



Crestron UC-PHONE and UC-PHONE-PLUS

**Connecting Microsoft Teams
Direct Routing using AudioCodes
Mediant Virtual Edition (VE)
and Avaya Aura v8.0**

October 2019

Document History

Rev. No.	Date	Document Owner	Description
1.0	Oct-18-2019	tekVizion	Configuration Guide

Table of Contents

1	Audience	7
1.1	Crestron UC-PHONE and UC-PHONE-PLUS	7
1.2	tekVizion Labs.....	7
2	SIP Trunking Network Components.....	9
2.1	Hardware Components.....	10
2.2	Software Requirements.....	10
3	Features	10
3.1	Features Supported.....	10
3.2	Caveats and Limitations	11
4	Configuration.....	12
4.1	Configuration Checklist	12
4.2	IP Address Worksheet	12
4.3	Microsoft Teams Configuration.....	13
4.3.1	Teams User Configuration	13
4.3.2	Configure Calling policy to Users	20
4.3.3	Configure user parameters.....	21
4.3.4	Create Online PSTN Gateway	21
4.3.5	Configure Online PSTN Usage.....	22
4.3.6	Configure Online Voice Route	22
4.3.7	Configure Online Voice Route Policy.....	23
4.3.8	Configure Online Voice Route Policy to user	23
4.3.9	Configure Tenant Dial Plan.....	23
4.3.10	Create Normalization Rule	24
4.3.11	Associate Normalization rule to tenant dial plan	24
4.3.12	Associate tenant Dial plan to user	24
4.3.13	Calling Line Identity Policy.....	24
4.4	AudioCodes VE SBC Configuration.....	26
4.4.1	General	26
4.4.2	Configure VLANs.....	26

4.4.3	Configure IP Network Interfaces	26
4.4.4	Configure DNS SRV Records	28
4.4.5	Configure SRTP	29
4.4.6	Configure TLS contexts	29
4.4.7	Configure Media Realms	31
4.4.8	Configure the SRD	32
4.4.9	Configure SIP Signaling Interface	34
4.4.10	Configure Proxy Sets	36
4.4.11	Configure IP Groups	39
4.4.12	Configure IP Profile	43
4.4.13	Configure SIP Definition and General Setting	51
4.4.14	Configure SBC General Settings	52
4.4.15	Configure IP-to-IP Routing Rules	52
4.4.16	IP Group	56
	Message Manipulation	59
4.5	Avaya Aura Communication Manager Configuration	69
4.5.1	Version	69
4.5.2	IP Node Name	69
4.5.3	IP Codec Set	70
4.5.4	IP Network Region	71
4.5.5	Signaling Groups	72
4.5.6	Trunk Groups	73
4.5.7	Route Pattern	74
4.5.8	Outbound Call Routing	75
4.5.9	Private Numbering Plan	76
4.6	Avaya Aura Session Manager Configuration	77
4.6.1	Version	79
4.6.2	Domains	80
4.6.3	Locations	80
4.6.4	Adaptation	82
4.6.5	SIP Entities and Entity Links	83

4.6.6	Routing Policies	88
4.6.7	Dial Patterns	90
4.7	Avaya SBCE Configuration	92
4.7.1	Version	92
4.7.2	Configure Profiles and Services	94
4.7.3	Domain Policies	107
4.7.4	Network & Flows.....	111
5	Acronyms	115
6	Summary of Tests and Results	116

1 Audience

This document is intended for the SIP trunk customer's technical staff and Value Added Retailer (VAR) having installation and operational responsibilities. This configuration guide provides steps for configuring **Crestron UC-PHONE and UC-PHONE-PLUS with Microsoft Teams Direct Routing using AudioCodes Mediant VE SBC and Avaya Aura v8.0 as Customer PBX.**

1.1 Crestron UC-PHONE and UC-PHONE-PLUS

The Crestron UC-PHONE and UC-PHONE-PLUS phones are designed for use with the Microsoft Teams intelligent communications platform. They enable superior voice calling and full-duplex hands-free conferencing in a stylish desktop package. A consistent user experience at every desk, workstation, and meeting space is provided via the familiar and intuitive Microsoft Teams touch screen UI, affording simple operation with comprehensive call and contact management features, built-in calendaring, and one-touch meeting joins.

The Crestron UC-PHONE and UC-PHONE-PLUS desk phones install easily and connect securely, with IoT cloud based provisioning and management via the Crestron XiO Cloud™ service. They work natively with any Microsoft Teams account for a streamlined deployment on any enterprise or SMB network.

1.2 tekVizion Labs

tekVizion Labs™ is an independent testing and Verification facility offered by tekVizion PVS, Inc. ("tekVizion"). tekVizion Labs offers several types of testing services including:

- Remote Testing – provides secure, remote access to certain products in tekVizion Labs for pre-Verification and ad hoc testing
- Verification Testing – Verification of interoperability performed on-site at tekVizion Labs between two products or in a multi-vendor configuration
- Product Assessment – independent assessment and verification of product functionality, interface usability, assessment of differentiating features as well as suggestions for added functionality, stress and performance testing, etc.

tekVizion is a systems integrator specifically dedicated to the telecommunications industry. Our core services include consulting/solution design, interoperability/Verification testing, integration, custom software development and solution support services. Our services helps service providers achieve a smooth transition to packet-voice networks, speeding delivery of integrated services. While we have expertise covering a wide range of technologies, we have

extensive experience surrounding our practice areas which include: SIP Trunking, Packet Voice, Service Delivery, and Integrated Services.

The tekVizion team brings together experience from the leading service providers and vendors in telecom. Our unique expertise includes legacy switching services and platforms, and unparalleled product knowledge, interoperability and integration experience on a vast array of VoIP and other next-generation products. We rely on this combined experience to do what we do best: help our clients advance the rollout of services that excite customers and result in new revenues for the bottom line. tekVizion leverages this real-world, multi-vendor integration and test experience and proven processes to offer services to vendors, network operators, enhanced service providers, large enterprises and other professional services firms. tekVizion's headquarters, along with a state-of-the-art test lab and Executive Briefing Center, is located in Plano, Texas.

For more information on tekVizion and its practice areas, please visit tekVizion Labs website at www.tekVizion.com

2 SIP Trunking Network Components

The network for the SIP trunk reference configuration is illustrated below and is representation of Crestron UC-PHONE and UC-PHONE-PLUS connected O365 Cloud with Microsoft Teams Direct Routing to Avaya Aura v8.0 environment using AudioCodes Mediant VE SBC and PSTN Gateway for PSTN connectivity. Media bypass enables Configured teams side used in this topology.

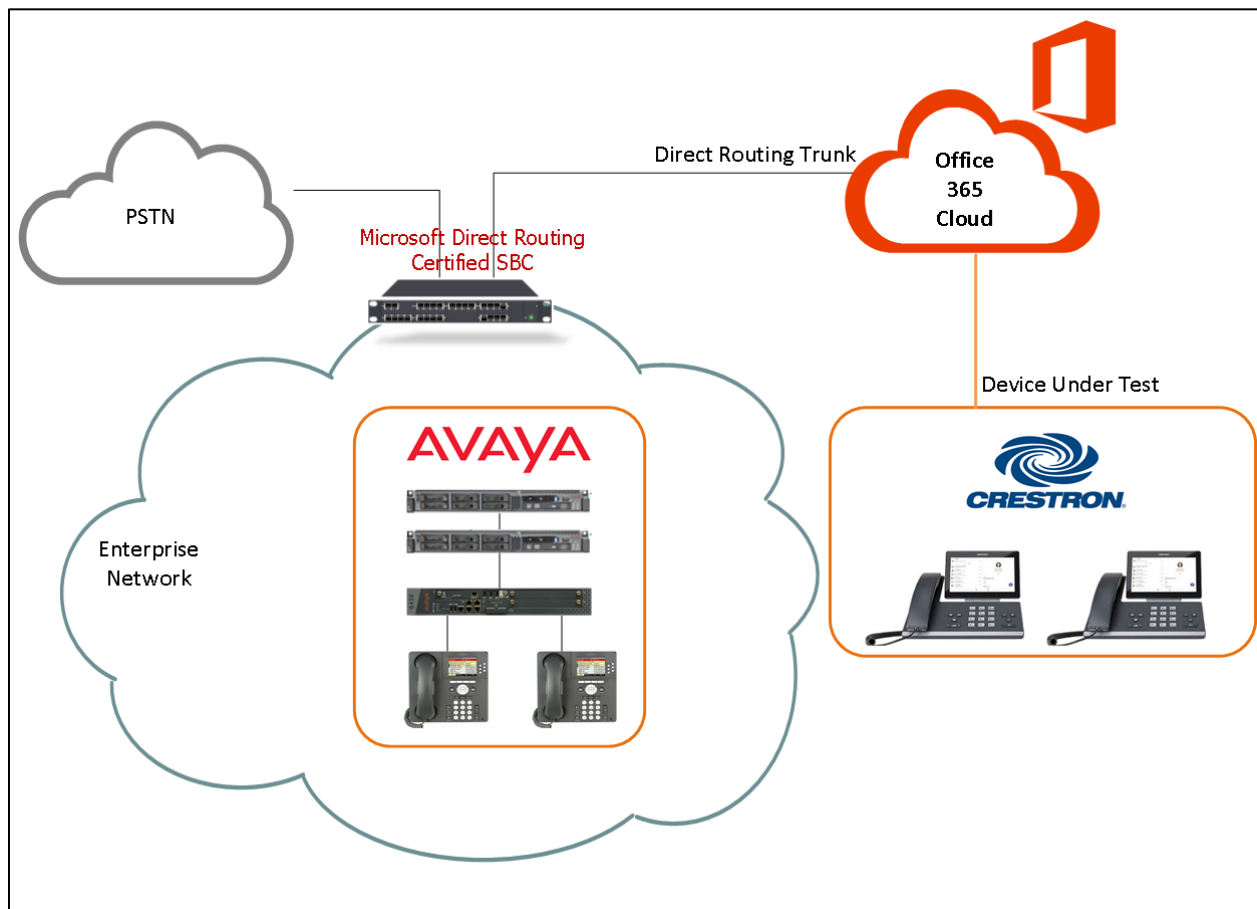


Figure 1 Network Topology

Numbering Plan

- Avaya users are configured with 4 digit extension 75XX
- Teams users are configured with E164 numbers +197259809XX

Dialing Plan

- Teams users and Avaya users call PSTN either doing 10 digits 11 digits dialing or E164 dialing

- Teams users call Avaya users by dialing 75XX
- Avaya users call Teams users by dialing 8XXX and AudioCodes will include the prefix +1972XXX and will send to Teams.

2.1 Hardware Components

- Microsoft Office 365 tenant with E5 without Audio Conferencing assigned to Teams users
- AudioCodes Mediant VE SBC for Teams Direct Routing serves as the demarcation point between customer's network and O365 WAN network
- Crestron UC-PHONE-PLUS and Crestron UC-PHONE phones
- Avaya Aura Communication Manager Configuration
- Avaya Aura Session Manager Configuration
- Avaya SBCE Configuration
- PSTN Gateway

2.2 Software Requirements

- AudioCodes Mediant VE SBC v7.20A.250.003
- Skype For Business 2015 Version (6.0.9319)
- Avaya Aura Communication Manager Configuration v8.0.1
- Avaya Aura Session Manager Configuration v8.0.1
- Avaya SBCE Configuration v8.0
- Crestron UC-PHONE-PLUS v58.15.91.15

3 Features

3.1 Features Supported

- Basic Inbound and Basic Outbound
- Call hold and resume
- Call transfer (semi-attended and consultative)
- Conference
- Call forward (all, no answer)
- Busy On Busy
- Simultaneous ring
- Calling line identification restriction
- DTMF relay both directions (RFC2833)

3.2 Caveats and Limitations

- Direct Routing supports call escalation to an adhoc conference without Audioconferencing license. However the UC-PHONE-PLUS and UC-PHONE desk phones could not add a user into conference without Audio Conferencing license.
- The UC-PHONE-PLUS desk phone is unable to resume a held call using soft-key, if the call has been answered by the phone using receiver or speaker button.

4 Configuration

4.1 Configuration Checklist

In this section we present an overview of the steps that are required to configure **Microsoft Teams, Avaya SBCE, Avaya Aura Session Manager, Avaya Aura Communication Manager and AudioCodes** for SIP Trunking with **Microsoft Teams Direct Routing**.

Table 1 – PBX Configuration Steps

Steps	Description	Reference
Step 1	Microsoft Teams Configuration	Section 4.3
Step 2	AudioCodes VE SBC Configuration	Section 4.4
Step 3	Avaya Aura Communication Manager	Section 4.5
Step 4	Avaya Aura Session Manager	Section 4.6
Step 5	Avaya SBCE	Section 4.7

4.2 IP Address Worksheet

The specific values listed in the table below and in subsequent sections are used in the lab configuration described in this document and are for **illustrative purposes only**. The customer must obtain and use the values for your deployment.

Table 2 – IP Addresses

Component	Lab Value
AudioCodes	
LAN IP Address	10.64.3.10
LAN Subnet Mask	255.255.255.0
WAN IP Address	192.XX.XX.XX
WAN Subnet Mask	255.255.255.128
Avaya Aura Communication Manager	
IP Address	10.89.33.4 (Signaling)/10.89.33.14 (Media)
Subnet Mask	255.255.255.0
Avaya Aura Session Manager	
LAN IP Address	10.89.33.7
LAN Subnet Mask	255.255.255.0
Avaya SBCE	
LAN IP Address	10.89.33.3

LAN Subnet Mask	255.255.255.0
WAN IP Address	192.65.79.204
WAN Subnet Mask	255.255.255.0

4.3 Microsoft Teams Configuration

This section with screen shots taken from Office 365 Portal and PowerShell Command used for the interoperability testing gives a general overview of the Microsoft Teams Configuration.

4.3.1 Teams User Configuration

Below are the steps to create a user in office 365 portal.

1. Login into <http://portal.office.com/> using your office 365 tenant administrator credentials.

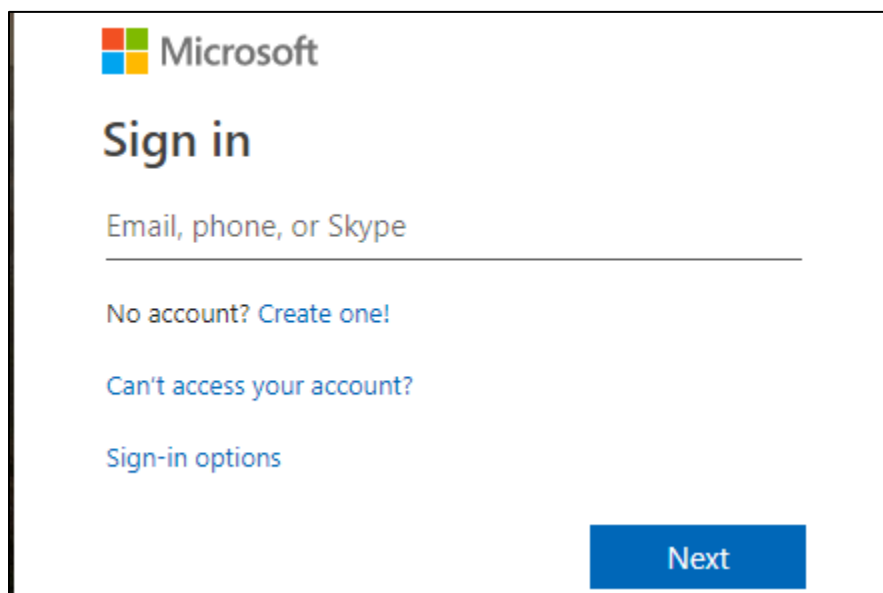


Figure 2: Office 365 Portal Login

2. Select the Office 365 Admin Icon to login Office 365 Admin Center as shown below.

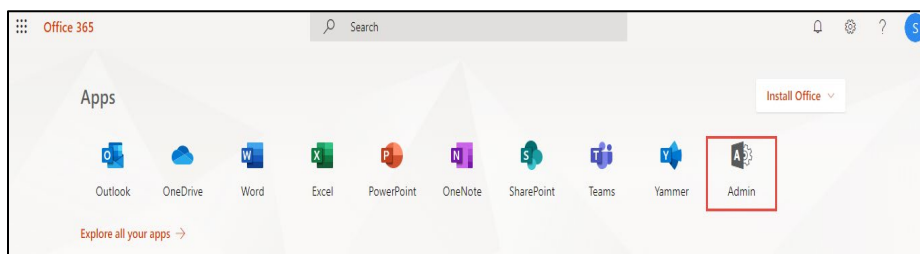


Figure 3: Office 365 Portal Login

3. Select "Add a user" from the Microsoft 365 Admin Center as shown below.

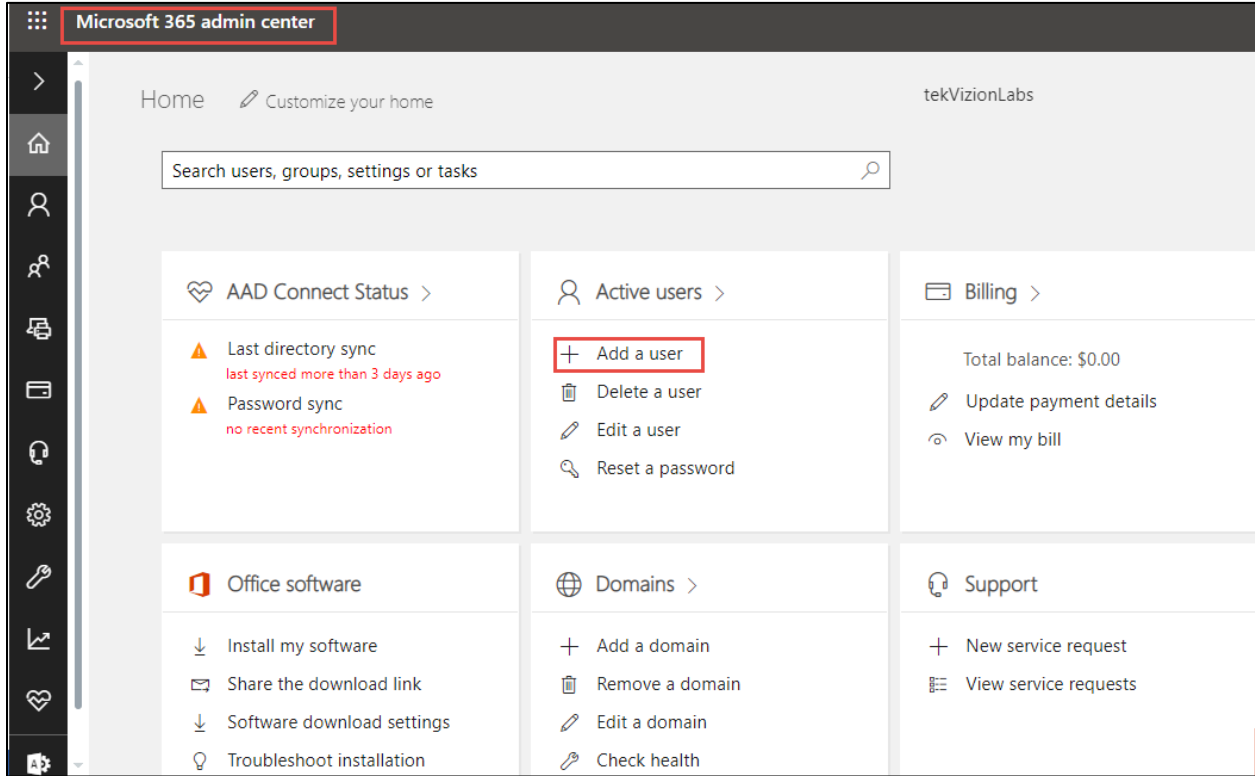


Figure 4: Teams User Creation

4. Enter the user details, password and assign required license to the users and Click Add

Add user

Basics

Product licenses

Optional settings

Finish

First name: crestron

Last name: teams5

Display name *: crestronteam5

Username *: crestroncrestronteam5@tekvisionlabs.com

Password settings

Auto-generate password

Let me create the password

Require this user to change their password when they first sign in

Send password in email upon completion

Next

Figure 5: Teams User Creation – Contd.

Add user

Basics

Product licenses

Optional settings

Finish

Select location *: United States

Licenses (1) *

Assign user a product license

Communications Credits
Unlimited licenses available

Domestic Calling Plan
3 of 5 licenses available

Intune
95 of 100 licenses available

Microsoft Teams Commercial Cloud (User Initiated)
Unlimited licenses available

Microsoft Teams Trial
Unlimited licenses available

Office 365 E5
6 of 13 licenses available

Office 365 E5 without Audio Conferencing
26 of 100 licenses available

Create user without product license (not recommended)
They may have limited or no access to Office 365 until you assign a product license.

Back **Next**

Figure 6: Teams User Creation – Contd.

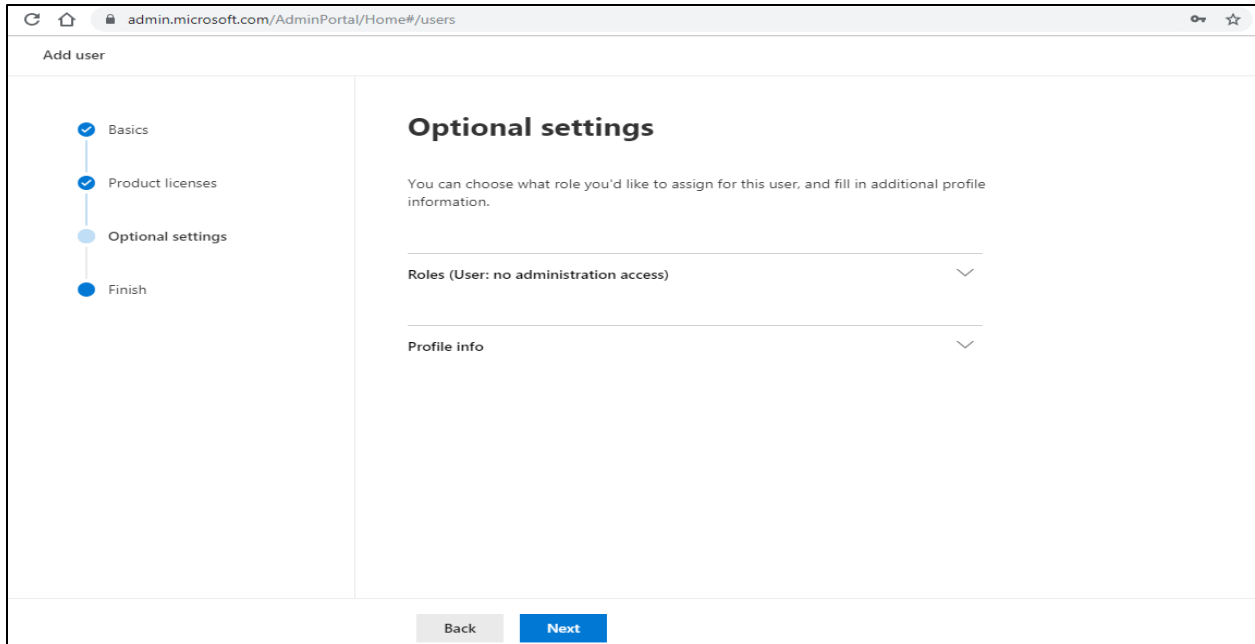


Figure 7: Teams User Creation – Contd.

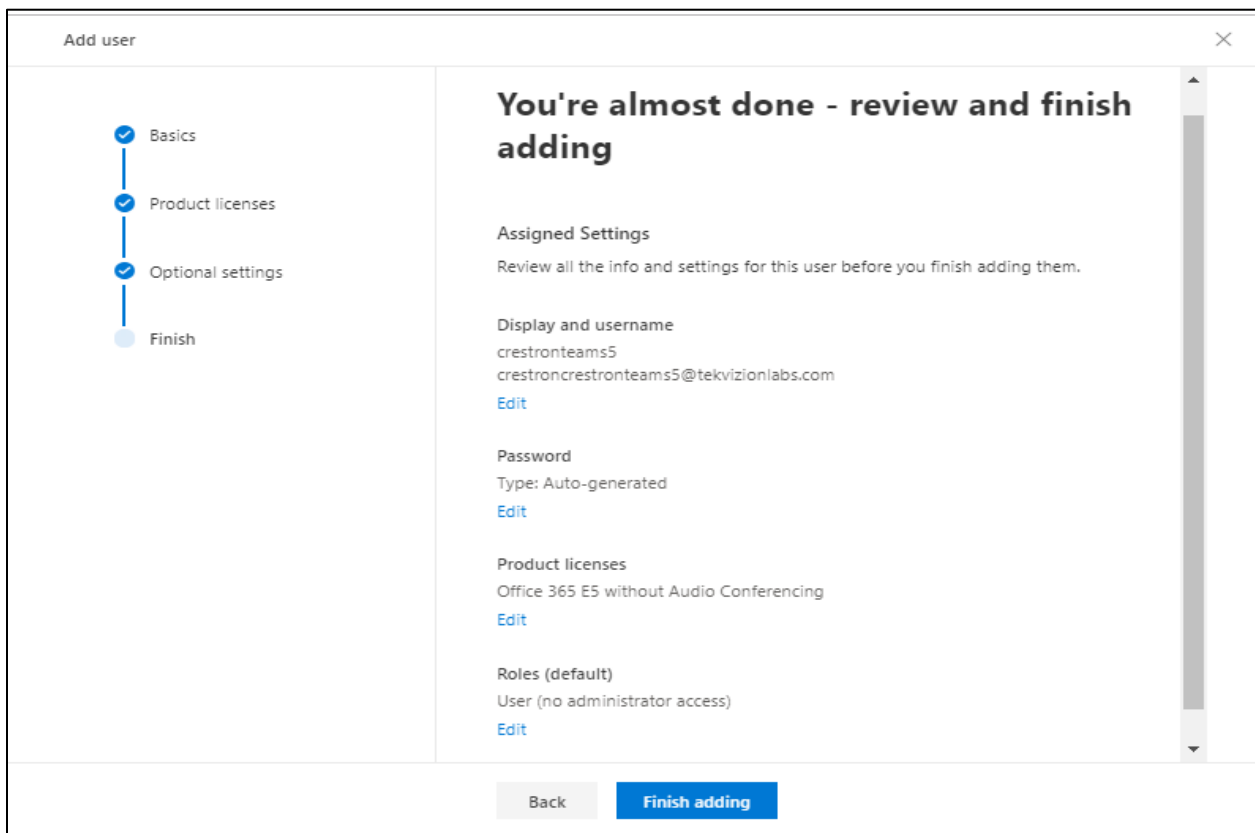


Figure 8: Teams User Creation – Contd.

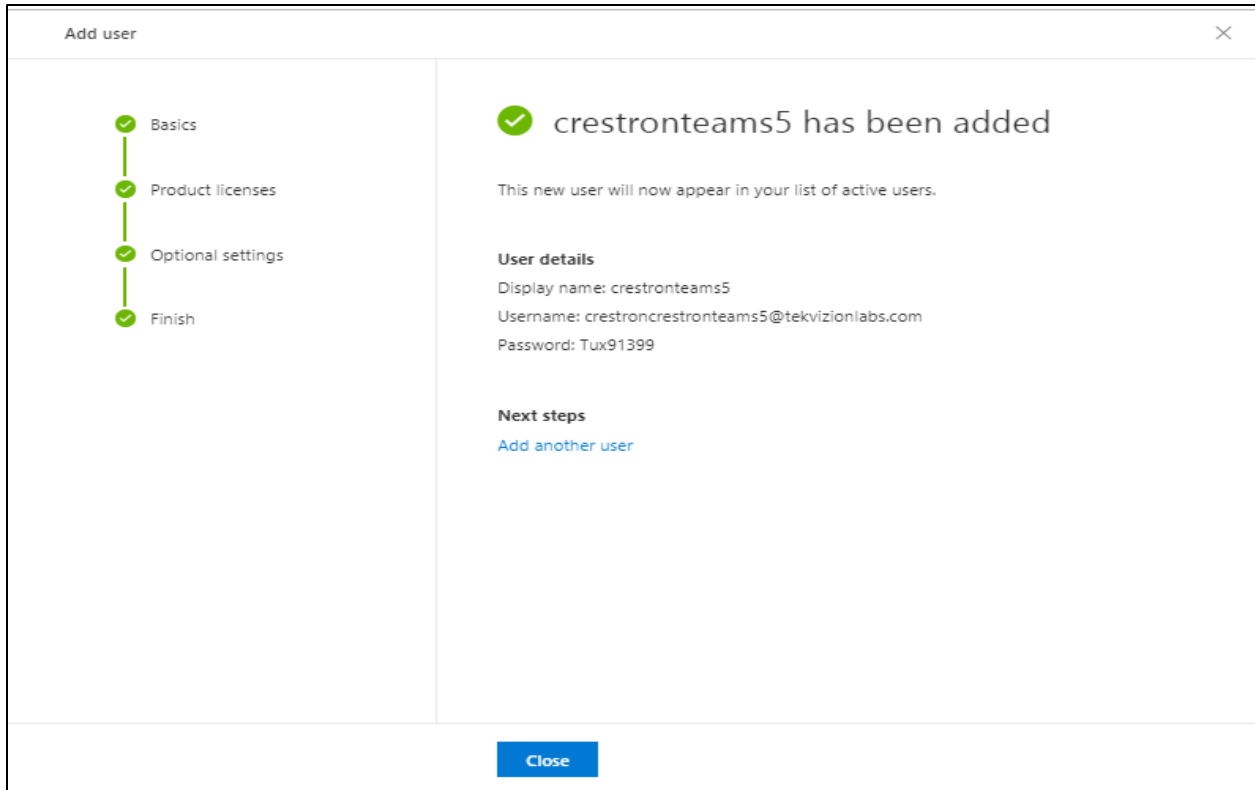


Figure 9: Teams User Creation – Contd.

5. Select the Admin icon from the Microsoft 365 Administrator Home page and navigate to Microsoft Teams admin center as shown below.

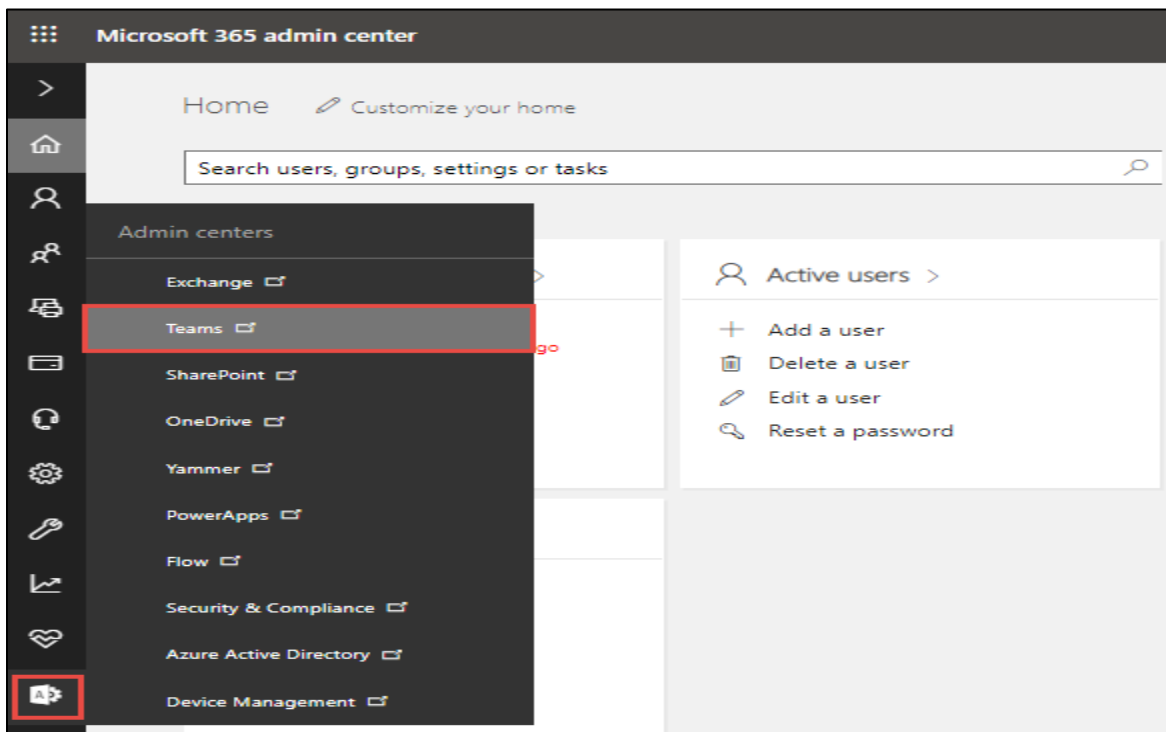


Figure 10: Microsoft O365 admin

6. Select Users from the Microsoft Teams Admin Center to view the list of available users.

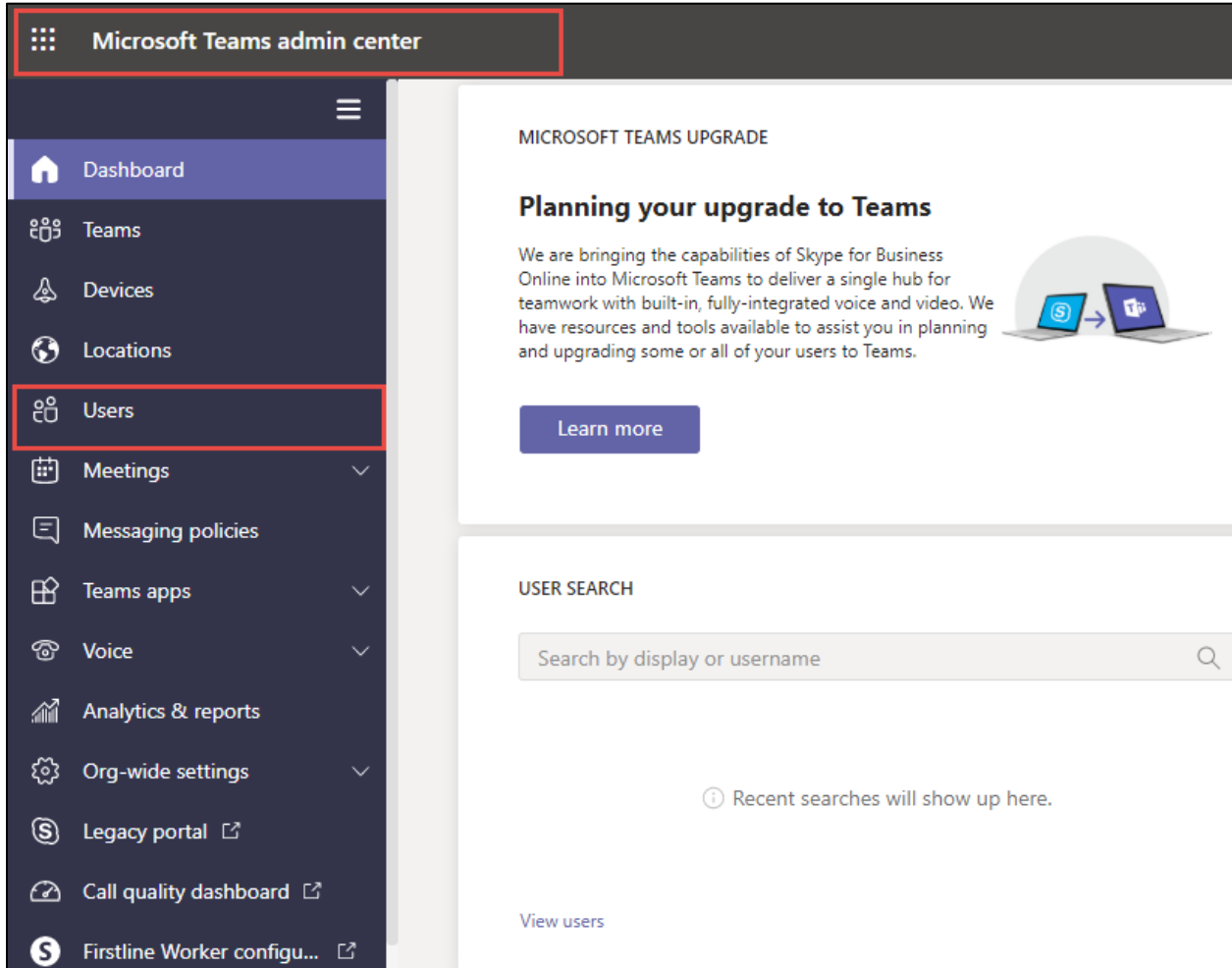


Figure 11: Microsoft O365 admin

7. Search for the user created above and click on the user display name to view user properties.

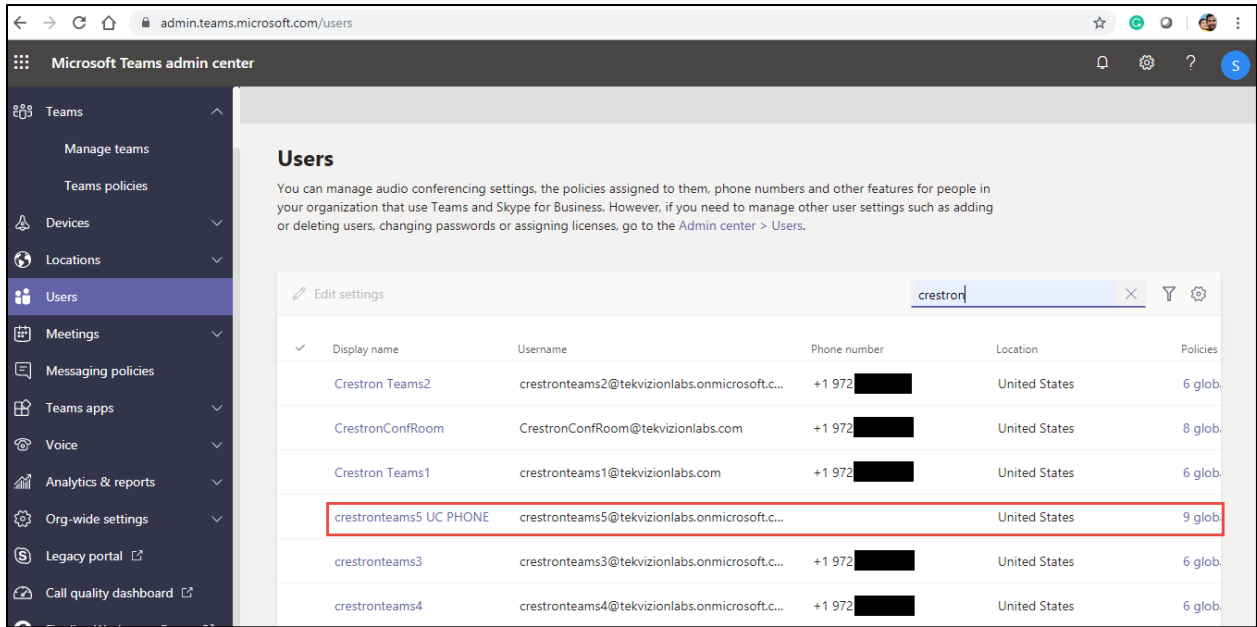


Figure 12: Microsoft O365 admin

- Under user properties, navigate to Account and set the teams upgrade mode to Teams only as shown below.

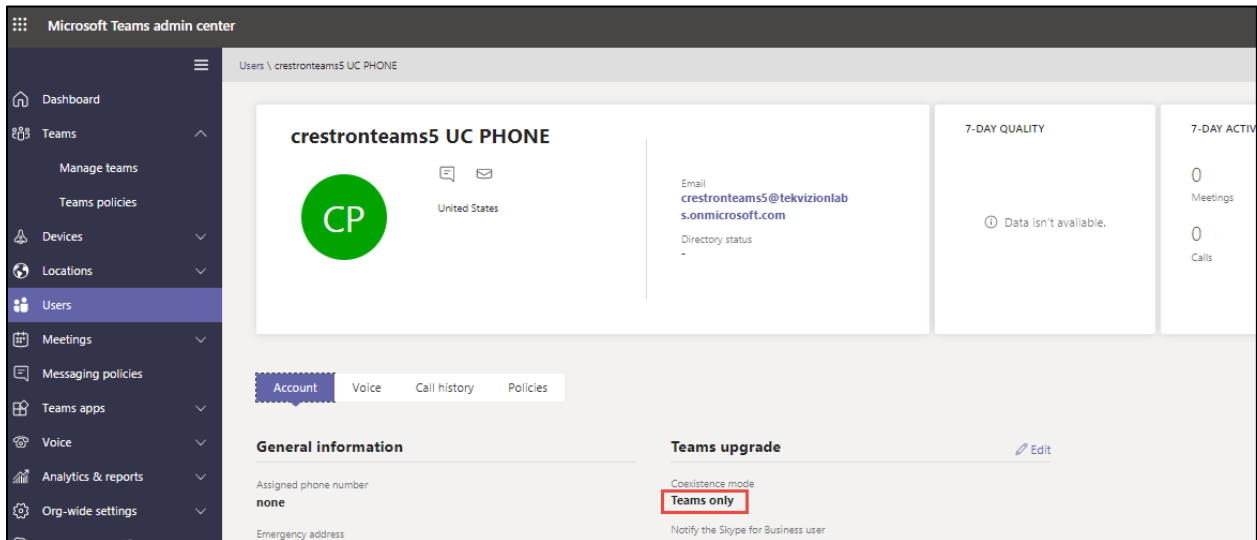


Figure 13: Teams User

4.3.2 Configure Calling policy to Users

- 1) Under user properties, navigate to Policies and set the Calling Policy as shown below. Here in the below example custom policy “Busy on Busy enabled” is assigned to user. Procedure to create custom policy is shown in the next section.

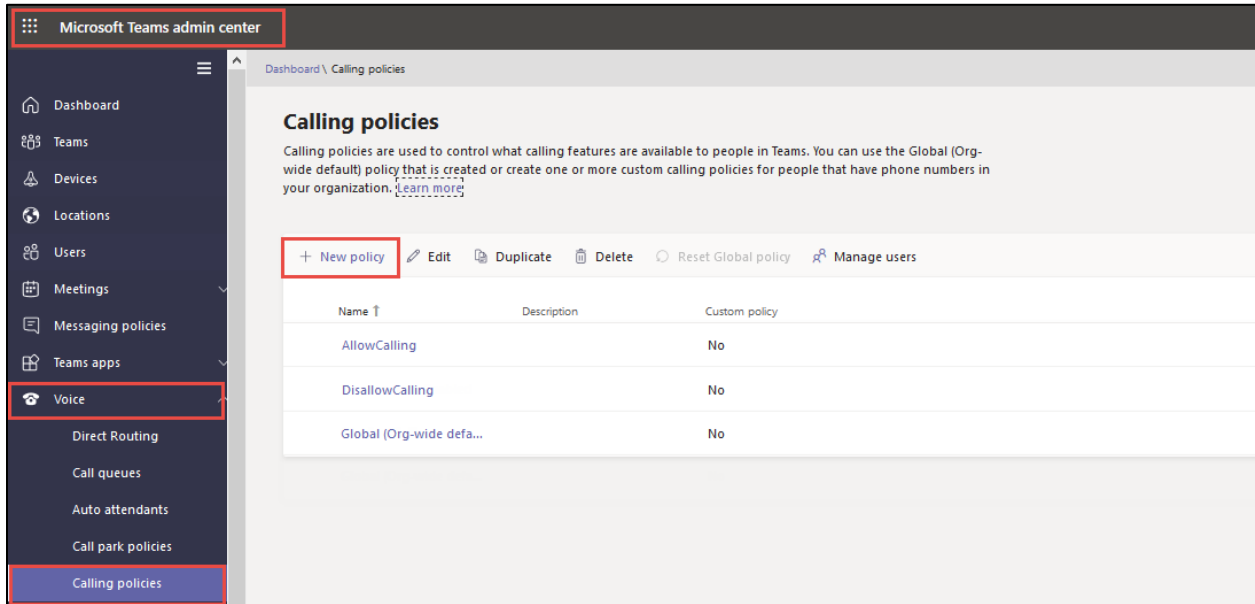


Figure 14 – Calling Policy

2. Below calling policy is created to turn on Busy on Busy. Click save to complete the configuration.

Dashboard \ Calling policies \ New policy

Busy on Busy Enabled

Description

Make private calls On

Call forwarding and simultaneous ringing to people in your organization On

Call forwarding and simultaneous ringing to external phone numbers On

Voicemail is available for routing inbound calls User controlled

Inbound calls can be routed to call groups On

Allow delegation for inbound and outbound calls On

Prevent toll bypass and send calls through the PSTN Off

Busy on busy is available when in a call On

Save Cancel

Figure 15 – Calling Policy

4.3.3 Configure user parameters.

Using the Remote PowerShell connect to Microsoft office 365 Tenant. Use the below commands to set DID and enable Enterprise Voice, Hosted Voicemail for Teams users.

```
Set-CsUser -identity "crestrontteams5@tekvizionlabs.com" -EnterpriseVocieEnabled $true -HostedVoicemail $true
```

```
Set-CsUser -identity "crestrontteams5@tekvizionlabs.com" -OnPremlineURI tel: +197259800xx
```

4.3.4 Create Online PSTN Gateway

Use the below command to pair the SBC to the tenant.

```
New-CsOnlinePSTNGateway -Fqdn <SBC FQDN> -SipSignallingPort <SBC SIP Port>
```

```
-ForwardCallHistory $true -ForwardPai $true -MaxConcurrentSessions <Max Concurrent Sessions the SBC can handle> -Enabled $true -MediaBypass $true
```

```

PS C:\Users\spandian> Get-CsOnlinePSTNGateway -Identity sbc4.tekvizionlabs.com

Identity           : sbc4.tekvizionlabs.com
Fqdn               : sbc4.tekvizionlabs.com
SipSignallingPort  : 5061
FailoverTimeSeconds : 10
ForwardCallHistory : True
ForwardPai        : True
SendSipOptions     : True
MaxConcurrentSessions : 100
Enabled           : True
MediaBypass       : True
GatewaySiteId     : 
GatewaySiteLbrEnabled : False
FailoverResponseCodes : 408, 503, 504
GenerateRingingWhileLocatingUser : True
PidfloSupported    : True
MediaRelayRoutingLocationOverride : 
ProxySbc          : 
BypassMode        : None

```

Figure 16 - Online PSTN Gateway

4.3.5 Configure Online PSTN Usage

Use the below command to add a new PSTN usage.

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
CCE
Non E.164
ThinkTel
sbc3
sbc4

```

Figure 17 - Microsoft Teams - Online PSTN usage reference

4.3.6 Configure Online Voice Route

Use the below command to add a new online Voice Route.

```

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

```

```
PS C:\WINDOWS\system32> Get-CsOnlineVoiceRoute -Identity sbc4

Identity           : sbc4
Priority            : 5
Description        :
NumberPattern      : .*
OnlinePstnUsages   : {sbc4}
OnlinePstnGatewayList : {sbc4.tekvizionlabs.com}
Name               : sbc4
```

Figure 18 - Microsoft Teams - Online PSTN Voice Route reference

4.3.7 Configure Online Voice Route Policy

Create a new online Voice Routing Policy using the below command.

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

```
PS C:\WINDOWS\system32> Get-CsOnlineVoiceRoutingPolicy

Identity           : Tag:sbc4
OnlinePstnUsages   : {sbc4}
Description        :
RouteType          : BYOT
```

Figure 19 - Microsoft Teams - Online Voice Route Policy

4.3.8 Configure Online Voice Route Policy to user

Assign a online Voice Routing Policy to user using the below command.

```
Grant-CsOnlineVoiceRoutingPolicy -Identity "<Teams User>" -PolicyName "<PSTN Usage>"
```

```
> Grant-CsOnlineVoiceRoutingPolicy -Identity "crestronteam5" -PolicyName "sbc4"
```

Figure 20 - Microsoft Teams - Online Voice Route Policy to User

4.3.9 Configure Tenant Dial Plan

Tenant dial plan added to provision custom dial plan to user. Example is shown below

```
New-CsTenantDialPlan -Identity <dial plan name> -Description "For Extension Calling"
```

```
> Get-CsTenantDialPlan -Identity crestron

Identity           : Tag:crestron
Description        : For Extention Dialing
```

```
NormalizationRules :  
{Description=crestron;Pattern=^(.*)$;Translation=$1;Name=crestron;IsInternalExtension=False}  
ExternalAccessPrefix :  
SimpleName : crestron  
OptimizeDeviceDialing : False
```

Figure 21 - Microsoft Teams – Configure Tenant Dial Plan

4.3.10 Create Normalization Rule

Create a new Voice Normalization Rule using the below command.

```
$rule1 = New-CsVoiceNormalizationRule -Parent Global -Description "description" -  
Pattern '^(.*)$' -Translation '$1' -Name <dial plan name> -IsInternalExtension $false  
-InMemory
```

```
> $rule1 = New-CsVoiceNormalizationRule -Parent Global -Description "crestron" -Pattern '^(.*)$' -Translation '$1' -Name crestron -IsInternalExtension $false -InMemory
```

Figure 22 - Microsoft Teams – Normalization Rule

4.3.11 Associate Normalization rule to tenant dial plan

Associate the Voice Normalization Rule to tenant dial plan created earlier using the below command.

```
Set-CsTenantDialPlan -Identity <dial plan name> -NormalizationRules  
@{add=$rule1}
```

```
> Set-CsTenantDialPlan -Identity crestron -NormalizationRules @{add=$rule1}
```

Figure 23 - Microsoft Teams – Normalization Rule to tenant dial plan

4.3.12 Associate tenant Dial plan to user

Assign the Tenant dial plan to the user using below command.

```
Grant-CsTenantDialPlan -identity <username> -PolicyName <dial plan name>
```

```
> Grant-CsTenantDialPlan -identity crestronteam5 -PolicyName crestron
```

Figure 24 - Microsoft Teams – tenant dial plan to user

4.3.13 Calling Line Identity Policy

Calling Line Identity Policy is used to present/restrict users Caller ID.

```
New-CsCallingLineIdentity -Identity anonymous_policy -Description "clid  
restricted" -CallingIDSubstitute Anonymous -EnableUserOverride $true
```


Use the command **Get-CsCallingLineIdentity** to view the Calling Line Identity policy created.

```
PS C:\WINDOWS\system32> Get-CsCallingLineIdentity -Identity anonymous_policy

Identity           : Tag:Anonymous_policy
Description        : clid restricted
EnableUserOverride : True
ServiceNumber     :
CallingIDSubstitute : Anonymous
BlockIncomingPstnCallerID : False
```

Figure 25 – Privacy Policy

Associate the policy created above to the users using the below command.

Grant-CsCallingLineIdentity -Identity "crestrontteams5@tekvizionlabs.com" - PolicyName anonymous_policy

User associated with the above policy gets an additional Option as “Caller ID” in their Teams Client.

Navigate to Settings -> Calls -> Caller ID in users Teams client, Check **“Hide my phone number and profile information”** to restrict caller ID.

4.4 AudioCodes VE SBC Configuration

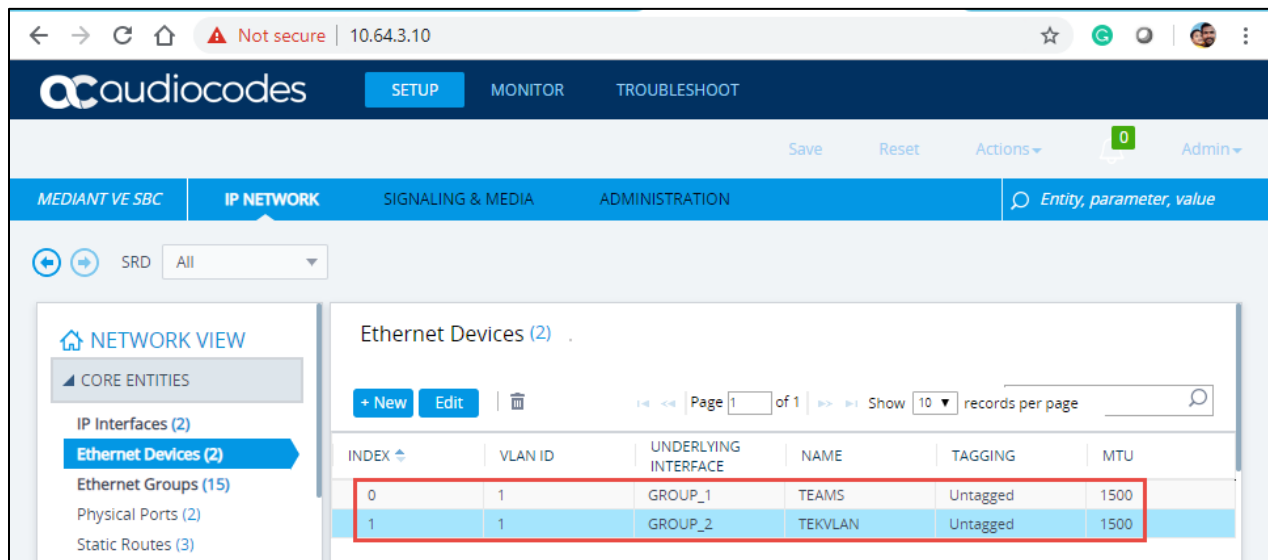
4.4.1 General

AudioCodes Mediant 1000 SBC was used as it can meet the requirements and support the enhancements for Microsoft Teams Direct Routing. PSTN Gateway SIP Trunk is a non-registering trunk that connects to E-SBC using UDP. Avaya SBCE SIP Trunk that connects to E-SBC using UDP. The SBC must be configured to perform back to back User Agent (B2BUA) functionality. For the B2BUA configuration, it is recommended that Physical interfaces are connected with two different customer WAN networks.

4.4.2 Configure VLANs

To configure VLANs, navigate to **IP Network tab** → **Core Entities menu** → **Ethernet Devices**

Add an entry with VLAN ID for underlying Teams and CenturyLink Voice Complete® interface Groups configured.



The screenshot shows the AudioCodes Mediant VE SBC configuration interface. The browser address bar shows the URL 10.64.3.10. The interface has a top navigation bar with 'audiocodes' logo and tabs for 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. Below this is a secondary navigation bar with 'MEDIANT VE SBC', 'IP NETWORK', 'SIGNALING & MEDIA', and 'ADMINISTRATION'. The 'IP NETWORK' tab is active. On the left, there is a 'CORE ENTITIES' menu with options: 'IP Interfaces (2)', 'Ethernet Devices (2)', 'Ethernet Groups (15)', 'Physical Ports (2)', and 'Static Routes (3)'. The 'Ethernet Devices (2)' option is selected. The main content area shows a table titled 'Ethernet Devices (2)'. The table has columns: INDEX, VLAN ID, UNDERLYING INTERFACE, NAME, TAGGING, and MTU. Two rows are visible, both highlighted with a red border. The first row has INDEX 0, VLAN ID 1, UNDERLYING INTERFACE GROUP_1, NAME TEAMS, TAGGING Untagged, and MTU 1500. The second row has INDEX 1, VLAN ID 1, UNDERLYING INTERFACE GROUP_2, NAME TEKVLAN, TAGGING Untagged, and MTU 1500.

INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING	MTU
0	1	GROUP_1	TEAMS	Untagged	1500
1	1	GROUP_2	TEKVLAN	Untagged	1500

Figure 26 – Ethernet Devices

4.4.3 Configure IP Network Interfaces

To configure IP Network interfaces, navigate to the **IP Network tab** → **Core Entities menu** → **Interfaces Table**.

Configure the WAN and LAN interface (interface towards Teams and LAN) as shown below:

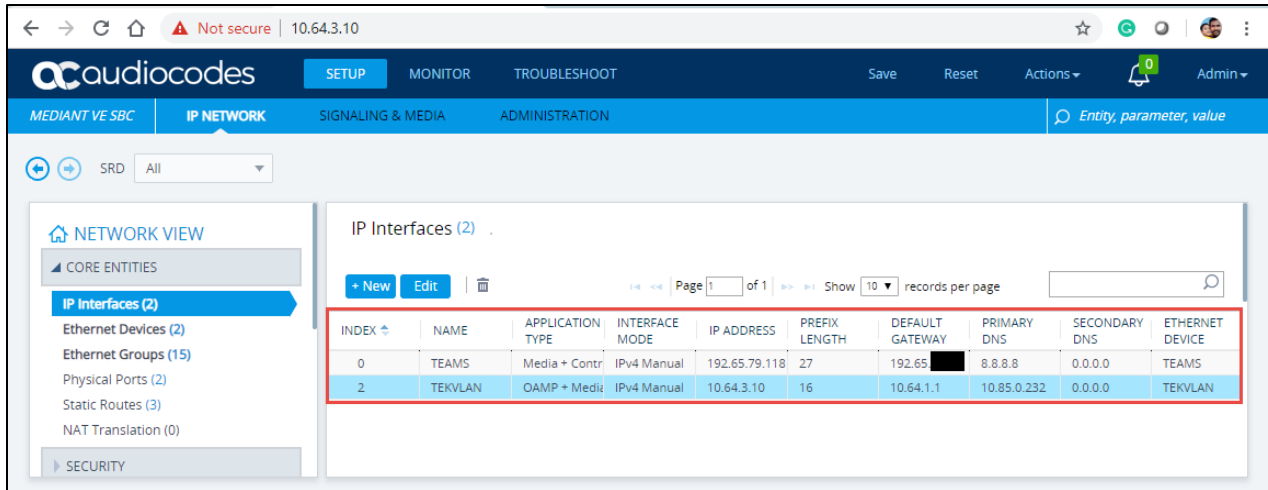


Figure 27 – IP interface Devices

IP interface TEAMS

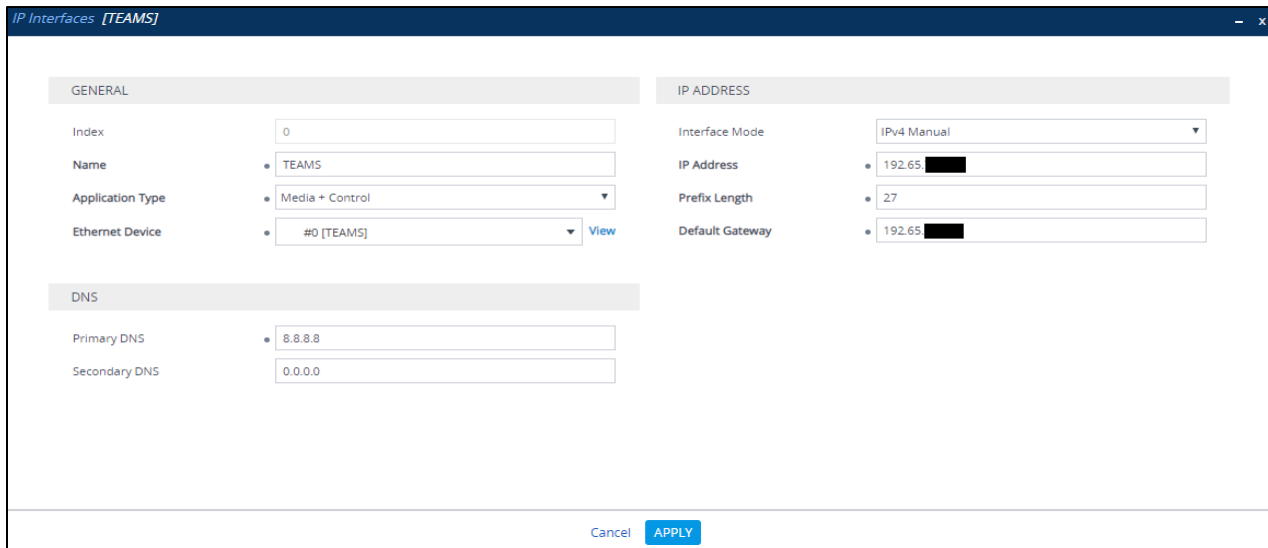


Figure 28 – IP interface Devices

IP Interfaces – TEKVLAN

Figure 29 – IP interface Devices

4.4.4 Configure DNS SRV Records

Microsoft Teams Direct Routing uses primary, secondary and tertiary datacenters for call routing.

AudioCodes Mediant 1000 SBC uses internal SRV records to resolve the FQDN of these datacenters.

To configure DNS SRV records, navigate to the **IP Network tab → DNS menu → Internal SRV Table**.

Configure a DNS SRV records as shown below and associate it under proxy set towards Teams

GENERAL		2ND ENTRY	
Domain Name	• teams.local	DNS Name 2	• sip2.pstnhub.microsoft.com
Transport Type	• TLS	Priority 2	• 2
1ST ENTRY		Weight 2	• 1
DNS Name 1	• sip.pstnhub.microsoft.com	Port 2	• 5061
Priority 1	• 1	3RD ENTRY	
Weight 1	• 1	DNS Name 3	• sip3.pstnhub.microsoft.com
Port 1	• 5061	Priority 3	• 3
		Weight 3	• 1
		Port 3	• 5061

Figure 30 – DNS SRV Records

4.4.5 Configure SRTP

By default, SRTP is disabled.

To enable SRTP, navigate to **Setup** → **Signaling and Media** → **Media** → **Media Security**. Set the parameter 'Media Security' to Enable; configure the other parameters as shown below

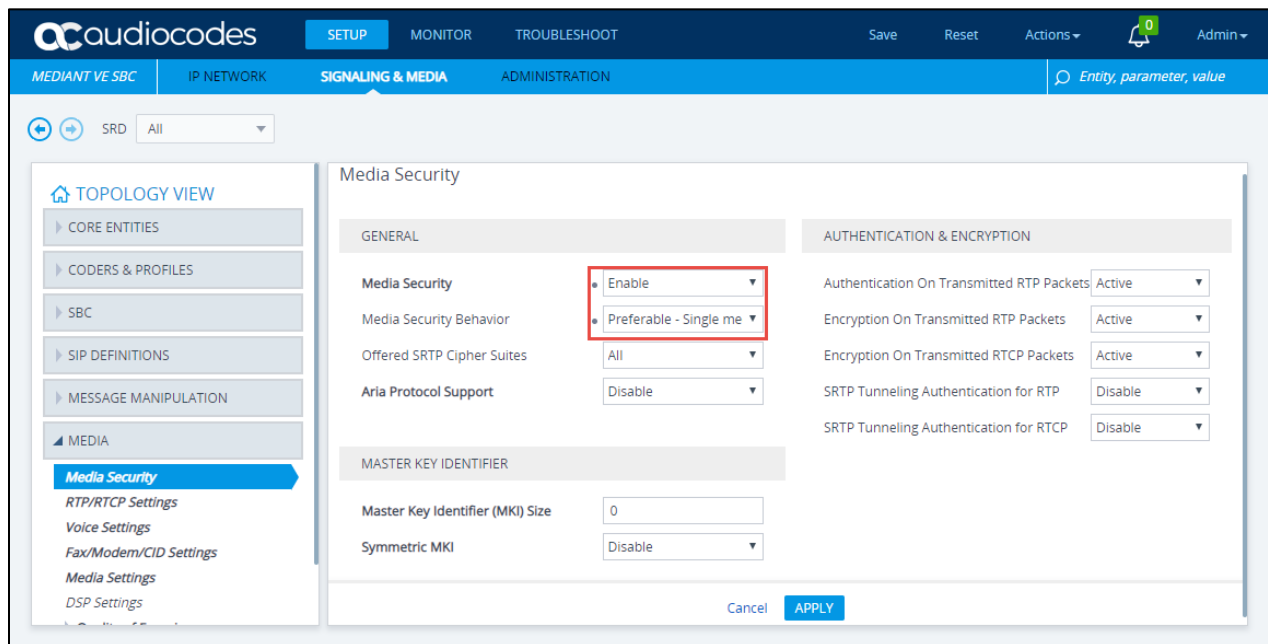


Figure 31 – Media Security

4.4.6 Configure TLS contexts

Microsoft Teams Direct Routing allows only TLS connections from SBCs for SIP traffic with a certificate signed by one of the trusted Certification Authorities. Currently, supported Certification Authorities are:

- AffirmTrust
- AddTrust External CA Root
- Baltimore CyberTrust Root
- Buypass
- Cybertrust
- Class 3 Public Primary Certification Authority
- Comodo Secure Root CA
- Deutsche Telekom

- DigiCert Global Root CA
- DigiCert High Assurance EV Root CA
- Entrust
- GlobalSign
- Go Daddy
- GeoTrust
- Verisign, Inc.
- Starfield
- Symantec Enterprise Mobile Root for Microsoft
- SwissSign
- Thawte Timestamping CA
- Trustwave
- TeliaSonera
- T-Systems International GmbH (Deutsche Telekom)
- QuoVadis

Please refer to the below URL for latest Certification Authorities trusted by Microsoft Teams Direct Routing. <https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan>

To configure TLS contexts, navigate to **IP Network** tab → **Security** menu → **TLS Contexts**. Create a new TLS context for Teams as shown below.

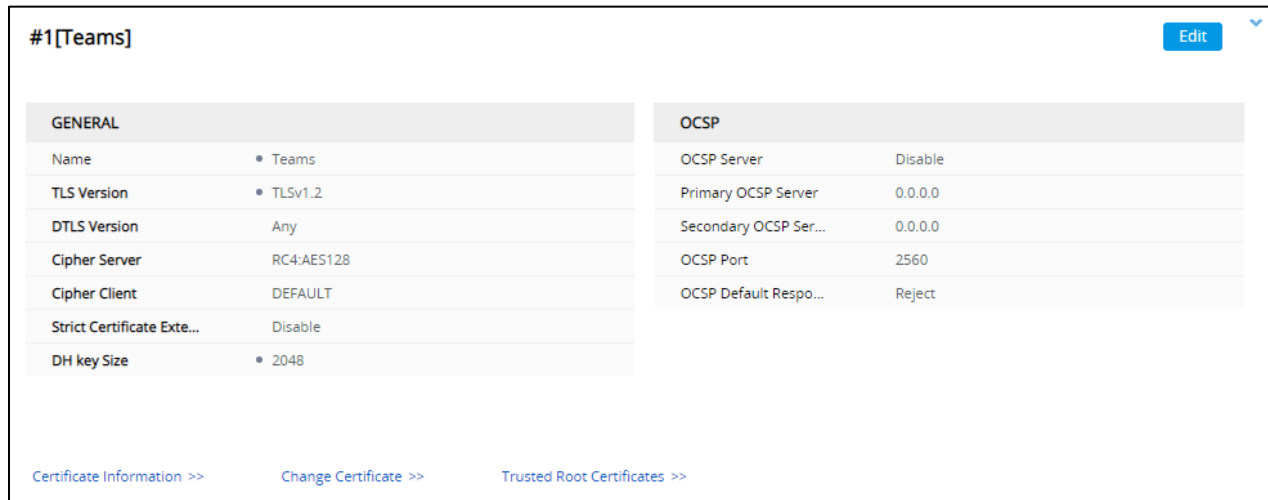


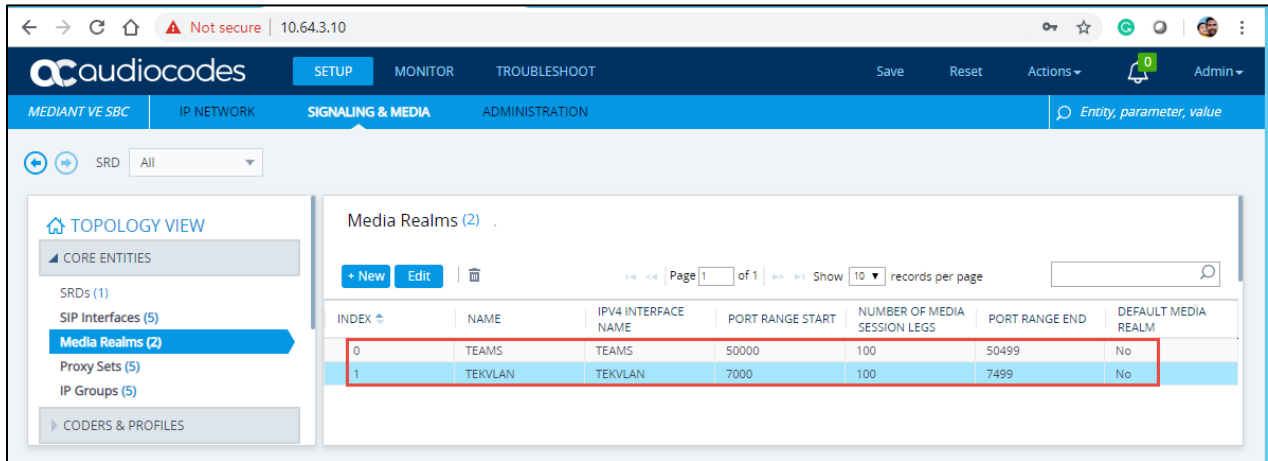
Figure 32 – Teams TLS

Once TLS context is configured, click on the change certificate and generate a CSR. Get the CSR signed from a CA trusted by direct routing and upload it to the same TLS context under change certificates. Import the root and intermediate Certificates to the trusted root certificates shown above.

Note: Root certificate used by Microsoft Direct Routing has to be uploaded to the SBC trusted root certificates.

4.4.7 Configure Media Realms

To configure Media Realm, navigate to **Signaling & Media** tab -> **Core Entities** menu -> **Media Realms**.

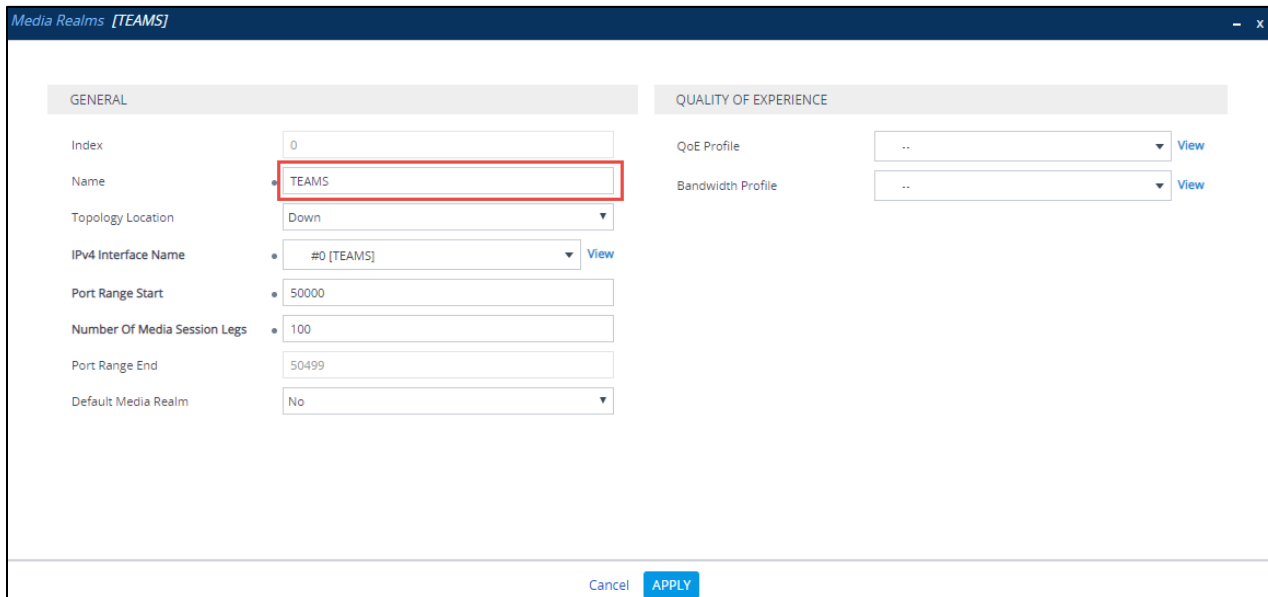


The screenshot shows the Audiocodes management console interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The main navigation tabs are 'MEDIANT VE SBC', 'IP NETWORK', 'SIGNALING & MEDIA', and 'ADMINISTRATION'. The 'SIGNALING & MEDIA' tab is active, and the 'CORE ENTITIES' menu is expanded to show 'Media Realms (2)'. The table below shows the configuration for two Media Realms:

INDEX	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	TEAMS	TEAMS	50000	100	50499	No
1	TEKVLAN	TEKVLAN	7000	100	7499	No

Figure 33 – Media Realms

Configure a Media Realm for WAN traffic – “Teams” as shown below:



The screenshot shows the configuration details for the 'TEAMS' Media Realm. The 'Name' field is highlighted with a red box. The configuration is as follows:

GENERAL	QUALITY OF EXPERIENCE
Index: 0	QoE Profile: .. View
Name: TEAMS	Bandwidth Profile: .. View
Topology Location: Down	
IPv4 Interface Name: #0 [TEAMS] View	
Port Range Start: 50000	
Number Of Media Session Legs: 100	
Port Range End: 50499	
Default Media Realm: No	

Figure 34 – Teams

Configure a Media Realm for LAN traffic – “TEKVLAN” as shown below:

GENERAL		QUALITY OF EXPERIENCE	
Index	1	QoS Profile	.. View
Name	TEKVLAN	Bandwidth Profile	.. View
Topology Location	Up		
IPv4 Interface Name	#2 [TEKVLAN] View		
Port Range Start	7000		
Number Of Media Session Legs	100		
Port Range End	7499		
Default Media Realm	No		

Figure 35 – LAN LAB

4.4.8 Configure the SRD

To configure Signaling Routing Domains (SRD), navigate to **Signaling & Media tab → Core Entities menu → SRD Table**

Here the default SRD is used as shown below.

#0[DefaultSRD] Edit

GENERAL		REGISTRATION	
Name	• DefaultSRD	Max. Number o...	-1
Sharing Policy	Shared	User Security M...	Accept All
SBC Operation ...	B2BUA	Enable Un-Auth...	Enable
SBC Routing Pol...	• # [Default_SBCRoutingPolicy] View		
Used By Routin...	Not Used		
Dial Plan	# [-] View		
CAC Profile	# [-] View		

Figure 36 – Default SRD

4.4.9 Configure SIP Signaling Interface

For this test, three external SIP interfaces were configured on the SBC. To configure SIP interfaces, navigate to **Signaling & Media** tab → **Core Entities** menu → **SIP Interface Table**.

Configure a SIP interface for the WAN (towards Teams) as shown below.

The screenshot shows the configuration page for a SIP interface named 'TEAMS'. The 'GENERAL' section includes fields for Index (0), Name (TEAMS), Topology Location (Down), Network Interface (#0 [TEAMS]), Application Type (SBC), UDP Port (5060), TCP Port (0), TLS Port (5061), Additional UDP Ports, Additional UDP Ports Mode (Always Open), and Encapsulating Protocol (No encapsulation). The 'MEDIA' section includes Media Realm (#0 [TEAMS]), Direct Media (Disable), and SECURITY section includes TLS Context Name (#1 [Teams]), TLS Mutual Authentication (Enable), Message Policy (--), User Security Mode (Not Configured), Enable Un-Authenticated Registrations (Not configured), and Max. Number of Registered Users (-1).

Figure 37 – Teams

The screenshot shows the bottom part of the configuration page. It includes fields for Enable TCP Keepalive (Enable), Used By Routing Server (Not Used), Pre-Parsing Manipulation Set (--), and CAC Profile (--). Below this is the CLASSIFICATION section with Classification Failure Response Type (0), Pre-classification Manipulation Set ID (-1), and Call Setup Rules Set ID (-1). At the bottom are Cancel and APPLY buttons.

Figure 38 – Teams

Configure a SIP interface for the LAN (towards PSTN Gateway) as shown below.

SIP Interfaces [PSTNGW]

SRD #0 [DefaultSRD]

GENERAL

Index: 1

Name: PSTNGW

Topology Location: Up

Network Interface: #2 [TEKVLAN]

Application Type: SBC

UDP Port: 5060

TCP Port: 0

TLS Port: 0

Additional UDP Ports:

Additional UDP Ports Mode: Always Open

Encapsulating Protocol: No encapsulation

MEDIA

Media Realm: #1 [TEKVLAN]

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

Figure 39 – PSTN

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

Cancel APPLY

Figure 40 – PSTN

Configure a SIP interface for the LAN (towards Avaya SBCE) as shown below.

SIP Interfaces [AVAYA]

SRD #0 [DefaultSRD]

GENERAL

Index: 3

Name: AVAYA

Topology Location: Down

Network Interface: #2 [TEKVLAN]

Application Type: SBC

UDP Port: 5064

TCP Port: 0

TLS Port: 0

Additional UDP Ports:

Additional UDP Ports Mode: Always Open

Encapsulating Protocol: No encapsulation

MEDIA

Media Realm: #1 [TEKVLAN]

Direct Media: Disable

SECURITY

TLS Context Name: #0 [default]

TLS Mutual Authentication:

Message Policy: ..

User Security Mode: Not Configured

Enable Un-Authenticated Registrations: Not configured

Max. Number of Registered Users: -1

Figure 41 – Avaya

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

Cancel APPLY

Figure 42 – Avaya

4.4.10 Configure Proxy Sets

The Proxy Set defines the destination address (IP address or FQDN) of the SIP entity server.

For the test, three Proxy Sets were configured: one for the Microsoft Teams, PSTN Gateway and another one towards Avaya SBCE. These proxy sets were later associated with IP Groups.

To configure Proxy Sets, navigate to **Signaling & Media** tab → **Core Entities** menu → **Proxy Sets Table**

Configure a Proxy Set for the Teams as shown below.

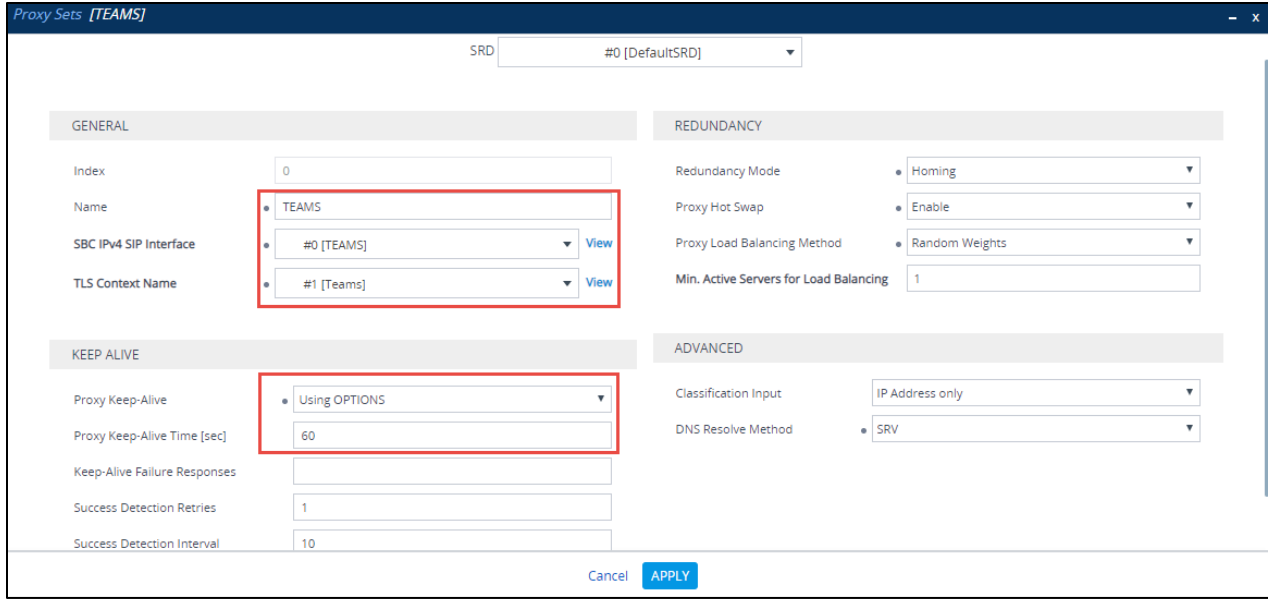


Figure 43 – Teams

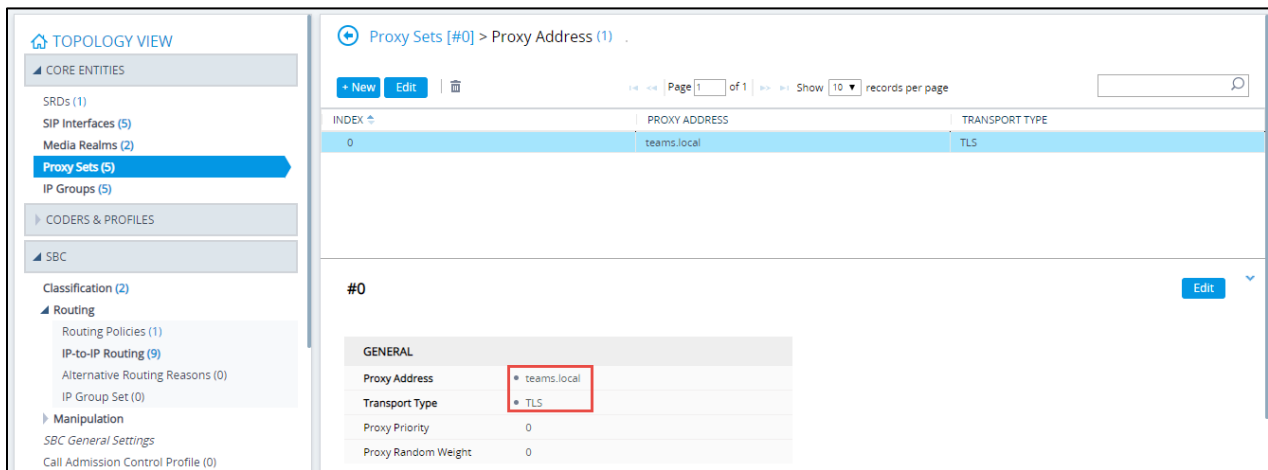


Figure 44 – Teams

Configure a Proxy Set for the PSTN Gateway as shown below.

Proxy Sets [PSTNGW]

SRD #0 [DefaultSRD]

GENERAL

Index: 1

Name: PSTNGW

SBC IPv4 SIP Interface: #1 [PSTNGW] [View](#)

TLS Context Name: .. [View](#)

REDUNDANCY

Redundancy Mode: [Dropdown]

Proxy Hot Swap: Disable

Proxy Load Balancing Method: Disable

Min. Active Servers for Load Balancing: 1

KEEP ALIVE

Proxy Keep-Alive: Using OPTIONS

Proxy Keep-Alive Time [sec]: 60

Keep-Alive Failure Responses: [Text Box]

Success Detection Retries: 1

Success Detection Interval: 10

ADVANCED

Classification Input: IP Address only

DNS Resolve Method: [Dropdown]

Figure 45 – PSTN Gateway

Keep-Alive Failure Responses: [Text Box]

Success Detection Retries: 1

Success Detection Interval: 10

Cancel [APPLY](#)

Figure 46 – PSTN Gateway

Configure a Proxy Set for the Avaya SBCE as shown below.

Proxy Sets [AVAYA]

SRD #0 [DefaultSRD]

GENERAL

Index: 3

Name: AVAYA

SBC IPv4 SIP Interface: #3 [AVAYA] [View](#)

TLS Context Name: .. [View](#)

REDUNDANCY

Redundancy Mode: [Dropdown]

Proxy Hot Swap: Disable

Proxy Load Balancing Method: Disable

Min. Active Servers for Load Balancing: 1

KEEP ALIVE

Proxy Keep-Alive: Using OPTIONS

Proxy Keep-Alive Time [sec]: 60

Keep-Alive Failure Responses: [Text Box]

Success Detection Retries: 1

Success Detection Interval: 10

ADVANCED

Classification Input: IP Address only

DNS Resolve Method: [Dropdown]

Figure 47 – Avaya

Success Detection Interval	<input type="text" value="10"/>
Failure Detection Retransmissions	<input type="text" value="-1"/>
<input type="button" value="Cancel"/> <input type="button" value="APPLY"/>	

Figure 48 – Avaya

4.4.11 Configure IP Groups

The IP Group represents an IP entity on the network with which the SBC communicates. 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 the source and destination of the call.

For the test, IP Groups were configured for the following IP entities:

- Microsoft Teams
- PSTN Gateway – SIP Trunk
- Avaya SBCE – SIP Trunk

To configure IP groups, navigate to **Signaling & Media** tab → **Core Entities** menu → **IP Group Table**

Configure an IP Group for Microsoft Teams as shown below

The screenshot shows the configuration page for an IP Group named 'TEAMS'. The 'GENERAL' section includes fields for Index (0), Name (TEAMS), Topology Location (Down), Type (Server), Proxy Set (#0 [TEAMS]), IP Profile (#1 [TEAMS_Profile]), Media Realm (#0 [TEAMS]), Contact User, SIP Group Name (sbc4.tekvizionlabs.com), Created By Routing Server (No), and Used By Routing Server (Not Used). The 'QUALITY OF EXPERIENCE' section includes QoS Profile and Bandwidth Profile dropdowns. The 'MESSAGE MANIPULATION' section includes Inbound and Outbound Message Manipulation Sets (both set to 1 and 2), two User-Defined String fields, and Proxy Keep-Alive settings (Enable). The 'SBC REGISTRATION AND AUTHENTICATION' section is partially visible at the bottom.

Figure 49 – IP Group – Teams – Contd.

IP Groups [TEAMS]

Proxy Set Connectivity: Connected

Max. Number of Registered Users: -1

Registration Mode: User Initiates Registration

User Stickiness: Disable

User UDP Port Assignment: Disable

Authentication Mode: User Authenticates

Authentication Method List:

SBC Server Authentication Type: According to Global Parameter

OAuth HTTP Service: .. View

Username: Admin

Password:

SBC GENERAL

Classify By Proxy Set: Disable

SBC Operation Mode: Not Configured

SBC Client Forking Mode: Sequential

CAC Profile: .. View

ADVANCED

Local Host Name: sbc4.tekvizionlabs.com

UII Format: Disable

Always Use Src Address: No

GW GROUP STATUS

GW Group Registered IP Address:

GW Group Registered Status: Not Registered

Figure 50 – IP Group – Teams – Contd.

SBC ADVANCED

Source URI Input:

Destination URI Input:

SIP Connect: No

SBC PSAP Mode: Disable

Route Using Request URI Port: Disable

DTLS Context: #1 [Teams] View

Keep Original Call-ID: No

Dial Plan: .. View

Call Setup Rules Set ID: -1

Tags:

Cancel APPLY

Figure 51 – IP Group – Teams

Configure an IP Group for PSTN Gateway as shown below

IP Groups [PSTNGW] SRD #0 [DefaultSRD]

GENERAL		QUALITY OF EXPERIENCE	
Index	1	QoE Profile	-- View
Name	PSTNGW	Bandwidth Profile	-- View
Topology Location	Up	MESSAGE MANIPULATION	
Type	Server	Inbound Message Manipulation Set	0
Proxy Set	#1 [PSTNGW] View	Outbound Message Manipulation Set	3
IP Profile	#2 [PSTNGW_Profile] View	Message Manipulation User-Defined String 1	
Media Realm	#1 [TEKVLAN] View	Message Manipulation User-Defined String 2	
Contact User		Proxy Keep-Alive using IP Group settings	Enable
SIP Group Name	10.64.1.72	SBC REGISTRATION AND AUTHENTICATION	
Created By Routing Server	No		
Used By Routing Server	Not Used		

Figure 52 – IP Group – PSTN – Contd.

IP Groups [PSTNGW] Connected

Proxy Set Connectivity	Connected	Max. Number of Registered Users	-1
SBC GENERAL		Registration Mode	User Initiates Registration
Classify By Proxy Set	Enable	User Stickiness	Disable
SBC Operation Mode	Not Configured	User UDP Port Assignment	Disable
SBC Client Forking Mode	Sequential	Authentication Mode	User Authenticates
CAC Profile	-- View	Authentication Method List	
ADVANCED		SBC Server Authentication Type	According to Global Parameter
Local Host Name		OAuth HTTP Service	-- View
UUI Format	Disable	Username	Admin
Always Use Src Address	No	Password	*****
		GW GROUP STATUS	
		GW Group Registered IP Address	
		GW Group Registered Status	Not Registered

Figure 53 – IP Group – PSTN – Contd.

SBC ADVANCED	
Source URI Input	<input type="text"/>
Destination URI Input	<input type="text"/>
SIP Connect	No
SBC PSAP Mode	Disable
Route Using Request URI Port	Disable
DTLS Context	#0 [default] View
Keep Original Call-ID	No
Dial Plan	-- View
Call Setup Rules Set ID	-1
Tags	<input type="text"/>

Cancel [APPLY](#)

Figure 54 – IP Group

Configure an IP Group for Avaya SBCE as shown below

IP Groups [AVAYA] - x

SRD

GENERAL	QUALITY OF EXPERIENCE
Index: <input type="text" value="3"/>	QoS Profile: <input type="text" value="--"/> View
Name: <input style="border: 2px solid red;" type="text" value="AVAYA"/>	Bandwidth Profile: <input type="text" value="--"/> View
Topology Location: <input type="text" value="Down"/>	
Type: <input type="text" value="Server"/>	
Proxy Set: <input style="border: 2px solid red;" type="text" value="#3 [AVAYA]"/> View	
IP Profile: <input style="border: 2px solid red;" type="text" value="#4 [AVAYA_Profile]"/> View	
Media Realm: <input style="border: 2px solid red;" type="text" value="#1 [TEKVLAN]"/> View	
Contact User: <input type="text"/>	
SIP Group Name: <input style="border: 2px solid red;" type="text" value="10.64.5.57"/>	
Created By Routing Server: <input type="text" value="No"/>	

MESSAGE MANIPULATION

Inbound Message Manipulation Set:

Outbound Message Manipulation Set:

Message Manipulation User-Defined String 1:

Message Manipulation User-Defined String 2:

Proxy Keep-Alive using IP Group settings:

Figure 55 – IP Group – Avaya – Contd.

Figure 56 – IP Group – Avaya – Contd.

Figure 57 – IP Group

4.4.12 Configure IP Profile

The IP Profile defines a set of call capabilities relating to signaling.

For this test, IP Profiles were configured for the following IP entities:

- Microsoft Teams
- PSTN Gateway – SIP Trunk
- Avaya SBCE – SIP Trunk

To configure IP profiles, navigate to **Signaling & Media** tab → **Coders and Profiles** → **IP Profile Settings**.
Click **Add**.

Configure the IP Profile for the Microsoft Teams as shown below.

The screenshot shows the configuration for the IP Profile 'TEAMS_Profile'. The settings are as follows:

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

Figure 58 – IP Profile – Teams – Contd.

The screenshot shows the configuration for the IP Profile 'TEAMS_Profile' in the SBC EARLY MEDIA, SBC REGISTRATION, and SBC FORWARD AND TRANSFER sections. The settings are as follows:

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

Figure 59 – IP Profile – Teams – Contd.

IP Profiles [TEAMS_Profile]

SBC MEDIA

Mediation Mode: RTP Mediation

Extension Coders Group: #0 [AudioCodersGroups_0]

Allowed Audio Coders: #0 [AllowedAudioCodersGroup_TEAMS]

Allowed Coders Mode: Preference

Allowed Video Coders: ..

Allowed Media Types:

Direct Media Tag:

RFC 2833 Mode: As Is

RFC 2833 DTMF Payload Type: 101

Alternative DTMF Method: As Is

Send Multiple DTMF Methods: Disable

Adapt RFC2833 BW to Voice coder BW: Disabled

SDP Ptime Answer: Preferred Value

Remote 3xx Mode: Handle Locally

SBC HOLD

Remote Hold Format: Inactive

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

Figure 60 – IP Profile – Teams – Contd.

IP Profiles [TEAMS_Profile]

Preferred PTime: 20

Use Silence Suppression: Add

RTP Redundancy Mode: As Is

RTCP Mode: Generate Always

Jitter Compensation: Disable

ICE Mode: Lite

SDP Handle RTCP: Don't Care

RTCP Mux: 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

GATEWAY

Coders Group: #0 [AudioCodersGroups_0]

LOCAL TONES

Local RingBack Tone Index: -1

Local Held Tone Index: -1

Figure 61 – IP Profile – Teams – Contd.

IP Profiles [TEAMS_Profile]

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 Canceled: Line

Input Gain (-32 to 31 dB): 0

Voice Volume (-32 to 31 dB): 0

Cancel APPLY

Figure 62 – IP Profile – Teams – Contd.

Configure the IP Profile for the PSTN Gateway as shown below.

IP Profiles [PSTNGW_Profile]

GENERAL

Index: 2

Name: PSTNGW_Profile

Created by Routing Server: No

MEDIA SECURITY

SBC Media Security Mode: RTP

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

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: Supported Only After Connect

Remote re-INVITE: Supported only with SDP

Remote Delayed Offer Support: Not Supported

Remote Representation Mode: According to Operation Mode

Keep Incoming Via Headers: According to Operation Mode

Keep Incoming Routing Headers: According to Operation Mode

Keep User-Agent Header: According to Operation Mode

Figure 63 – IP Profile – PSTN Gateway – Contd.

IP Profiles [PSTNGW_Profile]

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

Figure 64 – IP Profile – PSTN Gateway – Contd.

IP Profiles [PSTNGW_Profile]

SBC MEDIA		Remote 3xx Mode	Transparent
Mediation Mode	RTP Mediation	SBC HOLD	
Extension Coders Group	..	Remote Hold Format	Transparent
Allowed Audio Coders	#1 [AllowedAudioCodersGroup_PSTNGW]	Reliable Held Tone Source	Yes
Allowed Coders Mode	Restriction	Play Held Tone	No
Allowed Video Coders	..	SBC FAX	
Allowed Media Types		Fax Coders Group	..
Direct Media Tag		Fax Mode	As Is
RFC 2833 Mode	As Is	Fax Offer Mode	All coders
RFC 2833 DTMF Payload Type	101	Fax Answer Mode	Single coder
Alternative DTMF Method	As Is	Remote Renegotiate on Fax Detection	Transparent
Send Multiple DTMF Methods	Disable	Fax Rerouting Mode	Disable
Adapt RFC2833 BW to Voice coder BW	Disabled		
SDP Ptime Answer	Preferred Value		

Figure 65 – IP Profile – PSTN Gateway – Contd.

IP Profiles [PSTNGW_Profile]

Preferred PTime	20	
Use Silence Suppression	Add	▼
RTP Redundancy Mode	As Is	▼
RTCP Mode	Generate Always	▼
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 ▼
GATEWAY	
Coders Group	#0 [AudioCodersGroups_0] ▼
LOCAL TONES	
Local RingBack Tone Index	-1
Local Held Tone Index	-1

Figure 66 – IP Profile – PSTN Gateway – Contd.

IP Profiles [PSTNGW_Profile]

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 ▼
Input Gain (-32 to 31 dB)	0
Voice Volume (-32 to 31 dB)	0

Cancel **APPLY**

Figure 67 – IP Profile – PSTN Gateway

Configure the IP Profile for the Avaya as shown below.

IP Profiles [AVAYA_Profile]

GENERAL		SBC SIGNALING	
Index	4	PRACK Mode	Transparent
Name	AVAYA_Profile	P-Asserted-Identity Header Mode	Add
Created by Routing Server	No	Diversion Header Mode	Add
MEDIA SECURITY		History-Info Header Mode	As Is
SBC Media Security Mode	RTP	Session Expires Mode	Supported
Symmetric MKI	Disable	Remote Update Support	Supported
MKI Size	0	Remote re-INVITE	Supported
SBC Enforce MKI Size	Don't enforce	Remote Delayed Offer Support	Supported
SBC Media Security Method	SDES	Remote Representation Mode	According to Operation Mode
Reset SRTP Upon Re-key	Disable	Keep Incoming Via Headers	According to Operation Mode
Generate SRTP Keys Mode	Only If Required	Keep Incoming Routing Headers	According to Operation Mode
		Keep User-Agent Header	According to Operation Mode

Figure 68 – IP Profile – Avaya.

IP Profiles [AVAYA_Profile]

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

Figure 69 – IP Profile – Avaya – Contd.

IP Profiles [AVAYA_Profile]

SBC MEDIA		Remote 3xx Mode	Transparent
Mediation Mode	RTP Mediation	SBC HOLD	
Extension Coders Group	..	Remote Hold Format	Transparent
Allowed Audio Coders	#1 [AllowedAudioCodersGroup_PSTNGW]	Reliable Held Tone Source	Yes
Allowed Coders Mode	Restriction	Play Held Tone	No
Allowed Video Coders	..	SBC FAX	
Allowed Media Types		Fax Coders Group	..
Direct Media Tag		Fax Mode	As Is
RFC 2833 Mode	As Is	Fax Offer Mode	All coders
RFC 2833 DTMF Payload Type	0	Fax Answer Mode	Single coder
Alternative DTMF Method	As Is	Remote Renegotiate on Fax Detection	Transparent
Send Multiple DTMF Methods	Disable	Fax Rerouting Mode	Disable
Adapt RFC2833 BW to Voice coder BW	Disabled		
SDP Ptime Answer	Remote Answer		

Figure 70 – IP Profile – Avaya – Contd.

IP Profiles [AVAYA_Profile]

Use Silence Suppression	Transparent	MEDIA	
RTP Redundancy Mode	As Is	Broken Connection Mode	Disconnect
RTCP Mode	Transparent	Media IP Version Preference	Only IPv4
Jitter Compensation	Disable	RTP Redundancy Depth	Disable
ICE Mode	Disable	GATEWAY	
SDP Handle RTCP	Don't Care	Coders Group	#0 [AudioCodersGroups_0]
RTCP Mux	Not Supported	LOCAL TONES	
RTCP Feedback	Feedback Off	Local RingBack Tone Index	-1
Voice Quality Enhancement	Disable	Local Held Tone Index	-1
Max Opus Bandwidth	0		
Generate No-op	No		
Enhanced PLC	Disable		

Figure 71 – IP Profile – Avaya – Contd.

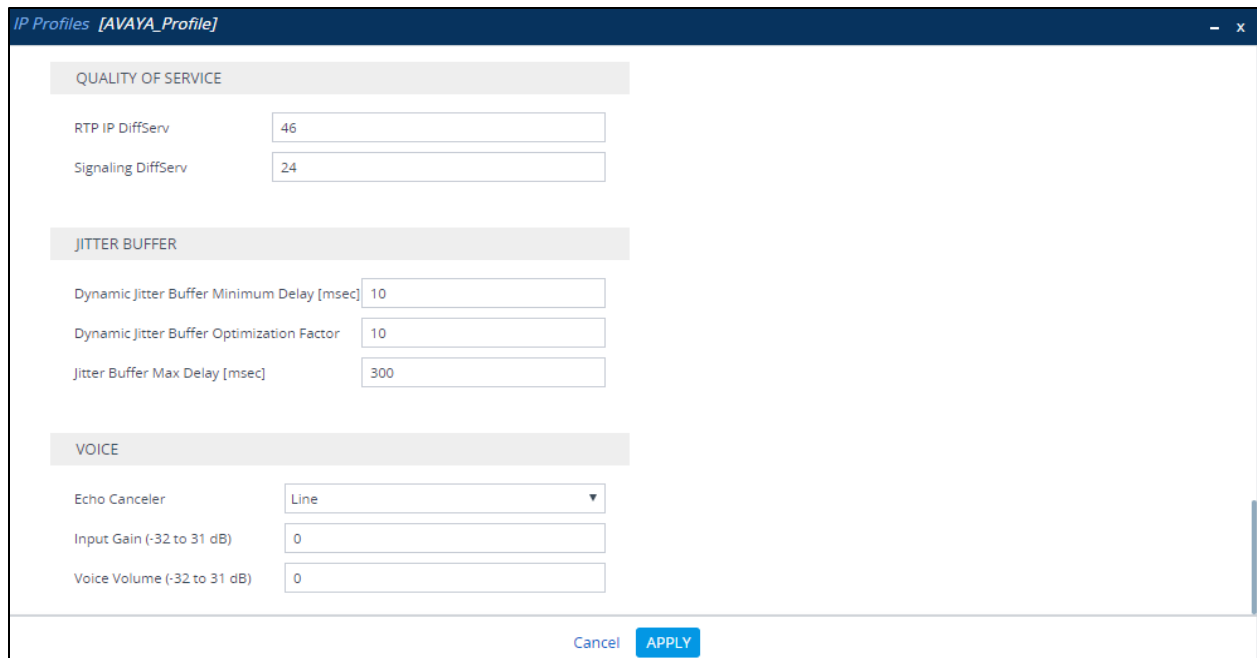


Figure 72 – IP Profile – Avaya

4.4.13 Configure SIP Definition and General Setting

The screenshot below captures the configuration of the **SIP Definitions General Settings** that were used during the test for the successful test execution

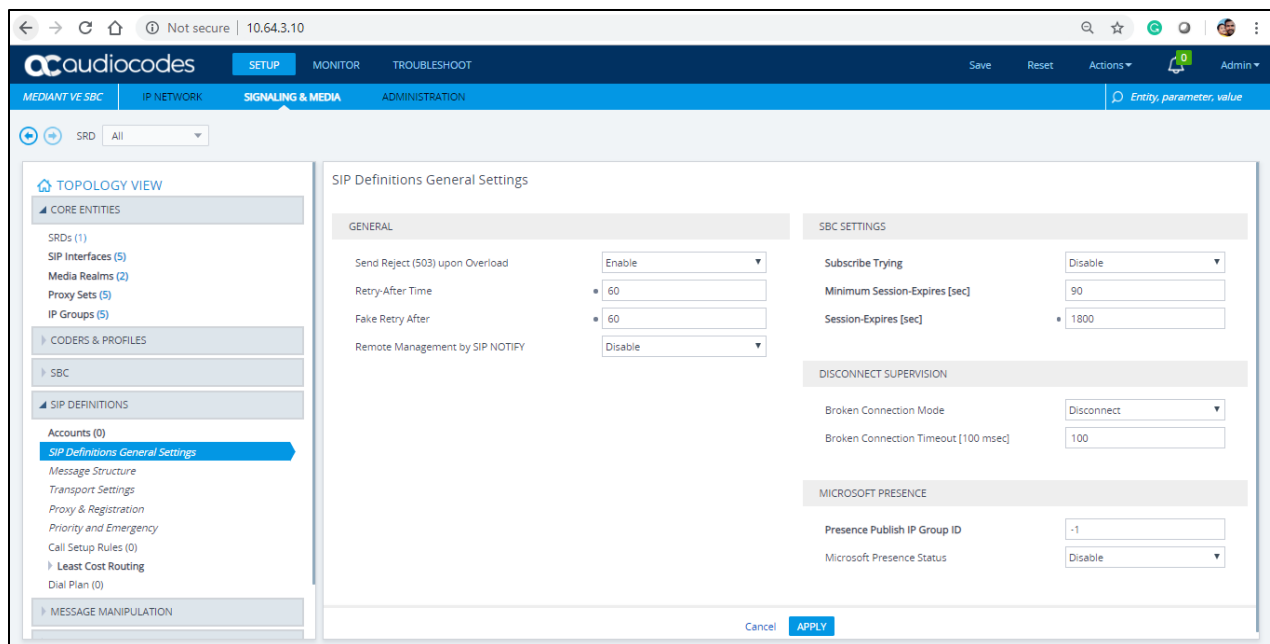


Figure 73 – SIP Definition

4.4.14 Configure SBC General Settings

The screenshot below captures the configuration of the **SBC General Parameters** that was used during the test for the successful test execution.

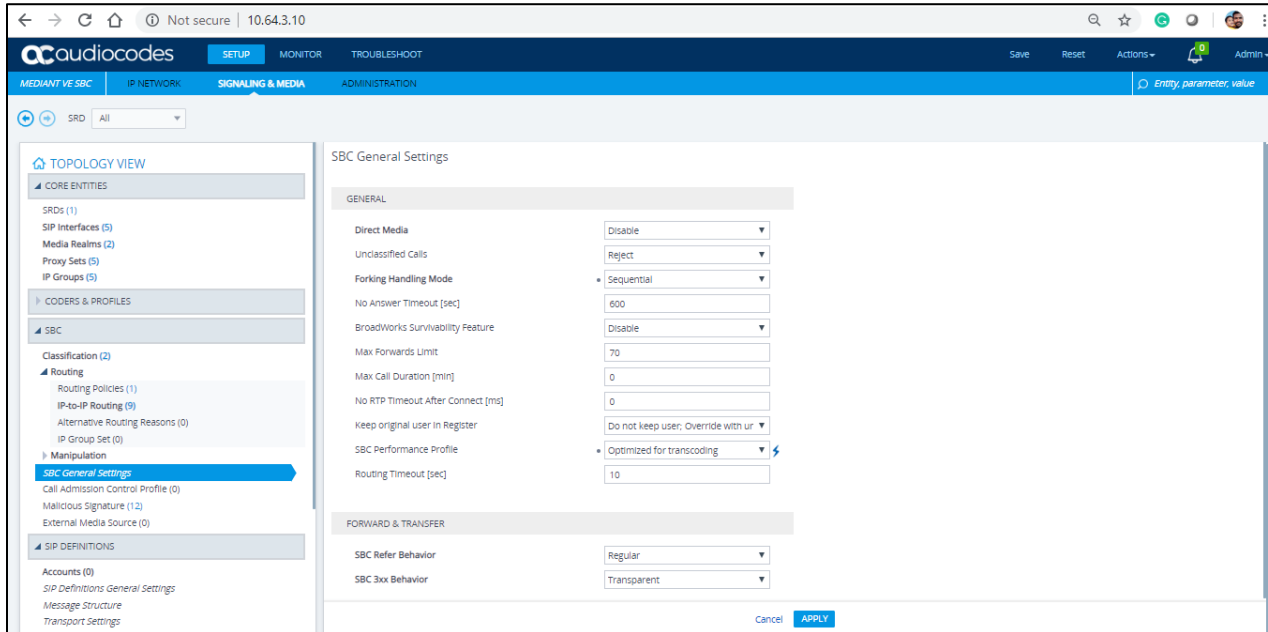


Figure 74 – SBC General Setting – Contd.

4.4.15 Configure IP-to-IP Routing Rules

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

For the test, the following IP-To-IP Routing rules were configured to route calls between the Teams and CenturyLink

- Calls from Teams to PSTN Gateway
- Calls from PSTN Gateway to Teams
- Calls from Teams to Avaya
- Calls from Avaya to Teams

To configure IP-to-IP routing rules, navigate to **Signaling & Media** tab → **SBC** menu → **Routing** → **IP-to-IP Routing Table**.

Click **Add**.

Calls from Teams to PSTN Gateway

Routing Policy: #0 [Default_SBCRoutingPolicy]

GENERAL

Index: 4

Name: TEAMS -> PSTN

Alternative Route Options: Route Row

MATCH

Source IP Group: #0 [TEAMS]

Request Type: All

Source Username Pattern: *

Source Host: *

Source Tag: (empty)

ACTION

Destination Type: IP Group

Destination IP Group: #1 [PSTNGW]

Destination SIP Interface: #1 [PSTNGW]

Destination Address: (empty)

Destination Port: 0

Destination Transport Type: (empty)

IP Group Set: ..

Call Setup Rules Set ID: -1

Group Policy: Sequential

Cost Group: ..

Buttons: Cancel, APPLY

Figure 75 – Teams to PSTN – Contd.

Destination Username Pattern: *

Destination Host: *

Destination Tag: (empty)

Message Condition: ..

Call Trigger: Any

ReRoute IP Group: Any

Routing Tag Name: default

Internal Action: (empty)

Buttons: Cancel, APPLY

Figure 76 – Teams to PSTN

Calls from PSTN Gateway to Teams

Routing Policy: #0 [Default_SBCRoutingPolicy]

GENERAL

Index: 6

Name: PSTNGW_to_TEAMS

Alternative Route Options: Route Row

MATCH

Source IP Group: #1 [PSTNGW]

Request Type: All

Source Username Pattern: *

Source Host: *

Source Tag: (empty)

Destination Username Pattern: *

ACTION

Destination Type: IP Group

Destination IP Group: #0 [TEAMS]

Destination SIP Interface: #0 [TEAMS]

Destination Address: (empty)

Destination Port: 0

Destination Transport Type: (empty)

IP Group Set: ..

Call Setup Rules Set ID: -1

Group Policy: Sequential

Cost Group: ..

Routing Tag Name: default

Buttons: Cancel, APPLY

Figure 77 – PSTN to Teams – Contd.

Destination Username Pattern	*	Routing Tag Name	default
Destination Host	*	Internal Action	<input type="text"/> Editor
Destination Tag			
Message Condition	.. View		
Call Trigger	Any		
ReRoute IP Group	Any View		
Cancel APPLY			

Figure 78 – PSTN to Teams

Calls from Teams to Avaya

IP-to-IP Routing [Teams -> Avaya]

Routing Policy #0 [Default_SBCRoutingPolicy]

GENERAL	ACTION
Index: <input type="text" value="3"/>	Destination Type: IP Group
Name: Teams -> Avaya	Destination IP Group: #3 [AVAYA] View
Alternative Route Options: Route Row	Destination SIP Interface: #3 [AVAYA] View
MATCH	
Source IP Group: #0 [TEAMS] View	Destination Address: <input type="text"/>
Request Type: All	Destination Port: <input type="text" value="0"/>
Source Username Pattern: <input type="text" value="*"/>	Destination Transport Type:
Source Host: <input type="text" value="*"/>	IP Group Set: .. View
Source Tag: <input type="text"/>	Call Setup Rules Set ID: <input type="text" value="-1"/>
	Group Policy: Sequential
	Cost Group: .. View

Figure 79 – Teams to Avaya.

Destination Username Pattern	7	Routing Tag Name	default
Destination Host	*	Internal Action	<input type="text"/> Editor
Destination Tag			
Message Condition	.. View		
Call Trigger	Any		
ReRoute IP Group	Any View		
Cancel APPLY			

Figure 80 – Teams to Avaya Contd.

IP-to-IP Routing [Avaya -> Teams]

Routing Policy #0 [Default_SBCRoutingPolicy]

GENERAL	ACTION
Index: 8	Destination Type: IP Group
Name: Avaya -> Teams	Destination IP Group: #0 [TEAMS] View
Alternative Route Options: Route Row	Destination SIP Interface: #0 [TEAMS] View
MATCH	
Source IP Group: #3 [AVAYA] View	Destination Address:
Request Type: All	Destination Port: 0
Source Username Pattern: *	Destination Transport Type:
Source Host: *	IP Group Set: -- View
Source Tag:	Call Setup Rules Set ID: -1
	Group Policy: Sequential
	Cost Group: -- View

Figure 81 –Avaya to Teams.

Destination Username Pattern: *	Routing Tag Name: default
Destination Host: *	Internal Action: Editor
Destination Tag:	
Message Condition: -- View	
Call Trigger: Any	
ReRoute IP Group: Any View	
Cancel APPLY	

Figure 82 –Avaya to Teams Contd.

4.4.16 IP Group

IP Group – Teams

The screenshot shows the configuration page for an IP Group named 'TEAMS'. The SRD is set to '#0 [DefaultSRD]'. The configuration is divided into three main sections:

- GENERAL:** Index: 0; Name: TEAMS; Topology Location: Down; Type: Server; Proxy Set: #0 [TEAMS]; IP Profile: #1 [TEAMS_Profile]; Media Realm: #0 [TEAMS]; Contact User: ; SIP Group Name: sdc4.tekvizionlabs.com; Created By Routing Server: No.
- QUALITY OF EXPERIENCE:** QoE Profile: --; Bandwidth Profile: --.
- MESSAGE MANIPULATION:** Inbound Message Manipulation Set: 1; Outbound Message Manipulation Set: 2; Message Manipulation User-Defined String 1: ; Message Manipulation User-Defined String 2: ; Proxy Keep-Alive using IP Group settings: Enable.

Figure 83 – IP Groups Teams – Contd.

The screenshot shows the configuration page for an IP Group named 'TEAMS', continuing from the previous section. The configuration is divided into three main sections:

- SBC GENERAL:** Classify By Proxy Set: Disable; SBC Operation Mode: Not Configured; SBC Client Forking Mode: Sequential; CAC Profile: --.
- ADVANCED:** Local Host Name: sdc4.tekvizionlabs.com; UI Format: Disable; Always Use Src Address: No.
- SBC REGISTRATION AND AUTHENTICATION:** Max. Number of Registered Users: -1; Registration Mode: User Initiates Registration; User Stickiness: Disable; User UDP Port Assignment: Disable; Authentication Mode: User Authenticates; Authentication Method List: ; SBC Server Authentication Type: According to Global Parameter; OAuth HTTP Service: --; Username: Admin; Password:

Figure 84 – IP Groups Teams – Contd.

SBC ADVANCED	
Source URI Input	<input type="text"/>
Destination URI Input	<input type="text"/>
SIP Connect	No
SBC PSAP Mode	Disable
Route Using Request URI Port	Disable
DTLS Context	#1 [Teams] View
Keep Original Call-ID	No
Dial Plan	.. View
Call Setup Rules Set ID	-1
Tags	<input type="text"/>

Cancel **APPLY**

Figure 85 – IP Groups Teams

IP Group – PSTN Gateway

IP Groups [PSTNGW]	
SRD: #0 [DefaultSRD]	
GENERAL	QUALITY OF EXPERIENCE
Index: 1	QoE Profile: .. View
Name: PSTNGW	Bandwidth Profile: .. View
Topology Location: Up	
Type: Server	MESSAGE MANIPULATION
Proxy Set: #1 [PSTNGW] View	Inbound Message Manipulation Set: 0
IP Profile: #2 [PSTNGW_Profile] View	Outbound Message Manipulation Set: 3
Media Realm: #1 [TEKVLAN] View	Message Manipulation User-Defined String 1: <input type="text"/>
Contact User: <input type="text"/>	Message Manipulation User-Defined String 2: <input type="text"/>
SIP Group Name: 10.64.1.72	Proxy Keep-Alive using IP Group settings: Enable
Created By Routing Server: No	

Figure 86 – IP Groups PSTN – Contd.

IP Groups [PSTNGW]	
Used By Routing Server: Not Used	SBC REGISTRATION AND AUTHENTICATION
Proxy Set Connectivity: Connected	Max. Number of Registered Users: -1
SBC GENERAL	Registration Mode: User Initiates Registration
Classify By Proxy Set: Enable	User Stickiness: Disable
SBC Operation Mode: Not Configured	User UDP Port Assignment: Disable
SBC Client Forking Mode: Sequential	Authentication Mode: User Authenticates
CAC Profile: .. View	Authentication Method List: <input type="text"/>
ADVANCED	SBC Server Authentication Type: According to Global Parameter
Local Host Name: <input type="text"/>	OAuth HTTP Service: .. View
UII Format: Disable	Username: Admin
Always Use Src Address: No	Password:
	GW GROUP STATUS
	GW Group Registered IP Address: <input type="text"/>

Figure 87 – IP Groups PSTN – Contd.

SBC ADVANCED	
Source URI Input	<input type="text"/>
Destination URI Input	<input type="text"/>
SIP Connect	No
SBC PSAP Mode	Disable
Route Using Request URI Port	Disable
DTLS Context	#0 [default] View
Keep Original Call-ID	No
Dial Plan	.. View
Call Setup Rules Set ID	-1
Tags	<input type="text"/>

Cancel **APPLY**

Figure 88 – IP Groups PSTN

IP Group – Avaya

SRD

GENERAL	QUALITY OF EXPERIENCE
Index: <input type="text" value="3"/>	QoE Profile: <input type="text" value="--"/> View
Name: <input type="text" value="AVAYA"/>	Bandwidth Profile: <input type="text" value="--"/> View
Topology Location: <input type="text" value="Down"/>	
Type: <input type="text" value="Server"/>	
Proxy Set: <input type="text" value="#3 [AVAYA]"/> View	
IP Profile: <input type="text" value="#4 [AVAYA_Profile]"/> View	
Media Realm: <input type="text" value="#1 [TEKVLAN]"/> View	
Contact User: <input type="text"/>	
SIP Group Name: <input type="text" value="10.64.5.57"/>	
Created By Routing Server: <input type="text" value="No"/>	

MESSAGE MANIPULATION	
Inbound Message Manipulation Set: <input type="text" value="6"/>	
Outbound Message Manipulation Set: <input type="text" value="7"/>	
Message Manipulation User-Defined String 1: <input type="text"/>	
Message Manipulation User-Defined String 2: <input type="text"/>	
Proxy Keep-Alive using IP Group settings: <input type="text" value="Disable"/>	

Figure 89 – IP Groups Avaya.

Figure 90 – IP Groups Avaya – Contd.

Figure 91 – IP Groups Avaya

Message Manipulation

A Message Manipulation rule defines a manipulation sequence for SIP messages. SIP message manipulation enables the normalization of SIP messaging fields between communicating network segments. SIP message manipulations can also be implemented to resolve incompatibilities between SIP devices inside the enterprise network.

Each Message Manipulation rule is configured with a Manipulation Set ID. Groups (sets) of Message Manipulation rules can be created by assigning each of the relevant Message Manipulation rules to the same Manipulation Set ID.

The SIP message manipulation feature supports the following:

- Manipulation on SIP message type (Method, Request/Response, and Response type)
- Addition of new SIP headers
- Removal of SIP headers
- Modification of SIP header components such as values, header values (e.g., URI value of the P-Asserted-Identity header can be copied to the From header), call's parameter values
- Deletion of SIP body (e.g., if a message body is not supported at the destination network this body is removed)
- Translating one SIP response code to another
- Topology hiding (generally present in SIP headers such as Via, Record Route, Route and Service-Route).
- Configurable identity hiding (information related to identity of subscribers, for example P-Asserted-Identity, Referred-By, Identity and Identity-Info)

To configure Message Manipulation rules, navigate to **Signaling & Media** tab → **Message Manipulations** menu → **Message Manipulations**.

Click **Add** and populate the required fields in the screen that appears as below:

GENERAL		ACTION	
Index	<input type="text" value="1"/>	Action Subject	<input type="text"/> Editor
Name	<input type="text"/>	Action Type	<input type="text" value="Add"/> ▼
Manipulation Set ID	<input type="text" value="0"/>	Action Value	<input type="text"/> Editor
Row Role	<input type="text" value="Use Current Condition"/> ▼		
MATCH			
Message Type	<input type="text"/> Editor		
Condition	<input type="text"/> Editor		

Figure 92 – SIP Message Manipulation

Then click **Add** again, once the parameters have been configured.

For this test, the following message manipulations were configured and assigned to one manipulation set ID.

Manipulation set ID = 1: Manipulation from Teams

Manipulation set ID = 2: Manipulation to Teams

Manipulation set ID = 3: Manipulation to PSTN

Manipulation set ID = 6: Manipulation from Avaya

Manipulation set ID = 7: Manipulation to Avaya

Manipulation from Teams

- To Remove "Privacy" header: To Remove Privacy Header from Teams

The screenshot shows a configuration window titled "Message Manipulations [Filter Privacy ID except for Anonymous]". It is divided into three main sections: GENERAL, MATCH, and ACTION. In the GENERAL section, the Name field is "Filter Privacy ID except for Anonymous" and the Manipulation Set ID is "1". In the MATCH section, the Message Type is "Invite.Request" and the Condition is "Header.From.URL.Host contains '.com'". In the ACTION section, the Action Subject is "header.privacy" and the Action Type is "Remove". The Action Value field is empty. At the bottom, there are "Cancel" and "APPLY" buttons.

Figure 93 – SIP Message Manipulation - Privacy

Manipulation to Teams

- To Modify "PAI" header: To display an FQDN instead of IP address for outbound calls towards Teams

The screenshot shows a configuration window titled "Message Manipulations [modify pai host towards teams]". It is divided into three main sections: GENERAL, MATCH, and ACTION. In the GENERAL section, the Index is "21", the Name is "modify pai host towards teams", and the Manipulation Set ID is "2". In the MATCH section, the Message Type is "Invite". In the ACTION section, the Action Subject is "header.P-Asserted-Identity.URL.Host", the Action Type is "Modify", and the Action Value is "'sbca4.tekvizionlabs.com'". At the bottom, there are "Cancel" and "APPLY" buttons.

Figure 94 – SIP Message Manipulation – PAI

- To Modify "TO" header: To display an FQDN instead of IP address for outbound calls towards Teams

The screenshot shows the 'Message Manipulations [modify to towards teams]' window. It is divided into three main sections: GENERAL, MATCH, and ACTION. In the GENERAL section, the Name field is set to 'modify to towards teams' and the Manipulation Set ID is '2'. In the MATCH section, the Message Type is 'invite.request'. In the ACTION section, the Action Subject is 'header.to.uri.host', the Action Type is 'Modify', and the Action Value is '*sip.pstnhub.microsoft.com*'. Red boxes highlight the Name, Manipulation Set ID, Message Type, and the entire ACTION section.

Figure 95 – SIP Message Manipulation - To

- To Modify "FROM" header: To display an FQDN instead of IP address for outbound calls towards Teams

The screenshot shows the 'Message Manipulations [Towards Teams FROM]' window. It is divided into three main sections: GENERAL, MATCH, and ACTION. In the GENERAL section, the Name field is set to 'Towards Teams FROM' and the Manipulation Set ID is '2'. In the MATCH section, the Message Type is 'Options' and the Condition is 'param.message.address.dst.sipinterface==0'. In the ACTION section, the Action Subject is 'Header.From.URL', the Action Type is 'Modify', and the Action Value is '*sip.admin@sbc4.tekvizionlabs.com*'. Red boxes highlight the Name, Manipulation Set ID, Message Type, Condition, and the entire ACTION section.

Figure 96 – SIP Message Manipulation - From

- To Modify "CONTACT" header: To display an FQDN instead of IP address for outbound calls towards Teams

Figure 97 – SIP Message Manipulation - Contact

- To Modify “FROM” header: To display an FQDN instead of IP address for outbound calls towards Teams

Figure 98 – SIP Message Manipulation - From

Manipulation to PSTN

- To Modify “TO” header: To display an IP for an PSTN Gateway

Message Manipulations [towards PSTNGW TO]

GENERAL	ACTION
Index: 3	Action Subject: header.to.url.host Editor
Name: towards PSTNGW TO	Action Type: Modify
Manipulation Set ID: 3	Action Value: '10.64.3.10' Editor
Row Role: Use Current Condition	
MATCH	
Message Type: Options Editor	
Condition: Param.Message.Address.dst.SIPinterface=='1' Editor	

Cancel [APPLY](#)

Figure 99 – SIP Message Manipulation – To

- To Modify “FROM” header: To display an IP for an AudioCodes

Message Manipulations [Towards PSTNGW FROM]

GENERAL	ACTION
Index: 4	Action Subject: Header.From.URL.host Editor
Name: Towards PSTNGW FROM	Action Type: Modify
Manipulation Set ID: 3	Action Value: '10.64.3.10' Editor
Row Role: Use Current Condition	
MATCH	
Message Type: Options Editor	
Condition: Param.Message.Address.dst.SIPinterface=='1' Editor	

Cancel [APPLY](#)

Figure 100 – SIP Message Manipulation – From

- To Modify “Referred-By” header: To display an IP for an AudioCodes in Referred by

Message Manipulations [Referred-By to PSTNGW]

GENERAL

Index: 5

Name: Referred-By to PSTNGW

Manipulation Set ID: 3

Row Role: Use Current Condition

MATCH

Message Type: Invite

Condition: Header.Referred-By exists

ACTION

Action Subject: Header.Referred-By.url.host

Action Type: Modify

Action Value: 10.64.3.10

Buttons: Cancel, APPLY

Figure 101 – SIP Message Manipulation – Referred – By

- To Modify “FROM” header: To display an IP for an AudioCodes in From

Message Manipulations [Towards PSTNGW Invite]

GENERAL

Index: 6

Name: Towards PSTNGW Invite

Manipulation Set ID: 3

Row Role: Use Current Condition

MATCH

Message Type: Invite.Request

Condition:

ACTION

Action Subject: Header.From.URL.Host

Action Type: Modify

Action Value: 10.64.3.10

Buttons: Cancel, APPLY

Figure 102 – SIP Message Manipulation – From

Manipulation to Avaya

- To Modify “Diversion” header: To display AudioCodes IP

Message Manipulations [Teams -> Avaya Modify Diversion header]

GENERAL		ACTION	
Index	22	Action Subject	header.Diversion.url.host Editor
Name	Teams -> Avaya Modify Diversion header	Action Type	Add
Manipulation Set ID	7	Action Value	'10.64.3.10' Editor
Row Role	Use Current Condition		
MATCH			
Message Type	invite.request Editor		
Condition	Header.Diversion exists Editor		

Cancel APPLY

Figure 103 – SIP Message Manipulation – Diversion

- To Modify “FROM” header: To display an IP for an AudioCodes in From

Message Manipulations [Modify SBC IP Teams -> Avaya]

GENERAL		ACTION	
Index	18	Action Subject	Header.From.URL.Host Editor
Name	Modify SBC IP Teams -> Avaya	Action Type	Modify
Manipulation Set ID	7	Action Value	'10.64.3.10' Editor
Row Role	Use Current Condition		
MATCH			
Message Type	Invite.Request Editor		
Condition	Editor		

Cancel APPLY

Figure 104 – SIP Message Manipulation – From

- To Modify “Referred-By” header: To display an IP for an AudioCodes in Referred by

Message Manipulations [Referred-By Teams -> Avaya]

GENERAL		ACTION	
Index	17	Action Subject	Header.Referred-By.url.host Editor
Name	Referred-By Teams -> Avaya	Action Type	Modify
Manipulation Set ID	7	Action Value	'10.64.3.10' Editor
Row Role	Use Current Condition		
MATCH			
Message Type	Invite Editor		
Condition	Header.Referred-By exists Editor		

Cancel APPLY

Figure 105 – SIP Message Manipulation – Referred By

- To Modify “FROM” header: To display an IP for an AudioCodes in From

Message Manipulations [From header Teams -> Avaya]

GENERAL		ACTION	
Index	15	Action Subject	Header.From.URL.host Editor
Name	From header Teams -> Avaya	Action Type	Modify
Manipulation Set ID	7	Action Value	'10.64.3.10' Editor
Row Role	Use Current Condition		
MATCH			
Message Type	Options Editor		
Condition	Param.Message.Address.dst.SIPInterface== Editor		

Cancel APPLY

Figure 106 – SIP Message Manipulation – From

- To Modify “TO” header: To display an IP for an AudioCodes in to

Message Manipulations [To header Teams -> Avaya]

GENERAL		ACTION	
Index	16	Action Subject	Header.To.URL.host Editor
Name	To header Teams -> Avaya	Action Type	Modify
Manipulation Set ID	7	Action Value	'10.64.3.10' Editor
Row Role	Use Current Condition		
MATCH			
Message Type	Options Editor		
Condition	Param.Message.Address.dst.SIPInterface== Editor		

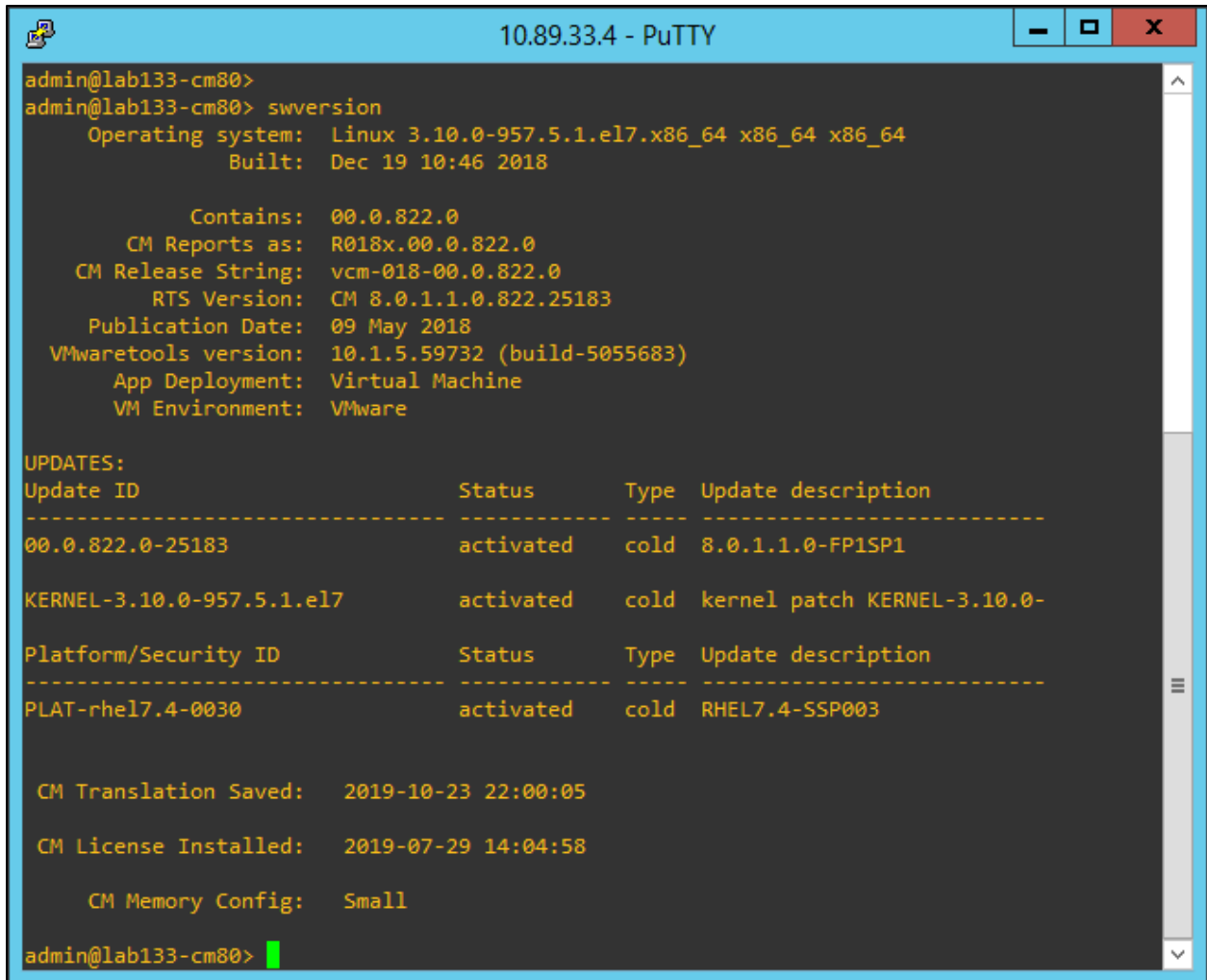
Cancel [APPLY](#)

Figure 107 – SIP Message Manipulation – to

4.5 Avaya Aura Communication Manager Configuration

4.5.1 Version

Execute **swversion** to find the version for Avaya Aura Communication Manager



```
admin@lab133-cm80>
admin@lab133-cm80> swversion
  Operating system:  Linux 3.10.0-957.5.1.el7.x86_64 x86_64 x86_64
                    Built:  Dec 19 10:46 2018

    Contains:  00.0.822.0
  CM Reports as:  R018x.00.0.822.0
CM Release String:  vcm-018-00.0.822.0
   RTS Version:  CM 8.0.1.1.0.822.25183
  Publication Date:  09 May 2018
VMwaretools version:  10.1.5.59732 (build-5055683)
  App Deployment:  Virtual Machine
   VM Environment:  VMware

UPDATES:
Update ID                Status      Type  Update description
-----
00.0.822.0-25183         activated   cold  8.0.1.1.0-FP1SP1

KERNEL-3.10.0-957.5.1.el7  activated   cold  kernel patch KERNEL-3.10.0-

Platform/Security ID      Status      Type  Update description
-----
PLAT-rhel7.4-0030         activated   cold  RHEL7.4-SSP003

  CM Translation Saved:  2019-10-23 22:00:05
  CM License Installed:  2019-07-29 14:04:58

    CM Memory Config:  Small

admin@lab133-cm80>
```

Figure 108 - Version

4.5.2 IP Node Name

Use the **change node-names ip** command to verify that node names have been properly defined for Communication Manager (procr) and Session Manager (ASM7 in this test). These node names will be needed for configuring a Signaling Group later.

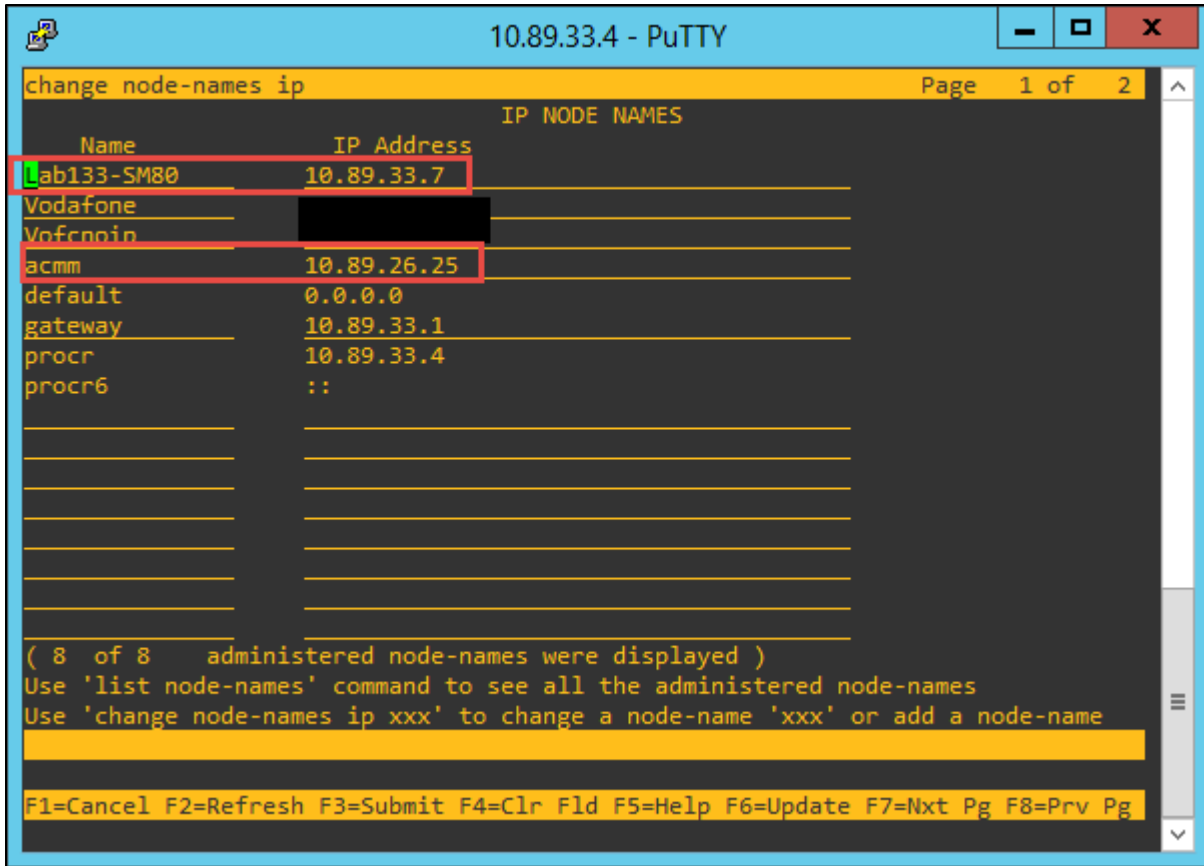


Figure 109 - IP Node Name

4.5.3 IP Codec Set

Use **change ip-codec-set <n>** command to define a list of codecs for calls from Avaya Aura

1. Set **Audio Codec**: G.711MU is entered
2. Leave other fields at default values

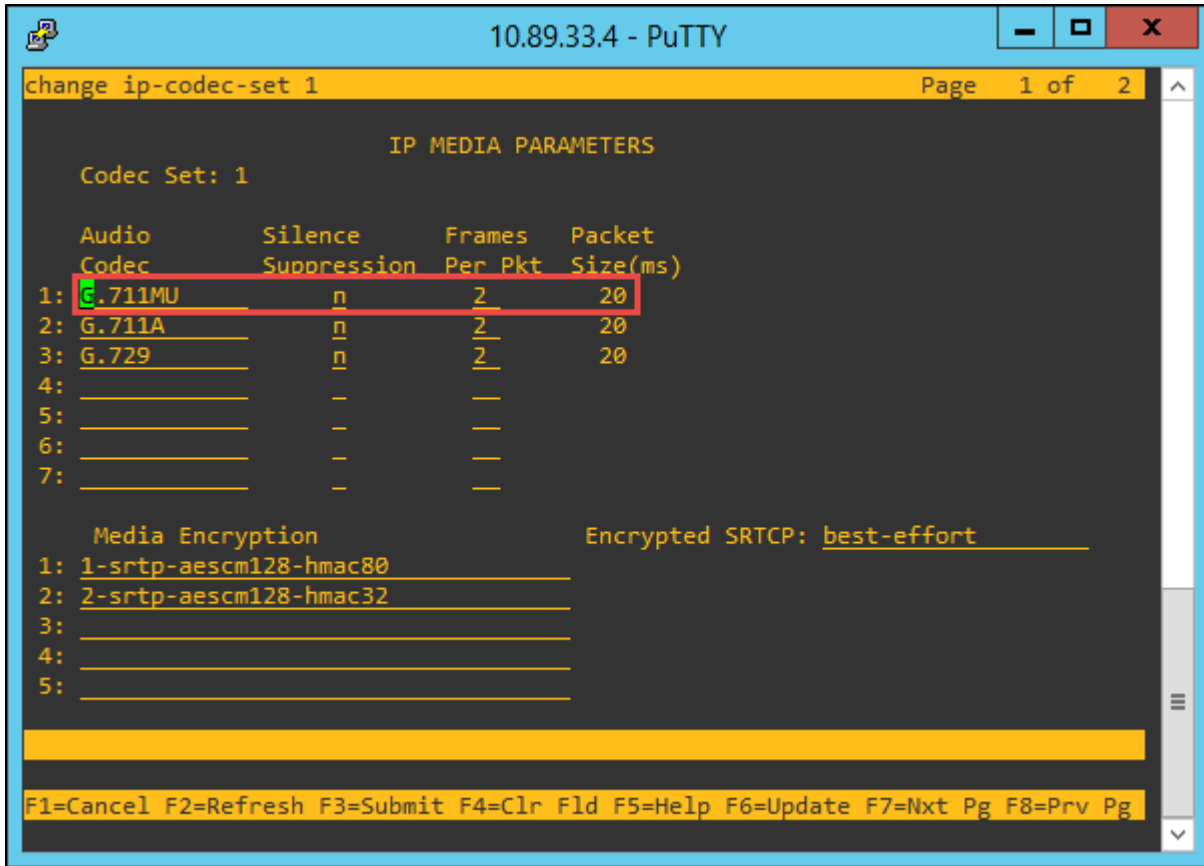


Figure 110 - IP Codec Set

4.5.4 IP Network Region

IP Network Region 1 is utilized. Command **change ip-network-region 1** is issued

1. Set **Codec Set**: 1, which is programmed in the previous step
2. Set **Intra-region IP-IP Direct Audio**: yes
3. Set **Inter-region IP-IP Direct Audio**: yes
4. Leave other fields at default values

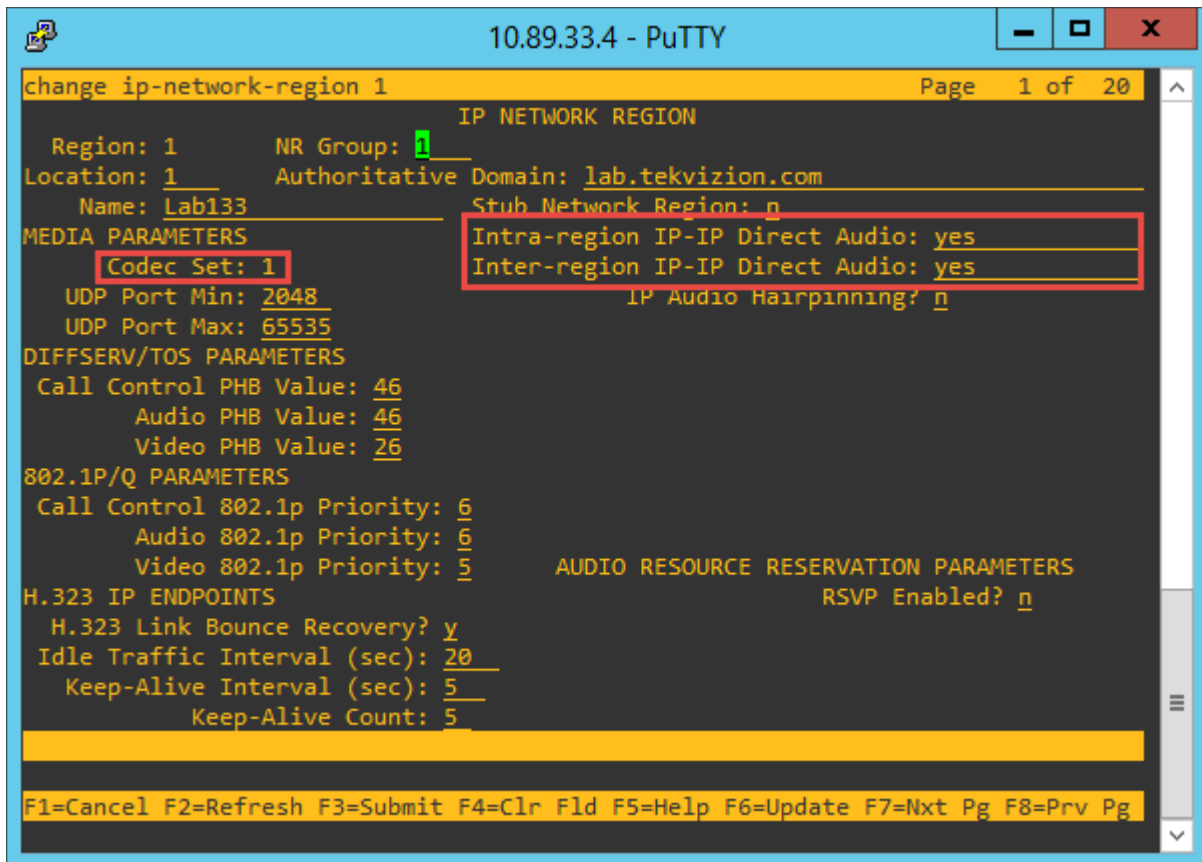


Figure 111 - IP Network Region

4.5.5 Signaling Groups

Signaling group is configured for SIP trunk.

Command **add signaling-group x** was used to create Signaling Group, command **change signaling-group <x>** is used to modify an existing Signaling Group. Signaling Group 1 is used for the SIP trunk.

1. Set **Group Type**: sip
2. Set **Transport Method**: tcp
3. Set **Peer Detection Enable**: y
4. Set **Near-end Node Name**: procr
5. Set **Near-end Listen Port**: 5060
6. Set **Far-end Node Name**: ASM7
7. Set **Far-end Listen Port**: 5060
8. Set **Far-end Network Region**: 1
9. Set **DTMF over IP**: rtp-payload
10. Set **Direct IP-IP Audio Connections?**: n
11. Leave other fields as default value


```
10.89.33.4 - PuTTY
change signaling-group 5 Page 1 of 2
SIGNALING GROUP
Group Number: 5 Group Type: sip
IMS Enabled? n Transport Method: tcp
Q-SIP? n
IP Video? n Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr Far-end Node Name: Lab133-SM80
Near-end Listen Port: 5060 Far-end Listen Port: 5060
Far-end Network Region: 2
Far-end Domain: lab.tekvizion.com
Incoming Dialog Loopbacks: eliminate Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload RFC 3389 Comfort Noise? n
Direct IP-IP Audio Connections? n
Session Establishment Timer(min): 3 IP Audio Hairpinning? n
Enable Layer 3 Test? y Alternate Route Timer(sec): 6
F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Figure 112 - Signaling Group

4.5.6 Trunk Groups

Similar to Signaling Group, Trunk Group is created for this setup, Trunk Group 1 is for the SIP Trunk. Command **change trunk-group 1**.

1. Set **Group Type**: sip
2. Set **Group Name**: Crestron_Teams, for example
3. Set **TAC**: #005, this value is given based on the system dial plan
4. Set **Direction**: two-way
5. Set **Service Type**: public-ntwrk
6. Set **Member Assignment Method**: auto
7. Set **Signaling Group**: 5
8. Set **Number of Members**: Enter a number between 1 and the max number of licensed SIP trunks

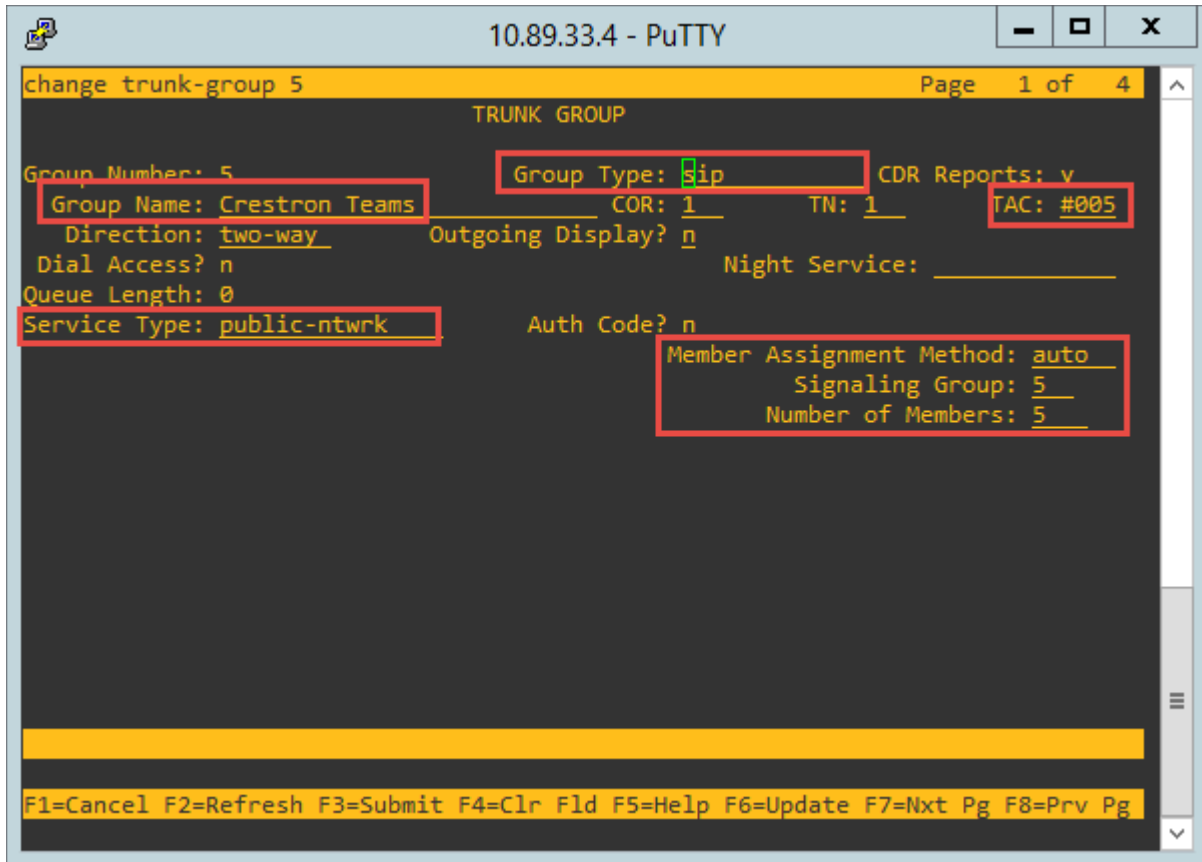


Figure 113 - Trunk Group

4.5.7 Route Pattern

Use **change route-pattern <x>** command to specify the routing preference, Route pattern 5 is for SIP Trunk.

1. Set **Pattern Name:** to ASM7
2. Set **Grp No:** Trunk group 5 is given here
3. Set **FRL:** 0 is given as it has the least restriction
4. Set **Numbering Format:** unk-unk
5. Leave all other fields at default values

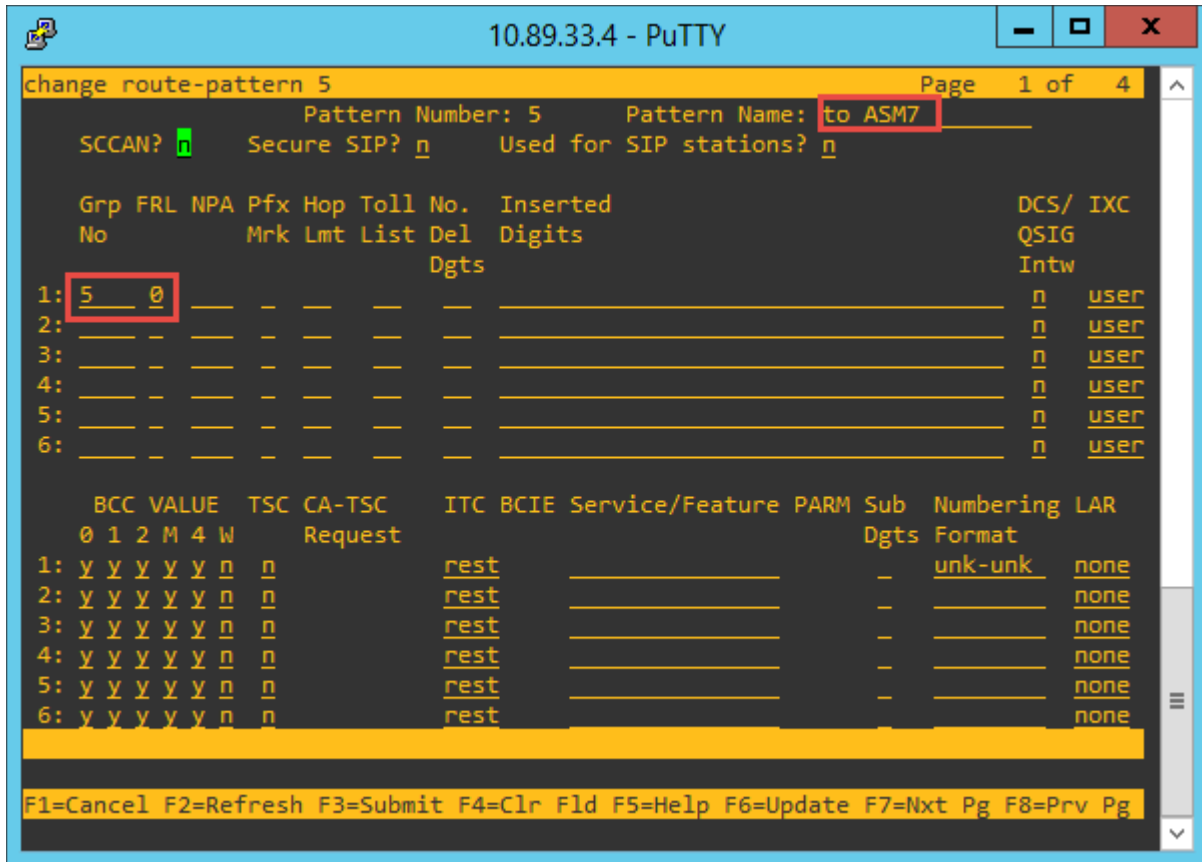


Figure 114 - Route Pattern

4.5.8 Outbound Call Routing

For outbound call to PSTN through AudioCodes, AAR is used. Use command **change aar analysis <x>** to configure the routing table. Here is an example to configure the AAR to call to Teams user

1. Set **Dialed String**: 8 is given for calling Teams user.
2. Set **Min**: 5 is given here
3. Set **Max**: 5 is given here
4. Set **Route Pattern**: The previously configured Route Pattern 5 is given here
5. Set **Call Type**: aar is given here

change aar analysis 8 Page 1 of 2

AAR DIGIT ANALYSIS TABLE
Location: all Percent Full: 3

Dialed String	Total		Route Pattern	Call Type	Node Num	ANI Reqd
	Min	Max				
800	5	5	5	aar	---	n
9	7	7	254	aar	---	n
	---	---	---	---	---	n
	---	---	---	---	---	n
	---	---	---	---	---	n
	---	---	---	---	---	n
	---	---	---	---	---	n
	---	---	---	---	---	n
	---	---	---	---	---	n
	---	---	---	---	---	n
	---	---	---	---	---	n
	---	---	---	---	---	n
	---	---	---	---	---	n
	---	---	---	---	---	n
	---	---	---	---	---	n

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg

Figure 115 - Outbound Call Routing

4.5.9 Private Numbering Plan

For inbound call to Avaya Communication Manager, the following configuration is made. Use command **change private-numbering <x>** to map the incoming number to extension. Here is an example to configure the incoming call termination.

1. Set **Ext code**: 7500 or 7501 is given for calling Teams user.
2. Set **Trk Grp(s)**: 3 is given here
3. Set **Private Prefix**: 7500 and 7501
4. Set **Total Len**: 4

10.89.33.4 - PuTTY

change private-numbering 1 Page 1 of 2

NUMBERING - PRIVATE FORMAT

Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len
4	26	2		4
4	265	3	043207	10
4	0982	5		10
4	0988	5		10
4	0989	5		10
4	0991	5		10
4	0992	5		10
4	7500	5	7500	4
5	7500	5	7500	4
4	7501	5	7501	4
5	7501	5	7501	4
4	7503	5	7503	4
5	70988	5		10
7	2137429	7		10
7	2149177	9		10
7	5980100	5		10

Total Administered: 16
Maximum Entries: 540

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg

Figure 116 - Inbound Call Routing

4.6 Avaya Aura Session Manager Configuration

Avaya Aura Session Manager Configuration is accomplished through the Avaya Aura System Manager.

1. Access Avaya Aura System Manager Web login screen via <https://<IP Address/FQDN>>, the IP address is 10.89.33.3 in our lab
2. Use admin as User ID and associated password
3. Click Log On

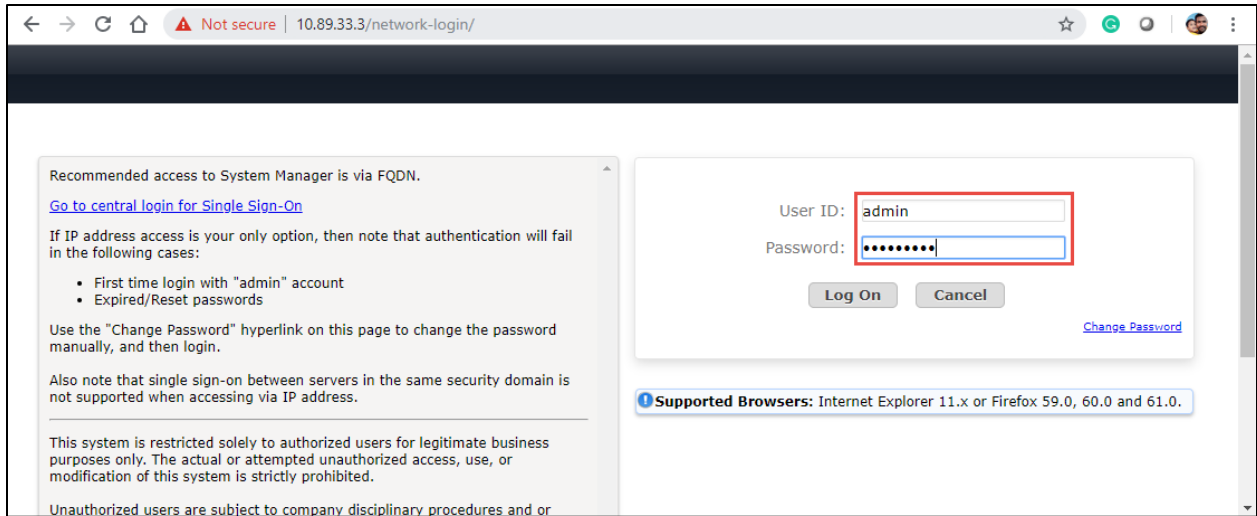


Figure 117 - Log into Avaya Aura System Manager

Navigate to Elements → Routing

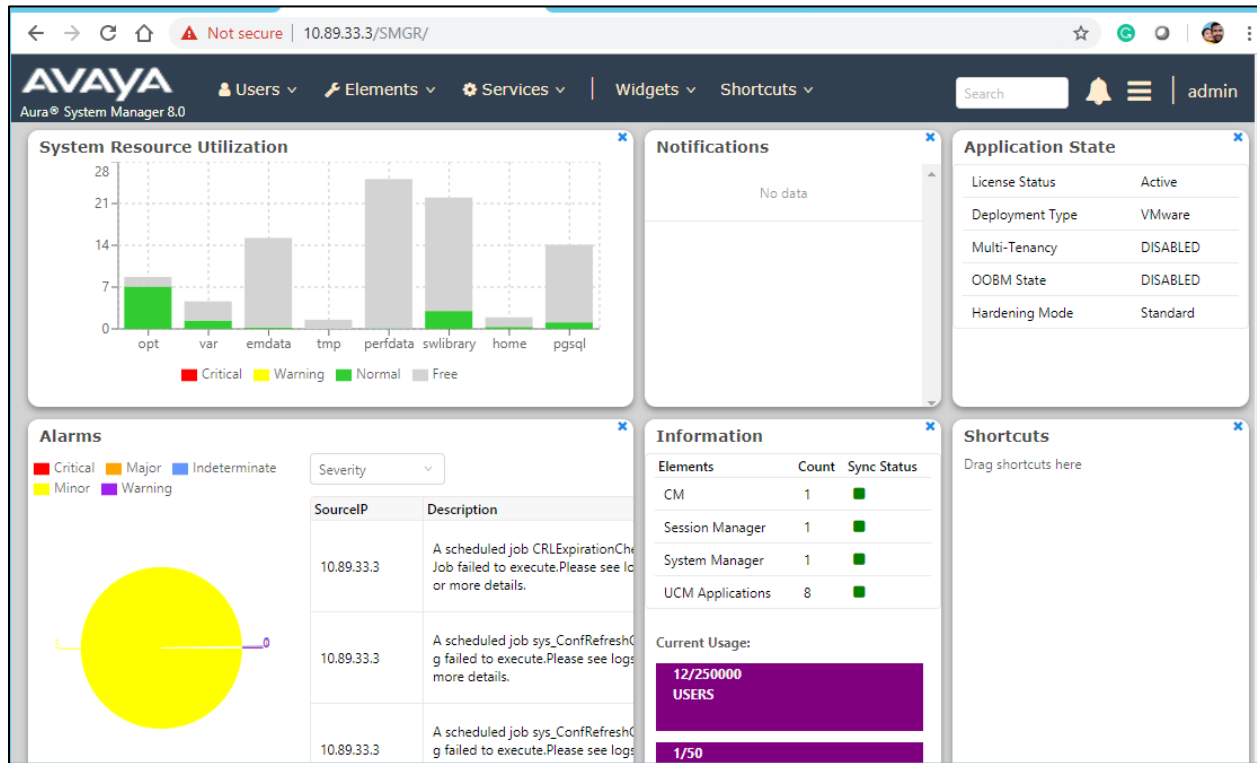


Figure 118 - Routing

4.6.1 Version

The version of Avaya System Manager used for the testing is given below

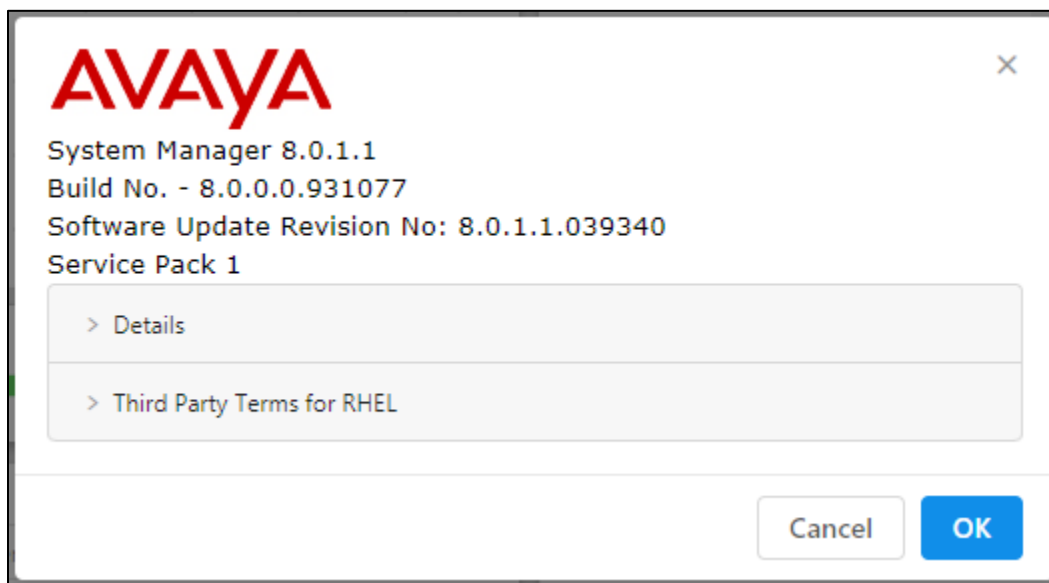


Figure 119 – Version

4.6.2 Domains

1. Navigate to **Routing -> Domains**
2. Click **New**

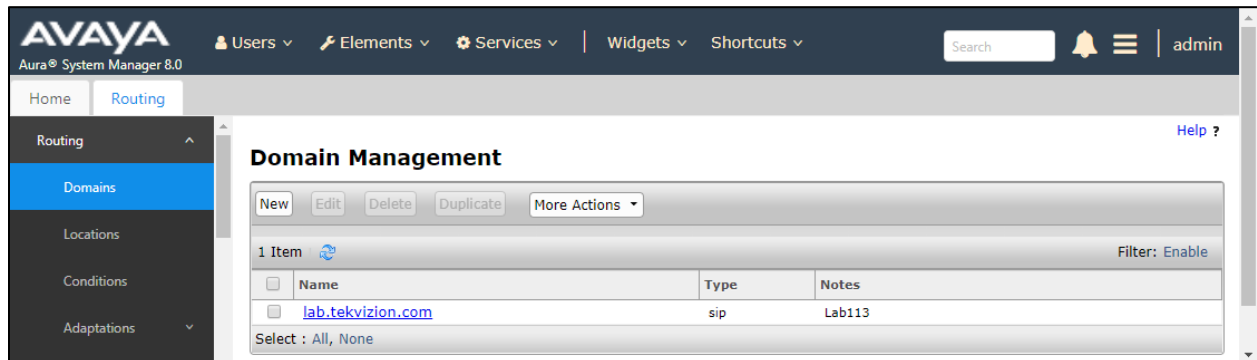


Figure 120 – Add Domain

3. Set **Name**: Enter the domain name of Avaya Aura PBX, lab.tekvizion.com is given for the test
4. Set **Type**: sip
5. Click **Commit**

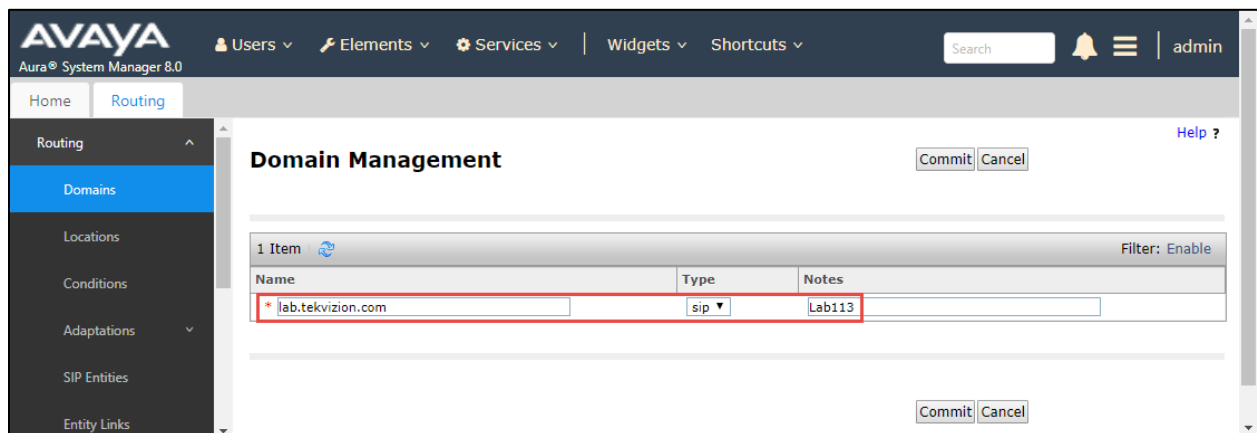


Figure 121 - Domain

4.6.3 Locations

1. Navigate to **Routing -> Locations**
2. Select **New**
3. Set **Name**: Enter the name of your location, Lab133-Plano is set here
4. Under Location Pattern, select **Add** to add IP Address Patterns for different networks that communication within the location
5. Set **IP Address Pattern**: 10.89.33.*
6. Leave all other fields at default values

7. Click **Commit**

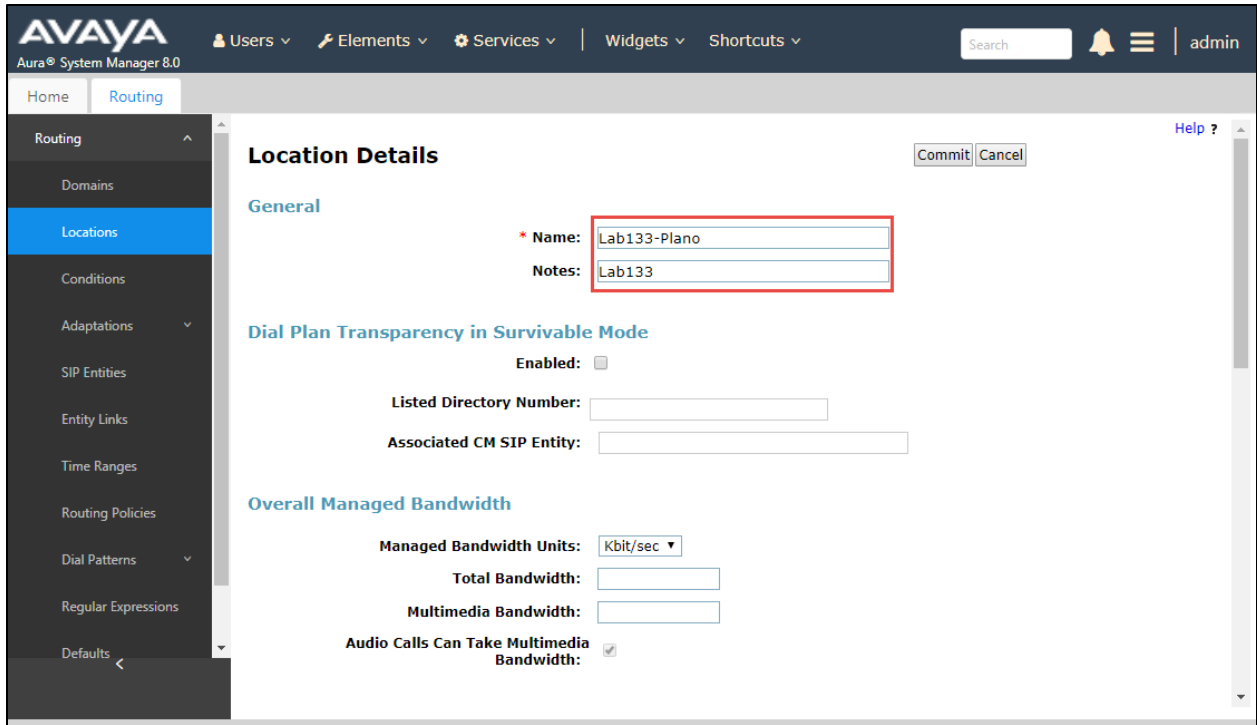


Figure 122- Add Location

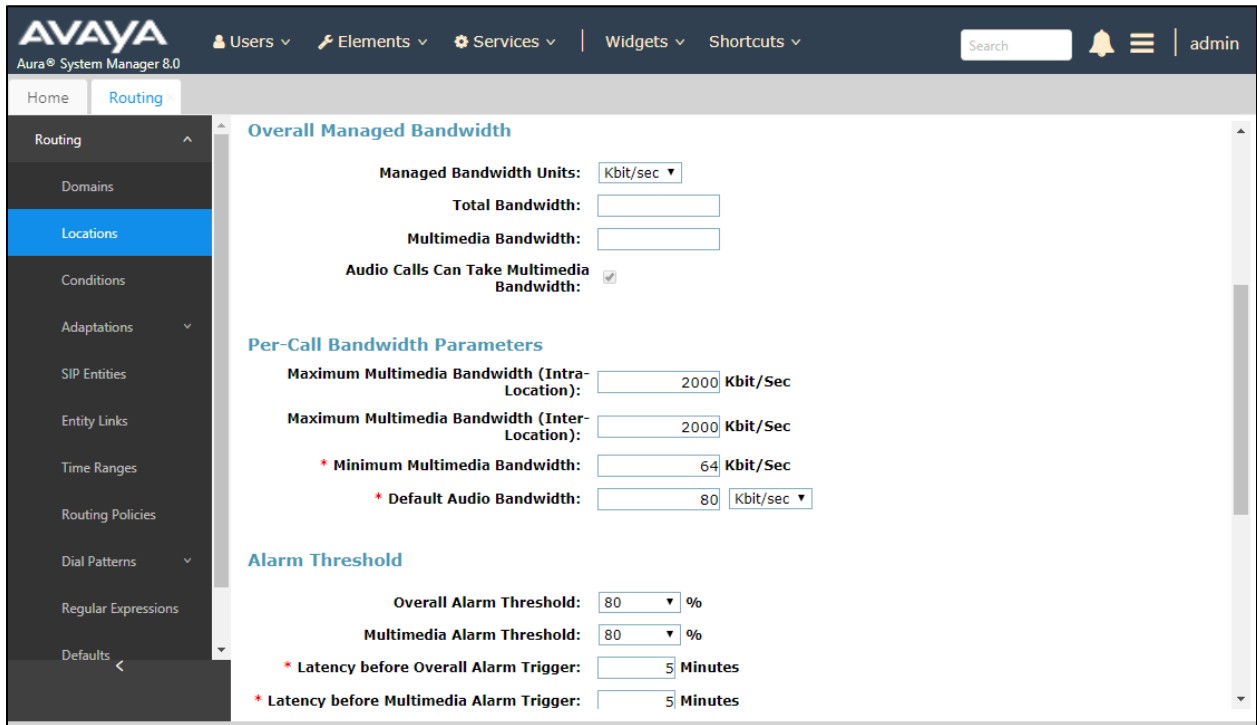


Figure 123 - Add Location

4.6.4 Adaptation

Adaptation was created at the Session Manager for Avaya CM

1. Navigate to **Routing** → **Adaptations**. Click **New**
2. Set **Adaptation Name**: Adaptation_for_ACM, for example
3. Set **Module Name**: DigitConversionAdapter
4. Set **Module Parameter Type**: Name-Value Parameter is selected from the drop down, Click **Add**
5. Set **Name/Value**: fromto/true
6. Leave all other fields at default values
7. Click **Commit**

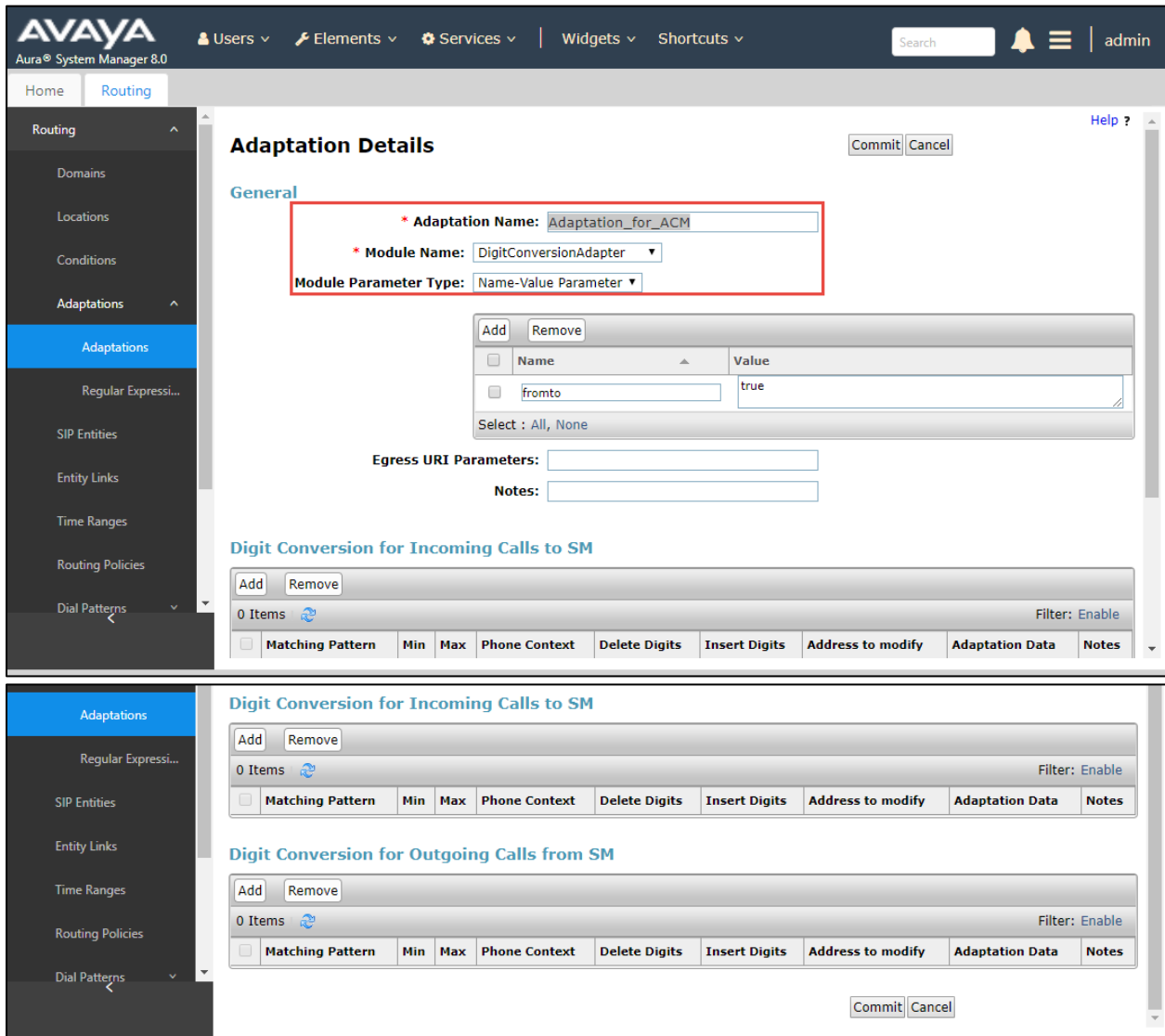


Figure 124 - Add Adaptation

4.6.5 SIP Entities and Entity Links

Navigate to: **Routing** → **SIP Entities**. Click **New**

4.6.5.1 SIP Entity for Avaya Aura Session Manager

1. Navigate to: **Routing → SIP Entities**. Click **New**
2. SIP Entity for Avaya Aura Session Manager
3. Set **Name**: Enter name of the host, Lab133-SM80 is used here for example
4. Set **FQDN or IP Address**: Enter the SIP address of the Session Manager
5. Set **Type**: Session Manager is selected from the drop down
6. Set **Location**: Select the location configured in the previous step
Under Listen Port:
7. Set **TCP/TLS Failover Port**: 5060/5061
8. Click **Add** to assign Domain lab.tekvizion.com for the following Ports and Protocols
9. Port **5060** and Protocol **TCP/UDP**
10. Leave all other fields at default values
11. Click **Commit**

The screenshot displays the Avaya Aura System Manager 8.0 interface. The left sidebar shows the navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'Commit' button. The 'General' section contains the following fields:

- Name:** Lab133-SM80
- IP Address:** 10.89.33.7
- SIP FQDN:** (empty)
- Type:** Session Manager
- Notes:** Lab133
- Location:** Lab133-Plano
- Outbound Proxy:** (empty)
- Time Zone:** America/Chicago
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)

The 'Monitoring' section includes:

- SIP Link Monitoring:** Use Session Manager Configuration
- CRLF Keep Alive Monitoring:** Use Session Manager Configuration

The 'Entity Links' section features an 'Add' button and a table with 9 items. The table columns are Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Deny New Service.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
* AMM_AMM_5060_TCP	Lab133-SM80	TCP	* 5060	AMM	* 5060	trusted	<input type="checkbox"/>
* Lab133-SM80_Corp_Gl	Lab133-SM80	UDP	* 5060	Corp_GW	* 5060	trusted	<input type="checkbox"/>
* Lab133-SM80_IPC_506	Lab133-SM80	TLS	* 5061	IPC	* 5061	trusted	<input type="checkbox"/>

Figure 125 - SIP Entity: Avaya Aura Session Manager

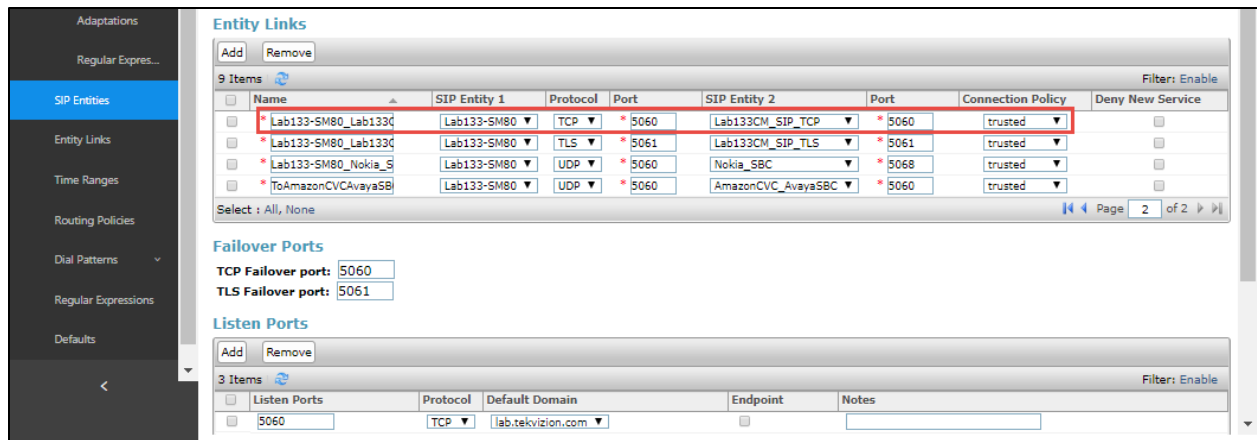


Figure 126 - SIP Entity: Avaya Aura Session Manager

4.6.5.2 SIP Entity for Communication Manager SIP Trunk

1. Set **Name**: Lab133CM_SIP_TCP
2. Set **FQDN or IP Address**: Enter the IP address of Avaya Aura Communication Manager
3. Set **Type**: CM
4. Set **Adaptation**: adaptation_for_CM
5. Set **Location**: Select the location configured in previous step
6. Under **Entity Links**, Click **Add**
7. Set **SIP Entity 1**: Select the SIP entity Lab133CM_SIP_TCP_5060_TCP
8. Set **SIP Entity 2**: Select the SIP entity Lab133CM_SIP_Trunk
9. Set **Protocol**: TCP was used for this test
10. Set **Ports**: Set SIP Entity 1 Port to 5060 and SIP Entity 2 Port to 5060
11. Set **Connection Policy**: trusted
12. Leave all other fields at default values
13. Click **Commit**

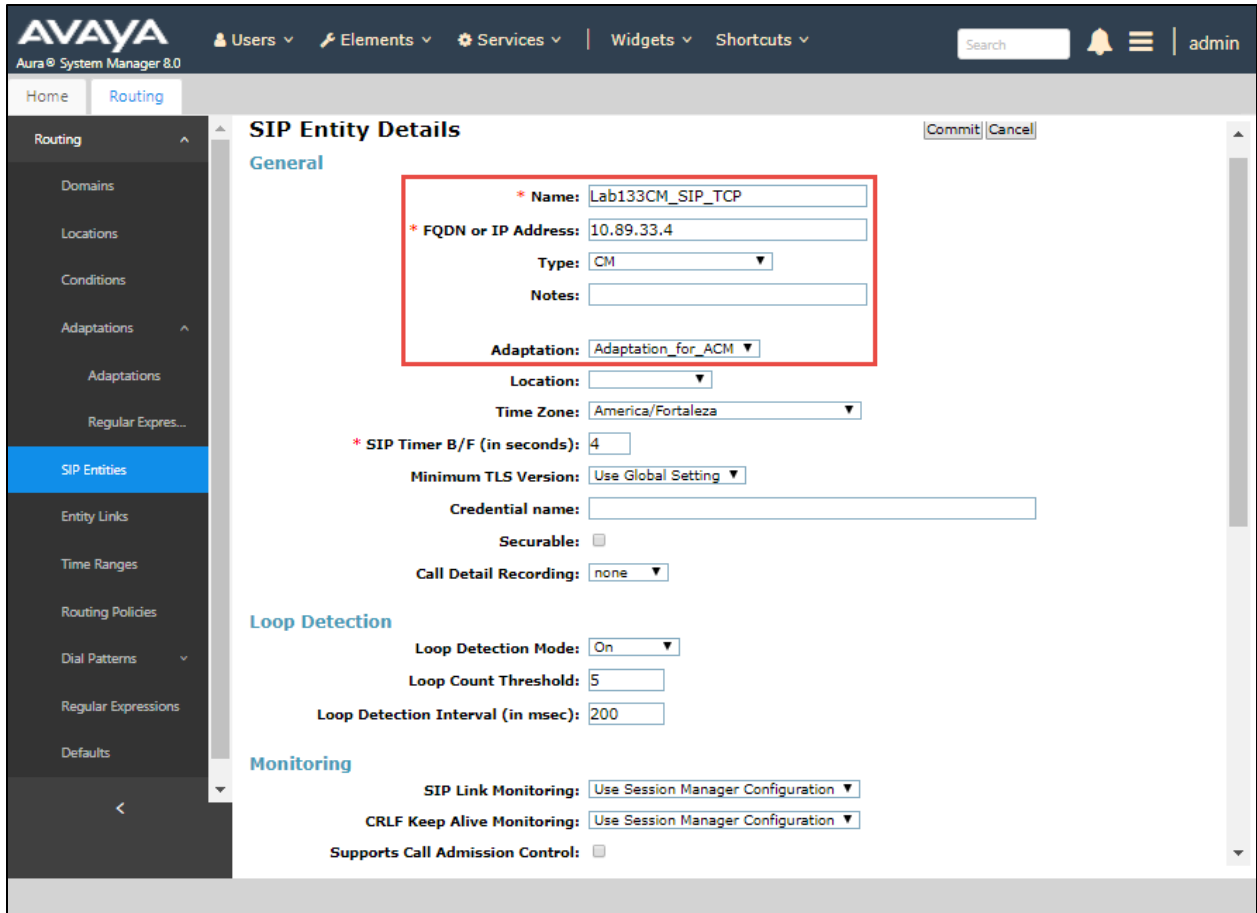


Figure 127- SIP Entity: Avaya Aura Communication Manager for SIP Trunk

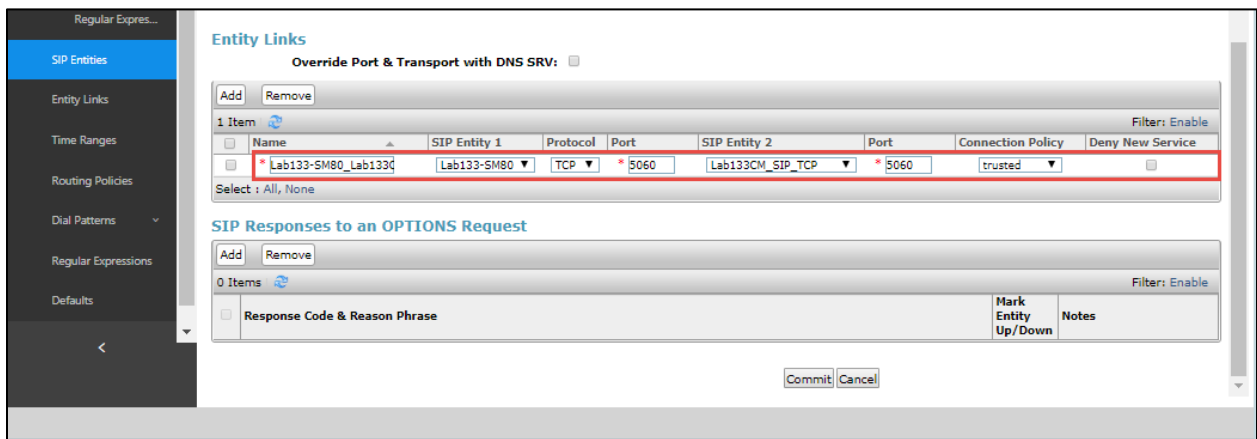


Figure 128 - SIP Entity: Avaya Aura Communication Manager for SIP Trunk

4.6.5.3 SIP Entity for Avaya SBCE

1. Set **Name:** Lab126_SBCE

2. Set **FQDN or IP Address**: Enter the IP address of Avaya SBCE interface facing Avaya Aura Session Manager
3. Set **Type**: SIP Trunk
4. Set **Location**: Select the location configured in the previous step
5. Under **Entity Links**, Click **Add**
6. Set **SIP Entity 1**: Select the SIP Entity Lab133_SM80 configured in previous step
7. Set **SIP Entity 2**: Select the SIP Entity AvayaSBC
8. Set **Protocol**: TCP was used for this test
9. Set **Ports**: Set both Ports to 5060
10. Set **Connection Policy**: trusted
11. Leave all other fields at default values
12. Click **Commit**

The screenshot shows the 'SIP Entity Details' configuration page in Avaya Aura System Manager 8.0. The 'General' section is highlighted, and a red box encloses the following fields:

- Name:** AvayaSBC
- FQDN or IP Address:** 10.89.33.13
- Type:** Other

Other visible fields include:

- Notes:** (empty)
- Adaptation:** Adaptation_for_SBC
- Location:** Lab133-Plano
- Time Zone:** America/Fortaleza
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:**
- Call Detail Recording:** none
- CommProfile Type Preference:** (empty)

The 'Loop Detection' section shows:

- Loop Detection Mode:** On
- Loop Count Threshold:** 5
- Loop Detection Interval (in msec):** 200

The 'Monitoring' section shows:

- SIP Link Monitoring:** Link Monitoring Enabled
- Proactive Monitoring Interval (in seconds):** 900

Figure 129 - SIP Entity: Avaya SBCE

The screenshot shows the 'Entity Links' configuration page. A table lists the configured links, with a red box highlighting the following row:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
* To_AvayaSBC	Lab133-SM80	UDP	* 5060	AvayaSBC	* 5060	trusted	<input type="checkbox"/>

Figure 130 - SIP Entity: Avaya SBCE

4.6.6 Routing Policies

Navigate to: **Routing → Routing Policies**. Click **New**

4.6.6.1 Routing Policy to Avaya Aura Communication Manager

1. Set **Name**: to_CM(TCP) is given here
2. Click **Select** under SIP Entity as Destination and the SIP Entities window shows
3. Select **Lab133_CM_SIP_TCP** as destination SIP Entity (This is the SIP Entity configured for Avaya CM)
4. Click **Select** and return back to Routing Policy Details page
5. Leave all other fields at default values
6. Click **Commit**

The screenshot displays the Avaya Aura System Manager 8.0 interface for configuring a Routing Policy. The left sidebar shows the navigation menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes a 'Commit' button and a 'Cancel' button. The 'General' section contains the following fields:

- Name:** to_CM(TCP)
- Disabled:**
- Retries:** 0
- Notes:** (empty text area)

The 'SIP Entity as Destination' section features a 'Select' button and a table with the following data:

Name	FQDN or IP Address	Type	Notes
Lab133CM_SIP_TCP	10.89.33.4	CM	

The 'Time of Day' section includes an 'Add' button, a 'Remove' button, and a 'View Gaps/Overlaps' button. It shows 1 item in a table:

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

The 'Dial Patterns' section includes an 'Add' button and a 'Remove' button. It shows 3 items in a table:

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
2137	4	12	<input type="checkbox"/>	-ALL-	Lab133-Plano	
750	4	12	<input type="checkbox"/>	-ALL-	Lab133-Plano	

Figure 131 - Routing Policy to Avaya Aura Communication Manager

4.6.6.2 Routing Policy to Avaya SBCE

1. Set **Name**: To_ASBC is given here as an example
2. Click **Select** under SIP Entity as Destination and SIP Entities window shows
3. Select **AvayaSBC** as destination SIP Entity (This is the SIP Entity configured for Avaya SBCE)
4. Click **Select** and return back to Routing Policy Details page
5. Leave all other fields at default values

6. Click **Commit**

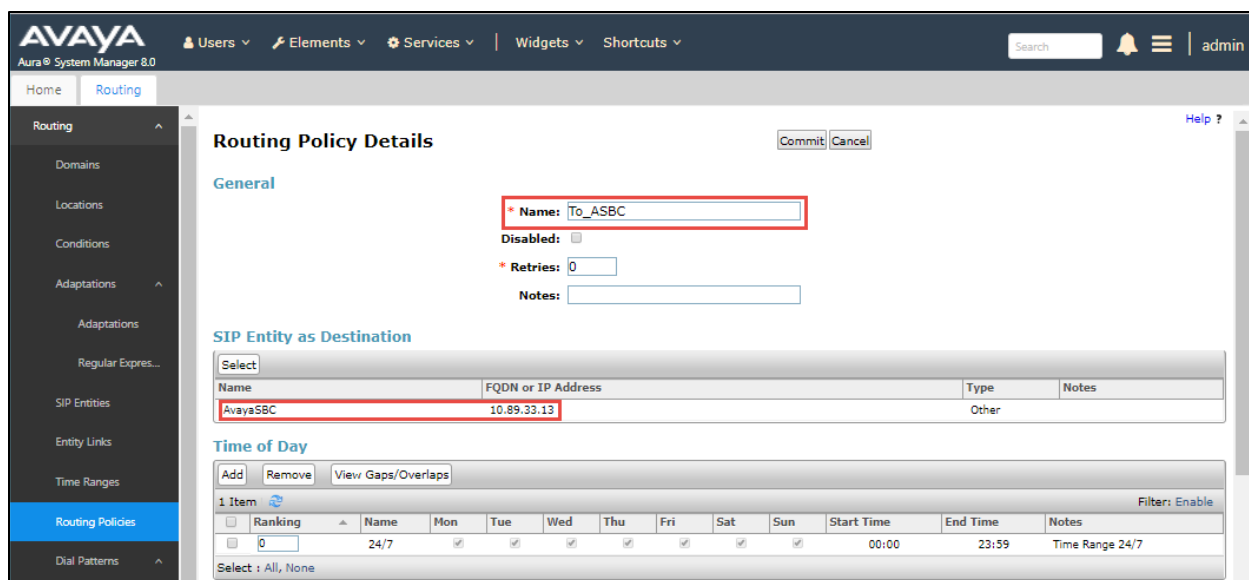


Figure 132 - Routing Policy to Avaya SBCE

4.6.7 Dial Patterns

Navigate to: **Routing** → **Dial Patterns**. Click **New**

4.6.7.1 Dial Pattern to Avaya Aura Communication Manager

1. Set **Pattern**: 750 - the leading Digits of the DID to be sent to Avaya CM for termination to extensions
2. Set **Min**: 4
3. Set **Max**: 12
4. Under **Originating Locations** and **Routing Policies**, Click **Add**, at the new window
5. **Originating Location**: Select your location, Lab133-Plano is used in this test
6. Check **Lab133_CM_SIP_TCP** as Routing Policy
7. Click **Select** to return to Dial Pattern Details page
8. Leave all other fields at default values.
9. Click **Commit**

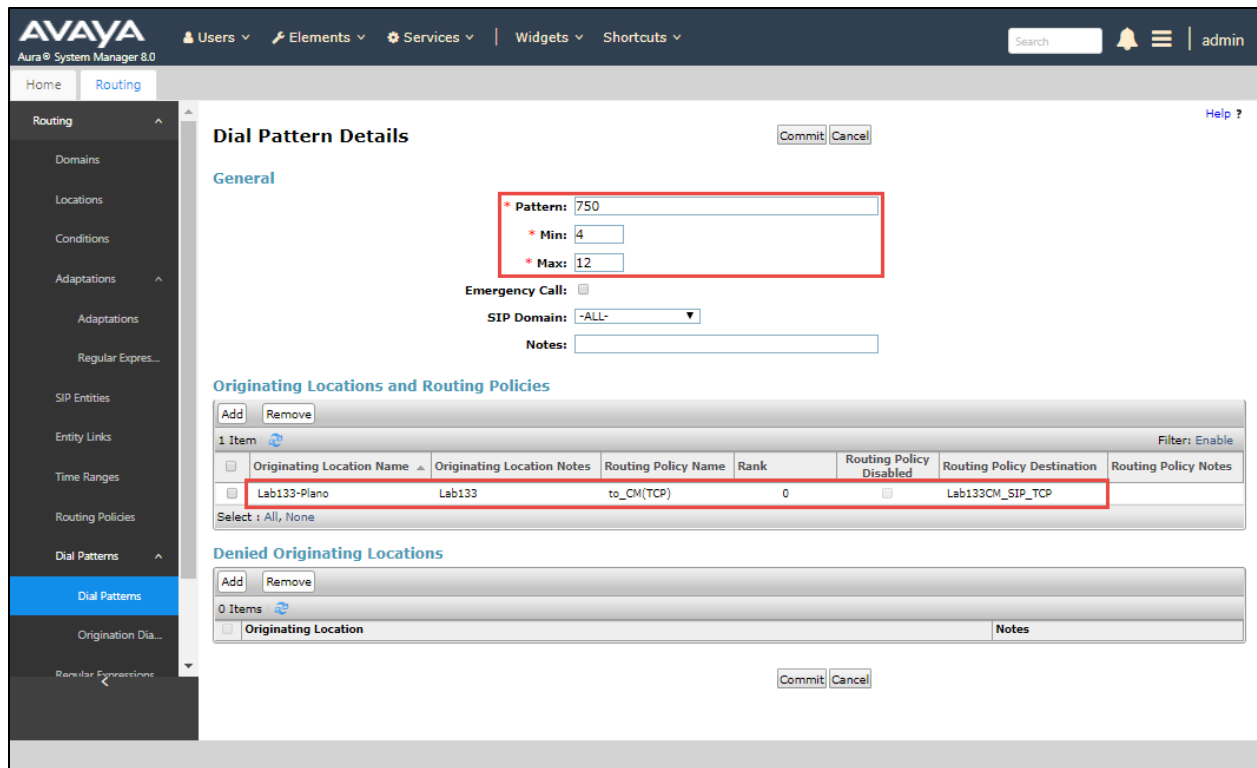


Figure 133 - Dial Pattern to Avaya Aura Communication Manager

4.6.7.2 Dial Patterns to AudioCodes via Avaya SBCE

1. Set **Pattern:** 8009 - the leading Digits of the Teams extensions to be dialed over the trunk
2. Set **Min:** 5
3. Set **Max:** 12
4. Under **Originating Locations** and **Routing Policies**, Click **Add**, at the new window
5. **Originating Location:** Select your location, Lab133-Plano is used in this test
6. Check **To_ASBC** as Routing Policy
7. Click **Select** to return to Dial Pattern Details page
8. Leave all other fields at default values.
9. Click **Commit**

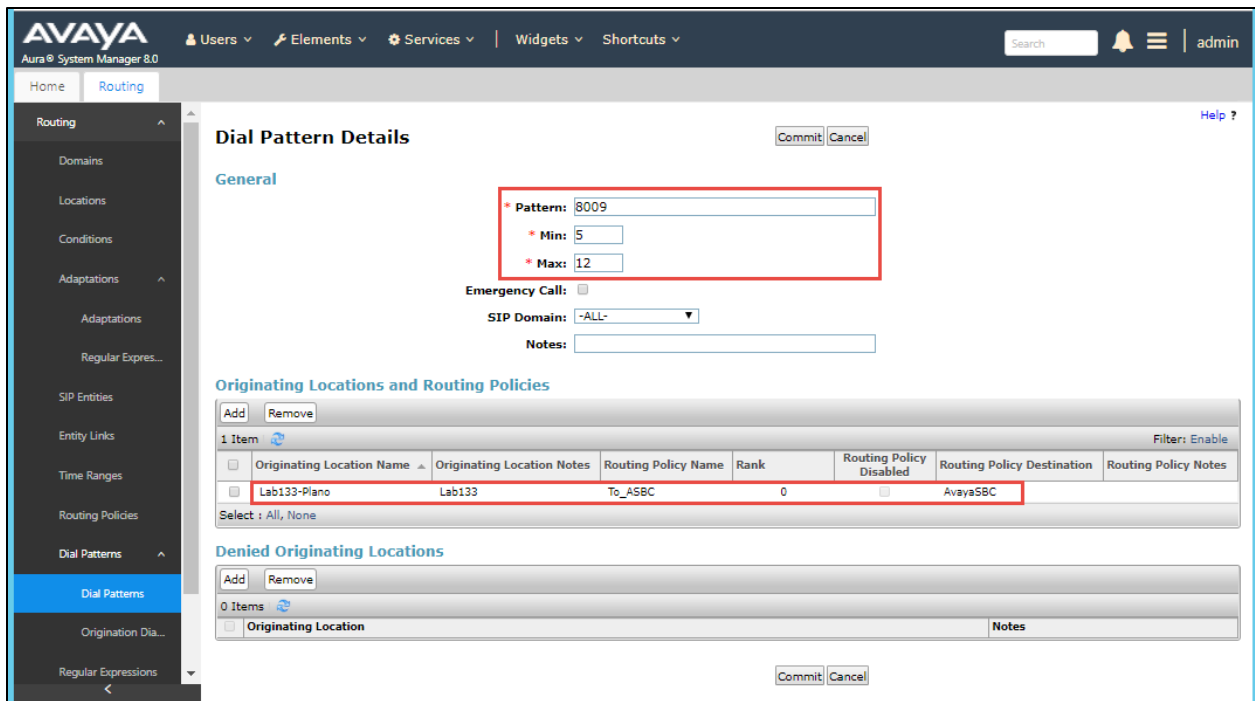


Figure 134 - Dial Pattern to Avaya SBCE

4.7 Avaya SBCE Configuration

4.7.1 Version

The following version of Avaya SBCE is used for this testing

Device: Lab126-ASBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

EMS
Lab126-ASBCE

er Controller for Enterprise

AVAYA

EMS Dashboard

- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

Dashboard

Information	
System Time	10:09:22 AM CDT Refresh
Version	8.0.0.0-19-16991
Build Date	Sat Jan 26 21:58:11 UTC 2019
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	10/24/2019 10:00:18 CDT
Failed Login Attempts	0

Installed Devices

- EMS
- Lab126-ASBCE

Active Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

- Lab126-ASBCE: General Method not allowed Out-Of-Dialog
- Lab126-ASBCE: No Subscriber Flow Matched
- Lab126-ASBCE: General Method not allowed Out-Of-Dialog
- Lab126-ASBCE: No Subscriber Flow Matched
- Lab126-ASBCE: General Method not allowed Out-Of-Dialog

Figure 135 – Version

4.7.2 Configure Profiles and Services

4.7.2.1 Sever Interworking

1. Navigate to: **Configure Profiles → Server Interworking**
2. Select the predefined Interworking Profile **avaya-ru**, click **Clone**
3. Set Clone Name: **Lab126ASM**, for example
4. Click **Finish**
5. Click newly cloned Profile **Lab126ASM**, under tab General, click **Edit**
6. Keep all other parameters at default values and save

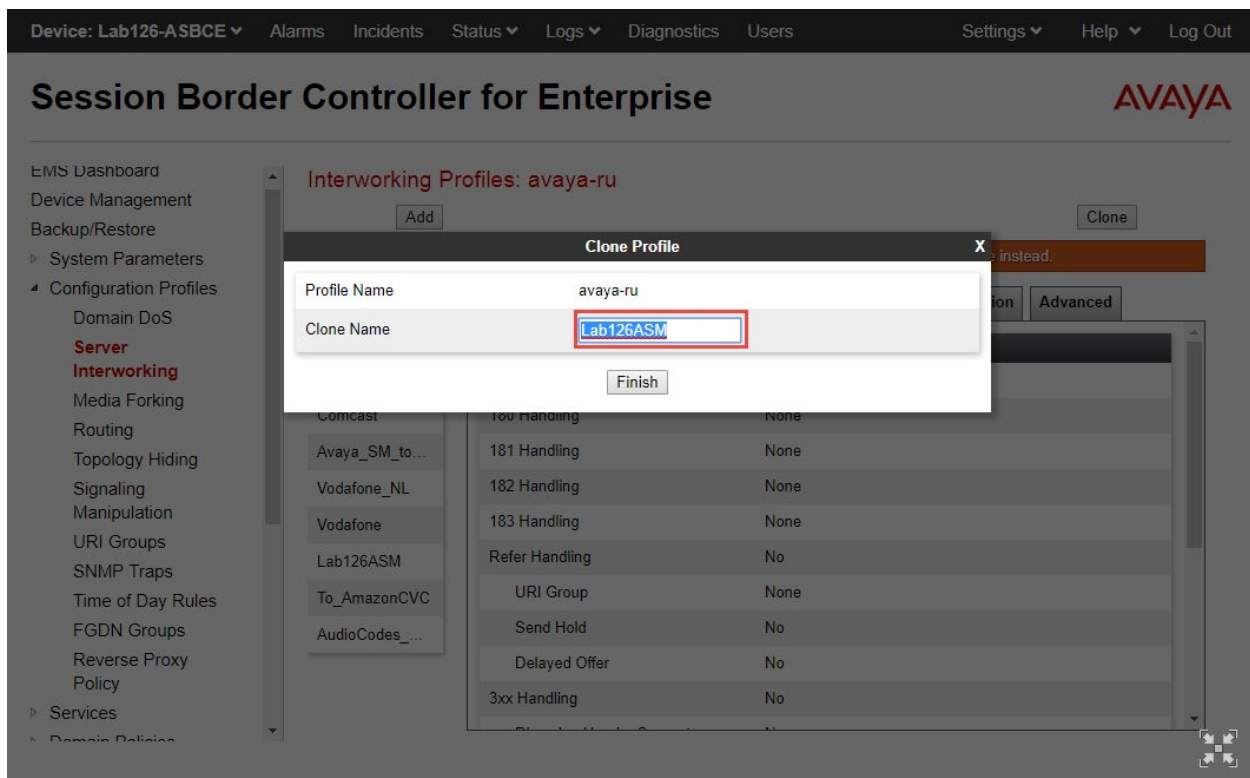


Figure 136 - Server Interworking for Avaya

4.7.2.2 SIP Servers – Avaya Aura Session Manager

1. Navigate to **Services → SIP Servers**
2. Click **Add**
3. Set Profile Name: **Avaya SM**
4. Click **Next**
5. Set **Server Type**: Select Trunk Server from the drop down
6. Set **IP Address/FQDN**: Enter the Avaya Aura Session Manager SIP IP Address
7. Set **Port**: 5060 is used in this setup
8. Set **Transport**: UDP is selected

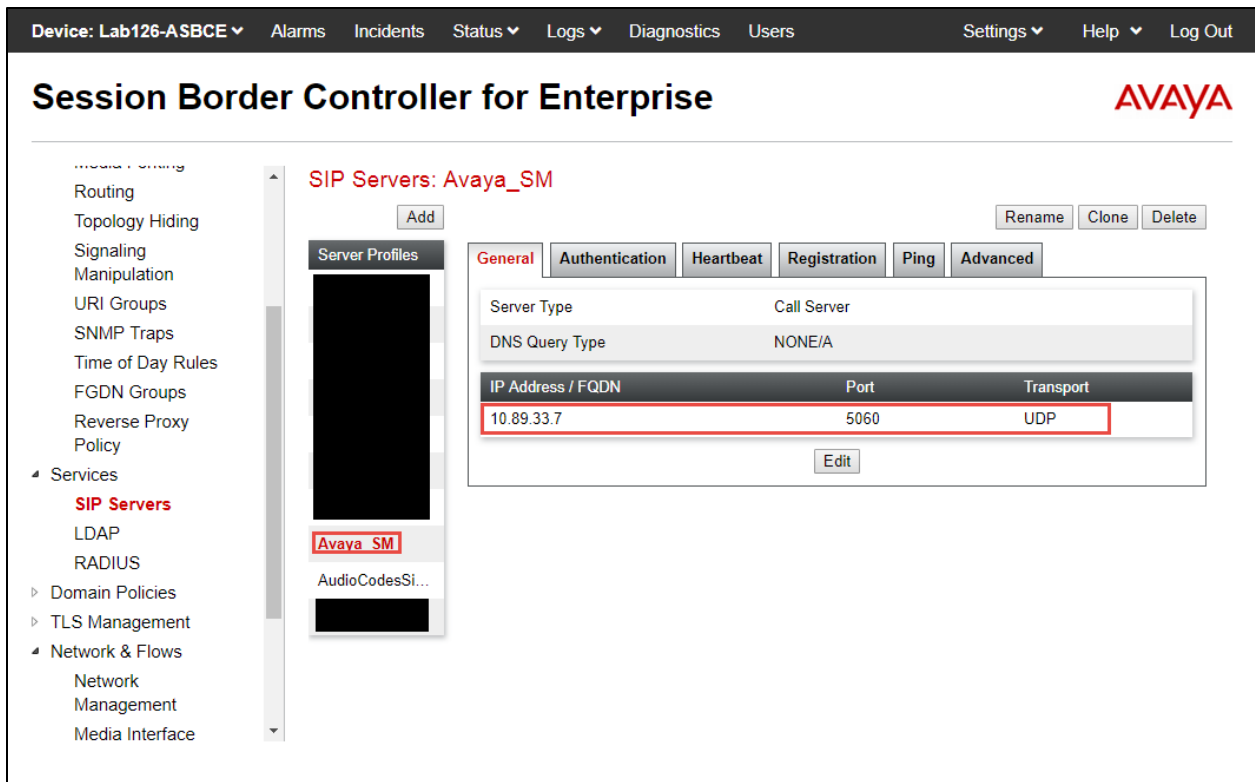


Figure 137- Add SIP Server – Avaya SM

9. Select **Authentication**

10. Keep the parameters at default values

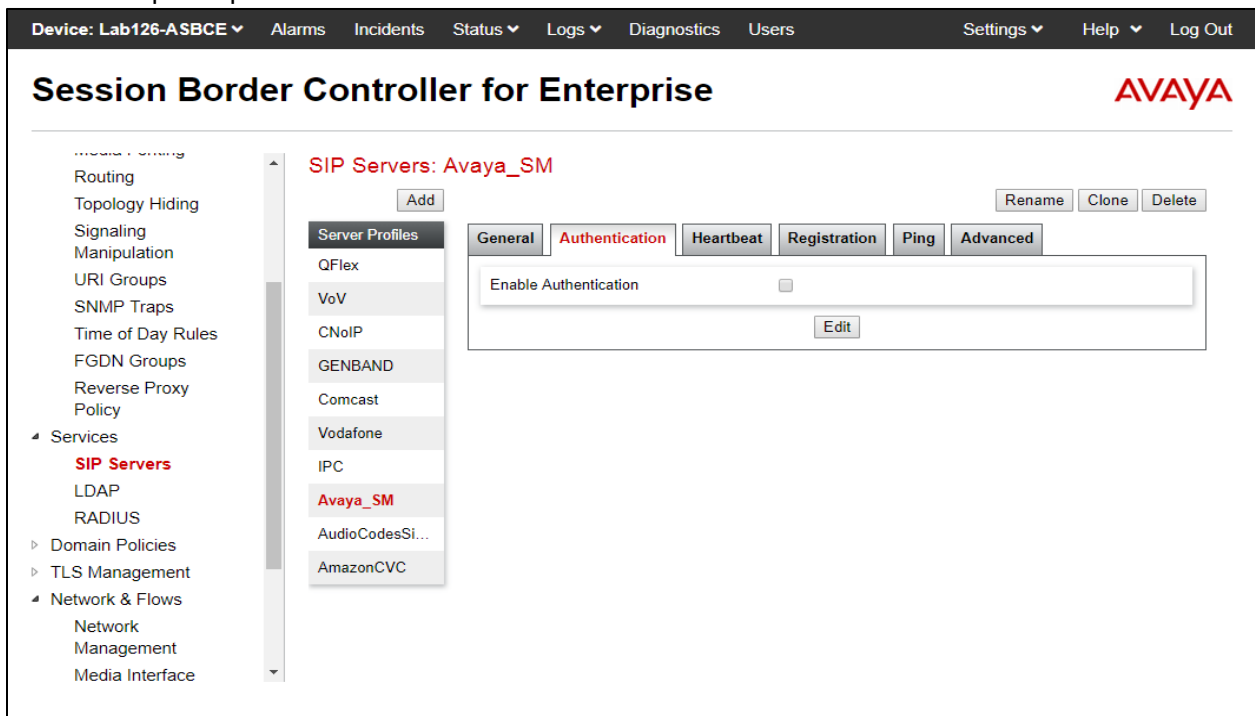


Figure 138 - Add SIP Server – Avaya SM

11. Select **Heartbeat**
12. Check **Enable Heartbeat**
13. Select **Method** as OPTIONS
14. Set **Frequency** as 30 seconds; **From URI** as ping@10.89.33.13, **To URI** as ping@10.89.33.7

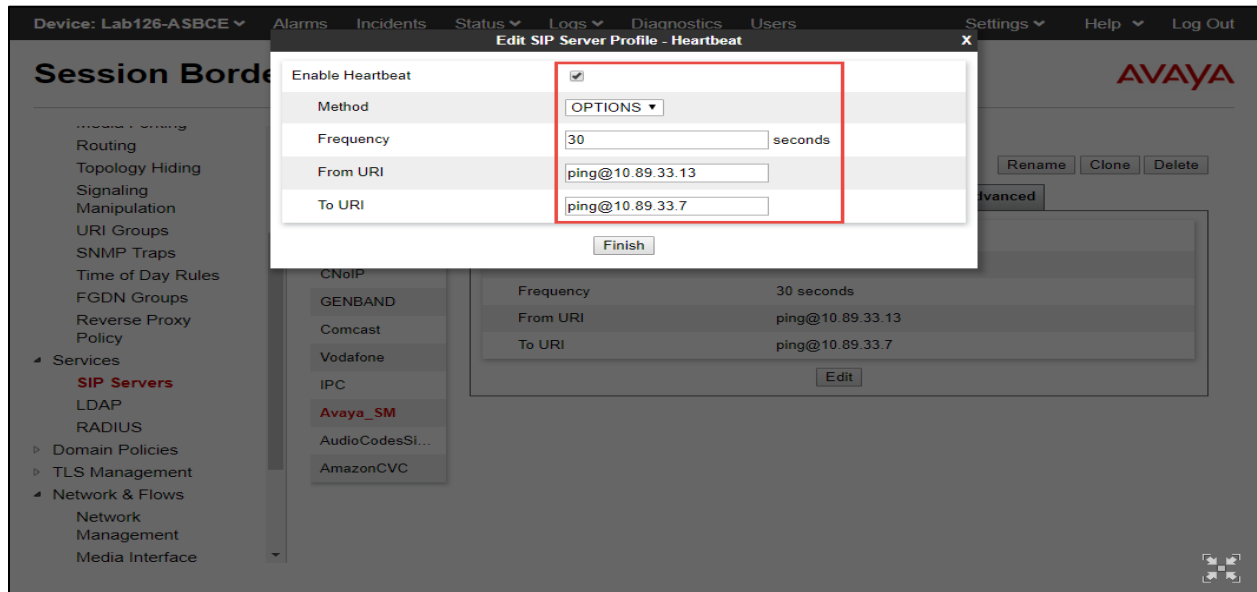


Figure 139 - Add SIP Server – Avaya SM

15. Select **Ping**
16. Keep the parameters at default values

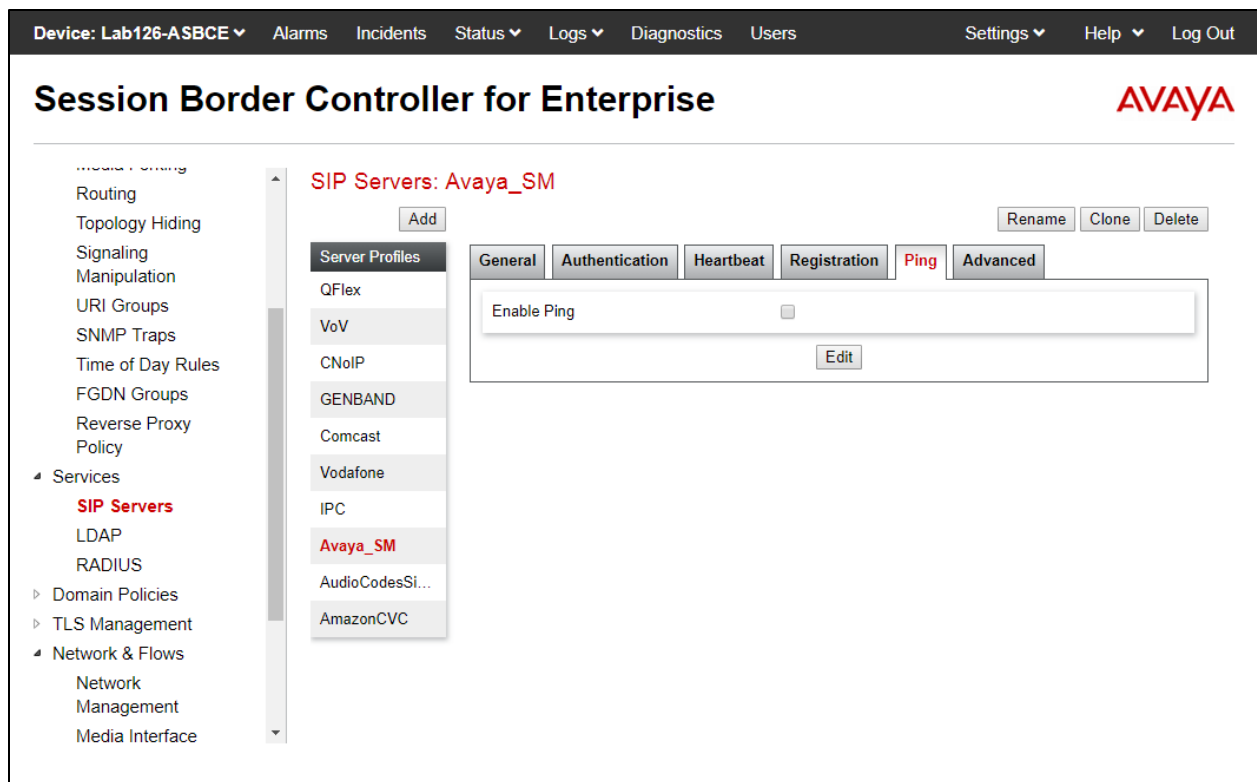


Figure 140 - Add SIP Server – Avaya SM

17. Select **Advanced**

18. Keep the parameters at default values

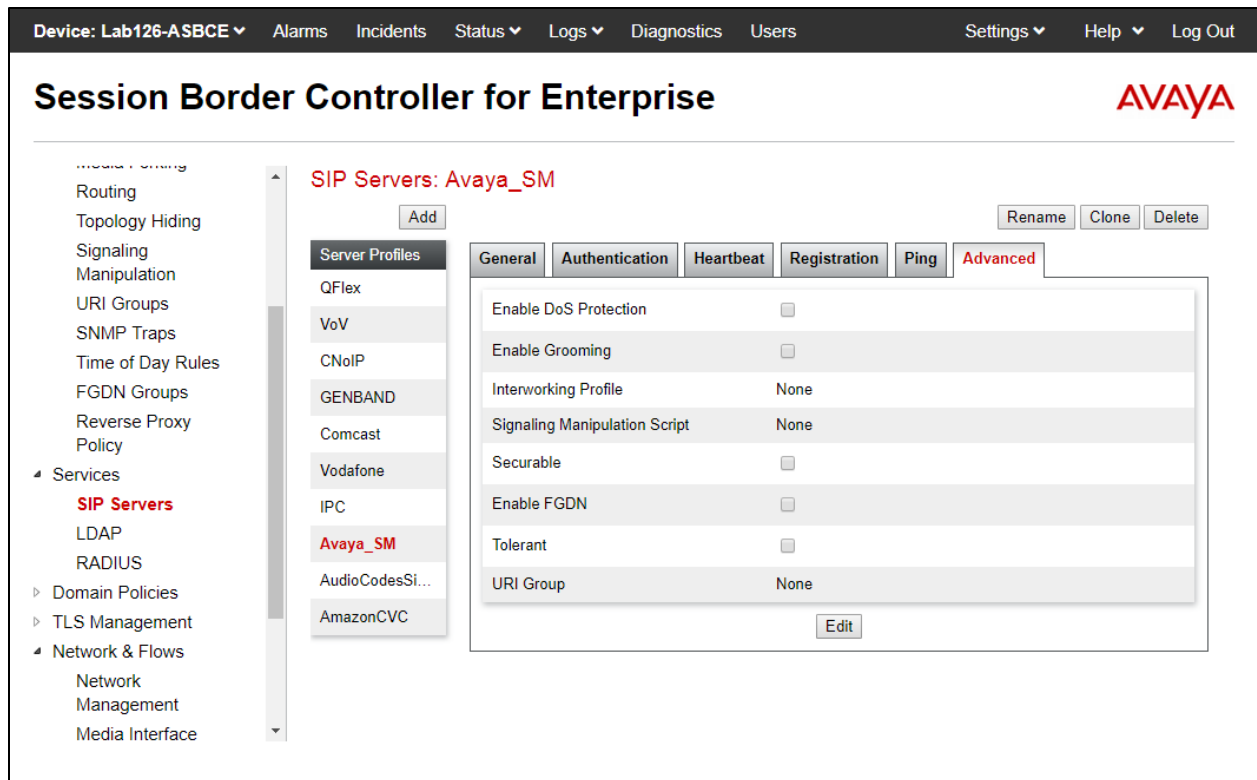


Figure 141 - Add SIP Server – Avaya SM

4.7.2.3 SIP Servers – AudioCodes Crestron

1. Navigate to **Services** → **SIP Servers**
2. Click **Add**
3. Set Profile Name: **AudioCodesSipServer**
4. Click **Next**
5. Set **Server Type**: Select Trunk Server from the drop down
6. Set **IP Address/FQDN**: Enter the AudioCodes IP
7. Set **Port**: 5064 is used in this setup
8. Set **Transport**: UDP is selected

Device: Lab126-ASBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise AVAYA

EMS Dashboard

Device Management

Backup/Restore

- System Parameters
- Configuration Profiles
- Services
 - SIP Servers**
 - LDAP
 - RADIUS
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

SIP Servers: AudioCodesSipServer

Server Profiles

AudioCodes...

Avaya_SM

General

Authentication

Heartbeat

Registration

Ping

Advanced

Server Type	Trunk Server	
SIP Domain	lab.tekvizion.com	
DNS Query Type	NONE/A	
IP Address / FQDN	Port	Transport
10.64.3.10	5064	UDP

Figure 142 - Add SIP Server – AudioCodes

9. Select **Authentication**
10. Keep the parameters at default values



Figure 143 - Add SIP Server – AudioCodes

11. Select **Heartbeat**
12. Check **Enable Heartbeat**
13. Select **Method** as OPTIONS
14. Set **Frequency** as 30 seconds; **From URI** as ping@10.64.5.57, **To URI** as ping@10.64.3.10
- 15.

Device: Lab126-ASBCE Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

EMS Lab126-ASBCE **er Controller for Enterprise** AVAYA

EMS Dashboard
 Device Management
 Backup/Restore
 System Parameters
 Configuration Profiles
 Services
 SIP Servers
 LDAP
 RADIUS
 Domain Policies
 TLS Management
 Network & Flows
 DMZ Services
 Monitoring & Logging

SIP Servers: AudioCodesSipServer

Add Rename Clone Delete

Server Profiles

AudioCodes...
Avaya_SM

General Authentication Heartbeat Registration Ping Advanced

Enable Heartbeat

Method	OPTIONS
Frequency	30 seconds
From URI	ping@10.64.5.57
To URI	ping@10.64.3.10

Edit

Figure 144 - Add SIP Server – AudioCodes

16. Select **Ping**

17. Keep the parameters at default values

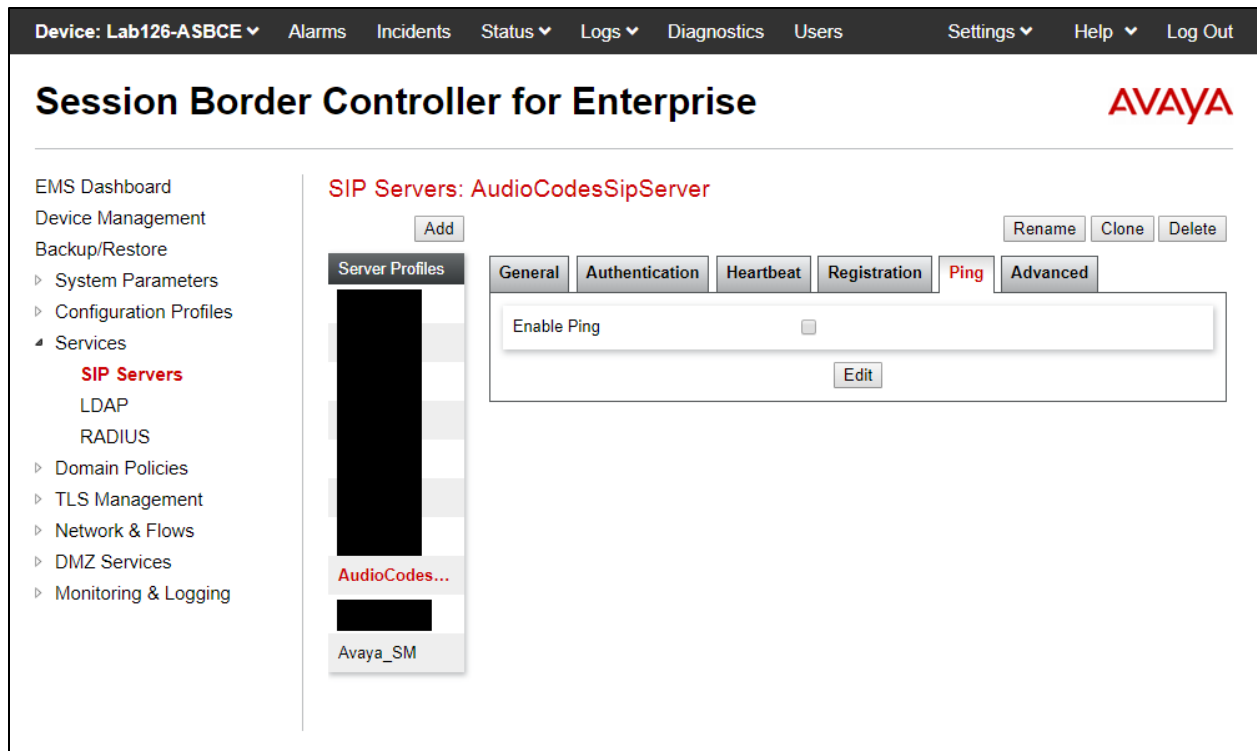


Figure 145 - Add SIP Server – AudioCodes

18. Select **Advanced**

19. Keep the parameters at default values

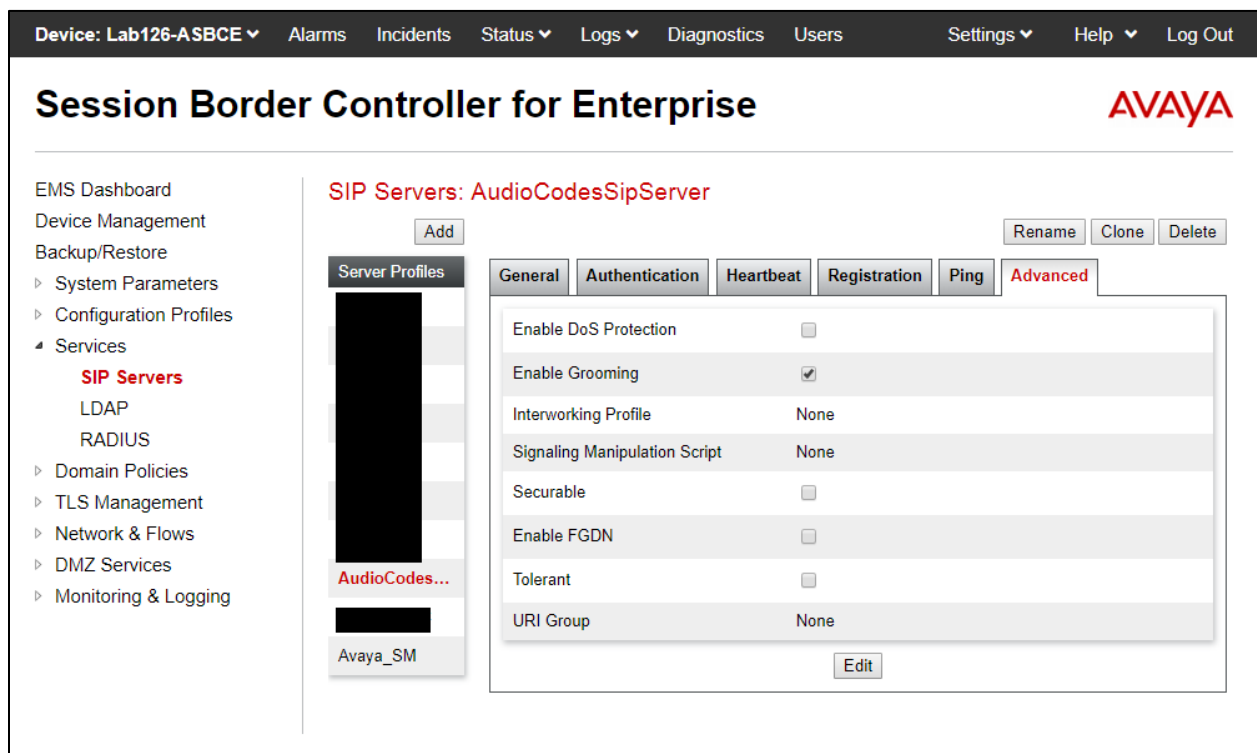


Figure 146 - Add SIP Server – AudioCodes

4.7.2.4 Topology Hiding

Topology Hiding profiles were added for Avaya Session Manager and AudioCodes SBC to overwrite and hiding certain headers

1. Navigate to: **Configure Profiles → Topology Hiding**
2. Two profiles are used for the testing. One is default and another one is created as below.

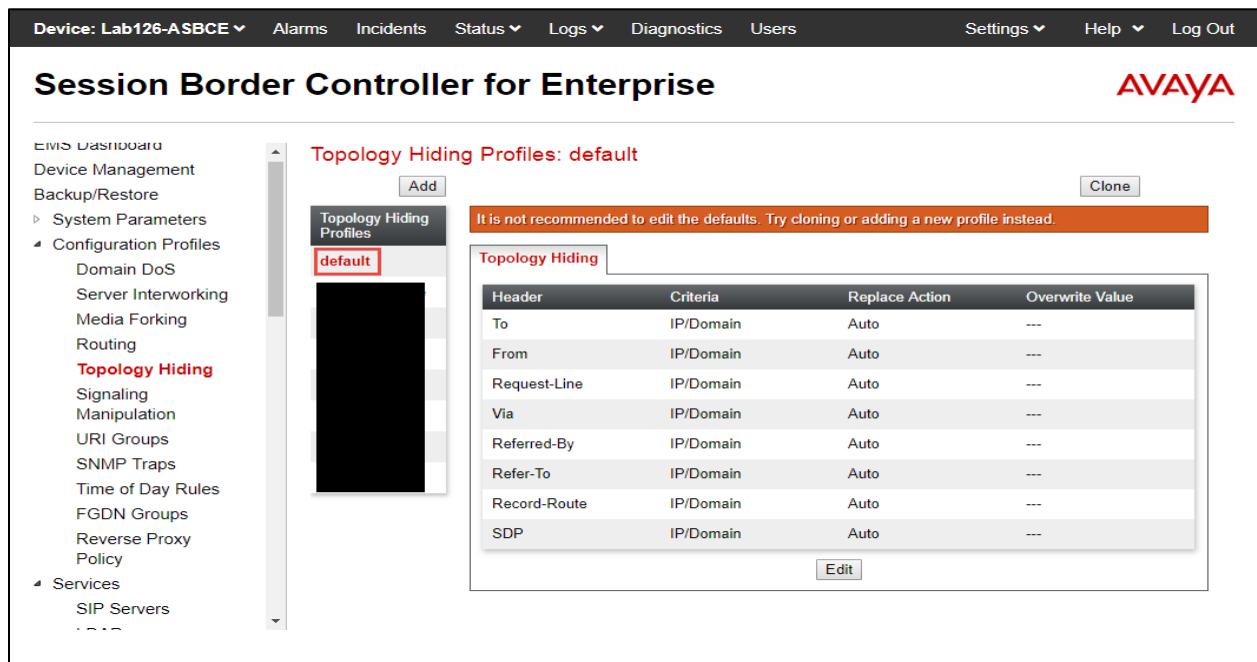


Figure 147 - Topology Hiding

3. Click **Add** and enter profile name
4. Add the following headers and keep Criteria and Replace Action with default values as below
5. Click **Finish**

Device: Lab126-ASBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise AVAYA

- EMS Dashboard
- Device Management
- Backup/Restore
- System Parameters
- ▾ Configuration Profiles
 - Domain DoS
 - Server Interworking
 - Media Forking
 - Routing
 - Topology Hiding**
 - Signaling Manipulation
 - URI Groups
 - SNMP Traps
 - Time of Day Rules
 - FGDN Groups
 - Reverse Proxy Policy
- ▾ Services

Topology Hiding Profiles: Avaya_SM

Add
Rename Clone Delete

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	lab.tekvizion.com
From	IP/Domain	Overwrite	lab.tekvizion.com
Request-Line	IP/Domain	Overwrite	lab.tekvizion.com

Edit

Figure 148 - Topology Hiding

4.7.2.5 Routing

1. Navigate to: **Configuration Profiles → Routing**
2. Click **Add**
3. Set **Profile Name**: AASM is given here
4. Click **Next**

At Routing Profile Window, click **Add**

5. Set **Server Configuration**: Avaya SM (which was configured under SIP Servers)
6. The Server IP, Port and Transport Protocol will populate automatically. Select UDP as Transport.
7. Leave all other fields as default
8. Click **Finish**

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	Delete
1				Avaya_S	10.89.33.7:5060	None	Delete

Figure 149 - Routing Profile – Avaya SM

9. Repeat same steps to create the Routing Profile AudioCodes for AudioCodes

Profile : AudioCodes_RP - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>
Next Hop Priority	<input checked="" type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>		
ENUM	<input type="checkbox"/>	ENUM Suffix	

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Custom	10.64.3.10:5064	UDP	Delete

Finish

Figure 150 - Routing Profile – AudioCodes

4.7.3 Domain Policies

4.7.3.1 Signaling Rules

1. Navigate to: **Domain Policies -> Signaling Rules**
2. Select **default** under Signaling Rules, click **Clone**
3. Set **Name**: Avaya_SM is given in this test
4. Click **Finish**
5. Select the newly cloned Signaling Rule **Avaya_SM**, under tab Request Headers, click **Add In Header Control** and configure the setting as below
6. Click **Finish**

Device: Lab126-ASBCE Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

EMS
Lab126-ASBCE

er Controller for Enterprise

AVAYA

EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
Application Rules
Border Rules
Media Rules
Security Rules
Signaling Rules
Charging Rules
End Point Policy Groups
Session Policies
TLS Management
Network & Flows
DMZ Services
Monitoring & Logging

Signaling Rules: Avaya_SM

Add Rename Clone Delete

Click here to add a description.

General Requests Responses **Request Headers** Response Headers Signaling QoS UCID

Add In Header Control Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
1	AV-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	P-AV-Message-Id	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	Reason	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
7	Alert-Info	ALL	Forbidden	Remove Header	No	IN	Edit	Delete

Figure 151 - Signaling Rule – Avaya SM

7. Repeat the same for Response Headers also

Device: Lab126-ASBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise AVAYA

EMS Dashboard

Device Management

Backup/Restore

- System Parameters
- Configuration Profiles
- Services
 - Domain Policies
 - Application Rules
 - Border Rules
 - Media Rules
 - Security Rules
 - Signaling Rules**
 - Charging Rules
 - End Point Policy Groups
 - Session Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

Signaling Rules: Avaya_SM

Rename Clone Delete

Add

Signaling Rules

- default
- No-Content-Type...
- Comcast
- Crestron
- Avaya_SM**
- test

Click here to add a description.

General
Requests
Responses
Request Headers
Response Headers
Signaling QoS
UCID

Add In Header Control
Add Out Header Control

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Endpoint-View	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	AV-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

Figure 152- Signaling Rule – Avaya SM

4.7.3.2 End Point Policy Groups

A new End Point Policy Group was created for Avaya Aura Session Manager. The default policy group was used for the AudioCodes side.

1. Navigate to: **Domain Policies -> End Point Policy Groups**
2. Two End Point Policy Groups are used for this testing. One is default-low and another one is created as below.

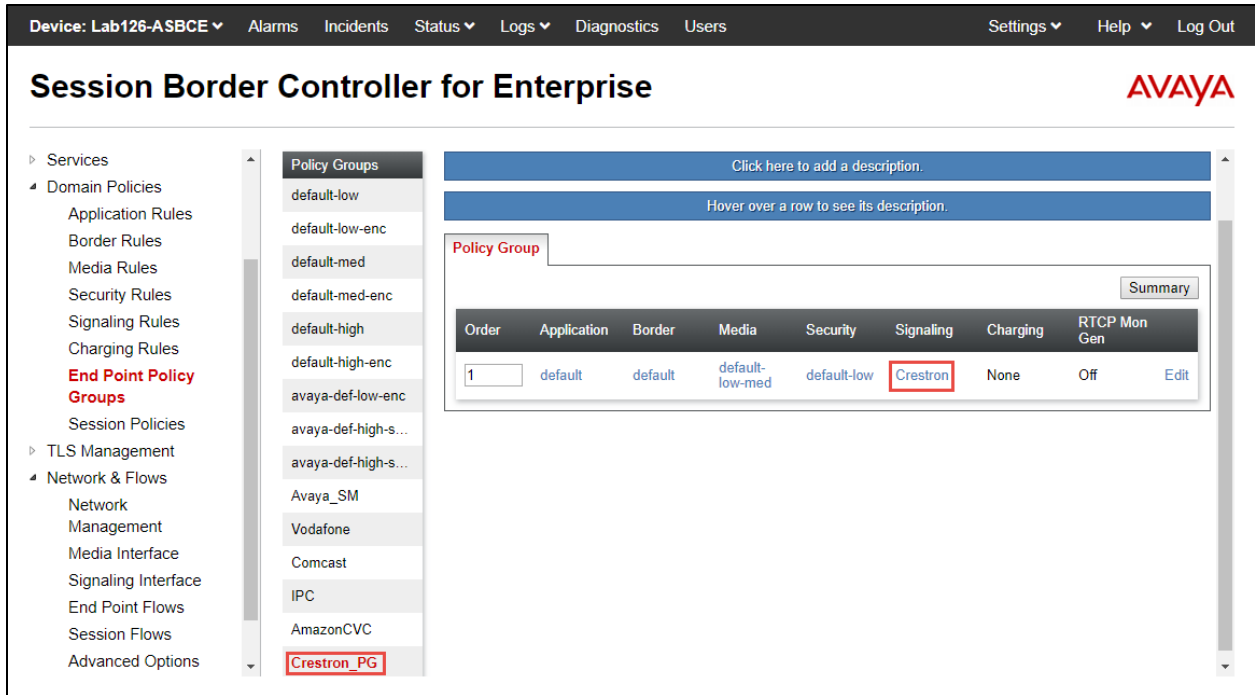
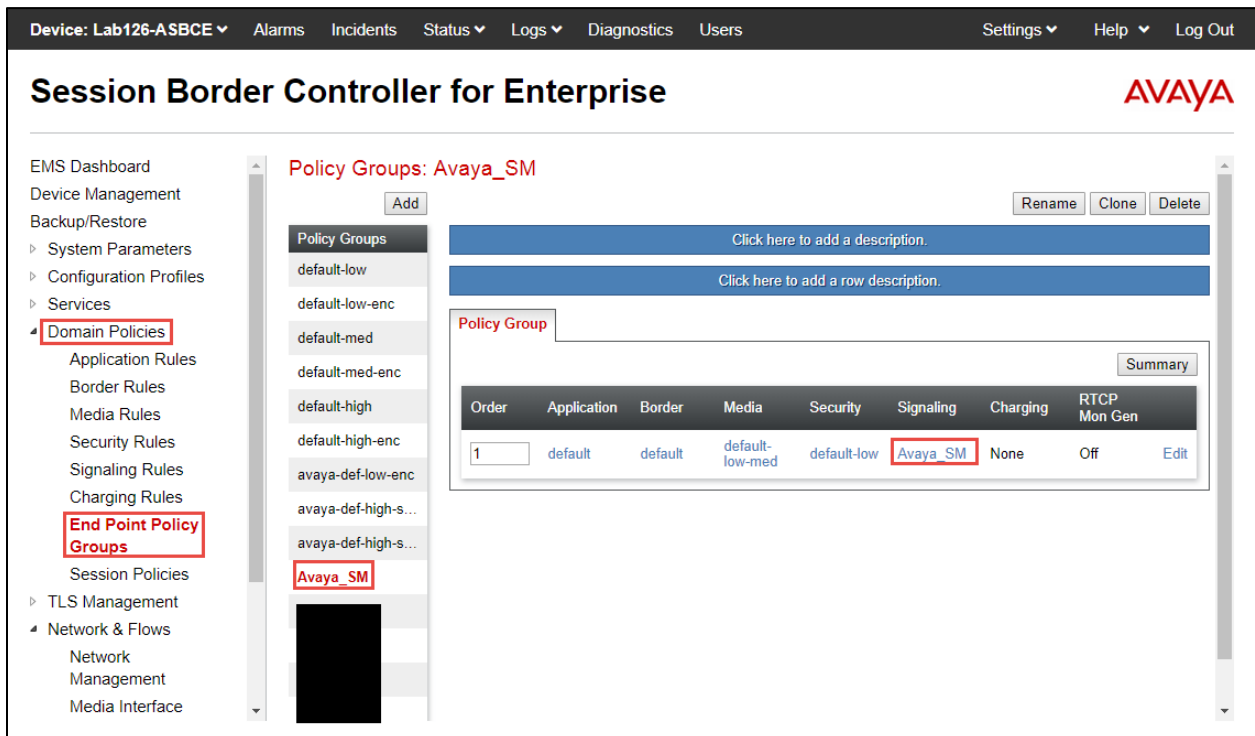


Figure 153- End Point Policy Group – Avaya SM

3. Select **Crestrin_PG** under Policy Groups
4. Click **Clone**
5. Set Clone Name: **Avaya_SM** is given
6. Click **Finish**



4.7.4 Network & Flows

4.7.4.1 Media Interface

1. Navigate to: **Device Specific Settings → Media Interface**. Click **Add**
2. Set **Name**: SBC LAN is given here
3. Set **IP Address**: Select SBC LAN from the drop down and the IP address will populate automatically. The IP address for Interface facing Avaya Aura Session Manager is 10.89.33.13
4. Set **Port Range**: 35000-40000 is used for this setup
5. Click **Finish**
6. Repeat the same steps to create a Media Interface facing AudioCodes with the name SBC WAN

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Lab126-ASBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main heading is 'Session Border Controller for Enterprise' with the AVAYA logo. The left sidebar shows a navigation menu with 'Media Interface' selected under 'Network & Flows'. The main content area is titled 'Media Interface' and contains a table with the following data:

Name	Media IP Network	Port Range	
Med_LAN	10.89.33.13 LAN-A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
Med_WAN	192.65.79.204 WAN-B1 (B1, VLAN 0)	35000 - 40000	Edit Delete

Figure 155- Media Interface

4.7.4.2 Signaling Interface

1. Navigate to: **Network & Flows → Signaling Interface**. Click **Add**, new Add Signaling Interface window will appear
2. Set **Name**: SBC LAN is given for the interface facing Avaya Aura Session Manager
3. Set **IP Address**: Select the signaling IP which is the Avaya Aura Session Manager facing interface
4. Set **UDP Port**: 5060 is set
5. Set **UDP/TLS Port**: Leave the boxes empty as only UDP is used between Avaya Aura Session Manager and Avaya SBCE
6. Leave all other fields at default values
7. Click **Finish**

8. Repeat same steps to create the Signaling Interface facing AudioCodes. UDP is the protocol between Avaya SBCE and AudioCodes.

Device: Lab126-ASBCE Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

EMS
Lab126-ASBCE

er Controller for Enterprise

AVAYA

- Domain Policies
 - Application Rules
 - Border Rules
 - Media Rules
 - Security Rules
 - Signaling Rules
 - Charging Rules
 - End Point Policy Groups
 - Session Policies
- TLS Management
- Network & Flows
 - Network Management
 - Media Interface
 - Signaling Interface**
 - End Point Flows

Signaling Interface

Signaling Interface Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
SIG_LAN	10.89.33.13 LAN-A1 (A1, VLAN 0)	---	5060	---	None	Edit Delete
SIG_WAN	192.65.79.204 WAN-B1 (B1, VLAN 0)	---	5060	---	None	Edit Delete

Figure 156 - Signaling Interface

4.7.4.3 Server Flows

1. Navigate to: **Network & Flows** → **End Point Flows** → **Server Flows**. Click **Add**
2. Set **Flow Name**: Avaya SM is given for enterprise
3. Set **SIP Server Profile**: Avaya_SM (created earlier)
4. Set **Transport**: UDP is selected here
5. Set **Receive Interface**: SIG_WAN (created earlier)
6. Set **Signaling Interface**: SIG_LAN (created earlier)
7. Set **Media Interface**: SIG_LAN (created earlier)
8. Set **End Point Policy Group**: default-low (created earlier)
9. Set **Routing Profile**: AudioCodes_RP (created earlier)
10. Set **Topology Hiding Profile**: Avaya_SM (created earlier)
11. Leave all other fields at default values
12. Click **Finish**

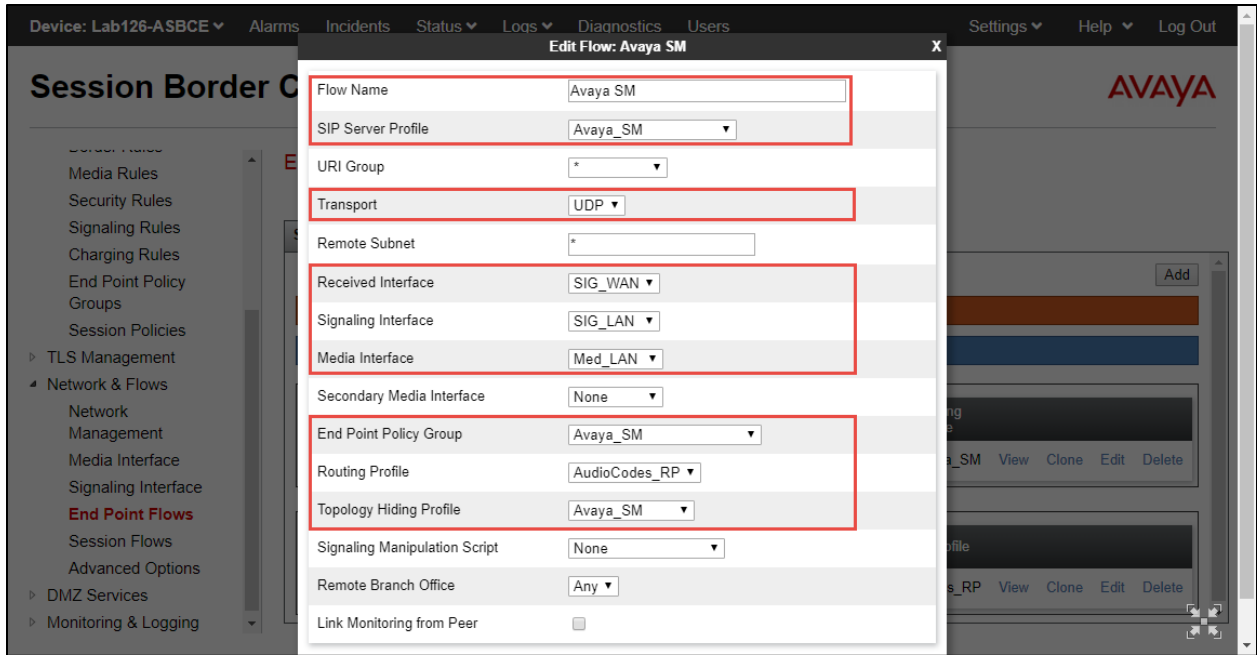


Figure 157 - Server Flow

13. Repeat the same steps for creating server flow for AudioCodes as below

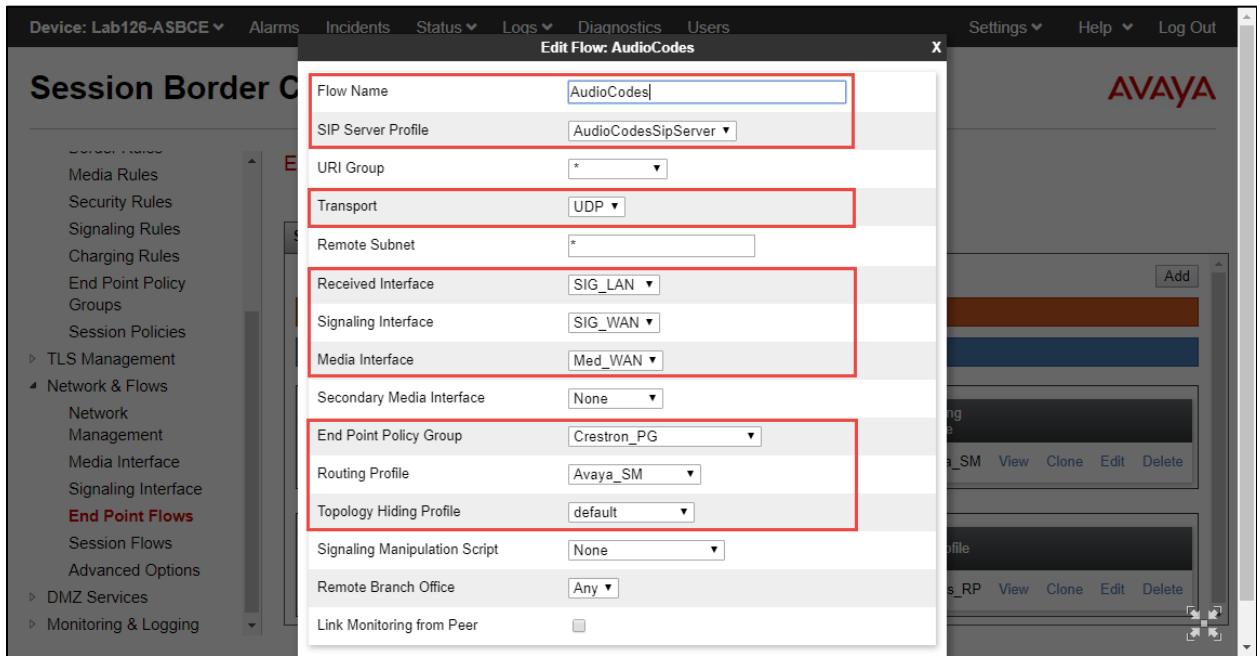


Figure 158 - Server Flow

5 Acronyms

Acronym	Definition
Avaya CM	Avaya Aura Communications Manager
Avaya SM	Avaya Aura Sessions Manager
Avaya SBCE	Avaya Session Border Controller for Enterprise
CLIP	Calling Line (Number) Identification Presentation
CLIR	Calling Line (Number) Identification Restriction
DNS	Domain Name Server
EXT	Extension
FQDN	Fully Qualified Domain Name
MRGL	Media Resource Group List
MTP	Media Termination Point
MWI	Message Waiting Indicator
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
RTP	Real Time Protocol
SRTP	Secure Real Time Protocol
SIP	Session Initiated Protocol
UDP	Uniform Dial Plan
VM	Voice Mail
B2BUA	Back to Back User Agent
SBC	Session Border Controller

6 Summary of Tests and Results

External ID	Title	Procedure	Expected Results	Status	Comments
1	Teams user Calls PBX A user	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX A user 2. Teams user hears Ring back Tone 3. PBX A user answers the call 4. Verify two way audio 5. Teams user hangs up the call 6. Verify call is cleared successfully 7. Repeat steps 1 to 4 8. PBX A user hangs up the call 9. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is connected with bi-directional audio, voice is clear, no echo 2. Call is disconnected 	PASSED	
2	Teams user Calls PBX B user	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX B user 2. Teams user hears Ring back Tone 3. PBX B user answers the call 4. Verify two way audio 5. Teams user hangs up the call 6. Verify call is cleared successfully 7. Repeat steps 1 to 4 8. PBX B user hangs up the call 9. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is connected with bi-directional audio, voice is clear, no echo 2. Call is disconnected 	NOT APPLICABLE	This testing is for only one PBX with Teams
3	Teams user Calls PSTN user	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PSTN user 2. Teams user hears Ring back Tone 3. PSTN user answers the call 	<ol style="list-style-type: none"> 1. Call is connected with bi-directional audio, voice is clear, no echo 	PASSED	

External ID	Title	Procedure	Expected Results	Status	Comments
		<ol style="list-style-type: none"> 4. Verify two way audio 5. Teams user hangs up the call 6. Verify call is cleared successfully 7. Repeat steps 1 to 4 8. PSTN user hangs up the call 9. Verify call is cleared successfully 	<ol style="list-style-type: none"> 2. Call is disconnected 		
4	Teams user Calls PBX A user and hangs up before answer	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX A user 2. PBX A user starts ringing 3. Teams user hears Ring back Tone 4. Teams user hangs up the call while PBX A user is ringing 5. PBX A user stops ringing 6. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is disconnected before answer 	PASSED	
5	Teams user Calls PBX B user and hangs up before answer	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX B user 2. PBX B user starts ringing 3. Teams user hears Ring back Tone 4. Teams user hangs up the call while PBX B user is ringing 5. PBX B user stops ringing 6. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is disconnected before answer 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
6	Teams user Calls PSTN user and hangs up before answer	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PSTN user 2. PSTN user starts ringing 3. Teams user hears Ring back Tone 4. Teams user hangs up the call while PSTN user is ringing 5. PSTN user stops ringing 6. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is disconnected before answer 	PASSED	
7	PBX A user Calls Teams user	<ol style="list-style-type: none"> 1. Make a voice call from PBX A user to Teams user 2. PBX A user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. PBX A user hangs up the call 6. Verify call is cleared successfully 7. Repeat steps 1 to 4 8. Teams user hangs up the call 9. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is connected with bi-directional audio, voice is clear, no echo 2. Call is disconnected 	PASSED	
8	PBX B user Calls Teams user	<ol style="list-style-type: none"> 1. Make a voice call from PBX B user to Teams user 2. PBX B user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. PBX B user hangs up the call 6. Verify call is cleared successfully 7. Repeat steps 1 to 4 8. Teams user hangs up the call 9. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is connected with bi-directional audio, voice is clear, no echo 2. Call is disconnected 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
9	PSTN user Calls Teams user	<ol style="list-style-type: none"> 1. Make a voice call from PSTN user to Teams user 2. PSTN user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. PSTN user hangs up the call 6. Verify call is cleared successfully 7. Repeat steps 1 to 4 8. Teams user hangs up the call 9. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is connected with bi-directional audio, voice is clear, no echo 2. Call is disconnected 	PASSED	
10	PBX A user Calls Teams user and hangs up before answer	<ol style="list-style-type: none"> 1. Make a voice call from PBX A user to Teams user 2. Teams user starts ringing 3. PBX A user hears Ring back Tone 4. PBX A user hangs up the call while Teams user is ringing 5. Teams user stops ringing 6. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is disconnected before answer 	PASSED	
11	PBX B user Calls Teams user and hangs up before answer	<ol style="list-style-type: none"> 1. Make a voice call from PBX B user to Teams user 2. Teams user starts ringing 3. PBX B user hears Ring back Tone 4. PBX B user hangs up the call while Teams user is ringing 5. Teams user stops ringing 6. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is disconnected before answer 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
12	PSTN user Calls Teams user and hangs up before answer	<ol style="list-style-type: none"> 1. Make a voice call from PSTN user to Teams user 2. Teams user starts ringing 3. PSTN user hears Ring back Tone 4. PSTN user hangs up the call while Teams user is ringing 5. Teams user stops ringing 6. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is disconnected before answer 	PASSED	
13	Teams user Calls PBX A user and performs hold/resume	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX A user 2. Teams user hears Ring back Tone 3. PBX A user answers the call 4. Verify two way audio 5. Teams user initiates call hold 6. Verify no audio is present while call is on hold 7. Teams user resumes the call 8. Verify two way audio is re-established between the two end points 9. Teams user hangs up the call 10. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is placed on hold successfully 2. No audio present during hold 3. Call is resumed successfully 4. Two way audio present after call is resumed 	PASSED	
14	Teams user Calls PBX B user and performs hold/resume	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX B user 2. Teams user hears Ring back Tone 3. PBX B user answers the call 4. Verify two way audio 5. Teams user initiates call hold 6. Verify no audio is present while call is 	<ol style="list-style-type: none"> 1. Call is placed on hold successfully 2. No audio present during hold 3. Call is resumed successfully 4. Two way audio 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
		<p>on hold</p> <p>7. Teams user resumes the call</p> <p>8. Verify two way audio is re-established between the two end points</p> <p>9. Teams user hangs up the call</p> <p>10. Verify call is cleared successfully</p>	present after call is resumed		
15	Teams user Calls PSTN user and performs hold/resume	<p>1. Make a voice call from Teams user to PSTN user</p> <p>2. Teams user hears Ring back Tone</p> <p>3. PSTN user answers the call</p> <p>4. Verify two way audio</p> <p>5. Teams user initiates call hold</p> <p>6. Verify no audio is present while call is on hold</p> <p>7. Teams user resumes the call</p> <p>8. Verify two way audio is re-established between the two end points</p> <p>9. Teams user hangs up the call</p> <p>10. Verify call is cleared successfully</p>	<p>1. Call is placed on hold successfully</p> <p>2. No audio present during hold</p> <p>3. Call is resumed successfully</p> <p>4. Two way audio present after call is resumed</p>	PASSED	
16	PBX A user Calls Teams user and Teams user performs hold/resume	<p>1. Make a voice call from PBX A user to Teams user</p> <p>2. PBX A user hears Ring back Tone</p> <p>3. Teams user answers the call</p> <p>4. Verify two way audio</p> <p>5. Teams user initiates call hold</p> <p>6. Verify no audio is present while call is on hold</p> <p>7. Teams user resumes the call</p>	<p>1. Call is placed on hold successfully</p> <p>2. No audio present during hold</p> <p>3. Call is resumed successfully</p> <p>4. Two way audio present after call is resumed</p>	FAILED	The UC-PHONE-PLUS desk phone is unable to resume a held call using Softkey, if the call has been answered by the phone using

External ID	Title	Procedure	Expected Results	Status	Comments
		<ul style="list-style-type: none"> 8. Verify two way audio is re-established between the two end points 9. PBX A user hangs up the call 10. Verify call is cleared successfully 			receiver or speaker button.
17	PBX B user Calls Teams user and Teams user performs hold/resume	<ul style="list-style-type: none"> 1. Make a voice call from PBX B user to Teams user 2. PBX B user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user initiates call hold 6. Verify no audio is present while call is on hold 7. Teams user resumes the call 8. Verify two way audio is re-established between the two end points 9. PBX B user hangs up the call 10. Verify call is cleared successfully 	<ul style="list-style-type: none"> 1. Call is placed on hold successfully 2. No audio present during hold 3. Call is resumed successfully 4. Two way audio present after call is resumed 	NOT APPLICABLE	PBX B is not tested with this cycle
18	PSTN user Calls Teams user and Teams performs hold/resume	<ul style="list-style-type: none"> 1. Make a voice call from PSTN user to Teams user 2. PSTN user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user initiates call hold 6. Verify no audio is present while call is on hold 7. Teams user resumes the call 8. Verify two way audio is re-established between the two end points 	<ul style="list-style-type: none"> 1. Call is placed on hold successfully 2. No audio present during hold 3. Call is resumed successfully 4. Two way audio present after call is resumed 	FAILED	The UC-PHONE-PLUS desk phone is unable to resume a held call using Softkey, if the call has been answered by the phone using receiver or speaker button.

External ID	Title	Procedure	Expected Results	Status	Comments
		9. PSTN user hangs up the call 10. Verify call is cleared successfully			
19	Teams user Calls PBX A user, Teams user performs Attended Transfer to PBX A user	1. Make a voice call from Teams user to PBX A user 1 2. Teams user hears Ring back Tone 3. PBX A user 1 answers the call 4. Verify two way audio 5. Teams user places a consultation call to PBX A user 2 6. Verify PBX A user 1 is placed on hold 7. PBX A user 2 answers the call 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PBX A user 1 and PBX A user 2 11. PBX A user 1 hangs up the call 12. Verify call is cleared successfully	1. Call is transferred successfully 2. Two way audio present after call is transferred	PASSED	
20	Teams user Calls PBX A user, Teams user performs Attended Transfer to PBX B user	1. Make a voice call from Teams user to PBX A user 2. Teams user hears Ring back Tone 3. PBX A user answers the call 4. Verify two way audio 5. Teams user places a consultation call to PBX B user 6. Verify PBX A user is placed on hold 7. PBX B user answers the call 8. Verify two way audio 9. Teams user completes the transfer	1. Call is transferred successfully 2. Two way audio present after call is transferred	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
		10. Verify two way audio between PBX A user and PBX B user 11. PBX A user hangs up the call 12. Verify call is cleared successfully			
21	Teams user Calls PBX A user, Teams user performs Attended Transfer to PSTN user	1. Make a voice call from Teams user to PBX A user 2. Teams user hears Ring back Tone 3. PBX A user answers the call 4. Verify two way audio 5. Teams user places a consultation call to PSTN user 6. Verify PBX A user is placed on hold 7. PSTN user answers the call 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PBX A user and PSTN user 11. PBX A user hangs up the call 12. Verify call is cleared successfully	1. Call is transferred successfully 2. Two way audio present after call is transferred	PASSED	
22	Teams user Calls PBX B user, Teams user performs Attended Transfer to PBX B user	1. Make a voice call from Teams user to PBX B user 1 2. Teams user hears Ring back Tone 3. PBX B user 1 answers the call 4. Verify two way audio 5. Teams user places a consultation call to PBX B user 2 6. Verify PBX B user 1 is placed on hold 7. PBX B user 2 answers the call	1. Call is transferred successfully 2. Two way audio present after call is transferred	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
		<ul style="list-style-type: none"> 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PBX B user 1 and PBX B user 2 11. PBX B user 1 hangs up the call 12. Verify call is cleared successfully 			
23	Teams user Calls PBX B user, Teams user performs Attended Transfer to PBX A user	<ul style="list-style-type: none"> 1. Make a voice call from Teams user to PBX B user 2. Teams user hears Ring back Tone 3. PBX B user answers the call 4. Verify two way audio 5. Teams user places a consultation call to PBX A user 6. Verify PBX B user is placed on hold 7. PBX A user answers the call 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PBX B user and PBX A user 11. PBX B user hangs up the call 12. Verify call is cleared successfully 	<ul style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams
24	Teams user Calls PBX B user, Teams user performs Attended	<ul style="list-style-type: none"> 1. Make a voice call from Teams user to PBX B user 2. Teams user hears Ring back Tone 3. PBX B user answers the call 4. Verify two way audio 5. Teams user places a consultation call to PSTN user 	<ul style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
	Transfer to PSTN user	<ul style="list-style-type: none"> 6. Verify PBX B user is placed on hold 7. PSTN user answers the call 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PBX B user and PSTN user 11. PBX B user hangs up the call 12. Verify call is cleared successfully 			
25	Teams user Calls PSTN user, Teams user performs Attended Transfer to PBX B user	<ul style="list-style-type: none"> 1. Make a voice call from Teams user to PSTN user 2. Teams user hears Ring back Tone 3. PSTN user answers the call 4. Verify two way audio 5. Teams user places a consultation call to PBX B user 6. Verify PSTN user is placed on hold 7. PBX B user answers the call 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PSTN user and PBX B user 11. PSTN user hangs up the call 12. Verify call is cleared successfully 	<ul style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams
26	Teams user Calls PSTN user, Teams user performs	<ul style="list-style-type: none"> 1. Make a voice call from Teams user to PSTN user 2. Teams user hears Ring back Tone 3. PSTN user answers the call 4. Verify two way audio 	<ul style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	PASSED	

External ID	Title	Procedure	Expected Results	Status	Comments
	Attended Transfer to PBX A user	<ol style="list-style-type: none"> 5. Teams user places a consultation call to PBX A user 6. Verify PSTN user is placed on hold 7. PBX A user answers the call 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PSTN user and PBX A user 11. PSTN user hangs up the call 12. Verify call is cleared successfully 			
27	Teams user Calls PSTN 1 user, Teams user performs Attended Transfer to PSTN 2 user	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PSTN user 1 2. Teams user hears Ring back Tone 3. PSTN user 1 answers the call 4. Verify two way audio 5. Teams user places a consultation call to PSTN user 2 6. Verify PSTN user 1 is placed on hold 7. PSTN user 2 answers the call 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PSTN user 1 and PSTN user 2 11. PSTN user 1 hangs up the call 12. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	PASSED	
28	PBX A user Calls Teams user, Teams	<ol style="list-style-type: none"> 1. Make a voice call from PBX A user 1 to Teams user 2. PBX A user 1 hears Ring back Tone 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio 	PASSED	

External ID	Title	Procedure	Expected Results	Status	Comments
	user performs Attended Transfer to PBX A user	<ol style="list-style-type: none"> 3. Teams user answers the call 4. Verify two way audio 5. Teams user places a consultation call to PBX A user 2 6. Verify PBX A user 1 is placed on hold 7. PBX A user 2 answers the call 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PBX A user 1 and PBX A user 2 11. PBX A user 1 hangs up the call 12. Verify call is cleared successfully 	present after call is transferred		
29	PBX A user Calls Teams user, Teams user performs Attended Transfer to PBX B user	<ol style="list-style-type: none"> 1. Make a voice call from PBX A user to Teams user 2. PBX A user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user places a consultation call to PBX B user 6. Verify PBX A user is placed on hold 7. PBX B user answers the call 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PBX A user and PBX B user 11. PBX A user hangs up the call 12. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
30	PBX A user Calls Teams user, Teams user performs Attended Transfer to PSTN user	<ol style="list-style-type: none"> 1. Make a voice call from PBX A user to Teams user 2. PBX A user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user places a consultation call to PSTN user 6. Verify PBX A user is placed on hold 7. PSTN user answers the call 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PBX A user and PSTN user 11. PBX A user hangs up the call 12. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	PASSED	
31	PBX B user Calls Teams user, Teams user performs Attended Transfer to PBX B user	<ol style="list-style-type: none"> 1. Make a voice call from PBX B user 1 to Teams user 2. PBX B user 1 hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user places a consultation call to PBX B user 2 6. Verify PBX B user 1 is placed on hold 7. PBX B user 2 answers the call 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PBX B user 1 and PBX B user 2 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
		<ol style="list-style-type: none"> 11. PBX B user 1 hangs up the call 12. Verify call is cleared successfully 			
32	PBX B user Calls Teams user, Teams user performs Attended Transfer to PBX A user	<ol style="list-style-type: none"> 1. Make a voice call from PBX B user to Teams user 2. PBX B user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user places a consultation call to PBX A user 6. Verify PBX B user is placed on hold 7. PBX A user answers the call 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PBX B user and PBX A user 11. PBX B user hangs up the call 12. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams
33	PBX B user Calls Teams user, Teams user performs Attended Transfer to PSTN user	<ol style="list-style-type: none"> 1. Make a voice call from PBX B user to Teams user 2. PBX B user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user places a consultation call to PSTN user 6. Verify PBX B user is placed on hold 7. PSTN user answers the call 8. Verify two way audio 9. Teams user completes the transfer 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
		10. Verify two way audio between PBX B user and PSTN user 11. PBX B user hangs up the call 12. Verify call is cleared successfully			
34	PSTN user Calls Teams user, Teams user performs Attended Transfer to PBX B user	1. Make a voice call from PSTN user to Teams user 2. PSTN user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user places a consultation call to PBX B user 6. Verify PSTN user is placed on hold 7. PBX B user answers the call 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PSTN user and PBX B user 11. PSTN user hangs up the call 12. Verify call is cleared successfully	1. Call is transferred successfully 2. Two way audio present after call is transferred	NOT APPLICABLE	This testing is for only one PBX with Teams
35	PSTN user Calls Teams user, Teams user performs Attended Transfer to PBX A user	1. Make a voice call from PSTN user to Teams user 2. PSTN user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user places a consultation call to PBX A user 6. Verify PSTN user is placed on hold 7. PBX A user answers the call	1. Call is transferred successfully 2. Two way audio present after call is transferred	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
		<ul style="list-style-type: none"> 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PSTN user and PBX A user 11. PSTN user hangs up the call 12. Verify call is cleared successfully 			
36	PSTN 1 user Calls Teams user, Teams user performs Attended Transfer to PSTN 2 user	<ul style="list-style-type: none"> 1. Make a voice call from PSTN user 1 to Teams user 2. PSTN user 1 hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user places a consultation call to PSTN user 2 6. Verify PSTN user 1 is placed on hold 7. PSTN user 2 answers the call 8. Verify two way audio 9. Teams user completes the transfer 10. Verify two way audio between PSTN user 1 and PSTN user 2 11. PSTN user 1 hangs up the call 12. Verify call is cleared successfully 	<ul style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	PASSED	
37	Teams user Calls PBX A user, Teams user performs Unattended	<ul style="list-style-type: none"> 1. Make a voice call from Teams user to PBX A user 1 2. Teams user hears Ring back Tone 3. PBX A user 1 answers the call 4. Verify two way audio 5. Teams user transfers the call to PBX A user 2 	<ul style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	PASSED	

External ID	Title	Procedure	Expected Results	Status	Comments
	Transfer to PBX A user	<ul style="list-style-type: none"> 6. PBX A user 2 starts ringing 7. PBX A user 1 hears Ring back Tone 8. PBX A user 2 answers the call 9. Verify two way audio between PBX A user 1 and PBX A user 2 10. PBX A user 1 hangs up the call 11. Verify call is cleared successfully 			
38	Teams user Calls PBX A user, Teams user performs Unattended Transfer to PBX B user	<ul style="list-style-type: none"> 1. Make a voice call from Teams user to PBX A user 2. Teams user hears Ring back Tone 3. PBX A user answers the call 4. Verify two way audio 5. Teams user transfers the call to PBX B user 6. PBX B user starts ringing 7. PBX A user hears Ring back Tone 8. PBX B user answers the call 9. Verify two way audio between PBX A user and PBX B user 10. PBX A user hangs up the call 11. Verify call is cleared successfully 	<ul style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
39	Teams user Calls PBX A user, Teams user performs Unattended Transfer to PSTN user	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX A user 2. Teams user hears Ring back Tone 3. PBX A user answers the call 4. Verify two way audio 5. Teams user transfers the call to PSTN user 6. PSTN user starts ringing 7. PBX A user hears Ring back Tone 8. PSTN user answers the call 9. Verify two way audio between PBX A user and PSTN user 10. PBX A user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	PASSED	
40	Teams user Calls PBX B user, Teams user performs Unattended Transfer to PBX B user	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX B user 1 2. Teams user hears Ring back Tone 3. PBX B user 1 answers the call 4. Verify two way audio 5. Teams user transfers the call to PBX B user 2 6. PBX B user 2 starts ringing 7. PBX B user 1 hears Ring back Tone 8. PBX B user 2 answers the call 9. Verify two way audio between PBX B user 1 and PBX B user 2 10. PBX B user 1 hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
41	Teams user Calls PBX B user, Teams user performs Unattended Transfer to PBX A user	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX B user 2. Teams user hears Ring back Tone 3. PBX B user answers the call 4. Verify two way audio 5. Teams user transfers the call to PBX A user 6. PBX A user starts ringing 7. PBX B user hears Ring back Tone 8. PBX A user answers the call 9. Verify two way audio between PBX B user and PBX A user 10. PBX B user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams
42	Teams user Calls PBX B user, Teams user performs Unattended Transfer to PSTN user	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX B user 2. Teams user hears Ring back Tone 3. PBX B user answers the call 4. Verify two way audio 5. Teams user transfers the call to PSTN user 6. PSTN user starts ringing 7. PBX B user hears Ring back Tone 8. PSTN user answers the call 9. Verify two way audio between PBX B user and PSTN user 10. PBX B user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
43	Teams user Calls PSTN user, Teams user performs Unattended Transfer to PBX B user	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PSTN user 2. Teams user hears Ring back Tone 3. PSTN user answers the call 4. Verify two way audio 5. Teams user transfers the call to PBX B user 6. PBX B user starts ringing 7. PSTN user hears Ring back Tone 8. PBX B user answers the call 9. Verify two way audio between PSTN user and PBX B user 10. PSTN user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams
44	Teams user Calls PSTN user, Teams user performs Unattended Transfer to PBX A user	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PSTN user 2. Teams user hears Ring back Tone 3. PSTN user answers the call 4. Verify two way audio 5. Teams user transfers the call to PBX A user 6. PBX A user starts ringing 7. PSTN user hears Ring back Tone 8. PBX A user answers the call 9. Verify two way audio between PSTN user and PBX A user 10. PSTN user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	PASSED	

External ID	Title	Procedure	Expected Results	Status	Comments
45	Teams user Calls PSTN 1 user, Teams user performs Unattended Transfer to PSTN 2 user	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PSTN user 1 2. Teams user hears Ring back Tone 3. PSTN user 1 answers the call 4. Verify two way audio 5. Teams user transfers the call to PSTN user 2 6. PSTN user 2 starts ringing 7. PSTN user 1 hears Ring back Tone 8. PSTN user 2 answers the call 9. Verify two way audio between PSTN user 1 and PSTN user 2 10. PSTN user 1 hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	PASSED	
46	PBX A user Calls Teams user, Teams user performs Unattended Transfer to PBX A user	<ol style="list-style-type: none"> 1. Make a voice call from PBX A user 1 to Teams user 2. PBX A user 1 hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user transfers the call to PBX A user 2 6. PBX A user 2 starts ringing 7. PBX A user 1 hears Ring back Tone 8. PBX A user 2 answers the call 9. Verify two way audio between PBX A user 1 and PBX A user 2 10. PBX A user 1 hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	PASSED	

External ID	Title	Procedure	Expected Results	Status	Comments
47	PBX A user Calls Teams user, Teams user performs Unattended Transfer to PBX B user	<ol style="list-style-type: none"> 1. Make a voice call from PBX A user to Teams user 2. PBX A user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user transfers the call to PBX B user 6. PBX B user starts ringing 7. PBX A user hears Ring back Tone 8. PBX B user answers the call 9. Verify two way audio between PBX A user and PBX B user 10. PBX A user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams
48	PBX A user Calls Teams user, Teams user performs Unattended Transfer to PSTN user	<ol style="list-style-type: none"> 1. Make a voice call from PBX A user to Teams user 2. PBX A user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user transfers the call to PSTN user 6. PSTN user starts ringing 7. PBX A user hears Ring back Tone 8. PSTN user answers the call 9. Verify two way audio between PBX A user and PSTN user 10. PBX A user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	PASSED	

External ID	Title	Procedure	Expected Results	Status	Comments
49	PBX B user Calls Teams user, Teams user performs Unattended Transfer to PBX B user	<ol style="list-style-type: none"> 1. Make a voice call from PBX B user 1 to Teams user 2. PBX B user 1 hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user transfers the call to PBX B user 2 6. PBX B user 2 starts ringing 7. PBX B user 1 hears Ring back Tone 8. PBX B user 2 answers the call 9. Verify two way audio between PBX B user 1 and PBX B user 2 10. PBX B user 1 hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams
50	PBX B user Calls Teams user, Teams user performs Unattended Transfer to PBX A user	<ol style="list-style-type: none"> 1. Make a voice call from PBX B user to Teams user 2. PBX B user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user transfers the call to PBX A user 6. PBX A user starts ringing 7. PBX B user hears Ring back Tone 8. PBX A user answers the call 9. Verify two way audio between PBX B user and PBX A user 10. PBX B user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
51	PBX B user Calls Teams user, Teams user performs Unattended Transfer to PSTN user	<ol style="list-style-type: none"> 1. Make a voice call from PBX B user to Teams user 2. PBX B user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user transfers the call to PSTN user 6. PSTN user starts ringing 7. PBX B user hears Ring back Tone 8. PSTN user answers the call 9. Verify two way audio between PBX B user and PSTN user 10. PBX B user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams
52	PSTN user Calls Teams user, Teams user performs Unattended Transfer to PBX B user	<ol style="list-style-type: none"> 1. Make a voice call from PSTN user to Teams user 2. PSTN user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user transfers the call to PBX B user 6. PBX B user starts ringing 7. PSTN user hears Ring back Tone 8. PBX B user answers the call 9. Verify two way audio between PSTN user and PBX B user 10. PSTN user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
53	PSTN user Calls Teams user, Teams user performs Unattended Transfer to PBX A user	<ol style="list-style-type: none"> 1. Make a voice call from PSTN user to Teams user 2. PSTN user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user transfers the call to PBX A user 6. PBX A user starts ringing 7. PSTN user hears Ring back Tone 8. PBX A user answers the call 9. Verify two way audio between PSTN user and PBX A user 10. PSTN user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	PASSED	
54	PSTN 1 user Calls Teams user, Teams user performs Unattended Transfer to PSTN 2 user	<ol style="list-style-type: none"> 1. Make a voice call from PSTN user 1 to Teams user 2. PSTN user 1 hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user transfers the call to PSTN user 2 6. PSTN user 2 starts ringing 7. PSTN user 1 hears Ring back Tone 8. PSTN user 2 answers the call 9. Verify two way audio between PSTN user 1 and PSTN user 2 10. PSTN user 1 hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	PASSED	

External ID	Title	Procedure	Expected Results	Status	Comments
55	PSTN user calls Teams user, Teams user performs Unattended Transfer to second Teams user	<ol style="list-style-type: none"> 1. Make a voice call from PSTN user to Teams user 1 2. PSTN user hears Ring back Tone 3. Teams user 1 answers the call 4. Verify two way audio 5. Teams user 1 transfers the call to Teams user 2 6. Teams user 2 starts ringing 7. Teams user 2 answers the call 8. Verify two way audio between PSTN user and Teams user 2 10. PSTN user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Call is transferred successfully 2. Two way audio present after call is transferred 	PASSED	
56	Teams user Calls PBX A user, Teams user adds PBX A user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX A user 1 2. Teams user hears Ring back Tone 3. PBX A user 1 answers the call 4. Verify two way audio 5. Teams user adds PBX A user 2 to the ongoing call 6. PBX A user 2 starts ringing 7. PBX A user 2 answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	FAILED	Crestron phone does not have an option to add a user into conference when its Teams user is assigned with E5 without Audio Conferencing license. Only on E5 without A/C license, audio conferencing a user works via Direct Routing.

External ID	Title	Procedure	Expected Results	Status	Comments
					Currently phone has the option to add a user into conference only with E5 (with A/C) license. With the E5 license, conferencing a user works directly through Microsoft and not via Direct Routing
57	Teams user calls PBX A user, Teams user adds PBX B user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX A user 2. Teams user hears Ring back Tone 3. PBX A user answers the call 4. Verify two way audio 5. Teams user adds PBX B user to the ongoing call 6. PBX B user starts ringing 7. PBX B user answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
58	Teams user user Calls PBX A user, Teams user adds PSTN user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX A user 2. Teams user hears Ring back Tone 3. PBX A user answers the call 4. Verify two way audio 5. Teams user adds PSTN user to the ongoing call 6. PSTN user starts ringing 7. PSTN user answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	FAILED	Crestron phone does not have an option to add a user into conference when its Teams user is assigned with E5 without Audio Conferencing license. Only on E5 without A/C license, audio conferencing a user works via Direct Routing. Currently phone has the option to add a user into conference only with E5 (with A/C) license. With the E5 license, conferencing a user works directly through Microsoft and not via Direct Routing

External ID	Title	Procedure	Expected Results	Status	Comments
59	Teams user user Calls PBX B user, Teams user adds PBX B user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX B user 1 2. Teams user hears Ring back Tone 3. PBX B user 1 answers the call 4. Verify two way audio 5. Teams user adds PBX B user 2 to the ongoing call 6. PBX B user 2 starts ringing 7. PBX B user 2 answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	NOT APPLICABLE	This testing is for only one PBX with Teams
60	Teams user user Calls PBX B user, Teams user adds PBX A user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX B user 2. Teams user hears Ring back Tone 3. PBX B user answers the call 4. Verify two way audio 5. Teams user adds PBX A user to the ongoing call 6. PBX A user starts ringing 7. PBX A user answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
61	Teams user user Calls PBX B user, Teams user adds PSTN user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX B user 2. Teams user hears Ring back Tone 3. PBX B user answers the call 4. Verify two way audio 5. Teams user adds PSTN user to the ongoing call 6. PSTN user starts ringing 7. PSTN user answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	NOT APPLICABLE	This testing is for only one PBX with Teams
62	Teams user user Calls PSTN user, Teams user adds PBX B user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PSTN user 2. Teams user hears Ring back Tone 3. PSTN user answers the call 4. Verify two way audio 5. Teams user adds PBX B user to the ongoing call 6. PBX B user starts ringing 7. PBX B user answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
63	Teams user user Calls PSTN user, Teams user adds PBX A user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PSTN user 2. Teams user hears Ring back Tone 3. PSTN user answers the call 4. Verify two way audio 5. Teams user adds PBX A user to the ongoing call 6. PBX A user starts ringing 7. PBX A user answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	FAILED	Crestron phone does not have an option to add a user into conference when its Teams user is assigned with E5 without Audio Conferencing license. Only on E5 without A/C license, audio conferencing a user works via Direct Routing. Currently phone has the option to add a user into conference only with E5 (with A/C) license. With the E5 license, conferencing a user works directly through Microsoft and not via Direct Routing

External ID	Title	Procedure	Expected Results	Status	Comments
64	Teams user user Calls PSTN 1 user, Teams user adds PSTN 2 user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PSTN user 1 2. Teams user hears Ring back Tone 3. PSTN user 1 answers the call 4. Verify two way audio 5. Teams user adds PSTN user 2 to the ongoing call 6. PSTN user 2 starts ringing 7. PSTN user 2 answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	FAILED	Crestron phone does not have an option to add a user into conference when its Teams user is assigned with E5 without Audio Conferencing license. Only on E5 without A/C license, audio conferencing a user works via Direct Routing. Currently phone has the option to add a user into conference only with E5 (with A/C) license. With the E5 license, conferencing a user works directly through Microsoft and not via Direct Routing

External ID	Title	Procedure	Expected Results	Status	Comments
65	PBX A user Calls Teams user, Teams user adds PBX A user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from PBX A user 1 to Teams user 2. PBX A user 1 hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user adds PBX A user 2 to the ongoing call 6. PBX A user 2 starts ringing 7. PBX A user 2 answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	FAILED	Crestron phone does not have an option to add a user into conference when its Teams user is assigned with E5 without Audio Conferencing license. Only on E5 without A/C license, audio conferencing a user works via Direct Routing. Currently phone has the option to add a user into conference only with E5 (with A/C) license. With the E5 license, conferencing a user works directly through Microsoft and not via Direct Routing

External ID	Title	Procedure	Expected Results	Status	Comments
66	PBX A user Calls Teams user, Teams user adds PBX B user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from PBX A user to Teams user 2. PBX A user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user adds PBXB user to the ongoing call 6. PBX B user starts ringing 7. PBX B user answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	NOT APPLICABLE	This testing is for only one PBX with Teams
67	PBX A user Calls Teams user, Teams user adds PSTN user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from PBX A user to Teams user 2. PBX A user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user adds PSTN user to the ongoing call 6. PSTN user starts ringing 7. PSTN user answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	FAILED	Crestron phone does not have an option to add a user into conference when its Teams user is assigned with E5 without Audio Conferencing license. Only on E5 without A/C license, audio conferencing a user works via Direct Routing.

External ID	Title	Procedure	Expected Results	Status	Comments
					Currently phone has the option to add a user into conference only with E5 (with A/C) license. With the E5 license, conferencing a user works directly through Microsoft and not via Direct Routing
68	PBX B user Calls Teams user, Teams user adds PBX B user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from PBX B user 1 to Teams user 2. PBX B user 1 hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user adds PBX B user 2 to the ongoing call 6. PBX B user 2 starts ringing 7. PBX B user 2 answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
69	PBX B user Calls Teams user, Teams user adds PBX A user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from PBX B user to Teams user 2. PBX B user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user adds PBX A user to the ongoing call 6. PBX A user starts ringing 7. PBX A user answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	NOT APPLICABLE	This testing is for only one PBX with Teams
70	PBX B user Calls Teams user, Teams user adds PSTN user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from PBX B user to Teams user 2. PBX B user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user adds PSTN user to the ongoing call 6. PSTN user starts ringing 7. PSTN user answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
71	PSTN user Calls Teams user, Teams user adds PBX B user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from PSTN user to Teams user 2. PSTN user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user adds PBX B user to the ongoing call 6. PBX B user starts ringing 7. PBX B user answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	NOT APPLICABLE	This testing is for only one PBX with Teams
72	PSTN user Calls Teams user, Teams user adds PBX A user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from PSTN user to Teams user 2. PSTN user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user adds PBX A user to the ongoing call 6. PBX A user starts ringing 7. PBX A user answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	FAILED	Crestron phone does not have an option to add a user into conference when its Teams user is assigned with E5 without Audio Conferencing license. Only on E5 without A/C license, audio conferencing a user works via Direct Routing.

External ID	Title	Procedure	Expected Results	Status	Comments
					Currently phone has the option to add a user into conference only with E5 (with A/C) license. With the E5 license, conferencing a user works directly through Microsoft and not via Direct Routing

External ID	Title	Procedure	Expected Results	Status	Comments
73	PSTN 1 user Calls Teams user, Teams user adds PSTN 2 user to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from PSTN user 1 to Teams user 2. PSTN user 1 hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Teams user adds PSTN user 2 to the ongoing call 6. PSTN user 2 starts ringing 7. PSTN user 2 answers the call 9. Verify all three users are able to hear each other 10. Teams user hangs up the call 11. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	FAILED	Crestron phone does not have an option to add a user into conference when its Teams user is assigned with E5 without Audio Conferencing license. Only on E5 without A/C license, audio conferencing a user works via Direct Routing. Currently phone has the option to add a user into conference only with E5 (with A/C) license. With the E5 license, conferencing a user works directly through Microsoft and not via Direct Routing

External ID	Title	Procedure	Expected Results	Status	Comments
74	PSTN user Calls Teams user, Teams user adds two or more users to the ongoing call	<ol style="list-style-type: none"> 1. Make a voice call from PSTN user to Teams user 1 2. PSTN user hears Ring back Tone 3. Teams user 1 answers the call 4. Verify two way audio 5. Teams user 1 adds Teams user 2 to the ongoing call 6. Verify Teams user 2 is added successfully to the call 7. Teams user 1 adds PBX A user to the ongoing call 9. Verify PBX A user is added successfully to the call 10. Teams user 1 adds PBX B user to the ongoing call 11. Verify PBX B user is added successfully to the call 12. Verify all four users are able to hear each other 13. All the users hang up and call is cleared successfully for all the users 	<ol style="list-style-type: none"> 1. Third user is added to the call successfully 2. All three users are able to hear each other 	FAILED	Crestron phone does not have an option to add a user into conference when its Teams user is assigned with E5 without Audio Conferencing license. Only on E5 without A/C license, audio conferencing a user works via Direct Routing. Currently phone has the option to add a user into conference only with E5 (with A/C) license. With the E5 license, conferencing a user works directly through Microsoft and not via Direct Routing

External ID	Title	Procedure	Expected Results	Status	Comments
75	PBX A user Calls Teams user, Teams user CFA to PBX A user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding all to PBX A user 2 2. Make a voice call from PBX A user 1 to Teams user 3. PBX A user 2 starts ringing 4. PBX A user 2 answers the call 5. Verify two way audio 6. PBX A user 1 hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call to correct destination	PASSED	
76	PBX A user Calls Teams user, Teams user CFA to PBX B user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding all to PBX B user 2. Make a voice call from PBX A user to Teams user 3. PBX B user starts ringing 4. PBX B user answers the call 5. Verify two way audio 6. PBX A user hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call to correct destination	NOT APPLICABLE	This testing is for only one PBX with Teams
77	PBX A user Calls Teams user, Teams user CFA to PSTN user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding all to PSTN user 2. Make a voice call from PBX A user to Teams user 3. PSTN user starts ringing 4. PSTN user answers the call 5. Verify two way audio 6. PBX A user hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call to correct destination	PASSED	

External ID	Title	Procedure	Expected Results	Status	Comments
78	PBX B user Calls Teams user, Teams user CFA to PBX B user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding all to PBX B user 2 2. Make a voice call from PBX B user 1 to Teams user 3. PBX B user 2 starts ringing 4. PBX B user 2 answers the call 5. Verify two way audio 6. PBX B user 1 hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call to correct destination	NOT APPLICABLE	This testing is for only one PBX with Teams
79	PBX B user Calls Teams user, Teams user CFA to PBX A user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding all to PBX A user 2. Make a voice call from PBX B user to Teams user 3. PBX A user starts ringing 4. PBX A user answers the call 5. Verify two way audio 6. PBX B user hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call to correct destination	NOT APPLICABLE	This testing is for only one PBX with Teams
80	PBX B user Calls Teams user, Teams user CFA to PSTN user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding all to PSTN user 2. Make a voice call from PBX B user to Teams user 3. PSTN user starts ringing 4. PSTN user answers the call 5. Verify two way audio 6. PBX B user hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call to correct destination	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
81	PSTN user Calls Teams user, Teams user CFA to PBX B user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding all to PBX B user 2. Make a voice call from PSTN user to Teams user 3. PBX B user starts ringing 4. PBX B user answers the call 5. Verify two way audio 6. PSTN user hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call to correct destination	NOT APPLICABLE	This testing is for only one PBX with Teams
82	PSTN user Calls Teams user, Teams user CFA to PBX A user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding all to PBX A user 2. Make a voice call from PSTN user to Teams user 3. PBX A user starts ringing 4. PBX A user answers the call 5. Verify two way audio 6. PSTN user hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call to correct destination	PASSED	
83	PSTN 1 user Calls Teams user, Teams user CFA to PSTN 2 user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding all to PSTN user 2 2. Make a voice call from PSTN user 1 to Teams user 3. PSTN user 2 starts ringing 4. PSTN user 2 answers the call 5. Verify two way audio 6. PSTN user 1 hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call to correct destination	PASSED	

External ID	Title	Procedure	Expected Results	Status	Comments
84	PBX A user Calls Teams user, Teams user CFNA to PBX A user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding no answer to PBX A user 2 2. Make a voice call from PBX A user 1 to Teams user 3. Teams user starts ringing 4. Teams user does not answer the call 5. Call gets forwarded after the no answer timeout value is reached 6. PBX A user 2 starts ringing 4. PBX A user 2 answers the call 5. Verify two way audio 6. PBX A user 1 hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call successfully on reaching the No answer timeout value	PASSED	
85	PBX A user Calls Teams user, Teams user CFNA to PBX B user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding no answer to PBX B user 2. Make a voice call from PBX A user to Teams user 3. Teams user starts ringing 4. Teams user does not answer the call 5. Call gets forwarded after the no answer timeout value is reached 6. PBX B user starts ringing 4. PBX B user answers the call 5. Verify two way audio 6. PBX A user hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call successfully on reaching the No answer timeout value	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
86	PBX A user Calls Teams user, Teams user CFNA to PSTN user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding no answer to PSTN user 2. Make a voice call from PBX A user to Teams user 3. Teams user starts ringing 4. Teams user does not answer the call 5. Call gets forwarded after the no answer timeout value is reached 6. PSTN user starts ringing 4. PSTN user answers the call 5. Verify two way audio 6. PBX A user hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call successfully on reaching the No answer timeout value	PASSED	This testing is for only one PBX with Teams
87	PBX B user Calls Teams user, Teams user CFNA to PBX B user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding no answer to PBX B user 2 2. Make a voice call from PBX B user 1 to Teams user 3. Teams user starts ringing 4. Teams user does not answer the call 5. Call gets forwarded after the no answer timeout value is reached 6. PBX B user 2 starts ringing 4. PBX B user 2 answers the call 5. Verify two way audio 6. PBX B user hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call successfully on reaching the No answer timeout value	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
88	PBX B user Calls Teams user, Teams user CFNA to PBX A user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding no answer to PBX A user 2. Make a voice call from PBX B user to Teams user 3. Teams user starts ringing 4. Teams user does not answer the call 5. Call gets forwarded after the no answer timeout value is reached 6. PBX A user starts ringing 4. PBX A user answers the call 5. Verify two way audio 6. PBX B user hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call successfully on reaching the No answer timeout value	NOT APPLICABLE	This testing is for only one PBX with Teams
89	PBX B user Calls Teams user, Teams user CFNA to PSTN user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding no answer to PSTN user 2. Make a voice call from PBX B user to Teams user 3. Teams user starts ringing 4. Teams user does not answer the call 5. Call gets forwarded after the no answer timeout value is reached 6. PSTN user starts ringing 4. PSTN user answers the call 5. Verify two way audio 6. PBX B user hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call successfully on reaching the No answer timeout value	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
90	PSTN user Calls Teams user, Teams user CFNA to PBX B user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding no answer to PBX B user 2. Make a voice call from PSTN user to Teams user 3. Teams user starts ringing 4. Teams user does not answer the call 5. Call gets forwarded after the no answer timeout value is reached 6. PBX B user starts ringing 4. PBX B user answers the call 5. Verify two way audio 6. PSTN user hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call successfully on reaching the No answer timeout value	NOT APPLICABLE	This testing is for only one PBX with Teams
91	PSTN user Calls Teams user, Teams user CFNA to PBX A user	<ol style="list-style-type: none"> 1. Teams user sets call forwarding no answer to PBX A user 2. Make a voice call from PSTN user to Teams user 3. Teams user starts ringing 4. Teams user does not answer the call 5. Call gets forwarded after the no answer timeout value is reached 6. PBX A user starts ringing 4. PBX A user answers the call 5. Verify two way audio 6. PSTN user hangs up the call 7. Verify call is cleared successfully 	1. Teams user is able to forward the incoming call successfully on reaching the No answer timeout value	PASSED	
92	PSTN 1 user Calls Teams	<ol style="list-style-type: none"> 1. Teams user sets call forwarding no answer to PSTN user 2 	1. Teams user is able to forward the	PASSED	

External ID	Title	Procedure	Expected Results	Status	Comments
	user, Teams user CFNA to PSTN 2 user	<ol style="list-style-type: none"> 2. Make a voice call from PSTN user 1 to Teams user 3. Teams user starts ringing 4. Teams user does not answer the call 5. Call gets forwarded after the no answer timeout value is reached 6. PSTN user 2 starts ringing 4. PSTN user 2 answers the call 5. Verify two way audio 6. PSTN user 1 hangs up the call 7. Verify call is cleared successfully 	incoming call successfully on reaching the No answer timeout value		
93	PSTN user calls Teams user, Teams user and users set for simultaneous ringing also rings	<ol style="list-style-type: none"> 1. Teams user sets simultaneous ringing to PBX A user and PBX B user 2. Make a voice call from PSTN user to Teams user 3. Teams user, PBX A user and PBX B user starts ringing 4. PBX A user answers the call 5. Verify two way audio 6. PSTN user hangs up 7. Verify call is cleared successfully 8. Repeat steps 2 to 6 where PBX B user answers the call 		PASSED	Tested only with PBX A

External ID	Title	Procedure	Expected Results	Status	Comments
94	Teams user with restricted Caller ID Calls PBX A user	<ol style="list-style-type: none"> 1. Make a voice call from Teams user with restricted caller ID to PBX A user 2. Teams user hears Ring back Tone 3. PBX A user starts ringing 4. Verify caller ID displayed on PBX A user is Unavailable/Private/Anonymous 5. PBX A user answers the call 6. Verify two way audio 7. Teams user hangs up the call 8. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Teams user is able to dial an outbound call with restricted caller ID 2. Call is successful with two way audio 	PASSED	
95	Teams user with restricted Caller ID Calls PBX B user	<ol style="list-style-type: none"> 1. Make a voice call from Teams user with restricted caller ID to PBX B user 2. Teams user hears Ring back Tone 3. PBX B user starts ringing 4. Verify caller ID displayed on PBX B user is Unavailable/Private/Anonymous 5. PBX B user answers the call 6. Verify two way audio 7. Teams user hangs up the call 8. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Teams user is able to dial an outbound call with restricted caller ID 2. Call is successful with two way audio 	NOT APPLICABLE	This testing is for only one PBX with Teams
96	Teams user with restricted Caller ID Calls PSTN user	<ol style="list-style-type: none"> 1. Make a voice call from Teams user with restricted caller ID to PSTN user 2. Teams user hears Ring back Tone 3. PSTN user starts ringing 4. Verify caller ID displayed on PSTN user is Unavailable/Private/Anonymous 	<ol style="list-style-type: none"> 1. Teams user is able to dial an outbound call with restricted caller ID 2. Call is successful with two way audio 	PASSED	

External ID	Title	Procedure	Expected Results	Status	Comments
		5. PSTN user answers the call 6. Verify two way audio 7. Teams user hangs up the call 8. Verify call is cleared successfully			
97	PBX A user with restricted Caller ID Calls Teams user	1. Make a voice call from PBX A user with restricted caller ID to Teams user 2. PBX A user hears Ring back Tone 3. Teams user starts ringing 4. Verify caller ID displayed on Teams user is Unavailable/Private/Anonymous 5. Teams user answers the call 6. Verify two way audio 7. PBX A user hangs up the call 8. Verify call is cleared successfully	1. Teams user is able to receive an inbound call with restricted caller ID 2. Call is successful with two way audio	PASSED	
98	PBX B user with restricted Caller ID Calls Teams user	1. Make a voice call from PBX B user with restricted caller ID to Teams user 2. PBX B user hears Ring back Tone 3. Teams user starts ringing 4. Verify caller ID displayed on Teams user is Unavailable/Private/Anonymous 5. Teams user answers the call 6. Verify two way audio 7. PBX B user hangs up the call 8. Verify call is cleared successfully	1. Teams user is able to receive an inbound call with restricted caller ID 2. Call is successful with two way audio	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
99	PSTN user with restricted Caller ID Calls Teams user	<ol style="list-style-type: none"> 1. Make a voice call from PSTN user with restricted caller ID to Teams user 2. PSTN user hears Ring back Tone 3. Teams user starts ringing 4. Verify caller ID displayed on Teams user is Unavailable/Private/Anonymous 5. Teams user answers the call 6. Verify two way audio 7. PSTN user hangs up the call 8. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Teams user is able to receive an inbound call with restricted caller ID 2. Call is successful with two way audio 	PASSED	
100	PBX A user Calls Teams user and leaves voicemail	<ol style="list-style-type: none"> 1. Make a voice call from PBX A user to Teams user 2. Teams user does not answer the call 3. Allow the call to get forwarded to voicemail 4. PBX A user successfully leaves voicemail 5. Teams user receives voicemail notification 6. Teams user successfully retrieves voicemail 	<ol style="list-style-type: none"> 1. Teams user is able to receive and retrieve voicemail successfully 	PASSED	
101	PBX B user Calls Teams user and	<ol style="list-style-type: none"> 1. Make a voice call from PBX B user to Teams user 2. Teams user does not answer the call 3. Allow the call to get forwarded to 	<ol style="list-style-type: none"> 1. Teams user is able to receive and retrieve voicemail successfully 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
	leaves voicemail	voicemail 4. PBX B user successfully leaves voicemail 5. Teams user receives voicemail notification 6. Teams user successfully retrieves voicemail			
102	PSTN user Calls Teams user and leaves voicemail	1. Make a voice call from PSTN user to Teams user 2. Teams user does not answer the call 3. Allow the call to get forwarded to voicemail 4. PSTN user successfully leaves voicemail 5. Teams user receives voicemail notification 6. Teams user successfully retrieves voicemail	1. Teams user is able to receive and retrieve voicemail successfully	PASSED	
103	Teams user Calls PBX A user and leaves voicemail	1. Make a voice call from Teams user to PBX A user 2. PBX A user does not answer the call 3. Allow the call to get forwarded to voicemail 4. Teams user successfully leaves voicemail and navigates voicemail menu using DTMF	1. Teams user is able to leave voicemail and navigate voice mail menu using DTMF successfully	PASSED	

External ID	Title	Procedure	Expected Results	Status	Comments
104	Teams user Calls PBX B user and leaves voicemail	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX B user 2. PBX B user does not answer the call 3. Allow the call to get forwarded to voicemail 4. Teams user successfully leaves voicemail and navigates voicemail menu using DTMF 	1. Teams user is able to leave voicemail and navigate voice mail menu using DTMF successfully	NOT APPLICABLE	This testing is for only one PBX with Teams
105	Teams user Calls PBX A user, PBX A returns call failure response	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX A user 2. PBX A returns 486 Busy 3. Verify Teams user gets appropriate notification or announcement and the call is cleared 4. Repeat steps 1 to 3 where PBX A returns 480, 404, 503 SIP responses 5. Document the observation on Teams user side 	1. Teams user handles the failure response successfully	PASSED	
106	Teams user Calls PBX A user using SIP URI	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX A user using SIP URI 2. PBX A user starts ringing 3. PBX A user answers the call 4. Verify two way audio 5. Teams user hangs up the call 6. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Teams user is able to call using SIP URI 2. Call is connected with two way audio successfully 	NOT TESTED	SIP URI Not tested for this PBX
107	Teams user Calls PBX B	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to PBX B user using SIP URI 2. PBX B user starts ringing 	<ol style="list-style-type: none"> 1. Teams user is able to call using SIP URI 2. Call is connected 	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
	user using SIP URI	<ol style="list-style-type: none"> 3. PBX B user answers the call 4. Verify two way audio 5. Teams user hangs up the call 6. Verify call is cleared successfully 	with two way audio successfully		
108	PBX A user Calls Teams user using SIP URI	<ol style="list-style-type: none"> 1. Make a voice call from PBX A user to Teams user using SIP URI 2. PBX A user starts ringing 3. PBX A user answers the call 4. Verify two way audio 5. PBX A user hangs up the call 6. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Teams user is able to call using SIP URI 2. Call is connected with two way audio successfully 	NOT TESTED	SIP URI Not tested for this PBX
109	PBX B user Calls Teams user using SIP URI	<ol style="list-style-type: none"> 1. Make a voice call from PBX B user to Teams user using SIP URI 2. PBX B user starts ringing 3. PBX B user answers the call 4. Verify two way audio 5. PBX B user hangs up the call 6. Verify call is cleared successfully 	<ol style="list-style-type: none"> 1. Teams user is able to call using SIP URI 2. Call is connected with two way audio successfully 	NOT APPLICABLE	This testing is for only one PBX with Teams
110	Teams user calls Skype for Business user	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to Skype for Business user 2. Teams user hears Ring back Tone 3. Skype for Business user answers the call 4. Verify two way audio 5. Teams user hangs up the call 6. Verify call is cleared successfully 7. Verify the same scenario where 		NOT APPLICABLE	Not applicable for this topology

External ID	Title	Procedure	Expected Results	Status	Comments
		Skype for Business user is internal and external			
111	Skype for Business user calls Teams user	<ol style="list-style-type: none"> 1. Make a voice call from Skype for Business user to Teams user 2. Skype for Business user hears Ring back Tone 3. Teams user answers the call 4. Verify two way audio 5. Skype for Business user hangs up the call 6. Verify call is cleared successfully 7. Verify the same scenario where Skype for Business user is internal and external 		NOT APPLICABLE	Not applicable for this topology
112	Teams user calls Skype for Business External Mobile user	<ol style="list-style-type: none"> 1. Skype for business user is an External Mobile user 2. Make a voice call from Teams user to Skype for Business user 3. Teams user hears Ring back Tone 4. Skype for Business user answers the call 5. Verify two way audio 6. Teams user hangs up the call 7. Verify call is cleared successfully 		NOT APPLICABLE	Not applicable for this topology

External ID	Title	Procedure	Expected Results	Status	Comments
113	Skype for Business External Mobile user calls Teams user	<ol style="list-style-type: none"> 1. Skype for business user is an External Mobile user 2. Make a voice call from Skype for Business user to Teams user 3. Skype for Business user hears Ring back Tone 4. Teams user answers the call 5. Verify two way audio 6. Skype for Business user hangs up the call 7. Verify call is cleared successfully 		NOT APPLICABLE	Not applicable for this topology
114	Teams user call other tenant users	<ol style="list-style-type: none"> 1. Make a voice call from Teams user to another tenant users (Teams desktop client user, Teams mobile user, Skype for Business Online user) 2. Verify call is successful 3. Make one call to each different user one by one 		NOT APPLICABLE	Not applicable for this topology
115	Teams users joins a meeting scheduled by Skype for business On-premises user	<ol style="list-style-type: none"> 1. Skype for business user schedules a meeting and invites Teams user 1 and Teams user 2 2. Teams user 1 joins the meeting using the Join button 3. Teams user 2 joins the meeting using the dial-in conferencing number 4. Verify Teams users are able to join the meeting successfully 5. Verify all three users are able to hear 		NOT APPLICABLE	Not applicable for this topology

External ID	Title	Procedure	Expected Results	Status	Comments
		each other 6. Skype for Business user ends the meeting			
116	Teams user invites Skype for business users for a meeting	1. Teams user schedules a meeting and invites Skype for Business user 1 and Skype for Business user 2 2. Skype for Business user 1 joins the meeting using the Meeting link 3. Skype for Business user 2 joins the meeting using the dial-in conferencing number 4. Verify all three users are able to hear each other 5. Teams user ends the meeting		NOT APPLICABLE	Not applicable for this topology