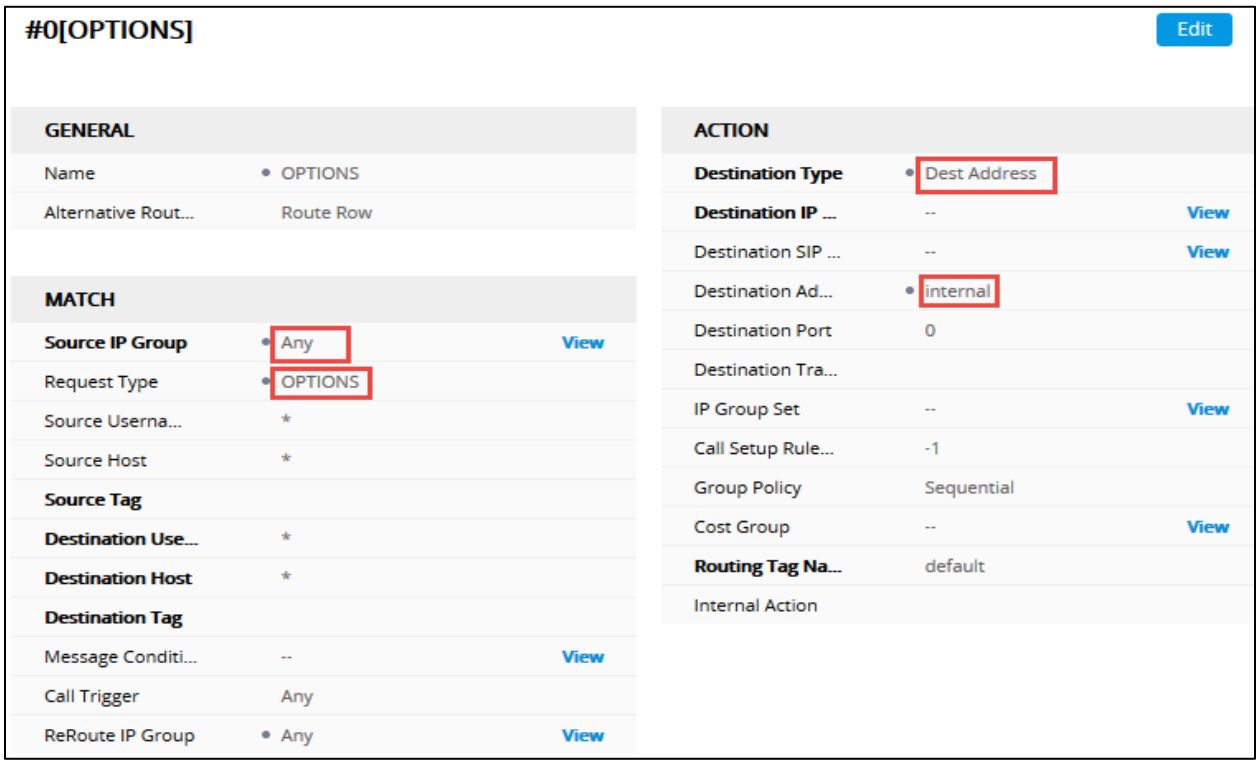

Figure 43: IP-to-IP Routing for OPTIONS

IP to IP routing from MS Teams to Amazon Chime Voice Connector.

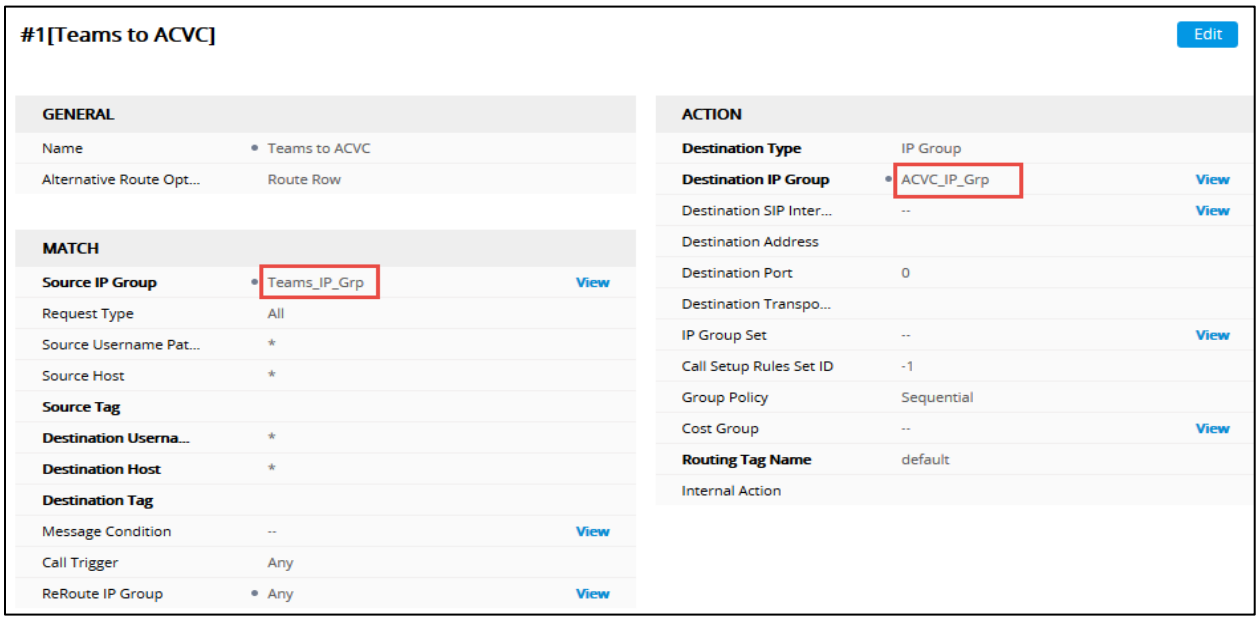

Figure 44: IP-to-IP Routing from MS Teams to Amazon Chime Voice Connector

IP to IP routing from Amazon Chime Voice Connector to MS Teams.

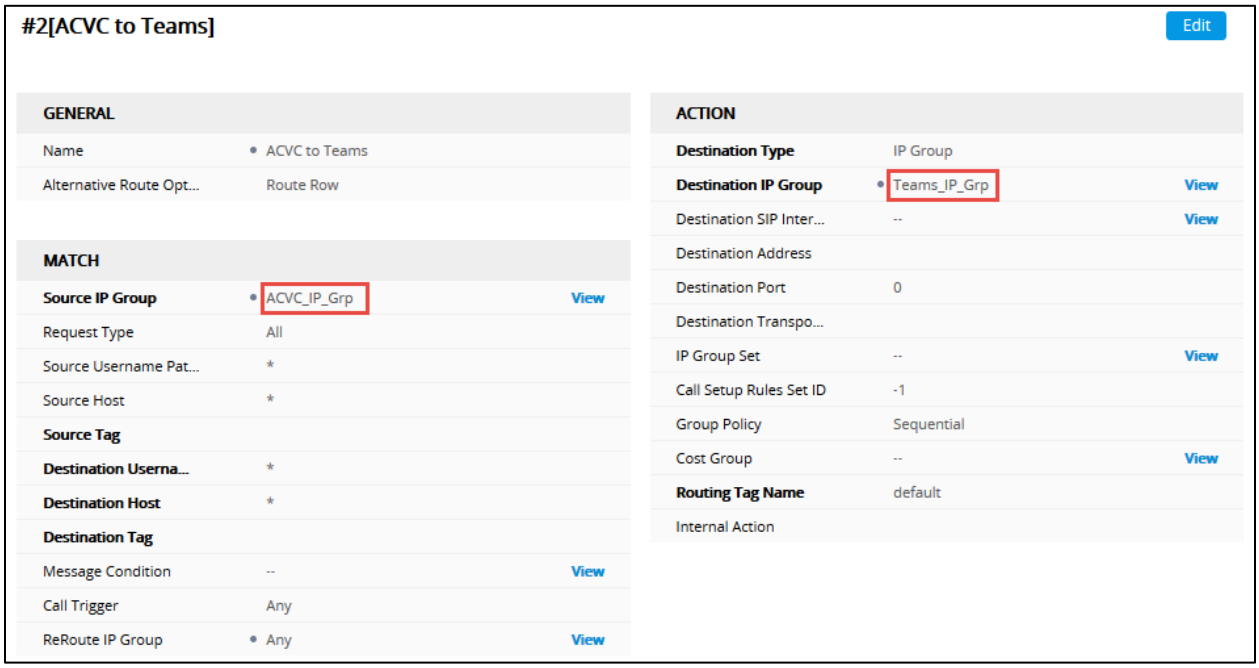

Figure 45: IP-to-IP Routing from Amazon Chime Voice Connector to MS Teams

4.3.10 TLS Configuration

TLS is configured between AudioCodes CE and Amazon Chime Voice Connector. Navigate to '*SETUP*' and select '*IP NETWORK'*. Expand '*SECURITY*' and click on '*TLS Contexts'*.

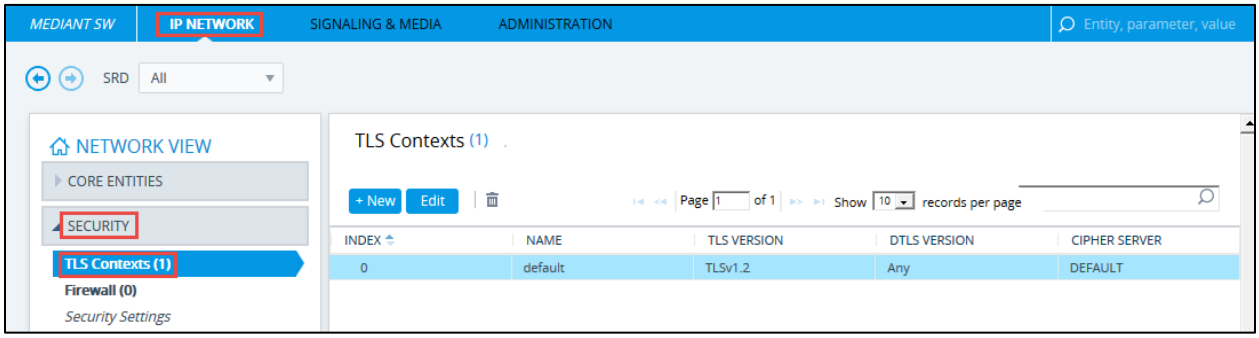

Figure 46: TLS Context list

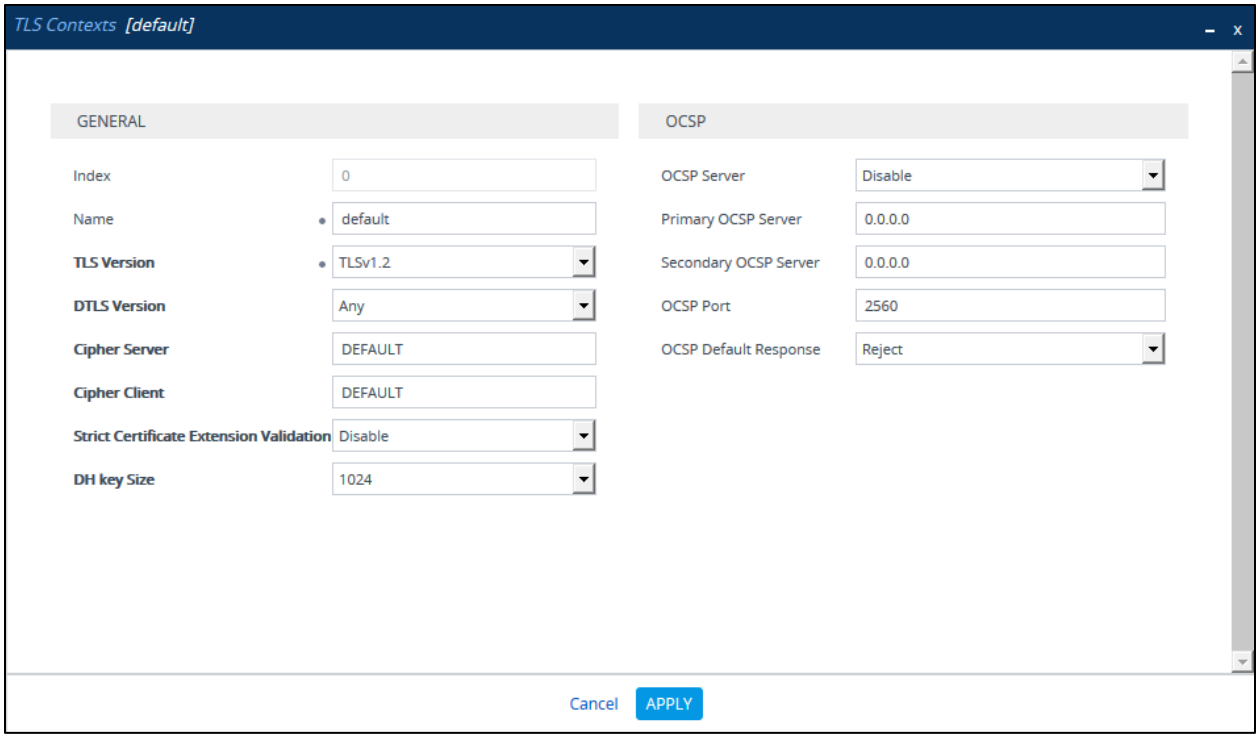

Figure 47: TLS Context for Amazon Chime Voice Connector

Amazon Trust Root Certificate is to be installed in the Trusted Root Certificates list under TLS Context. In the TLS Context page, select the *TLS Context* for Amazon Chime Voice Connector and click '*Trusted Root Certificates*' link located in the bottom. Click on *Import* button and select the certificate file.

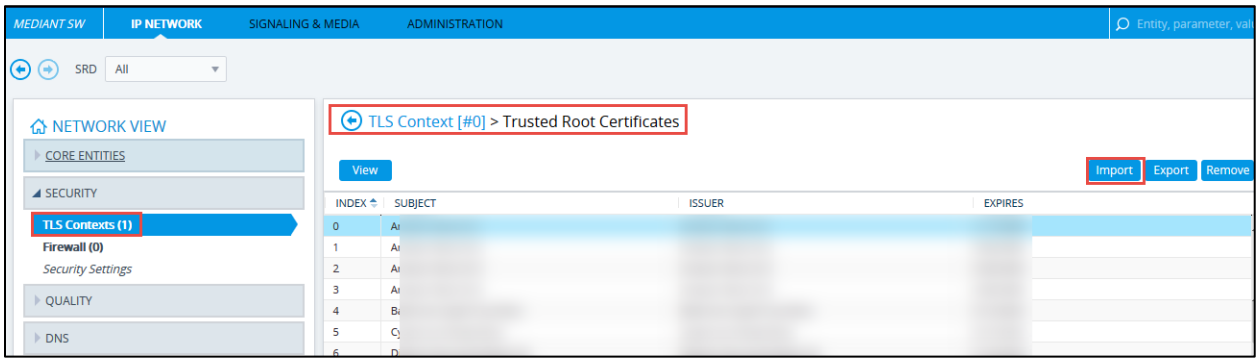

Figure 48: Trusted Root Certificate Import option

Amazon Chime Voice Connector Root Certificate can be downloaded from Amazon Chime Voice Connector account.

TLS is configured between AudioCodes CE and MS Teams. MS Teams allows only TLS connections from SBC. A certificate signed by one of the trusted Certificate Authorities is required for establishing TLS session with MS Teams from SBC.

Navigate to '*SETUP*' and select '*IP NETWORK'*. Expand '*SECURITY*' and click on '*TLS Contexts'* to create TLS Context for MS Teams. Click on +New button to create a new TLS Context. The TLS Contexts created for MS Teams is below

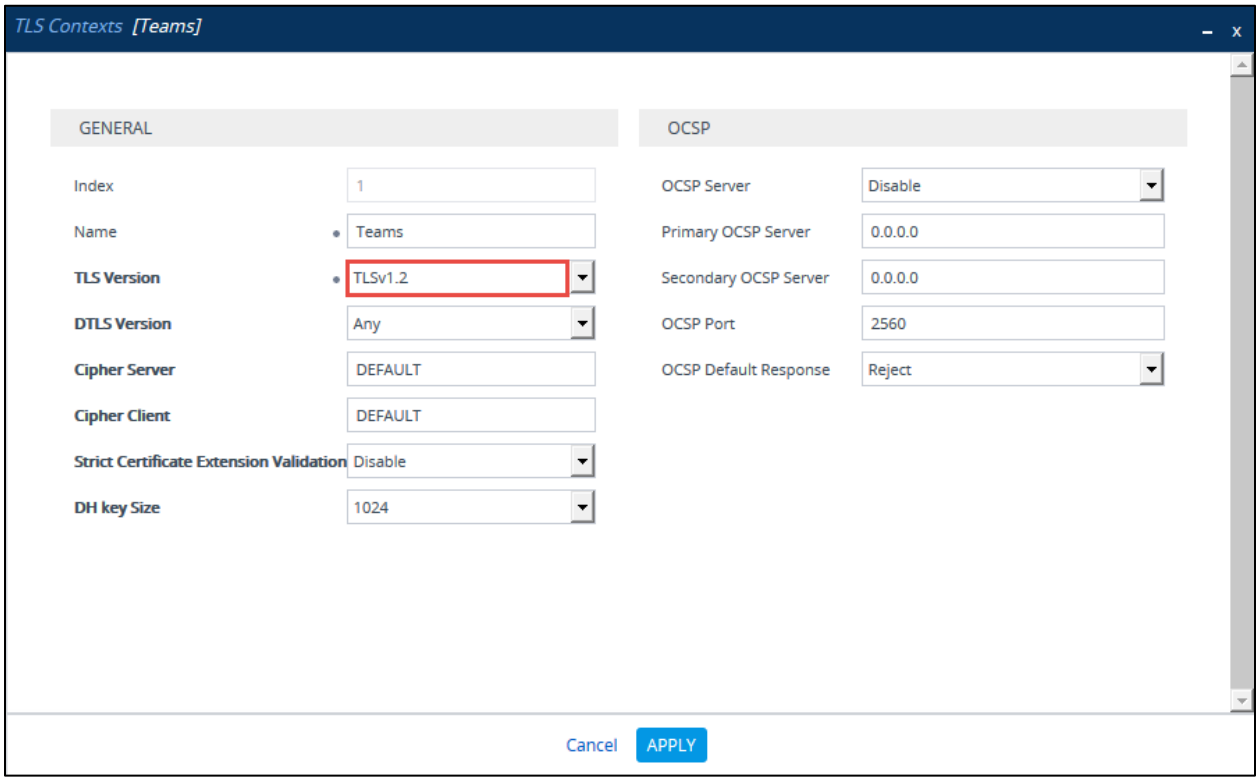

Figure 49: TLS Context for MS Teams

Next CSR (Certificate Signing Request) has to be generated and obtain the certificate from a supported Certificate Authority. To generate CSR, navigate to TLS Contexts page and select the TLS Context created for MS Teams. Click on '*Change Certificate*' link located in the bottom of the table.

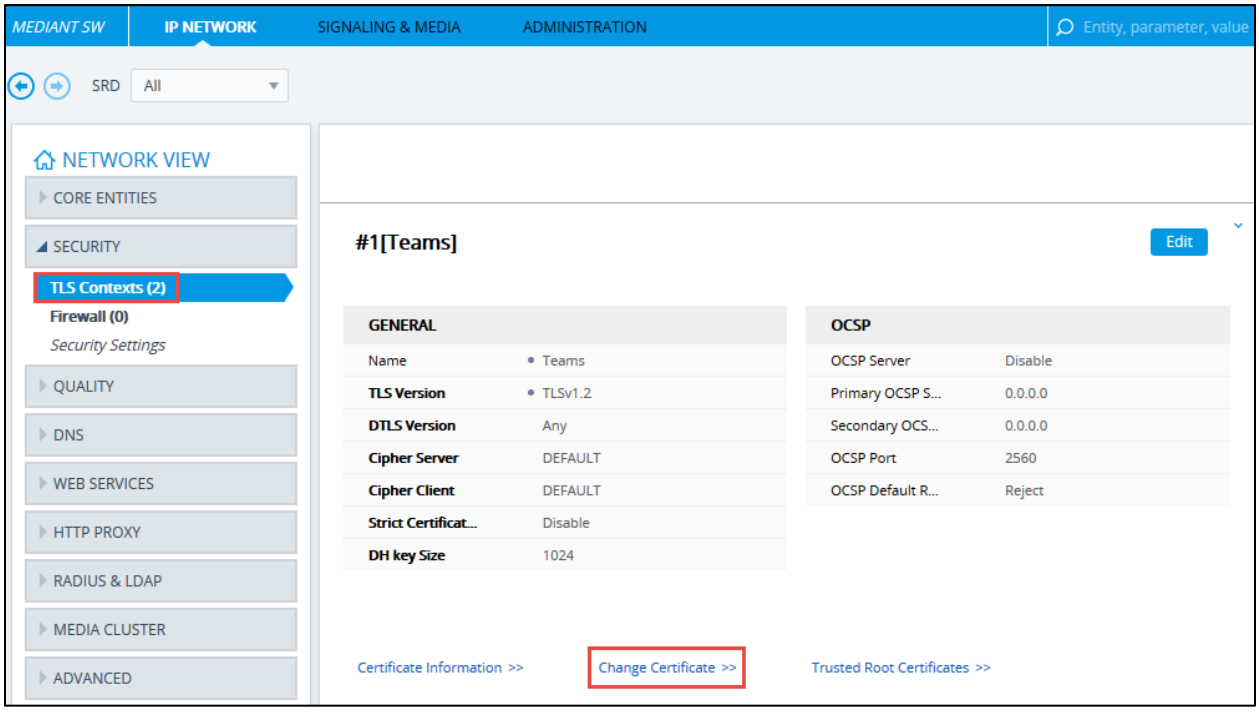

Figure 50: Change Certificate for MS Teams

In the Certificate Signing Request page, enter the necessary information like Common Name, Organization details etc. Change the '*Private key Size*' as 2048. To change the key size, navigate to '*Generate New Private key and Self-Signed Certificate'* section and change the '*Private Key Size*' to 2048 and then click on '*Generate Private key'* button. After entering the necessary information, click on '*Create CSR*' button. Example CSR page is below.

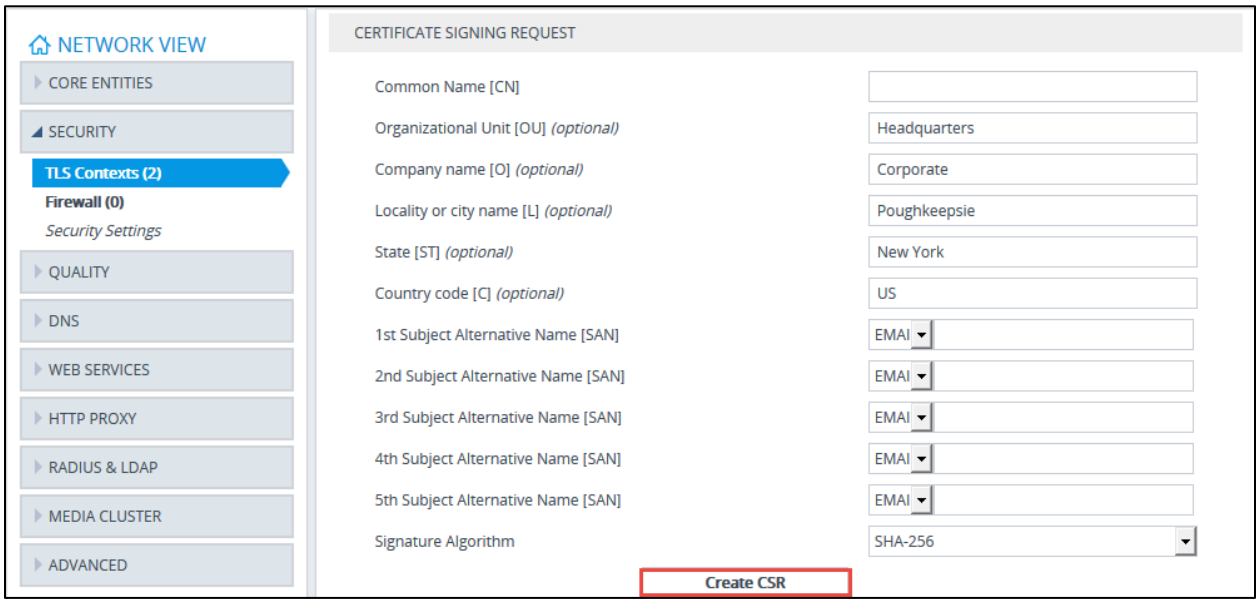

Figure 51: Generate CSR page

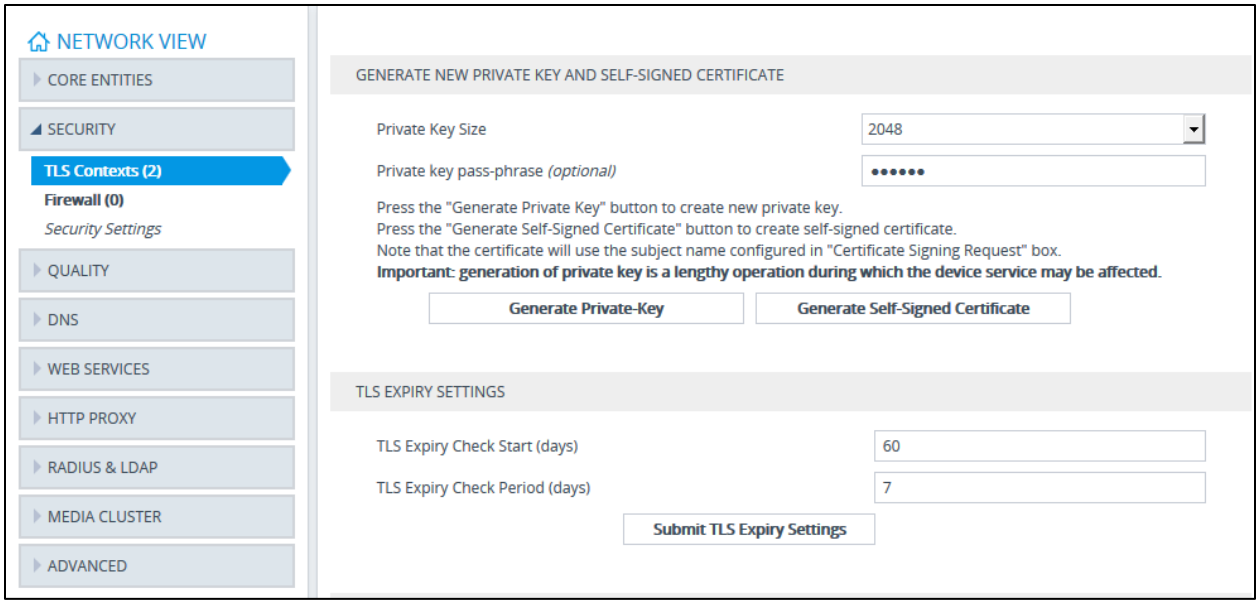

Figure 52: Generate CSR page continuation

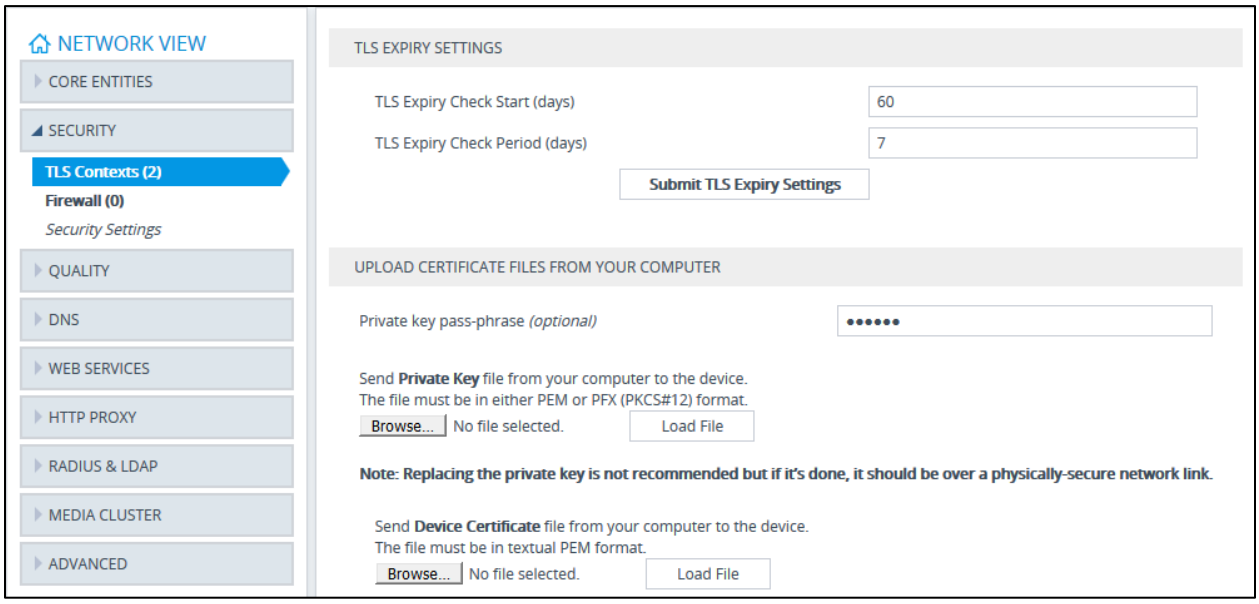

Figure 53: Generate CSR page continuation

After obtaining the signed certificate and trusted root/intermediate certificate from Certificate Authority, install the certificate. In the TLS context page for MS Teams, click on '*Browse'* button under '*Upload Certificate files from your computer*' section for *'Send Device Certificate'.* Select the signed certificate and click on '*Load File*' button to upload the certificate in SBC.

Next upload the trusted root/intermediate certificate provided by Certificate Authority. In the TLS Contexts page for MS Teams, click on 'Trusted Root

Certificates' link located at the bottom. Click on *'Import'* button to add the root/intermediate certificates.

Baltimore trusted root certificate has to be installed as trusted root certificate since Microsoft Teams certificate are signed by Baltimore CyberTrust Root.

To configure media security, navigate to '*SETUP*' and select '*SIGNALING & MEDIA'*. Expand '*MEDIA*' and click on '*Media Security'*. Under General section, set *Media Security* as Enable.

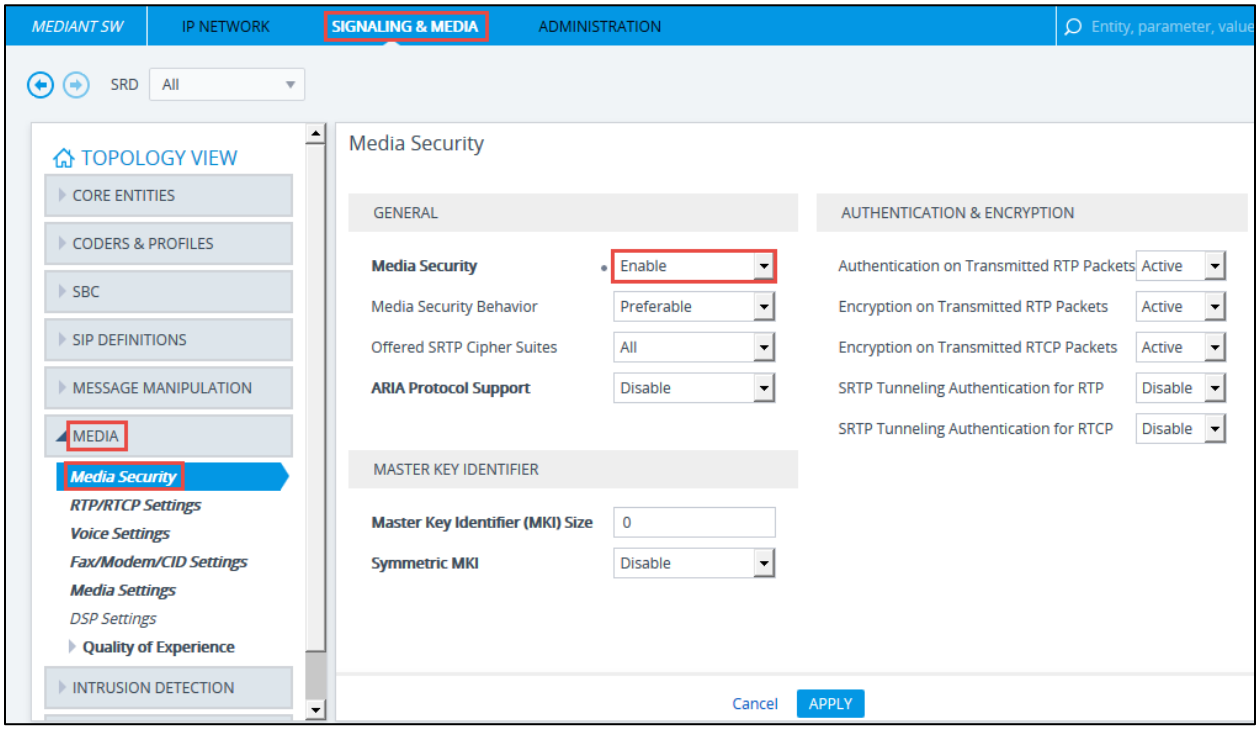

Figure 54: Media Security

In the IP Profile for Amazon Chime Voice Connector SRTP has to be enabled for TLS based test scenario.

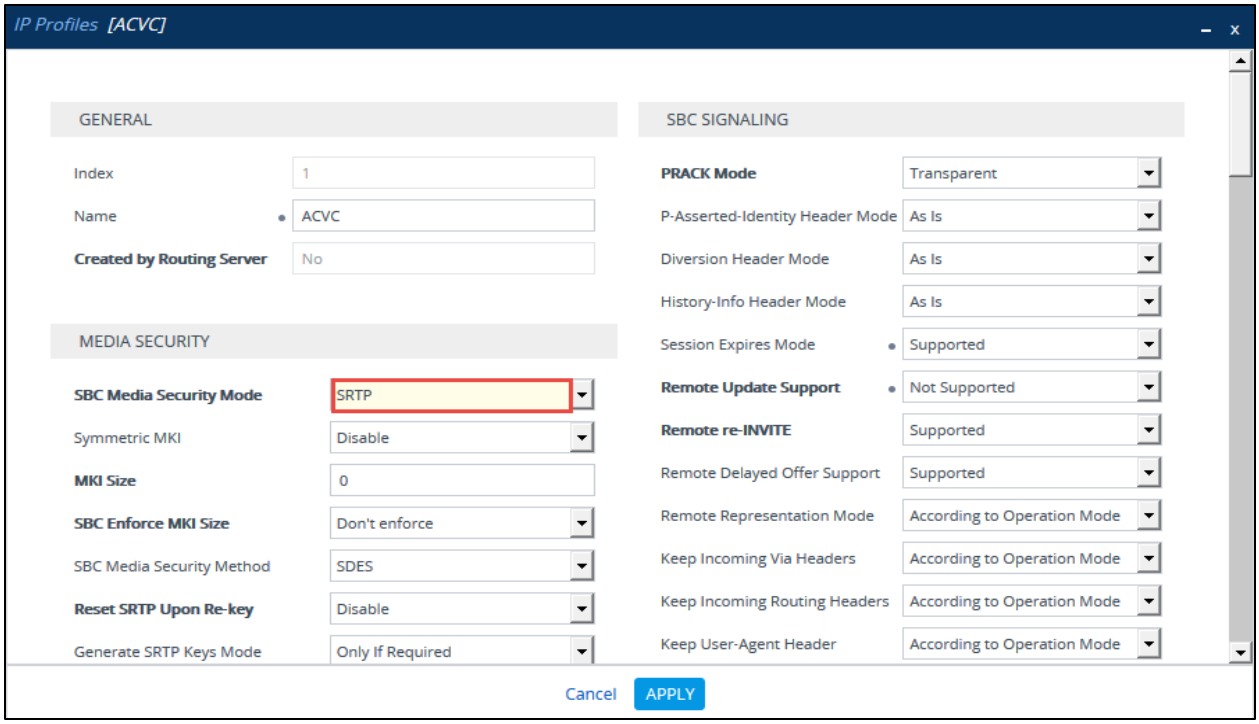

Figure 55: SRTP option in IP Profile

4.3.11 Message Manipulation configuration

SIP message manipulation rules are created to modify SIP headers for each IP entity based on manipulation sets enabled in IP Groups. The following are the message manipulation created for interoperability between MS Teams and Amazon Chime Voice Connector.

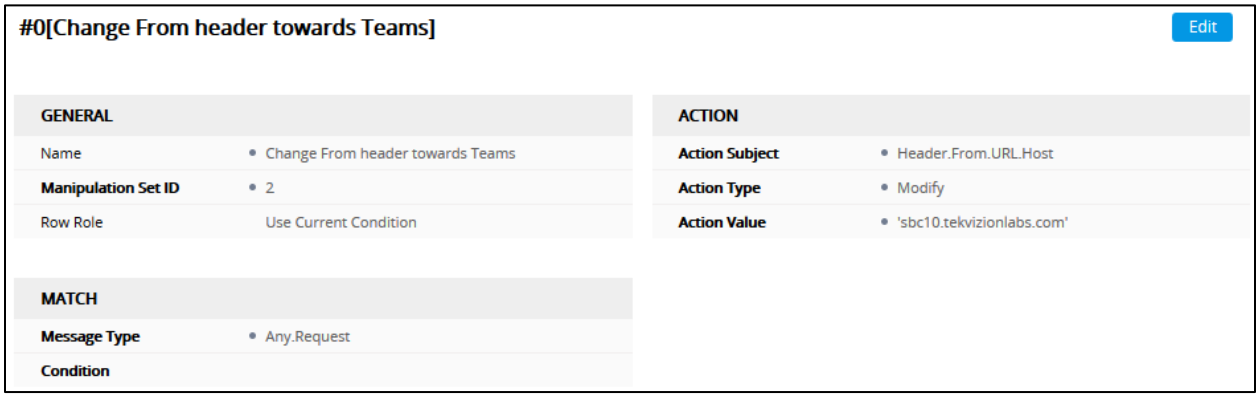

Figure 56: From header modification MS Teams

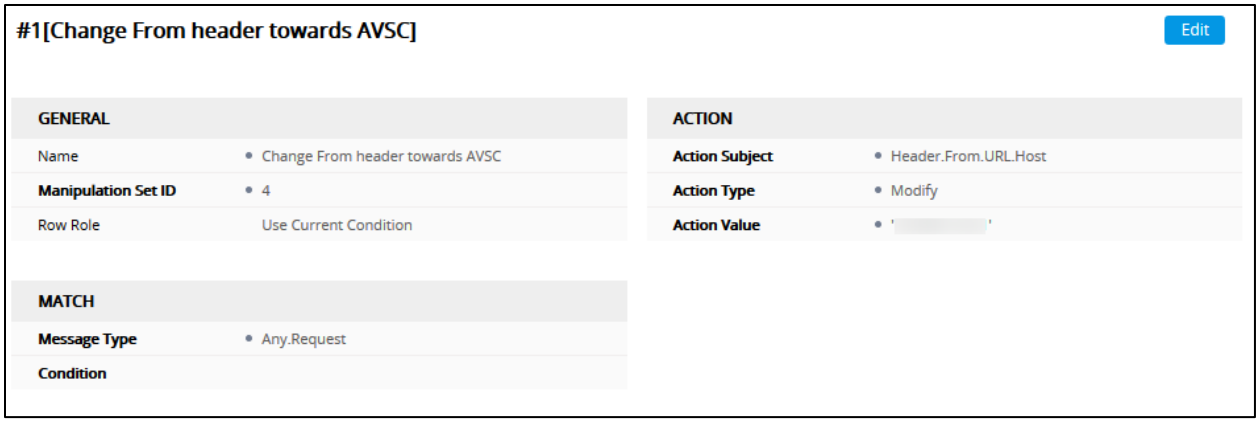

Figure 57: From header Modification Amazon Chime Voice Connector

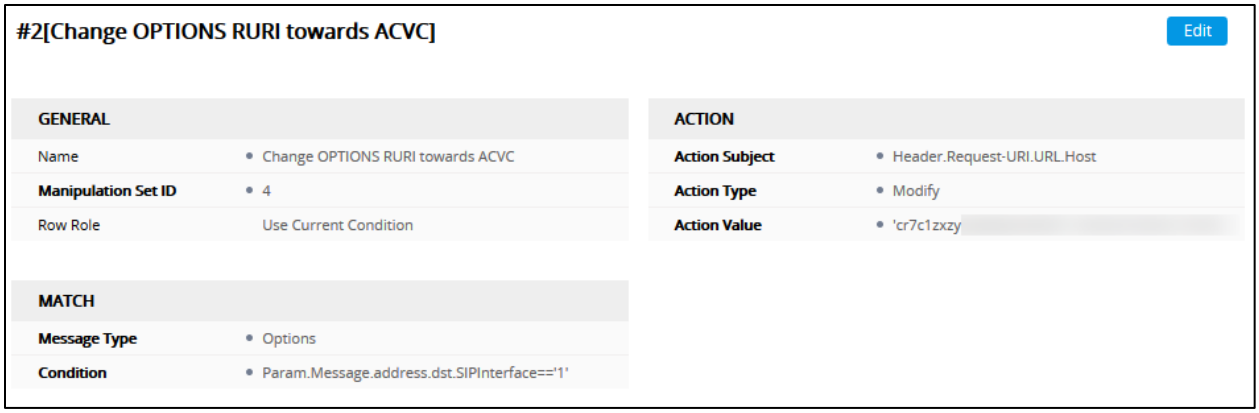

Figure 58: OPTIONS RURI modification

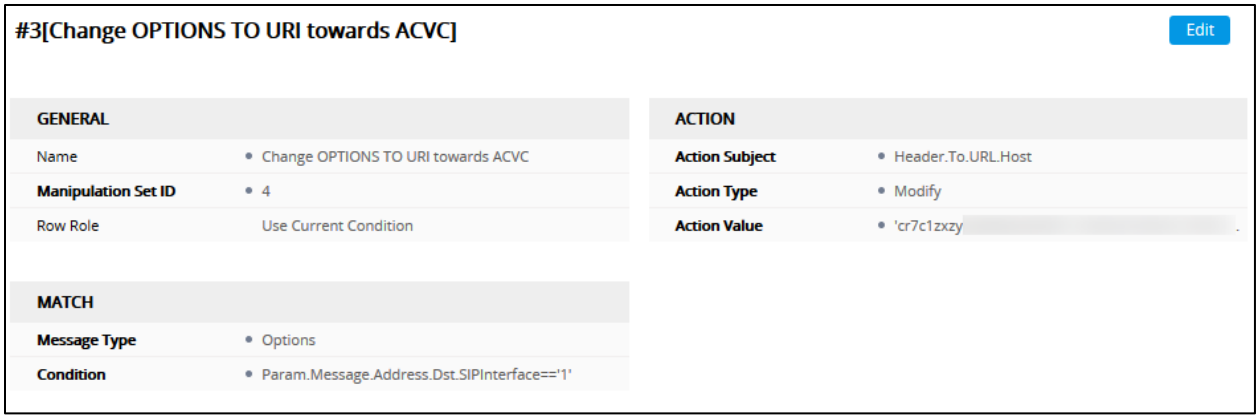

Figure 59: OPTIONS To header modification

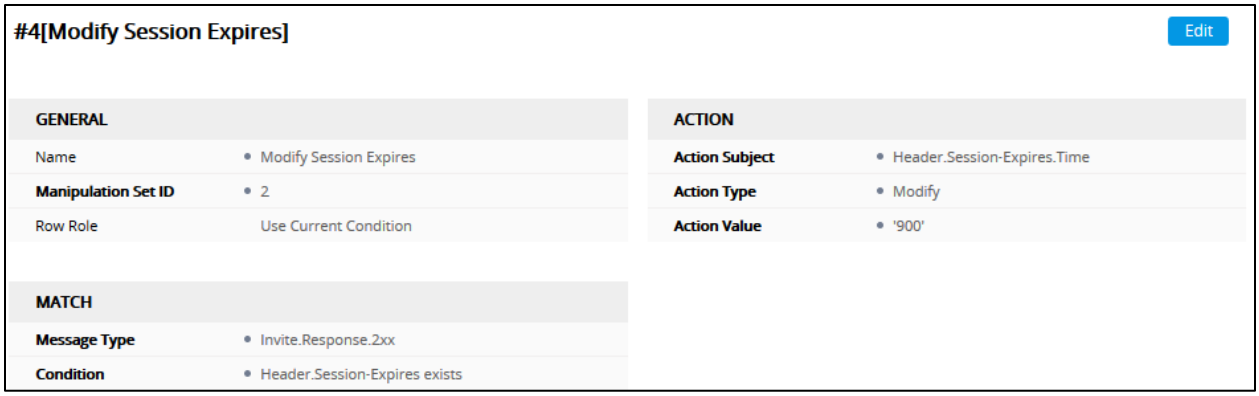

Figure 60: Session Expires value modification

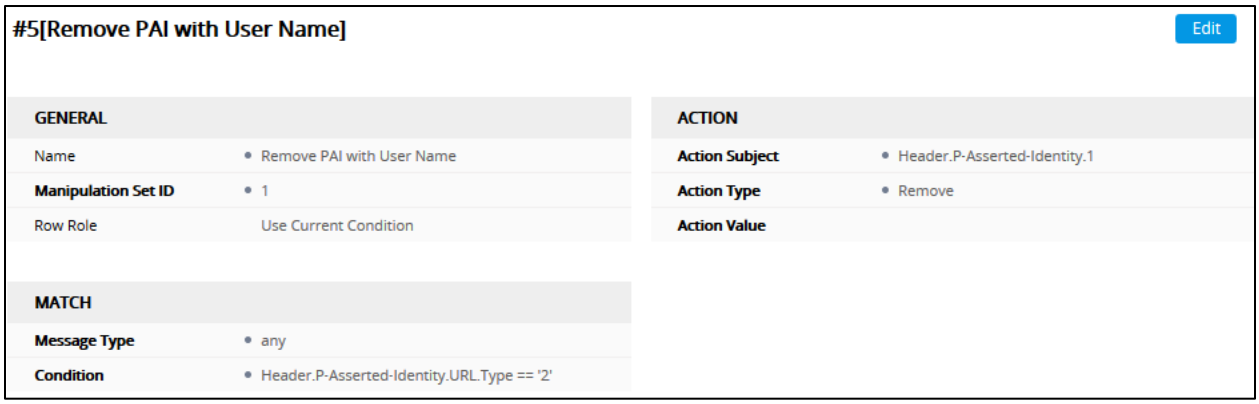

Figure 61: Remove PAI with SIP towards from MS Teams

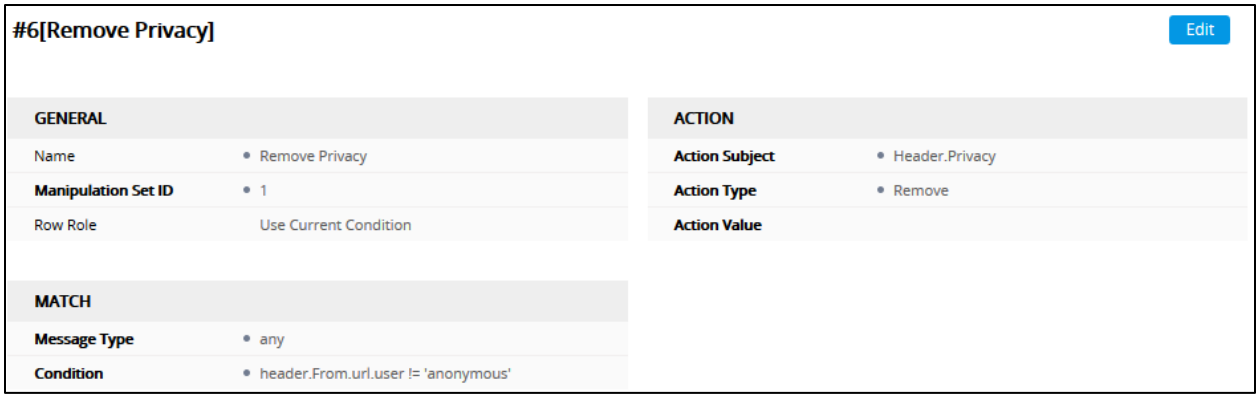

Figure 62: Remove Privacy from MS Teams