



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

1	Audience.....	5
1.1	Amazon Chime Voice Connector.....	6
2	SIP Trunking Network Components.....	7
2.1	Hardware Components.....	8
2.2	Software Requirements.....	8
3	Features.....	8
3.1	Features Supported.....	8
3.2	Features Not Supported.....	9
3.3	Features Not Tested.....	9
3.4	Caveats and Limitations.....	9
4	Configuration.....	10
4.1	Configuration Checklist.....	10
4.2	Microsoft Teams Configuration.....	10
4.2.1	Create Online PSTN Gateway.....	10
4.2.2	Configure Online PSTN Usage.....	11
4.2.3	Configure Online Voice Route.....	12
4.2.4	Configure Online Voice Routing Policy.....	12
4.2.5	Teams User Configuration.....	13
4.3	AudioCodes CE Configuration.....	13
4.3.1	Network IP Interface configuration.....	13
4.3.2	Media Realm configuration.....	13
4.3.3	SRD configuration.....	15
4.3.4	SIP Interface configuration.....	16
4.3.5	Proxy Sets configuration.....	19
4.3.6	IP Group Table configuration.....	21
4.3.7	Coder Groups configuration.....	25
4.3.8	IP Profile configuration.....	26
4.3.9	IP-to-IP Routing.....	32
4.3.10	TLS Configuration.....	34
4.3.11	Message Manipulation configuration.....	40

Table of Figures

Figure 1: Network Topology.....	7
Figure 2: Microsoft Teams-OnlinePSTNGateway.....	11
Figure 3: Microsoft Teams-Online PSTN Usage	11
Figure 4: Microsoft Teams-Online Voice Route	12
Figure 5: Microsoft Teams-Online Voice Routing Policy.....	12
Figure 6: IP Interfaces	13
Figure 7: Media Realms Table.....	14
Figure 8: Media Realm for MS Teams	14
Figure 9: Media Realm for Amazon Chime Voice Connector.....	15
Figure 10: Default SRD.....	15
Figure 11: SRD Table Details	16
Figure 12: SIP Interfaces.....	16
Figure 13: SIP Interface for MS Teams.....	17
Figure 14: SIP Interface for MS Teams Continuation	17
Figure 15: SIP Interface for Amazon Chime Voice Connector.....	18
Figure 16: SIP Interface for Amazon Chime Voice Connector Continuation.....	19
Figure 17: Proxy Sets table.....	19
Figure 18: Proxy Set table for MS Teams.....	20
Figure 19: Proxy Address for MS Teams.....	20
Figure 20: Proxy Set table for Amazon Chime Voice Connector	20
Figure 21: Proxy Address for Amazon Chime Voice Connector	21
Figure 22: IP Group Table	21
Figure 23: IP Group Table for MS Teams	22
Figure 24: IP Group table for MS Teams	22
Figure 25: IP Group table for MS Teams Continuation	23
Figure 26: IP Group table for Amazon Chime Voice Connector.....	24
Figure 27: IP Group table for Amazon Chime Voice Connector Continuation	24
Figure 28: IP Group table for Amazon Chime Voice Connector Continuation	25
Figure 29: Coder Groups.....	25
Figure 30: Allowed Audio Coders.....	26
Figure 31: IP Profiles	26
Figure 32: IP Profile for MS Teams	27
Figure 33: IP Profile for MS Teams Continuation.....	27
Figure 34: IP Profile for MS Teams Continuation.....	28
Figure 35: IP Profile for MS Teams Continuation.....	28
Figure 36: IP Profile for MS Teams Continuation.....	29
Figure 37: IP Profile for Amazon Chime Voice Connector	30
Figure 38: IP Profile for Amazon Chime Voice Connector Continuation	30
Figure 39: IP Profile for Amazon Chime Voice Connector Continuation	31
Figure 40: IP Profile for Amazon Chime Voice Connector Continuation	31
Figure 41: IP Profile for Amazon Chime Voice Connector Continuation	32

Figure 42: IP-to-IP Routing.....	32
Figure 43: IP-to-IP Routing for OPTIONS.....	33
Figure 44: IP-to-IP Routing from MS Teams to Amazon Chime Voice Connector.....	33
Figure 45: IP-to-IP Routing from Amazon Chime Voice Connector to MS Teams.....	34
Figure 46: TLS Context list.....	34
Figure 47: TLS Context for Amazon Chime Voice Connector.....	35
Figure 48: Trusted Root Certificate Import option.....	35
Figure 49: TLS Context for MS Teams	36
Figure 50: Change Certificate for MS Teams	37
Figure 51: Generate CSR page	37
Figure 52: Generate CSR page continuation.....	38
Figure 53: Generate CSR page continuation.....	38
Figure 54: Media Security.....	39
Figure 55: SRTP option in IP Profile.....	40
Figure 56: From header modification MS Teams.....	40
Figure 57: From header Modification Amazon Chime Voice Connector.....	41
Figure 58: OPTIONS RURI modification	41
Figure 59: OPTIONS To header modification	41
Figure 60: Session Expires value modification	42
Figure 61: Remove PAI with SIP towards from MS Teams.....	42
Figure 62: Remove Privacy from MS Teams	42

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

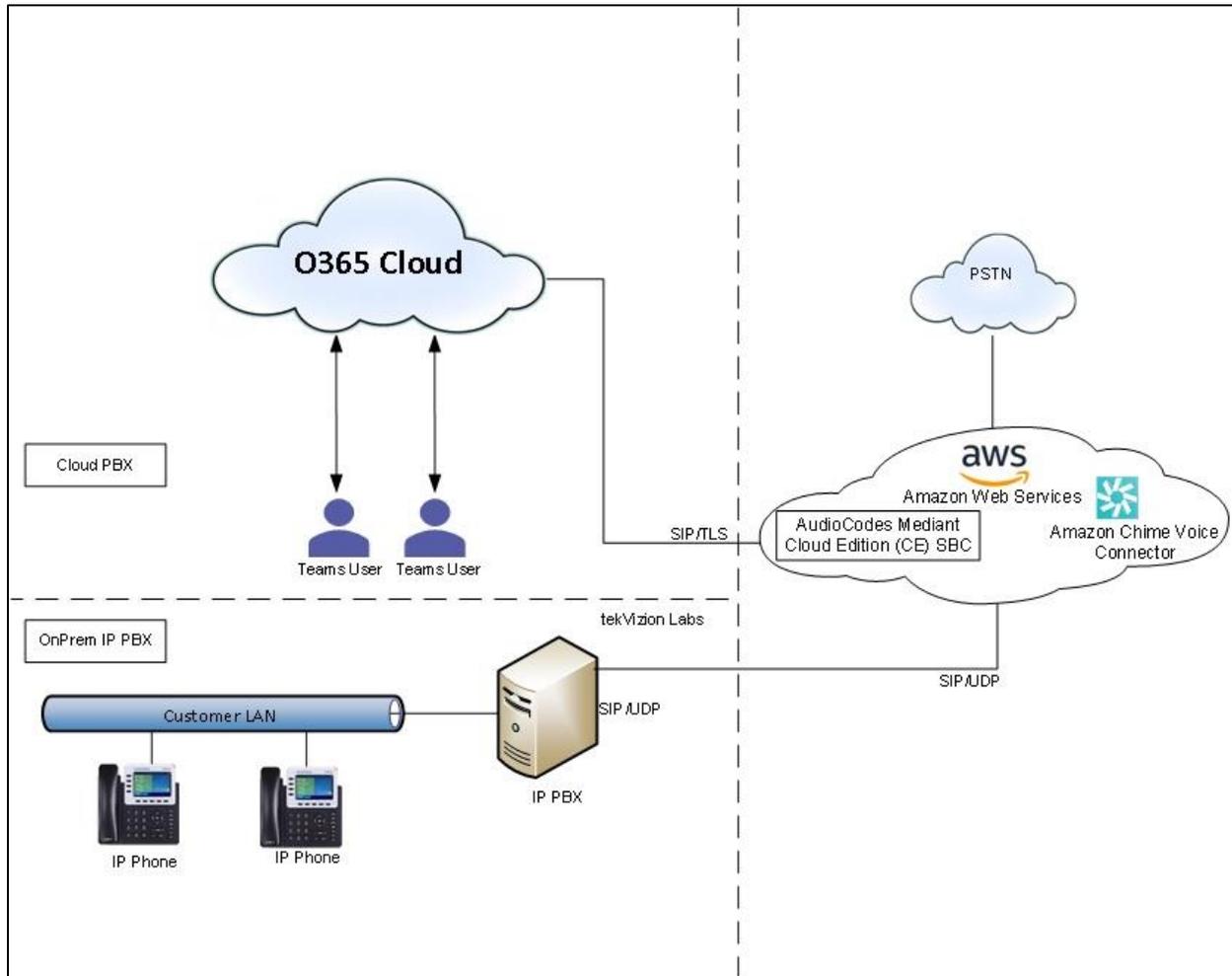


Figure 1: Network Topology

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

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

Identity           : sbc
Priority            : 5
Description        :
NumberPattern      : .*
OnlinePstnUsages   : {sbc }
OnlinePstnGatewayList : {sbc }
Name               : sbc
```

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.

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

Identity           : Tag:sbc
OnlinePstnUsages   : {sbc }
Description        :
RouteType          : BYOT
```

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.

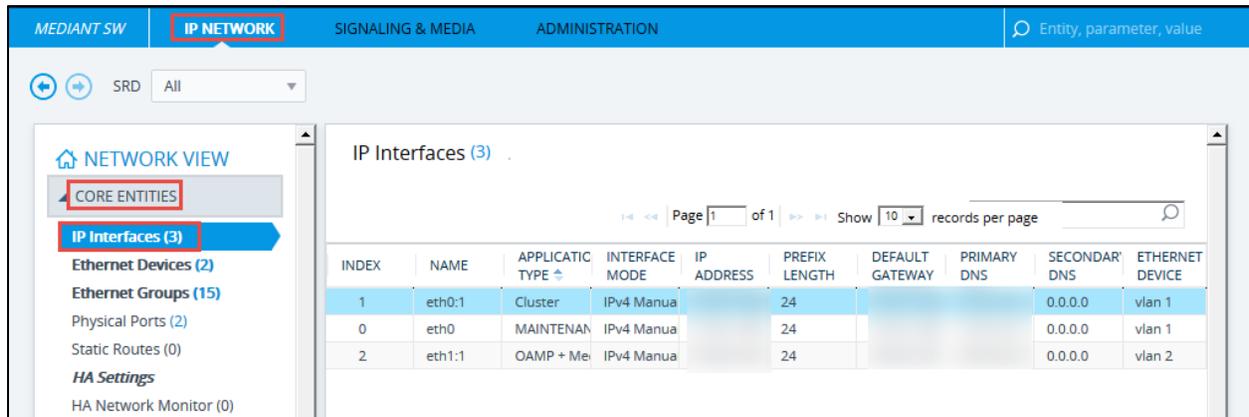


Figure 6: IP Interfaces

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'.

INDEX	NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	Teams_MR	6000	100	6399	Yes
1	ACVC_MR	7000	100	7399	No

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.

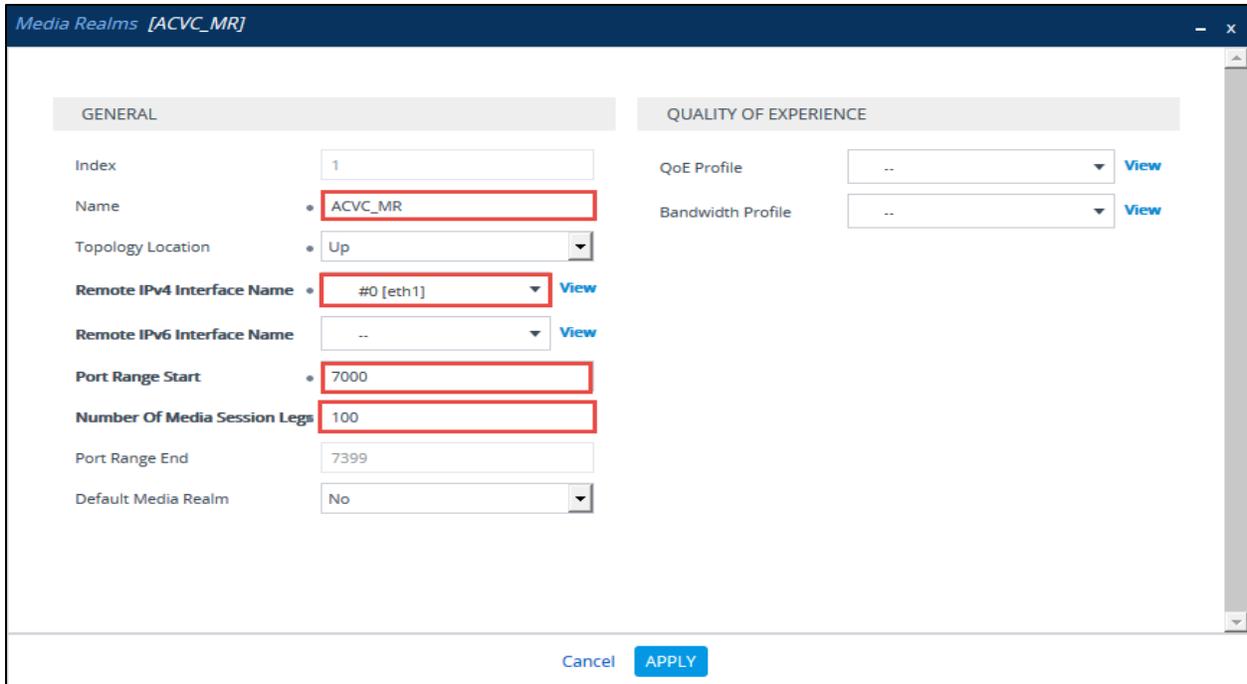


Figure 9: Media Realm for Amazon Chime Voice Connector

4.3.3 SRD configuration

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

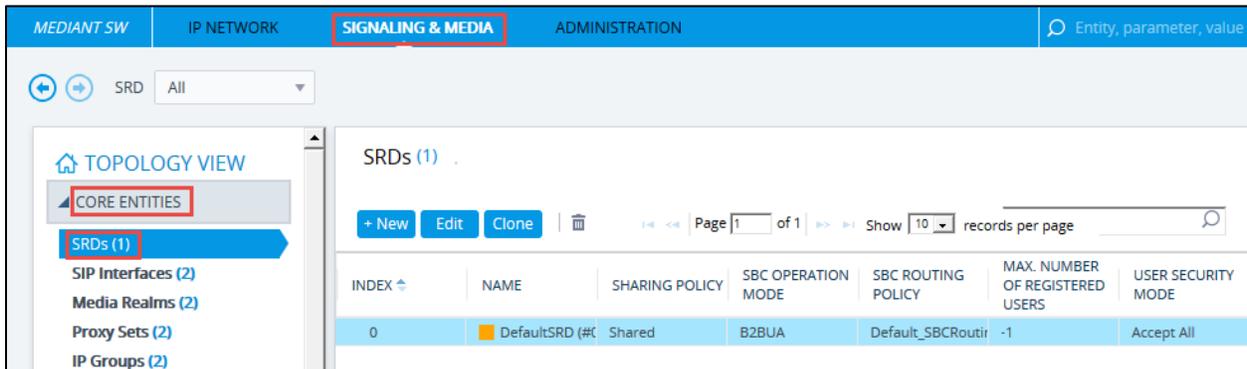


Figure 10: Default SRD

The default SRD configuration is used.

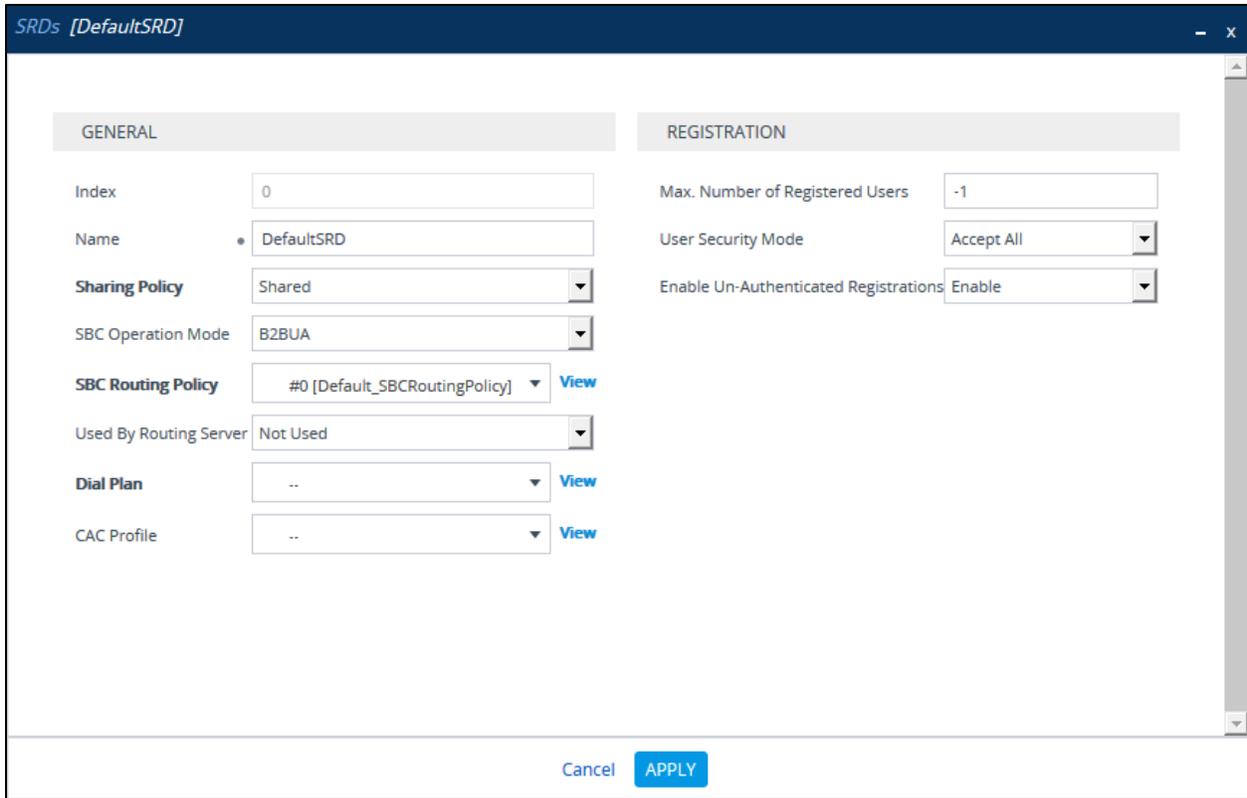


Figure 11: SRD Table Details

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.

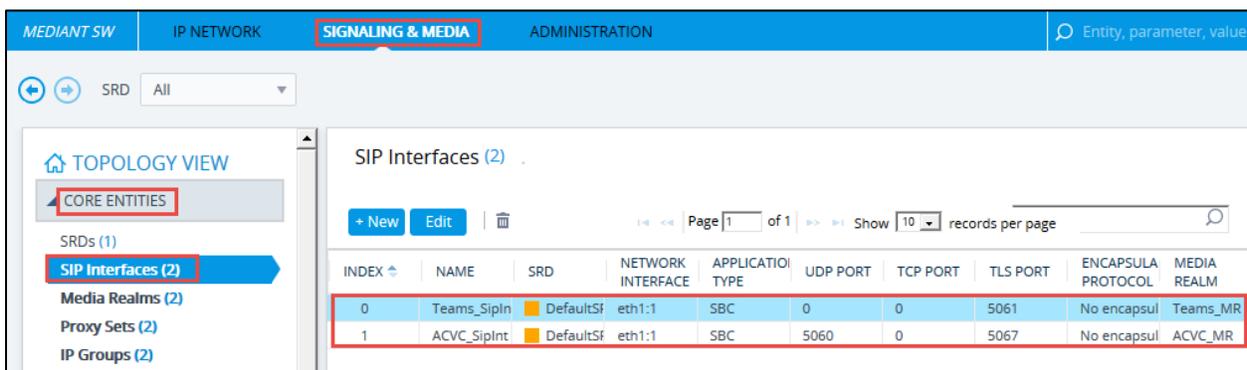


Figure 12: SIP Interfaces

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.

SIP Interfaces [Teams_Siplnt]

SRD: #0 [DefaultSRD]

GENERAL	MEDIA
Index: 0	Media Realm: #0 [Teams_MR] View
Name: Teams_Siplnt	Direct Media: Disable
Topology Location: Down	
Network Interface: #2 [eth1:1] View	
Application Type: SBC	
UDP Port: 0	
TCP Port: 0	
TLS Port: 5061	
Additional UDP Ports:	
Additional UDP Ports Mode: Always Open	
	SECURITY
	TLS Context Name: #1 [Teams] View
	TLS Mutual Authentication: Enable
	Message Policy: .. View
	User Security Mode: Not Configured
	Enable Un-Authenticated Registrations: Not configured
	Max. Number of Registered Users: -1

Cancel APPLY

Figure 13: SIP Interface for MS Teams

SIP Interfaces [Teams_Siplnt]

TCP Port: 0	Message Policy: .. View
TLS Port: 5061	User Security Mode: Not Configured
Additional UDP Ports:	Enable Un-Authenticated Registrations: Not configured
Additional UDP Ports Mode: Always Open	Max. Number of Registered Users: -1
Encapsulating Protocol: No encapsulation	
Enable TCP Keepalive: Disable	
Used By Routing Server: Not Used	
Pre-Parsing Manipulation Set: .. View	
CAC Profile: .. View	
CLASSIFICATION	
Classification Failure Response Type: 500	
Pre-classification Manipulation Set ID: -1	
Call Setup Rules Set ID: -1	

Cancel APPLY

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.

SIP Interfaces [ACVC_SipInt]

SRD #0 [DefaultSRD]

GENERAL

Index: 1

Name: ACVC_SipInt

Topology Location: Up

Network Interface: #2 [eth1:1]

Application Type: SBC

UDP Port: 5060

TCP Port: 0

TLS Port: 5067

Additional UDP Ports:

Additional UDP Ports Mode: Always Open

MEDIA

Media Realm: #1 [ACVC_MR]

Direct Media: Disable

SECURITY

TLS Context Name: ..

TLS Mutual Authentication:

Message Policy: ..

User Security Mode: Not Configured

Enable Un-Authenticated Registrations: Not configured

Max. Number of Registered Users: -1

Cancel APPLY

Figure 15: SIP Interface for Amazon Chime Voice Connector

SIP Interfaces [ACVC_SipInt]

TCP Port: 0

TLS Port: 5067

Additional UDP Ports:

Additional UDP Ports Mode: Always Open

Encapsulating Protocol: No encapsulation

Enable TCP Keepalive: Disable

Used By Routing Server: Not Used

Pre-Parsing Manipulation Set: ..

CAC Profile: ..

CLASSIFICATION

Classification Failure Response Type: 500

Pre-classification Manipulation Set ID: -1

Call Setup Rules Set ID: -1

Message Policy: ..

User Security Mode: Not Configured

Enable Un-Authenticated Registrations: Not configured

Max. Number of Registered Users: -1

Cancel APPLY

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.

INDEX	NAME	SRD	SBC IPv4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	Teams_ProxySet	DefaultSRD (#0)	Teams_SipInt	60		Enable
1	ACVC_ProxySet	DefaultSRD (#0)	ACVC_SipInt	60		Disable

Figure 17: Proxy Sets table

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

SRD: #0 [DefaultSRD]

GENERAL

Index: 0

Name: Teams_ProxySet

SBC IPv4 SIP Interface: #0 [Teams_SipInt] [View](#)

TLS Context Name: #1 [Teams] [View](#)

KEEP ALIVE

Proxy Keep-Alive: Using OPTIONS

Proxy Keep-Alive Time [sec]: 60

Keep-Alive Failure Responses:

Success Detection Retries: 1

REDUNDANCY

Redundancy Mode:

Proxy Hot Swap: Enable

Proxy Load Balancing Method: Random Weights

Min. Active Servers for Load Balancing: 1

ADVANCED

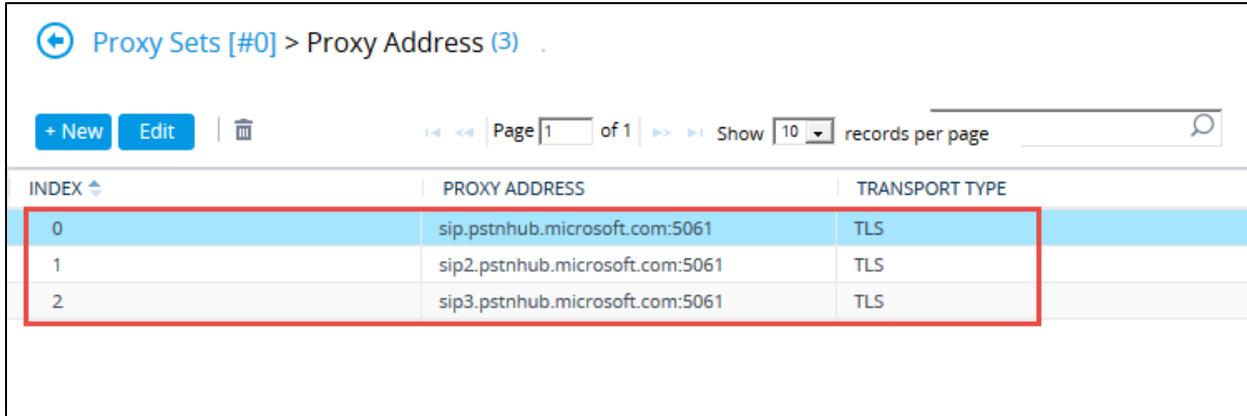
Classification Input: IP Address only

DNS Resolve Method:

Buttons: Cancel, APPLY

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

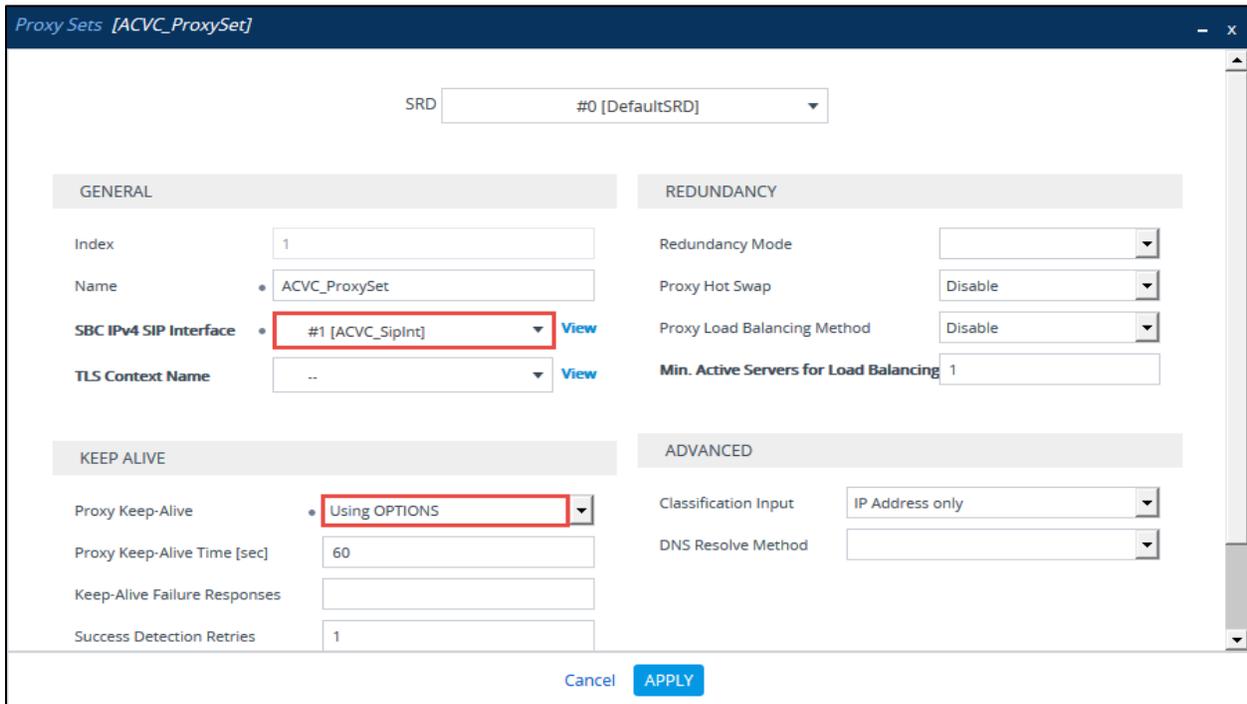


The screenshot shows a web interface for managing Proxy Sets. At the top, there is a breadcrumb 'Proxy Sets [#0] > Proxy Address (3)'. Below this are navigation buttons: '+ New', 'Edit', and a trash icon. A pagination bar shows 'Page 1 of 1' and 'Show 10 records per page'. The main content is a table with three columns: INDEX, PROXY ADDRESS, and TRANSPORT TYPE. The table contains three rows, with the first row (index 0) highlighted in light blue and enclosed in a red rectangular box.

INDEX	PROXY ADDRESS	TRANSPORT TYPE
0	sip.pstnhub.microsoft.com:5061	TLS
1	sip2.pstnhub.microsoft.com:5061	TLS
2	sip3.pstnhub.microsoft.com:5061	TLS

Figure 19: Proxy Address for MS Teams

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



The screenshot shows the configuration page for a Proxy Set named 'ACVC_ProxySet'. At the top, there is a dropdown for 'SRD' set to '#0 [DefaultSRD]'. The configuration is divided into several sections: GENERAL, REDUNDANCY, KEEP ALIVE, and ADVANCED. In the GENERAL section, 'SBC IPv4 SIP Interface' is set to '#1 [ACVC_SipInt]' and is highlighted with a red box. In the KEEP ALIVE section, 'Proxy Keep-Alive' is set to 'Using OPTIONS' and is also highlighted with a red box. Other settings include 'Index' (1), 'Name' (ACVC_ProxySet), 'TLS Context Name' (..), 'Redundancy Mode', 'Proxy Hot Swap' (Disable), 'Proxy Load Balancing Method' (Disable), 'Min. Active Servers for Load Balancing' (1), 'Classification Input' (IP Address only), and 'DNS Resolve Method'. At the bottom, there are 'Cancel' and 'APPLY' buttons.

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.

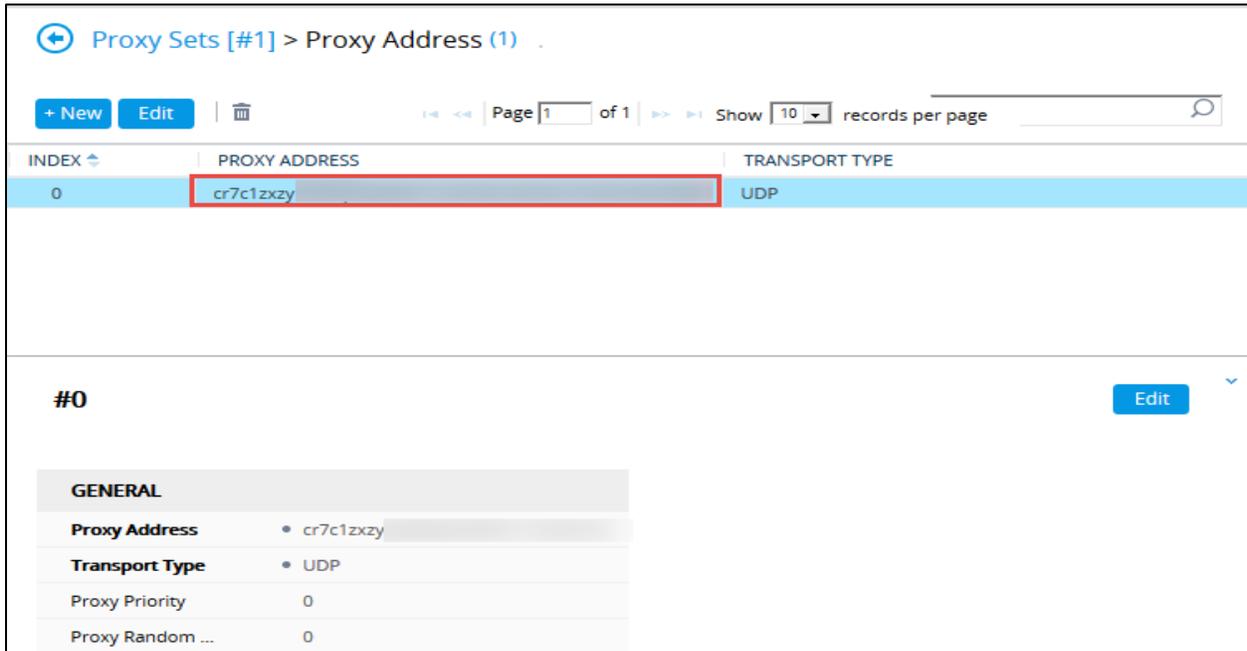


Figure 21: Proxy Address for Amazon Chime Voice Connector

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.

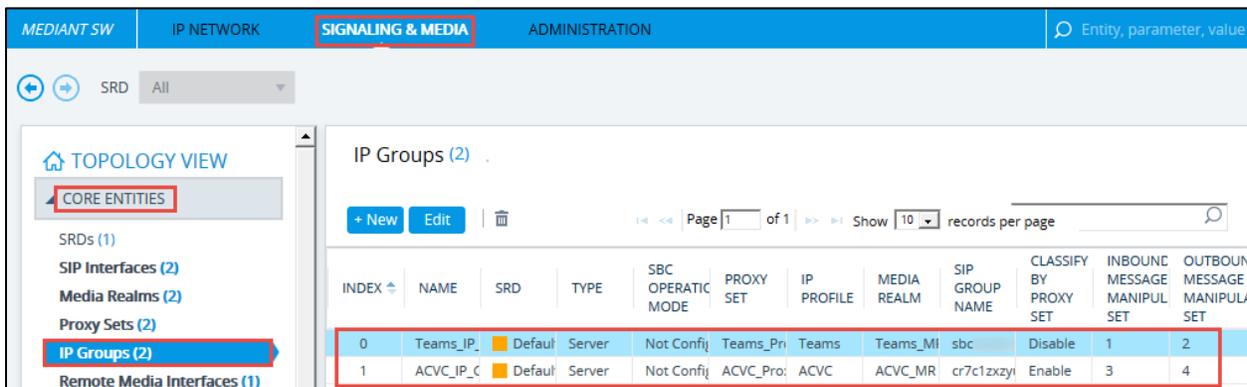


Figure 22: IP Group Table

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.

IP Groups [Teams_IP_Grp] - x

SRD #0 [DefaultSRD]

GENERAL	QUALITY OF EXPERIENCE
Index: <input type="text" value="0"/>	QoE Profile: <input type="text" value=".."/> View
Name: <input type="text" value="Teams_IP_Grp"/>	Bandwidth Profile: <input type="text" value=".."/> View
Topology Location: <input type="text" value="Down"/>	
Type: <input type="text" value="Server"/>	
Proxy Set: #0 [Teams_ProxySet] View	
IP Profile: #0 [Teams] View	
Media Realm: #0 [Teams_MR] View	
Contact User: <input type="text"/>	
SIP Group Name: <input type="text" value="sbc"/>	
Created By Routing Server: <input type="text" value="No"/>	

Cancel APPLY

Figure 23: IP Group Table for MS Teams

IP Groups [Teams_IP_Grp] - x

Used By Routing Server: <input type="text" value="Not Used"/>	
Proxy Set Connectivity: <input type="text" value="Connected"/>	
SBC GENERAL	SBC REGISTRATION AND AUTHENTICATION
Classify By Proxy Set: <input type="text" value="Disable"/>	Max. Number of Registered Users: <input type="text" value="-1"/>
SBC Operation Mode: <input type="text" value="Not Configured"/>	Registration Mode: <input type="text" value="User Initiates Registration"/>
SBC Client Forking Mode: <input type="text" value="Sequential"/>	User Stickiness: <input type="text" value="Disable"/>
CAC Profile: <input type="text" value=".."/> View	User UDP Port Assignment: <input type="text" value="Disable"/>
	Authentication Mode: <input type="text" value="User Authenticates"/>
ADVANCED	Authentication Method List: <input type="text"/>
Local Host Name: <input type="text" value="sbc"/>	SBC Server Authentication Type: <input type="text" value="According to Global Parameter"/>
UI Format: <input type="text" value="Disable"/>	OAuth HTTP Service: <input type="text" value=".."/> View
	Username: <input type="text"/>
	Password: <input type="text"/>
	GW GROUP STATUS
	GW Group Registered IP Address: <input type="text"/>

Cancel APPLY

Figure 24: IP Group table for MS Teams

The screenshot shows a configuration window for IP Groups. The title bar reads "IP Groups [Teams_IP_Grp]". The main area is divided into two columns. The left column contains the following settings:

- UUI Format: Disable
- Always Use Src Address: Yes
- SBC ADVANCED** (Section Header)
- Source URI Input: [Empty]
- Destination URI Input: [Empty]
- SIP Connect: No
- SBC PSAP Mode: Disable
- Route Using Request URI Port: Disable
- DTLS Context: .. (with a "View" link)
- Keep Original Call-ID: No
- Dial Plan: .. (with a "View" link)
- Call Setup Rules Set ID: -1
- Tags: [Empty]

The right column contains:

- GW Group Registered IP Address: [Empty]
- GW Group Registered Status: Not Registered

At the bottom of the window, there are two buttons: "Cancel" and "APPLY".

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.

IP Groups [ACVC_IP_Grp]

SRD #0 [DefaultSRD]

GENERAL		QUALITY OF EXPERIENCE	
Index	1	QoE Profile	.. View
Name	ACVC_IP_Grp	Bandwidth Profile	.. View
Topology Location	Up	MESSAGE MANIPULATION	
Type	Server	Inbound Message Manipulation Set	3
Proxy Set	#1 [ACVC_ProxySet] View	Outbound Message Manipulation Set	4
IP Profile	#1 [ACVC] View	Message Manipulation User-Defined String 1	
Media Realm	#1 [ACVC_MR] View	Message Manipulation User-Defined String 2	
Contact User		Proxy Keep-Alive using IP Group settings	Disable
SIP Group Name	cr7c1zxzyuaaeqeuews5s1.voiceconnector.cf		
Created By Routing Server	No		

Cancel APPLY

Figure 26: IP Group table for Amazon Chime Voice Connector

IP Groups [ACVC_IP_Grp]

Used By Routing Server Not Used

Proxy Set Connectivity Connected

SBC GENERAL		SBC REGISTRATION AND AUTHENTICATION	
Classify By Proxy Set	Enable	Max. Number of Registered Users	-1
SBC Operation Mode	Not Configured	Registration Mode	User Initiates Registration
SBC Client Forking Mode	Sequential	User Stickiness	Disable
CAC Profile	.. View	User UDP Port Assignment	Disable
ADVANCED		Authentication Mode	SBC as Client
Local Host Name		Authentication Method List	
UUI Format	Disable	SBC Server Authentication Type	According to Global Parameter
		OAuth HTTP Service	.. View
		Username	
		Password	
		GW GROUP STATUS	
		GW Group Registered IP Address	

Cancel APPLY

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

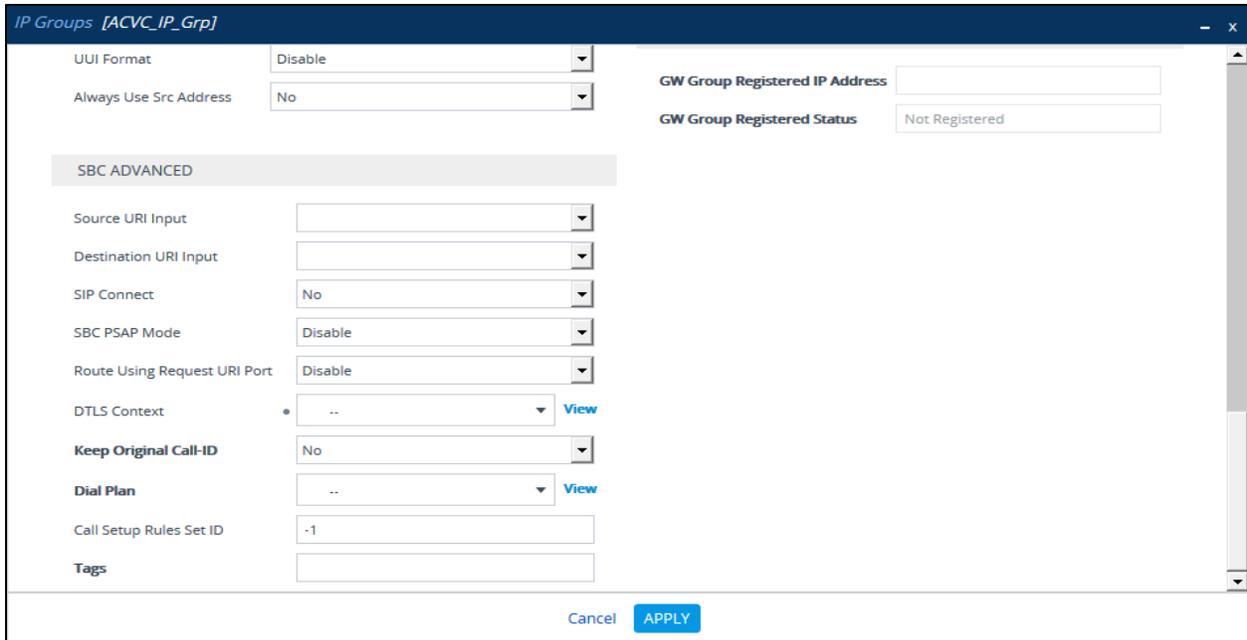


Figure 28: IP Group table for Amazon Chime Voice Connector Continuation

4.3.7 Coder Groups configuration

Navigate to 'SETUP' and select 'SIGNALING & MEDIA'. Expand 'CODERS & PROFILES' and select 'Coder Groups'. G.711 U-law is configured in Coder Groups.

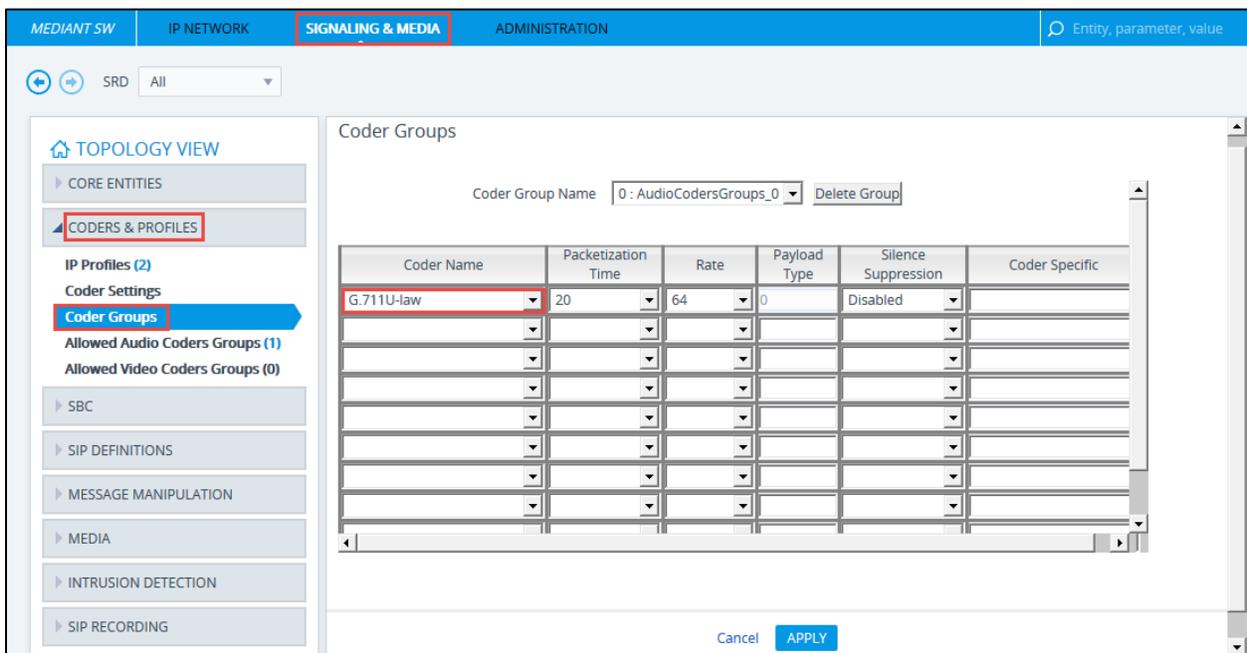


Figure 29: Coder Groups

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.

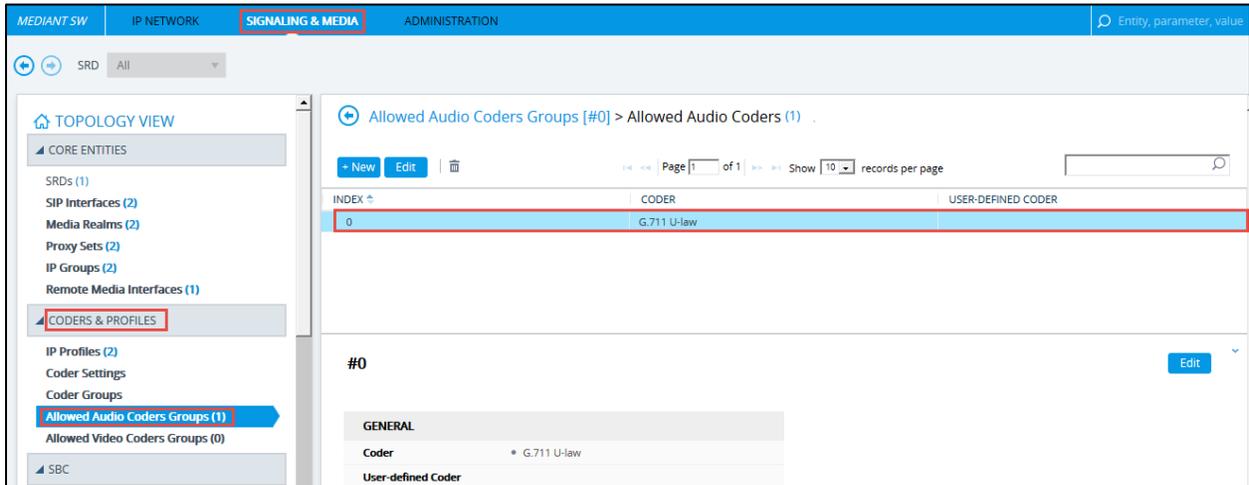


Figure 30: Allowed Audio Coders

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.

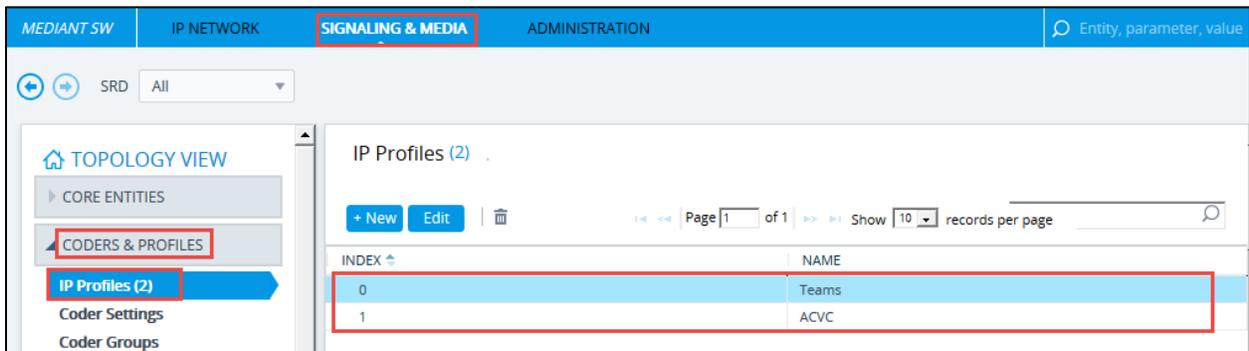


Figure 31: IP Profiles

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.

IP Profiles [Teams]

GENERAL	SBC SIGNALING
Index: 0	PRACK Mode : Transparent
Name: Teams	P-Asserted-Identity Header Mode: As Is
Created by Routing Server: No	Diversion Header Mode: As Is
MEDIA SECURITY	
SBC Media Security Mode : SRTP	History-Info Header Mode: As Is
Symmetric MKI: Disable	Session Expires Mode: Supported
MKI Size: 0	Remote Update Support : Supported
SBC Enforce MKI Size : Don't enforce	Remote re-INVITE : Supported only with SDP
SBC Media Security Method: SDES	Remote Delayed Offer Support: Not Supported
Reset SRTP Upon Re-key : Disable	Remote Representation Mode: According to Operation Mode
Generate SRTP Keys Mode: Only If Required	Keep Incoming Via Headers: According to Operation Mode
SBC Remove Crypto Lifetime in SDP: No	Keep Incoming Routing Headers: According to Operation Mode
	Keep User-Agent Header: According to Operation Mode
	Handle X-Detect: No

Cancel APPLY

Figure 32: IP Profile for MS Teams

IP Profiles [Teams]

SBC Remove Unknown Crypto: No	ISUP Body Handling: Transparent	
SBC EARLY MEDIA		
Remote Early Media : Supported	ISUP Variant: Itu92	
Remote Multiple 18x : Supported	Max Call Duration [min]: 0	
Remote Early Media Response Type: Transparent	SBC REGISTRATION	
Remote Multiple Early Dialogs: According to Operation Mode	User Registration Time: 0	
Remote Multiple Answers Mode: Disable	NAT UDP Registration Time: -1	
Remote Early Media RTP Detection Mode : By Media	NAT TCP Registration Time: -1	
Remote RFC 3960 Support: Not Supported	SBC FORWARD AND TRANSFER	
Remote Can Play Ringback: Yes	Remote REFER Mode : Regular	
Generate RTP: None	Remote Replaces Mode: Standard	
SBC MEDIA		Play RBT To Transferee: No
	Remote 3xx Mode : Transparent	

Cancel APPLY

Figure 33: IP Profile for MS Teams Continuation

IP Profiles [Teams]

Mediation Mode	RTP Mediation	
Extension Coders Group	#0 [AudioCodersGroups_0]	
Allowed Audio Coders	#0 [G711]	View
Allowed Coders Mode	Restriction	
Allowed Video Coders	..	View
Allowed Media Types		
Direct Media Tag		
RFC 2833 Mode	As Is	
RFC 2833 DTMF Payload Type	0	
Alternative DTMF Method	As Is	
Send Multiple DTMF Methods	Disable	
Adapt RFC2833 BW to Voice coder BW	Disabled	
SDP Ptime Answer	Remote Answer	
Preferred PTime	0	

SBC HOLD	
Remote Hold Format	Transparent
Reliable Held Tone Source	Yes
Play Held Tone	No
SBC FAX	
Fax Coders Group	..
Fax Mode	As Is
Fax Offer Mode	All coders
Fax Answer Mode	Single coder
Remote Renegotiate on Fax Detection	Transparent
Fax Rerouting Mode	Disable

Cancel APPLY

Figure 34: IP Profile for MS Teams Continuation

IP Profiles [Teams]

Preferred PTime	0
Use Silence Suppression	Transparent
RTP Redundancy Mode	As Is
RTCP Mode	Transparent
Jitter Compensation	Disable
ICE Mode	Disable
SDP Handle RTCP	Don't Care
RTCP Mux	Not Supported
RTCP Feedback	Feedback Off
Voice Quality Enhancement	Disable
Max Opus Bandwidth	0
Generate No-op	No
Enhanced PLC	Disable

MEDIA	
Broken Connection Mode	Disconnect
Media IP Version Preference	Only IPv4
RTP Redundancy Depth	Disable
LOCAL TONES	
Local RingBack Tone Index	-1
Local Held Tone Index	-1

Cancel APPLY

Figure 35: IP Profile for MS Teams Continuation

The screenshot shows a configuration window titled "IP Profiles [Teams]". It is divided into three sections: "QUALITY OF SERVICE", "JITTER BUFFER", and "VOICE".

- QUALITY OF SERVICE:**
 - RTP IP DiffServ: 46
 - Signaling DiffServ: 24
- JITTER BUFFER:**
 - Dynamic Jitter Buffer Minimum Delay [msec]: 10
 - Dynamic Jitter Buffer Optimization Factor: 10
 - Jitter Buffer Max Delay [msec]: 300
- VOICE:**
 - Echo Canceler: Line (dropdown menu)
 - Input Gain (-32 to 31 dB): 0
 - Voice Volume (-32 to 31 dB): 0

At the bottom of the window, there are two buttons: "Cancel" and "APPLY".

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.

IP Profiles [ACVC]

GENERAL	SBC SIGNALING
Index: 1	PRACK Mode : Transparent
Name: ACVC	P-Asserted-Identity Header Mode: As Is
Created by Routing Server: No	Diversion Header Mode: As Is
	History-Info Header Mode: As Is
	Session Expires Mode: Not Supported
MEDIA SECURITY	Remote Update Support : Not Supported
SBC Media Security Mode : RTP	Remote re-INVITE : Supported
Symmetric MKI: Disable	Remote Delayed Offer Support: Supported
MKI Size: 0	Remote Representation Mode: According to Operation Mode
SBC Enforce MKI Size : Don't enforce	Keep Incoming Via Headers: According to Operation Mode
SBC Media Security Method: SDES	Keep Incoming Routing Headers: According to Operation Mode
Reset SRTP Upon Re-key : Disable	Keep User-Agent Header: According to Operation Mode
Generate SRTP Keys Mode: Only If Required	

Cancel APPLY

Figure 37: IP Profile for Amazon Chime Voice Connector

IP Profiles [ACVC]

SBC Remove Crypto Lifetime in SDP: No	Handle X-Detect: No
SBC Remove Unknown Crypto: No	ISUP Body Handling: Transparent
	ISUP Variant: Itu92
	Max Call Duration [min]: 0
SBC EARLY MEDIA	SBC REGISTRATION
Remote Early Media : Supported	User Registration Time: 0
Remote Multiple 18x : Not Supported	NAT UDP Registration Time: -1
Remote Early Media Response Type: Transparent	NAT TCP Registration Time: -1
Remote Multiple Early Dialogs: According to Operation Mode	
Remote Multiple Answers Mode: Disable	SBC FORWARD AND TRANSFER
Remote Early Media RTP Detection Mode : By Signaling	Remote REFER Mode : Regular
Remote RFC 3960 Support: Not Supported	Remote Replaces Mode: Standard
Remote Can Play Ringback: Yes	Play RBT To Transferee: No
Generate RTP: None	

Cancel APPLY

Figure 38: IP Profile for Amazon Chime Voice Connector Continuation

IP Profiles [ACVC]

SBC MEDIA

Mediation Mode: RTP Mediation

Extension Coders Group: #0 [AudioCodersGroups_0]

Allowed Audio Coders: #0 [G711] [View](#)

Allowed Coders Mode: Restriction

Allowed Video Coders: .. [View](#)

Allowed Media Types:

Direct Media Tag:

RFC 2833 Mode: As Is

RFC 2833 DTMF Payload Type: 0

Alternative DTMF Method: As Is

Send Multiple DTMF Methods: Disable

Adapt RFC2833 BW to Voice coder BW: Disabled

SDP Ptime Answer: Remote Answer

Remote 3xx Mode: Transparent

SBC HOLD

Remote Hold Format: Transparent

Reliable Held Tone Source: Yes

Play Held Tone: No

SBC FAX

Fax Coders Group: ..

Fax Mode: As Is

Fax Offer Mode: All coders

Fax Answer Mode: Single coder

Remote Renegotiate on Fax Detection: Transparent

Fax Rerouting Mode: Disable

Cancel **APPLY**

Figure 39: IP Profile for Amazon Chime Voice Connector Continuation

IP Profiles [ACVC]

SDP Ptime Answer: Remote Answer

Preferred PTime: 0

Use Silence Suppression: Transparent

RTP Redundancy Mode: As Is

RTCP Mode: Transparent

Jitter Compensation: Disable

ICE Mode: Disable

SDP Handle RTCP: Don't Care

RTCP Mux: Not Supported

RTCP Feedback: Feedback Off

Voice Quality Enhancement: Disable

Max Opus Bandwidth: 0

Generate No-op: No

Enhanced PLC: Disable

Fax Rerouting Mode: Disable

MEDIA

Broken Connection Mode: Disconnect

Media IP Version Preference: Only IPv4

RTP Redundancy Depth: Disable

LOCAL TONES

Local RingBack Tone Index: -1

Local Held Tone Index: -1

Cancel **APPLY**

Figure 40: IP Profile for Amazon Chime Voice Connector Continuation

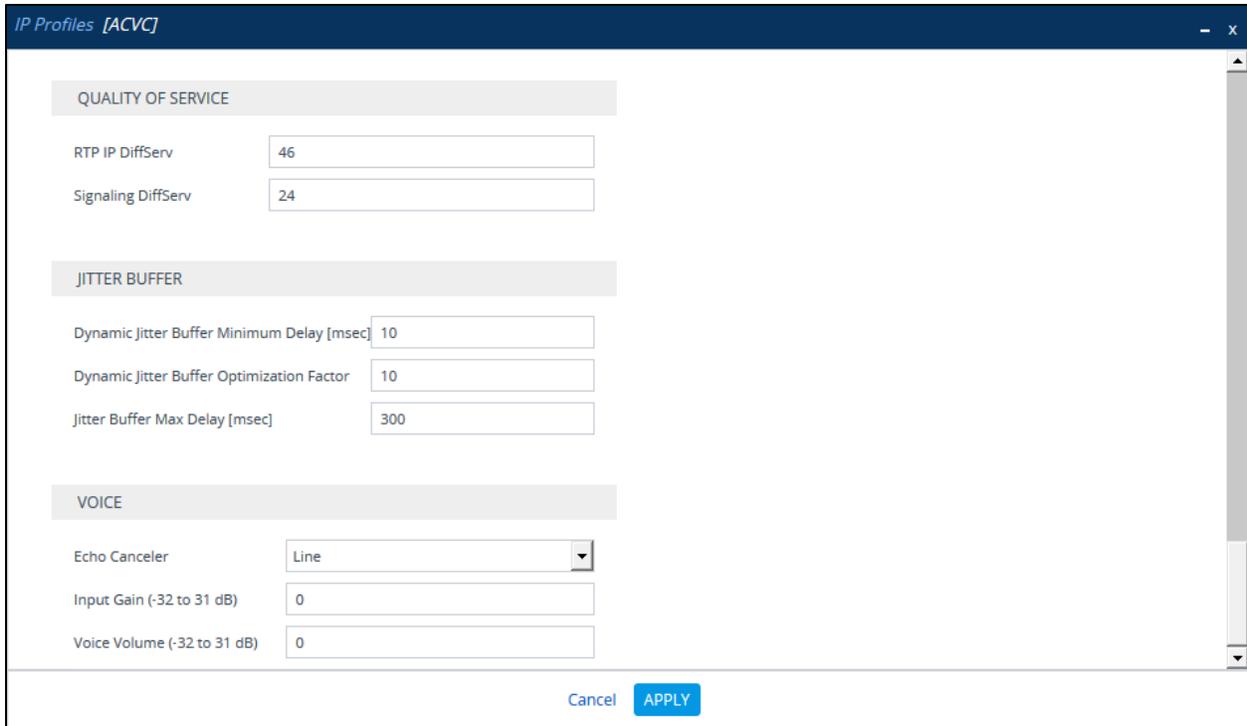


Figure 41: IP Profile for Amazon Chime Voice Connector Continuation

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.

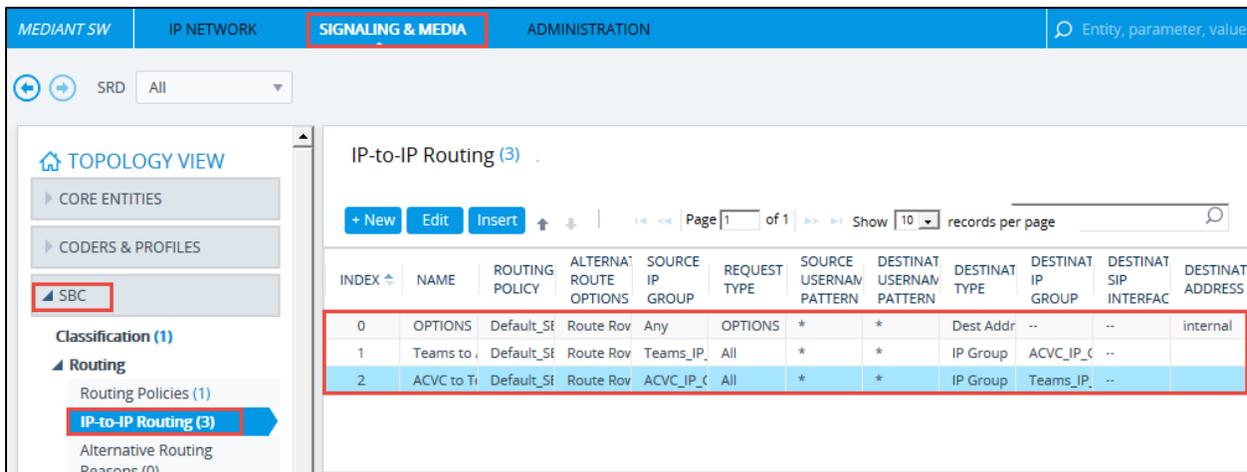


Figure 42: IP-to-IP Routing

IP to IP routing for OPTIONS message

#0[OPTIONS] Edit

GENERAL	
Name	• OPTIONS
Alternative Rout...	Route Row

MATCH	
Source IP Group	• Any View
Request Type	• OPTIONS
Source Userna...	*
Source Host	*
Source Tag	
Destination Use...	*
Destination Host	*
Destination Tag	
Message Condi...	-- View
Call Trigger	Any
ReRoute IP Group	• Any View

ACTION	
Destination Type	• Dest Address
Destination IP ...	-- View
Destination SIP ...	-- View
Destination Ad...	• internal
Destination Port	0
Destination Tra...	
IP Group Set	-- View
Call Setup Rule...	-1
Group Policy	Sequential
Cost Group	-- View
Routing Tag Na...	default
Internal Action	

Figure 43: IP-to-IP Routing for OPTIONS

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

#1[Teams to ACVC] Edit

GENERAL	
Name	• Teams to ACVC
Alternative Route Opt...	Route Row

MATCH	
Source IP Group	• Teams_IP_Grp View
Request Type	All
Source Username Pat...	*
Source Host	*
Source Tag	
Destination Userna...	*
Destination Host	*
Destination Tag	
Message Condition	-- View
Call Trigger	Any
ReRoute IP Group	• Any View

ACTION	
Destination Type	IP Group
Destination IP Group	• ACVC_IP_Grp View
Destination SIP Inter...	-- View
Destination Address	
Destination Port	0
Destination Transpo...	
IP Group Set	-- View
Call Setup Rules Set ID	-1
Group Policy	Sequential
Cost Group	-- View
Routing Tag Name	default
Internal Action	

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.

#2[ACVC to Teams] Edit

GENERAL		ACTION	
Name	• ACVC to Teams	Destination Type	IP Group
Alternative Route Opt...	Route Row	Destination IP Group	• Teams_IP_Grp View
		Destination SIP Inter...	-- View
		Destination Address	
		Destination Port	0
		Destination Transpo...	
		IP Group Set	-- View
		Call Setup Rules Set ID	-1
		Group Policy	Sequential
		Cost Group	-- View
		Routing Tag Name	default
		Internal Action	

MATCH	
Source IP Group	• ACVC_IP_Grp View
Request Type	All
Source Username Pat...	*
Source Host	*
Source Tag	
Destination Userna...	*
Destination Host	*
Destination Tag	
Message Condition	-- View
Call Trigger	Any
ReRoute IP Group	• Any View

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'.

MEDIANT SW IP NETWORK SIGNALING & MEDIA ADMINISTRATION Entity, parameter, value

SRD All

NETWORK VIEW

CORE ENTITIES

SECURITY

TLS Contexts (1)

Firewall (0)

Security Settings

TLS Contexts (1)

+ New Edit 🗑️

Page 1 of 1 Show 10 records per page

INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	default	TLSv1.2	Any	DEFAULT

Figure 46: TLS Context list

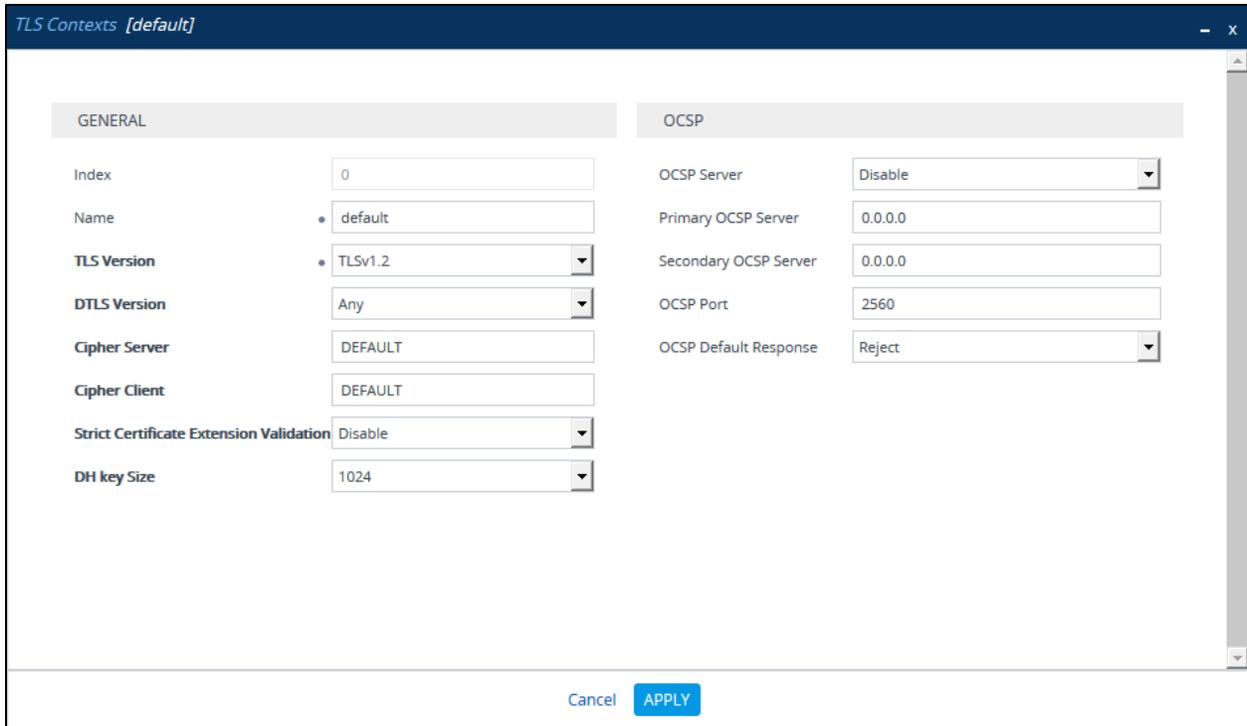


Figure 47: TLS Context for Amazon Chime Voice Connector

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.

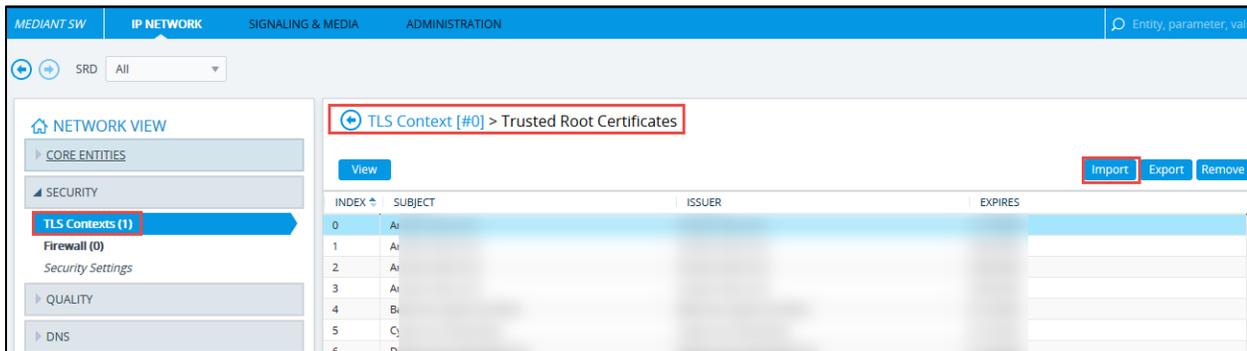


Figure 48: Trusted Root Certificate Import option

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

GENERAL		OCSP	
Index	1	OCSP Server	Disable
Name	Teams	Primary OCSP Server	0.0.0.0
TLS Version	TLSv1.2	Secondary OCSP Server	0.0.0.0
DTLS Version	Any	OCSP Port	2560
Cipher Server	DEFAULT	OCSP Default Response	Reject
Cipher Client	DEFAULT		
Strict Certificate Extension Validation	Disable		
DH key Size	1024		

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.

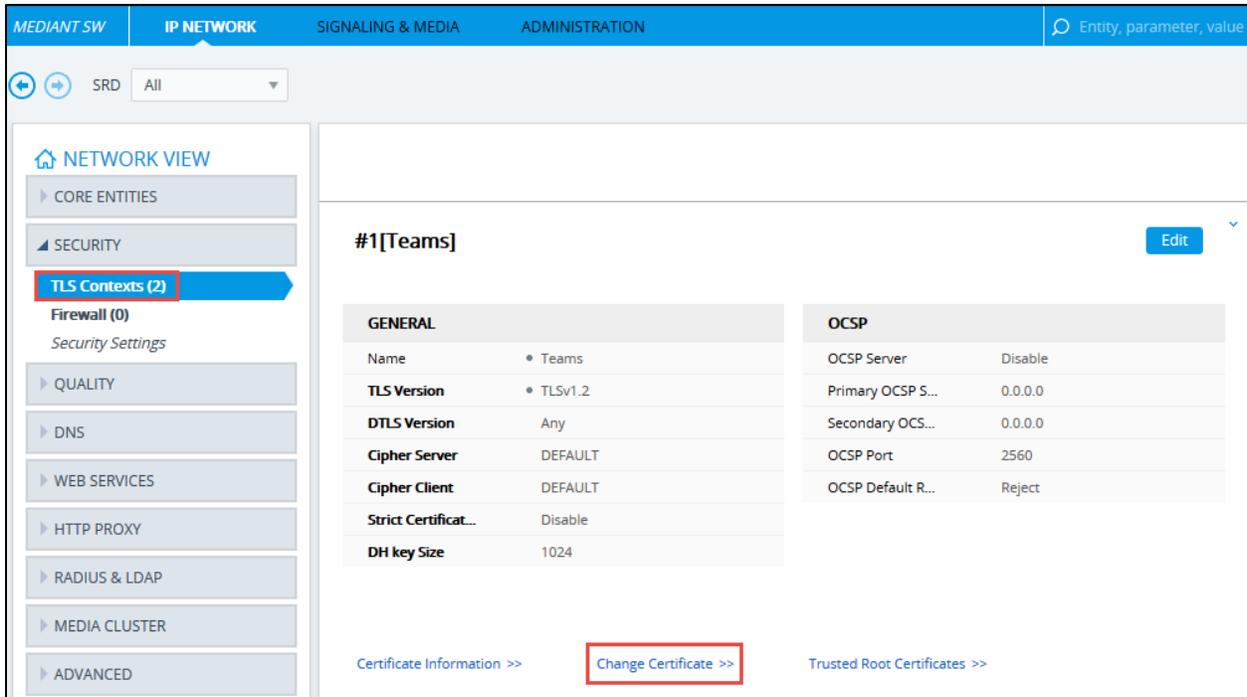


Figure 50: Change Certificate for MS Teams

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.

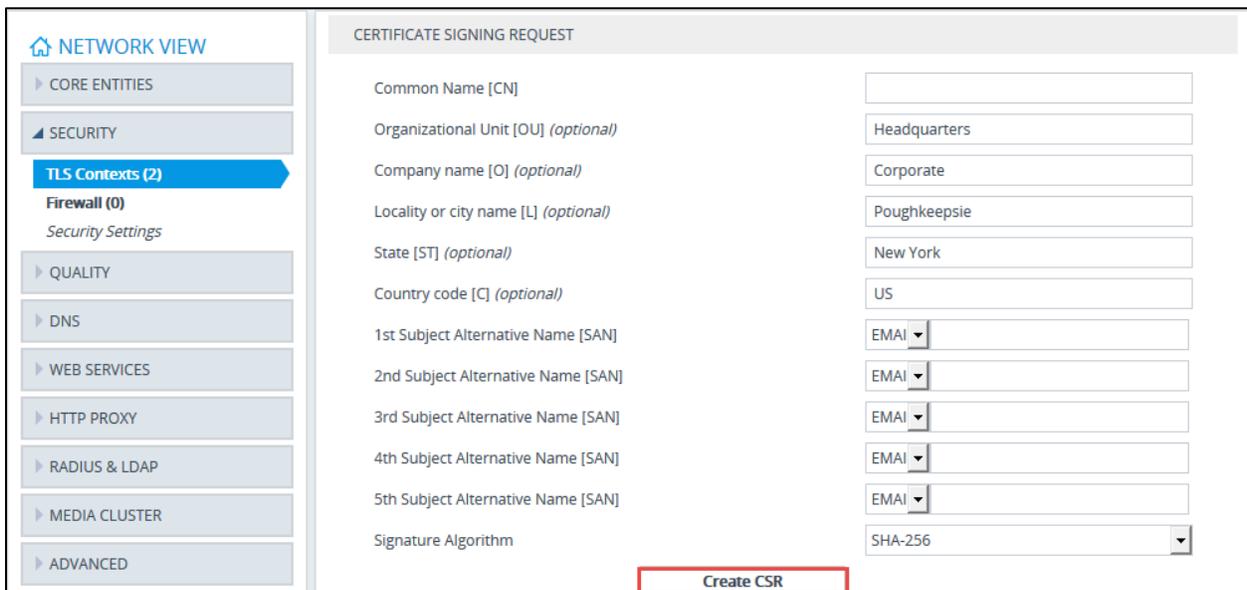


Figure 51: Generate CSR page

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.

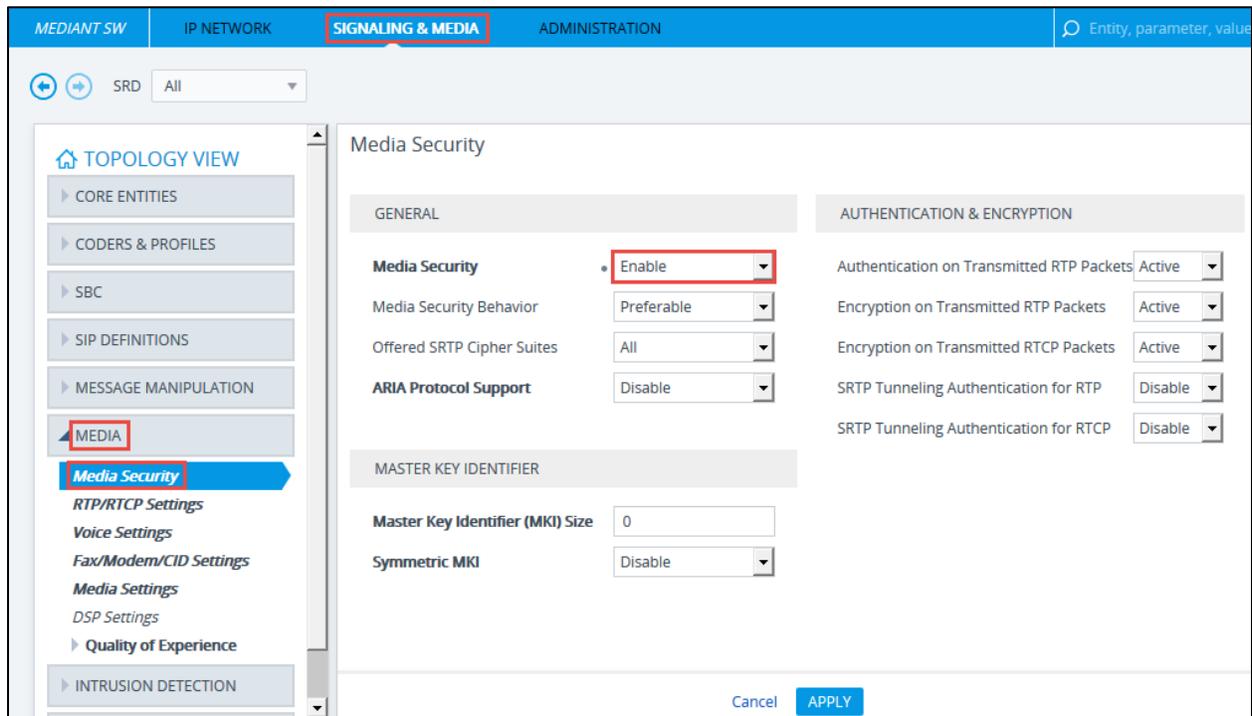


Figure 54: Media Security

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

The screenshot shows the 'IP Profiles [ACVC]' configuration window. It is divided into two main sections: 'GENERAL' and 'SBC SIGNALING'.
GENERAL Section:
 - Index: 1
 - Name: ACVC
 - Created by Routing Server: No
MEDIA SECURITY Section:
 - SBC Media Security Mode: SRTP (highlighted with a red box)
 - Symmetric MKI: Disable
 - MKI Size: 0
 - SBC Enforce MKI Size: Don't enforce
 - SBC Media Security Method: SDES
 - Reset SRTP Upon Re-key: Disable
 - Generate SRTP Keys Mode: Only If Required
SBC SIGNALING Section:
 - PRACK Mode: Transparent
 - P-Asserted-Identity Header Mode: As Is
 - Diversion Header Mode: As Is
 - History-Info Header Mode: As Is
 - Session Expires Mode: Supported
 - Remote Update Support: Not Supported
 - Remote re-INVITE: Supported
 - Remote Delayed Offer Support: Supported
 - Remote Representation Mode: According to Operation Mode
 - Keep Incoming Via Headers: According to Operation Mode
 - Keep Incoming Routing Headers: According to Operation Mode
 - Keep User-Agent Header: According to Operation Mode
 At the bottom, there are 'Cancel' and 'APPLY' buttons.

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.

The screenshot shows a configuration for a message manipulation rule titled '#0[Change From header towards Teams]'. It includes an 'Edit' button in the top right corner.
GENERAL Section:
 - Name: Change From header towards Teams
 - Manipulation Set ID: 2
 - Row Role: Use Current Condition
MATCH Section:
 - Message Type: Any.Request
 - Condition: (empty)
ACTION Section:
 - Action Subject: Header.From.URL.Host
 - Action Type: Modify
 - Action Value: 'sbct10.tekvizionlabs.com'

Figure 56: From header modification MS Teams

#1[Change From header towards AVSC]
Edit

GENERAL		ACTION	
Name	• Change From header towards AVSC	Action Subject	• Header.From.URL.Host
Manipulation Set ID	• 4	Action Type	• Modify
Row Role	Use Current Condition	Action Value	• ' '
MATCH			
Message Type	• Any.Request		
Condition			

Figure 57: From header Modification Amazon Chime Voice Connector

#2[Change OPTIONS RURI towards ACVC]
Edit

GENERAL		ACTION	
Name	• Change OPTIONS RURI towards ACVC	Action Subject	• Header.Request-URI.URL.Host
Manipulation Set ID	• 4	Action Type	• Modify
Row Role	Use Current Condition	Action Value	• 'cr7c1zxzy'
MATCH			
Message Type	• Options		
Condition	• Param.Message.address.dst.SIPInterface=='1'		

Figure 58: OPTIONS RURI modification

#3[Change OPTIONS TO URI towards ACVC]
Edit

GENERAL		ACTION	
Name	• Change OPTIONS TO URI towards ACVC	Action Subject	• Header.To.URL.Host
Manipulation Set ID	• 4	Action Type	• Modify
Row Role	Use Current Condition	Action Value	• 'cr7c1zxzy'
MATCH			
Message Type	• Options		
Condition	• Param.Message.Address.Dst.SIPInterface=='1'		

Figure 59: OPTIONS To header modification

#4[Modify Session Expires]
Edit

GENERAL		ACTION	
Name	• Modify Session Expires	Action Subject	• Header.Session-Expires.Time
Manipulation Set ID	• 2	Action Type	• Modify
Row Role	Use Current Condition	Action Value	• '900'
MATCH			
Message Type	• Invite.Response.2xx		
Condition	• Header.Session-Expires exists		

Figure 60: Session Expires value modification

#5[Remove PAI with User Name]
Edit

GENERAL		ACTION	
Name	• Remove PAI with User Name	Action Subject	• Header.P-Asserted-Identity.1
Manipulation Set ID	• 1	Action Type	• Remove
Row Role	Use Current Condition	Action Value	
MATCH			
Message Type	• any		
Condition	• Header.P-Asserted-Identity.URL.Type == '2'		

Figure 61: Remove PAI with SIP towards from MS Teams

#6[Remove Privacy]
Edit

GENERAL		ACTION	
Name	• Remove Privacy	Action Subject	• Header.Privacy
Manipulation Set ID	• 1	Action Type	• Remove
Row Role	Use Current Condition	Action Value	
MATCH			
Message Type	• any		
Condition	• header.From.url.user != 'anonymous'		

Figure 62: Remove Privacy from MS Teams