



# 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

Property of tekVizionLabs - 2

# **Document History**

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

# Table of Contents

1	Auc	dience	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	Fea	atures	10
	3.1	Features Supported	10
	3.2	Caveats and Limitations	11
4	Con	nfiguration	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
	Messag	e Manipulation	59
4	4.5 Ava	aya 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	4.6 Ava	aya 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

Property of tekVizionLabs - 5

	4.6.6	Routing Policies	88
	4.6.7	Dial Patterns	90
4.	7 Ava	aya 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	Acronyr	ms	115
6	Summa	ry 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<sup>™</sup> 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<sup>™</sup> 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 <u>www.tekVizion.com</u>* 

# 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.

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

Table	1	– PBX	Configuration	Steps
-------	---	-------	---------------	-------

# 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.

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 Comm	unication Manager					
IP Address	10.89.33.4 (Signaling)/10.89.33.14 (Media)					
Subnet Mask	255.255.255.0					
Avaya Aura Se	ssion Manager					
LAN IP Address	10.89.33.7					
LAN Subnet Mask	255.255.255.0					
Avaya SBCE						
LAN IP Address	10.89.33.3					

Table	2 -	IP Ad	dresses

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.

Microsoft	
Sign in	
Email, phone, or Skype	
No account? Create one!	
Can't access your account?	
Sign-in options	
	Next

*Figure 2: Office 365 Portal Login* 

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

 Office 365			Q	Search						Q	0	?	S
Apps										Install Office V			Î
0	۵	W	x		N	5	ជ្	<b>M</b>	A				
Outlook	OneDrive	Word	Excel	PowerPoint	OneNote	SharePoint	Teams	Yammer	Admin	e /			
Explore all you	ir apps $ ightarrow$												

Figure 3: Office 365 Portal Login

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

	Microsoft 365 admin center		
>	► Home 🖉 Customize your home		tekVizionLabs
G Q	Search users, groups, settings or tasks		
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		Active users >	🖽 Billing >
\$ \$ \$	<ul> <li>Last directory sync last synced more than 3 days ago</li> <li>Password sync no recent synchronization</li> </ul>	<ul> <li>+ Add a user</li> <li>i Delete a user</li> <li>✓ Edit a user</li> <li>♀ Reset a password</li> </ul>	Total balance: \$0.00 Update payment details View my bill
Ŋ	Office software	Domains >	ତି Support
Ŀ	↓ Install my software Share the download link	+ Add a domain Remove a domain	<ul> <li>+ New service request</li> <li></li></ul>
8		<ul> <li>Edit a domain</li> <li>Check health</li> </ul>	u

Figure 4: Teams User Creation

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

Add user				×
Basics	First name crestron		Last name teams5	•
O Product licenses	Display name * crestronteams5			- 1
Optional settings	Username *			_
O Finish	crestroncrestronteams5	@	tekvizionlabs.com $\checkmark$	_
	Password settings  Auto-generate password  Let me create the password  Require this user to change their pas  Send password in email upon compl	sword v	when they first sign in	
	Next			

*Figure 5: Teams User Creation – Contd.* 

admin.microsoft.com/Adm	inPortal/Home#/users	07
Add user		
Basics	Select location * United States	
Product licenses	Licenses (1) *	
Optional settings	Assign user a product license     Communications Credits     Unlimited licenses available	
<ul> <li>Finish</li> </ul>	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	
	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.

C 🛆 admin.microsoft.com/AdminPorta	I/Home#/users		<b>o-</b> ¢
Add user			
Basics	Optional settings		
Optional settings	You can choose what role you'd like to assign for this user, information.	and fill in additional profile	
Finish	Roles (User: no administration access)	~	
	Profile info	~	
	Back Next		

Figure 7: Teams User Creation – Contd.

Add user		×
Basics	You're almost done - review and finish adding	•
Product licenses		
Ĩ	Assigned Settings	
<ul> <li>Optional settings</li> </ul>	Review all the info and settings for this user before you finish adding them.	
Finish	Display and username crestronteams5 crestroncrestronteams5@tekvizionlabs.com Edit	L
	Password	
	Type: Auto-generated Edit	
	Product licenses Office 365 E5 without Audio Conferencing	L
	Edit	
	Roles (default)	
	User (no administrator access)	
	Edit	-
	Back Finish adding	

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.

	Microsoft 365 admin center	
>	Home 🖉 Customize your home	
ଜ	Search users, groups, settings or tasks	
8		
Å	Admin centers	
	Exchange 🗂	Active users >
48	Teams 😅	+ Add a user
	SharePoint 🗖	🗊 Delete a user
G	OneDrive 🗖	<ul> <li>Edit a user</li> <li>Reset a password</li> </ul>
ŝ	Yammer 😅	
ß	PowerApps □	
<u>ا</u> ما	Flow C	
~	Security & Compliance 🗖	
÷	Azure Active Directory 😅	
<b>A</b> 3	Device Management 😅	

#### Figure 10: Microsoft O365 admin

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

	Microsoft Teams admin c	nter
	≡	
ĥ	Dashboard	MICROSOFT TEAMS OPGRADE
දීරි	Teams	Planning your upgrade to Teams
\$	Devices	We are bringing the capabilities of Skype for Business Online into Microsoft Teams to deliver a single hub for teamwork with built-in, fully-integrated voice and video. We
٢	Locations	have resources and tools available to assist you in planning and upgrading some or all of your users to Teams.
සී	Users	Learn more
÷	Meetings ~	
Ę	Messaging policies	
BŶ	Teams apps V	USER SEARCH
6	Voice ~	Search by display or username Q
<i>.</i> 11	Analytics & reports	
ණ	Org-wide settings $\sim$	(i) Recent searches will show up here
S	Legacy portal	C Receit searches will show up here.
Ø	Call quality dashboard	View users
S	Firstline Worker configu	View Galla

Figure 11: Microsoft O365 admin

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

←	$\rightarrow$ C $\triangle$ admin.te	eams.microso	oft.com/u	Isers				☆ (	) ()	6	
	Microsoft Teams admin	center						Q	ø	?	s
දීලී9	Teams	^									
	Manage teams		User	5							
	Teams policies		You can	manage audio conferencing set	tings, the policies assigned to them, phone numb	ers and other feature	es for people in				
ا	Devices	~ 0	or deleti	ng users, changing passwords o	r assigning licenses, go to the Admin center > Us	ers.	such as duuring				
٢	Locations	~									
::	Users		🖉 Ed	it settings			crestron	×	_ 7	63	
Ē	Meetings	~	~	Display name	Username	Phone number	Location			Policies	
Ę	Messaging policies			Crestron Teams2	crestronteams2@tekvizionlabs.onmicrosoft.c	+1 972	United States			6 glob	
B	Teams apps	~		CrestronConfRoom	CrestronConfRoom@tekvizionlabs.com	+1 972	United States			8 glob	
6	Voice	$\sim$					officer officer			e giesi	
<b>.</b>	Analytics & reports	~		Crestron Teams1	crestronteams1@tekvizionlabs.com	+1 972	United States			6 glob	
ණ	Org-wide settings	$\sim$		crestronteams5 UC PHONE	crestronteams5@tekvizionlabs.onmicrosoft.c		United States			9 glob	
S	Legacy portal			crestronteams3	crestronteams3@tekvizionlabs.onmicrosoft.c	+1 972	United States			6 glob	
	Call quality dashboard			crestronteams4	crestronteams4@tekvizionlabs.onmicrosoft.c	+1 972	United States			6 glob	

Figure 12: Microsoft O365 admin

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

	Microsoft Teams adm	in cent	er			
		≡	Users \ crestronteams5 UC PHONE			
ඛ	Dashboard					-
දීලී3	Teams	^	crestronteams5 UC PHONE		7-DAY QUALITY	7-DAY ACTIV
	Manage teams		E 🛛	Email		0
	Teams policies		United States	crestronteams5@tekvizionlab s.onmicrosoft.com		Meetings
\$	Devices	$\sim$	CP	Directory status	<ul> <li>Data isn't available.</li> </ul>	0
٢	Locations	$\sim$		-		Calls
::	Users					
Ē	Meetings	$\sim$				
Ę	Messaging policies		Account Voice Call history Policies			
BŶ	Teams apps	$\sim$				
☜	Voice	$\sim$	General information	Teams upgrade	🖉 Edit	
<b>111</b>	Analytics & reports	$\sim$	Assigned phone number	Coexistence mode		
٢	Org-wide settings	$\sim$	none	Teams only		
$\sim$			Emergency address	Notity the Skype for Business user		

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.

	Microsoft Teams admin cen	ter
	≡ ^	Dashboard \ Calling policies
ଜ	Dashboard	Calling policies
ະຕິຈ	Teams	Calling policies are used to control what calling features are available to people in Teams. You can use the Global (Org-
\$	Devices	wide default) policy that is created or create one or more custom calling policies for people that have phone numbers in your organization. <u>Learn more</u>
Ø	Locations	
පී	Users	+ New policy 🖉 Edit 🕼 Duplicate 🗴 Delete 💭 Reset Global policy 🕫 Manage users
<b></b>	Meetings ~	
E	Messaging policies	Name T Description Custom policy
B	Teams apps 🗸 🗸	AllowCalling No
ଚ	Voice A	DisallowCalling No
	Direct Routing	Global (Org-wide defa No
	Call queues	
	Auto attendants	
	Call park policies	
	Calling policies	

Figure 14 – Calling Policy

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

Jusy on Dusy Lindbled		
escription		
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 On	
Voicemail is available for routing inbound calls	User controlled	~
Inbound calls can be routed to call groups	On 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 On	

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 "crestronteams5@tekvizionlabs.com" – EnterpriseVocieEnabled \$true –HostedVoicemail \$true

Set-CsUser –identity "crestronteams5@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-CsOnline	PSTNGateway -Identity sbc4.tekvizionlabs.com
Identity	: sbc4.tekvizion]abs.com
SinSignallingPort	: 5061
FailoverTimeSeconds	: 10
ForwardCallHistory	: True
ForwardPai	: True
SendSipOptions	: True
MaxConcurrentSessions	: 100
Enabled	: True
MediaBypass	: True
GatewaySiteId	: _
GatewaySiteLbrEnabled	: False
FailoverResponseCodes	: 408,503,504
GenerateRingingWhileLocatingUser	: True
PidtLoSupported	: 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.



*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 Priority Description NumberPattern OnlinePstnUsages OnlinePstnGatewayList Name	: sbc4 : 5 : .* : {sbc4} : {sbc4.tekvizionlabs.com} : 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>"



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 "crestronteams5" -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

```
Srule1 = 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 crestronteams5 -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 "crestronteams5@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 nonregistering 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** $\rightarrow$ **Core Entities menu** $\rightarrow$ **Ethernet Devices**

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

$\leftarrow \rightarrow$ C $\triangle$ Not secure   10.64.3.10 $\Rightarrow$ O $\bigcirc$											
	ocodes	SETUP	MONITOR	TROUBLESHOOT							
					Save	Reset Act	ions <del>、</del>	0 Admin <del>-</del>			
MEDIANT VE SBC		SIGNALING	i & MEDIA	ADMINISTRATION			🔎 Entity, pa	rameter, value			
€ ● srd All	VIEW	Ethernet D	evices (2)								
CORE ENTITIES IP Interfaces (2) Ethernet Device	s (2)	+ New Edit	VLAN ID	UNDERLYING	of 1   >> >= NAME	Show 10 V recor	ds per page	Л			
Ethernet Group: Physical Ports (2 Static Routes (3)	<b>s (15)</b> 2)	0	1 1	GROUP_1 GROUP_2	TEAMS TEKVLAN	Untagge Untagge	ed 1 ed 1	500 500			

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:

← → C ☆ ▲ Not secure   10.	64.3.10								☆ 🤇	) 🛛 🎯 :
Caudiocodes	SETUP	MONITOR	TROUBLESHOO	т		:	Save F	Reset Ad	tions <del>-</del>	Admin <del>-</del>
MEDIANT VE SBC IP NETWORK	SIGNALING 8	MEDIA	ADMINISTRATION						🔎 Entity, p	arameter, value
SRD All 🔻										
A NETWORK VIEW	IP Inte	erfaces (2)								
CORE ENTITIES	+ Now	Edit		Pag	al of t	S. Show 1	0 - records			
IP Interfaces (2)	- new			1.08		S Pr Show [	v records	hei haße		
Ethernet Devices (2)	INDEX 🗢	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDA DNS	RY ETHERNET DEVICE
Ethernet Groups (15)	0	TEAMS	Media + Contr	IPv4 Manual	192.65.79.118	27	192.65.	8.8.8.8	0.0.00	TEAMS
Physical Ports (2)	2	TEKVLAN	OAMP + Media	IPv4 Manual	10.64.3.10	16	10.64.1.1	10.85.0.23	2 0.0.0.0	TEKVLAN
Static Routes (3) NAT Translation (0)										
> SECURITY										

Figure 27 – IP interface Devices

### IP interface TEAMS

PInterfaces [TEAMS]					-
GENERAL			IP ADDRESS		
Index Name Application Type Ethernet Device	0	v v View	Interface Mode IP Address Prefix Length Default Gateway	IPv4 Manual           192.65.           27           192.65.	▼ 
DNS					
Primary DNS Secondary DNS	<ul> <li>8.8.8.8</li> <li>0.0.0.0</li> </ul>				
		Cancel	APPLY		

Figure 28 – IP interface Devices

#### IP Interfaces – TEKVLAN

IP Interfaces [TEKVLAN]					- x
CENEDAL			10 4000555		
GENERAL			IP ADDRESS		
Index	2		Interface Mode	IPv4 Manual	٣
Name	TEKVLAN		IP Address	• 10.64.3.10	
Application Type	OAMP + Media + Control	*	Prefix Length	16	
Ethernet Device	• #1 [TEKVLAN]	▼ View	Default Gateway	• 10.64.1.1	
DNS					
Primary DNS	• 10.85.0.232				
Secondary DNS	0.0.0.0				
		Cancel A	PPLY		

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**  $\rightarrow$  **DNS menu**  $\rightarrow$  **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	<ul> <li>sip2.pstnhub.microsoft.com</li> </ul>
Transport Type	• TLS	Priority 2	• 2
		Weight 2	• 1
1ST ENTRY		Port 2	<ul> <li>5061</li> </ul>
DNS Name 1	<ul> <li>sip.pstnhub.microsoft.com</li> </ul>		
Priority 1	• 1	3RD ENTRY	
Weight 1	• 1	DNS Name 3	<ul> <li>sip3.pstnhub.microsoft.com</li> </ul>
Port 1	• 5061	Priority 3	• 3
		Weight 3	• 1
		Port 3	• 5061

#### 4.4.5 Configure SRTP

By default, SRTP is disabled.

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

<b>C</b> audiocodes	SETUP MONITOR TROUBLESHOOT	Sa	ve Reset Actions <del>-</del>	Admin <del>-</del>
MEDIANT VE SBC IP NETWORK	SIGNALING & MEDIA ADMINISTRATION		Q E	ntity, parameter, value
🔶 🔿 SRD All 🔻				
CTOPOLOGY VIEW	Media Security			
CORE ENTITIES	GENERAL	AUTHENT	ICATION & ENCRYPTION	
CODERS & PROFILES	Media Security • Enable	▼ Authentic	ation On Transmitted RTP Packets	Active 🔻
▶ SBC	Media Security Behavior • Prefera	ble - Single me 🔻 Encryption	n On Transmitted RTP Packets	Active 🔻
SIP DEFINITIONS	Offered SRTP Cipher Suites All	<ul> <li>Encryption</li> </ul>	n On Transmitted RTCP Packets	Active 🔻
MESSAGE MANIPULATION	Aria Protocol Support Disable	<ul> <li>SRTP Tuni</li> </ul>	neling Authentication for RTP	Disable 🔻
		SRTP Tuni	neling Authentication for RTCP	Disable 🔻
Media Security	MASTER KEY IDENTIFIER			
RTP/RTCP Settings Voice Settings Fax/Modem/CID Settings	Master Key Identifier (MKI) Size 0 Symmetric MKI Disable	· · · · · · · · · · · · · · · · · · ·		
Media Settings DSP Settings		Cancel APPLY		

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. <u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan</u>

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

#1[Teams]					Edit
GENERAL			OCSP		
Name	• Teams		OCSP Server	Disable	
TLS Version	• TLSv1.2		Primary OCSP Server	0.0.0.0	
DTLS Version	Any		Secondary OCSP Ser	0.0.0.0	
Cipher Server	RC4:AES128		OCSP Port	2560	
Cipher Client	DEFAULT		OCSP Default Respo	Reject	
Strict Certificate Exte	Disable				
DH key Size	• 2048				
Certificate Information >>	Change Certificate >>	Trusted Root Certific	ates >>		

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.** 

← → C ☆ ▲ Not secure   10.64.	3.10					<b>07</b> Å	<b>O</b>	d) :
acoudiocodes	SETUP MONITO	R TROUBLESHOO			Save Res	et Actions <del>-</del>	L <sup>0</sup>	Admin <del>-</del>
MEDIANT VE SBC IP NETWORK SI	IGNALING & MEDIA	ADMINISTRATION	1			© Ent	ity, parameter, v	alue
(+) (+) SRD All -								
								_
C TOPOLOGY VIEW	Media Realm	s (2) .						
▲ CORE ENTITIES	+ Now Edit	â	Page 1	of 1 as a Show		-		
SRDs (1)	+ New Eult	<b>Ш</b>	ra ca   rage	of the prishow	Tecords per pa	Re		~
SIP Interfaces (5)	INDEX 🗢	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MED REALM	IA
Media Realms (2)	0	TEAMS	TEAMS	50000	100	50499	No	
Proxy Sets (5)	1	TEKVLAN	TEKVLAN	7000	100	7499	No	
IP Groups (5)								
CODERS & PROFILES								
								_

Figure 33 – Media Realms

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

ledia Realms [TEAMS]						-			
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	•							
		Cancel	APPLY						
		Figure 34 –	Teams						

Media I	Realms [TEKVLAN]								- >
	GENERAL					QUALITY OF EXPERIENCE			
	Index		1			QoE Profile	 •	View	
	Name	•	TEKVLAN			Bandwidth Profile	 •	View	
	Topology Location	•	Up	٠					
	IPv4 Interface Name	•	#2 [TEKVLAN]	Viev	v				
	Port Range Start	•	7000						
	Number Of Media Session Legs	•	100						
	Port Range End		7499						
	Default Media Realm		No	۳					
					_				
				Car	ncel	APPLY			

#### Configure a Media Realm for LAN traffic – "TEKVLAN" as shown below:

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.

IP Interfaces [TEAMS]		
	SRD	#0 [DefaultSRD]
GENERAL		MEDIA
Index	0	Media Realm 🔹 #0 [TEAMS] 👻 View
Name	TEAMS	Direct Media Disable 🔻
Topology Location	Down	Y
Network Interface	• #0 [TEAMS]	/iew SECURITY
Application Type	SBC	TLS Context Name     #1 [Teams]     View
UDP Port	5060	TLS Mutual Authentication
TCP Port	• 0	Message Policy View
TLS Port	5061	User Security Mode Not Configured
Additional UDP Ports		Enable Un-Authenticated Registrations Not configured
Additional UDP Ports Mode	Always Open	Max Number of Registered Users
Encapsulating Protocol	No encapsulation	v

Figure 37 – Teams

Enable TCP Keepalive	Enable	
Used By Routing Server	Not Used	•
Pre-Parsing Manipulation Set		▼ View
CAC Profile		▼ View
CLASSIFICATION		
Classification Failure Response Type	e • 0	
Pre-classification Manipulation Set II	ID -1	
Call Setup Rules Set ID	-1	
		Can

Figure 38 – Teams

rfaces [PSTNGW]							
	SRD	#0 [Defa	ultSRD] 🔹				
GENERAL			MEDIA				
Index	1		Media Realm	#	1 [TEKVLAN]	•	View
Name •	PSTNGW		Direct Media	Disabl	le		•
Topology Location	Up	•					
Network Interface	#2 [TEKVLAN] VI	ew	SECURITY				
Application Type	SBC	•	TLS Context Name	•		•	View
UDP Port	5060		TLS Mutual Authentication				٣
TCP Port •	0		Message Policy			•	View
TLS Port •	0		User Security Mode		Not Configured		•
Additional UDP Ports			Enable Un-Authenticated Registra	tions	Not configured		Ŧ
Additional UDP Ports Mode	Always Open	Ŧ	Max. Number of Registered Users		-1		
Encapsulating Protocol	No encapsulation	Ŧ	max number of neglistered osers				
Enable TCP Keepalive	Disable	Ŧ					
Used By Routing Server	Not Used	•					
Pre-Parsing Manipulation Set		iew					
The Parsing Manipulation Sec	· · ·						
CAC Profile	··· V	lew					
CLASSIFICATION							
Classification Failure Response Type	500						
Pre-classification Manipulation Set ID	0 -1						
Call Setup Rules Set ID	-1						
		ancel 🗛					

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

Figure 40 – PSTN

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

IP Interfaces [AVAYA]		-
	SRD	0 [DefaultSRD]
GENERAL		MEDIA
Index	3	Media Realm • #1 [TEKVLAN] View
Name	AVAYA	Direct Media Disable 🔻
Topology Location	Down	
Network Interface	• #2 [TEKVLAN]    Vie	SECURITY
Application Type	SBC	TLS Context Name #0 [default] View
UDP Port	• 5064	TLS Mutual Authentication
TCP Port	• 0	Message Policy View
TLS Port	• 0	User Security Mode Not Configured 🔻
Additional UDP Ports		Enable Un-Authenticated Registrations Not configured
Additional UDP Ports Mode	Always Open	Max. Number of Registered Users -1
Encapsulating Protocol	No encapsulation	

Figure 41 – Avaya

Enable TCP Keepalive	Disable		۳
Used By Routing Server	Not Used		۳
Pre-Parsing Manipulation Set		<b>•</b> V	/iew
CAC Profile		<b>•</b> \	/iew
CLASSIFICATION			
Classification Failure Response Type	500		
Pre-classification Manipulation Set II	0 -1		
Call Setup Rules Set ID	-1		
			Callic



#### 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.
xy Sets <b>[TEAMS]</b>	
	SRD #0 [DefaultSRD]
GENERAL	REDUNDANCY
Index	0 Redundancy Mode   Homing
Name	TEAMS     Proxy Hot Swap     Enable     Teable
SBC IPv4 SIP Interface	#0 [TEAMS]     View     Proxy Load Balancing Method     Random Weights
TLS Context Name	#1 [Teams]      View Min. Active Servers for Load Balancing
KEEP ALIVE	ADVANCED
Proxy Keep-Alive	Using OPTIONS     Classification Input     IP Address only     T
Proxy Keep-Alive Time [sec]	60 DNS Resolve Method    SRV
Keep-Alive Failure Responses	
Success Detection Retries	1
Success Detection Interval	10
Success Detection Interval	Cancel APPLY

Figure 43 – Teams

🟠 TOPOLOGY VIEW	Proxy Sets [#0] > Pro	oxy Address (1)		
CORE ENTITIES	+ New Edit 🔟	I≪ Page 1 of 1 → ► S	Show 10 T records per page	Q
SRDs (1)				
SIP Interfaces (5)	INDEX 🗢	PROXY ADDRESS	TRANSPORT TYPE	
Media Realms (2)	0	teams.local	TLS	
Proxy Sets (5)				
IP Groups (5)				
CODERS & PROFILES				
▲ SBC				
Classification (2)	#0			Edit
Routing				
Routing Policies (1)				
IP-to-IP Routing (9)	GENERAL			
Alternative Routing Reasons (0)	Proxy Address	• teams.local		
IP Group Set (0)	Transport Type	• TLS		
Manipulation	Proxy Priority	0		
SBC General Settings	Brow Bandom Weight	0		
Call Admission Control Profile (0)	Froxy Karldom Weight	v		

Figure 44 – Teams

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

Proxy S	ets [PSTNGW]										– x
			SRD	2	#	0 [DefaultSRD]	•				
	GENERAL					REDU	NDANCY				
	Index		1			Redun	dancy Mode			٣	
	Name	•	PSTNGW			Proxy	Hot Swap		Disable	Ŧ	
	SBC IPv4 SIP Interface	•	#1 [PSTNGW]	•	View	Proxy	Load Balancing Method		Disable	٣	
	TLS Context Name			•	View	Min. A	ctive Servers for Load Bala	incing	1		
	KEEP ALIVE					ADVA	NCED				
	Proxy Keep-Alive	Г	Using OPTIONS		•	Classif	ication Input	IP Ad	ldress only	Ŧ	
	Proxy Keep-Alive Time [sec]		60			DNS R	esolve Method			٣	
	Keep-Alive Failure Responses										
	Success Detection Retries		1								
I	Success Detection Interval		10								

Figure 45 – PSTN Gateway

Keep-Alive Failure Responses			
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]							– x
	SRD	#0 [Defa	aultSRD] 🔹				
GENERAL			REDUNDANCY				
Index	3		Redundancy Mode			•	
Name •	AVAYA		Proxy Hot Swap		Disable	•	
SBC IPv4 SIP Interface •	#3 [AVAYA]	▼ View	Proxy Load Balancing Me	thod	Disable	Ŧ	
TLS Context Name		▼ View	Min. Active Servers for Lo	ad Balancing	1		
KEEP ALIVE			ADVANCED				
Proxy Keep-Alive	Using OPTIONS	•	Classification Input	IP Addre	ess only	•	
Proxy Keep-Alive Time [sec]	60		DNS Resolve Method			•	
Keep-Alive Failure Responses							
Success Detection Retries	1						
Success Detection Interval	10						
		Cancel	APPLY				

Figure 47 – Avaya

Success Detection Interval	10
Failure Detection Retransmissions	4
	Cancel 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** 

IP Groups	5 [TEAMS]									- x
			SRD	#	0 [Defa	ultSRD] 🔻				
C	GENERAL					QUALITY OF EXPERIENCE				
	Index	[	0			QoE Profile		•	View	
	Name	•	TEAMS			Bandwidth Profile		•	View	
1	Topology Location		Down	۲	•					
1	Туре		Server	•	. 1	MESSAGE MANIPULATION				
	Proxy Set	•	#0 [TEAMS]	View		Inbound Message Manipulation Set	• 1			
	IP Profile	•	#1 [TEAMS_Profile]	View		Outbound Message Manipulation Se	et e 2			
	Media Realm	•[	#0 [TEAMS]	View		Message Manipulation User-Defined	d String 1			
0	Contact User					Message Manipulation User-Defined	d String 2			
5	SIP Group Name	•[	sbc4.tekvizionlabs.com			Proxy Keep-Alive using IP Group set	ttings • Enable		•	
(	Created By Routing Server		No							
	Used By Routing Server		Not Used	۳		SBC REGISTRATION AND AUTHEN	NTICATION			

Configure an IP Group for Microsoft Teams as shown below

Figure 49 – IP Group – Teams – Contd.

oups [TEAMS]						
Proxy Set Connectivity	Con	inected		Max. Number of Registered Users	-1	
				Registration Mode	User Initiates Registration	•
SBC GENERAL				User Stickiness	Disable	•
Classify By Proxy Set	• Disa	able	•	User UDP Port Assignment	Disable	•
SBC Operation Mode	Not	Configured	•	Authentication Mode	User Authenticates	•
SBC Client Forking Mode	Sequ	uential	•	Authentication Method List		
CAC Profile			▼ View	SBC Server Authentication Type	According to Global Parameter	•
				OAuth HTTP Service	<b>v</b>	/iew
ADVANCED				Username •	Admin	
Local Host Name	• sbc4	4.tekvizionlabs.com		Password •	,	
UUI Format	Disa	able	•	GW GROUP STATUS		
Always Use Src Address	No		•	GW Group Registered IP Address		
				GW Group Registered Status	Not Registered	

Figure 50 – IP Group – Teams – Contd.

Figure 51 – IP Group – Teams

Configure an IP Group for PSTN Gateway as shown below

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

Figure 52 – IP Group – PSTN – Contd.

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

Figure 53 – IP Group – PSTN – Contd.

Source URI Input		•		
Destination URI Input		¥		
SIP Connect	No	•		
SBC PSAP Mode	Disable	Ŧ		
Route Using Request URI Port	Disable	Ŧ		
DTLS Context	#0 [default]	▼ View		
Keep Original Call-ID	No	•		
Dial Plan		▼ View		
Call Setup Rules Set ID	-1			
Tags				

Figure 54 – IP Group

### Configure an IP Group for Avaya SBCE as shown below

IP Groups [AVAYA]						– x
	SRD #	#0 [Defa	ultSRD]			
GENERAL			QUALITY OF EXPERIENCE			
Index	3		QoE Profile		•	View
Name	AVAYA		Bandwidth Profile		•	View
Topology Location	Down 🔻					
Туре	Server 🔻		MESSAGE MANIPULATION			
Proxy Set	• #3 [AVAYA] View	N	Inbound Message Manipulatio	on Set 🔹	6	
IP Profile	• #4 [AVAYA_Profile]	N	Outbound Message Manipula	tion Set 🔹	7	
Media Realm	#1 [TEKVLAN] View	N	Message Manipulation User-D	efined String	1	
Contact User			Message Manipulation User-D	efined String	2	
SIP Group Name	10.64.5.57		Proxy Keep-Alive using IP Gro	up settings	Disable	*
Created By Routing Server	No					

Figure 55 – IP Group – Avaya – Contd.

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

Figure 56 – IP Group – Avaya – Contd.

			GW Group Registered Status	Not Registered	
SBC ADVANCED					
Source URI Input		٣			
Destination URI Input		•			
SIP Connect	No	T			
SBC PSAP Mode	Disable	•			
Route Using Request URI Port	Disable	Ŧ			
DTLS Context	#0 [default]	▼ View			
Keep Original Call-ID	No	Ŧ			
Dial Plan		▼ View			
Call Setup Rules Set ID	-1				
Tags					
		Cancel	APPLY		

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.** 

IP Profiles [TEAMS\_Profile] GENERAL SBC SIGNALING PRACK Mode Index Optional TEAMS\_Profile Name P-Asserted-Identity Header Mode As Is Created by Routing Server No Diversion Header Mode As Is ۳ History-Info Header Mode As Is ۳ MEDIA SECURITY Session Expires Mode Transparent ۳ Ŧ SRTP Remote Update Support Not Supported SBC Media Security Mode \* v Not Supported Remote re-INVITE Disable ۳ Symmetric MKI v Remote Delayed Offer Support Not Supported • 1 MKI Size Ŧ Remote Representation Mode According to Operation Mode SBC Enforce MKI Size Don't enforce \* Keep Incoming Via Headers According to Operation Mode . SDES \* SBC Media Security Method . Keep Incoming Routing Headers According to Operation Mode Ŧ Reset SRTP Upon Re-key Disable Keep User-Agent Header According to Operation Mode . Always • Generate SRTP Keys Mode

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

Figure 58 – IP Profile – Teams – Contd.

files [TEAMS_Profile]						_
SBC Remove Crypto Lifetime in SDP 1	Νο			Handle X-Detect	No	7
SBC Remove Unknown Crypto	No	•		ISUP Body Handling	Transparent	•
				ISUP Variant	ltu92	•
SBC EARLY MEDIA				Max Call Duration [min]	0	
Remote Early Media	Supported	•				
Remote Multiple 18x	Supported	•		SBC REGISTRATION		
Remote Early Media Response Type	Transparent	•	1	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 Media	•				
Remote RFC 3960 Support	Not Supported	•		SBC FORWARD AND TRANSFER		
Remote Can Play Ringback	• No	•		Remote REFER Mode	Regular	•
Generate RTP	None			Remote Replaces Mode	Standard	•
				Play RBT To Transferee •	Yes	•

Figure 59 – IP Profile – Teams – Contd.

– x

Profiles [TEAMS_Profile]					-
SBC MEDIA			Remote 3xx Mode •	Handle Locally	Ŧ
Mediation Mode	RTP Mediation	•			
Extension Coders Group	#0 [AudioCodersGroups_0]	•	SBC HOLD		
Allowed Audio Coders	#0 [AllowedAudioCodersGroup_TEAMS]	•	Remote Hold Format •	Inactive	Ŧ
Allowed Coders Mode	Preference	•	Reliable Held Tone Source	Yes	•
Allowed Video Coders		•	Play Held Tone	No	Ŧ
Allowed Media Types					
Direct Media Tag			SBC FAX		
RFC 2833 Mode	As Is	Ŧ	Fax Coders Group		-
RFC 2833 DTMF Payload Type	101		Fax Mode	As Is	*
Alternative DTMF Method	As Is	•	Fax Offer Mode	All coders	*
Send Multiple DTMF Methods	Disable	Ŧ	Fax Answer Mode	Single coder	*
Adapt RFC2833 BW to Voice coder BW	Disabled	•	Remote Renegotiate on Fax Detecti	ion Transparent	*
SDP Ptime Answer	Preferred Value	Ŧ	Fax Rerouting Mode	Disable	*

Figure 60 – IP Profile – Teams – Contd.

IP Profiles [TEAMS_Profile]					- x
Preferred PTime •	20				
Use Silence Suppression •	Add	7	MEDIA		
RTP Redundancy Mode	As Is	,	Broken Connection Mode	Disconnect 🔻	
RTCP Mode	Generate Always	,	Media IP Version Preference	Only IPv4	
Jitter Compensation	Disable •	7	RTP Redundancy Depth	Disable	
ICE Mode •	Lite	7			
SDP Handle RTCP	Don't Care	'	GATEWAY		
RTCP Mux •	Supported 🔻	,	Coders Group	#0 [AudioCodersGroups 0]	
RTCP Feedback	Feedback Off	,			
Voice Quality Enhancement	Disable •	'	LOCAL TONES		. 1
Max Opus Bandwidth	0				
Generate No-op	No	7	Local RingBack Tone Index	-1	
Enhanced PLC	Disable	,	Local Held Tone Index	-1	

Figure 61 – IP Profile – Teams – Contd.

s [TEAMS_Profile]			
QUALITY OF SERVICE			
RTP IP DiffServ	46		
Signaling DiffServ	24		
ITTER BUFFER			
Dynamic Jitter Buffer Minimum Dela	y [msec] 10		
Dynamic Jitter Buffer Optimization F	actor 10		
Jitter Buffer Max Delay [msec]	300		
VOICE			
Echo Canceler	Line	Ŧ	
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.

P Profiles [PSTNGW_I	Profile]					- :
GENERAL				SBC SIGNALING		
Index		2		PRACK Mode	Transparent	•
Name		PSTNGW_Profile		P-Asserted-Identity Header Mode	As Is	•
Created by Rou	ting Server	No		Diversion Header Mode	As Is	•
				History-Info Header Mode	As Is	Ŧ
MEDIA SECURI	TY			Session Expires Mode	Supported	•
SBC Media Secu	irity Mode	• RTP	•	Remote Update Support	Supported Only After Connect	•
Symmetric MKI		Disable	Ŧ	Remote re-INVITE	Supported only with SDP	•
MKI Size		0		Remote Delayed Offer Support	Not Supported	•
SBC Enforce MK	1 Size	Don't enforce	•	Remote Representation Mode	According to Operation Mode	•
SBC Media Secu	irity Method	SDES	•	Keep Incoming Via Headers	According to Operation Mode	•
Reset SRTP Upo	n Re-key	Disable	•	Keep Incoming Routing Headers	According to Operation Mode	•
Generate SRTP	Keys Mode	Only If Required	•	Keep User-Agent Header	According to Operation Mode	v

Figure 63 – IP Profile – PSTN Gateway – Contd.

IP Profiles [PSTNGW_Profile]					– x
SBC Remove Crypto Lifetime in SDP	No	•	Handle X-Detect	No	Ŧ
SBC Remove Unknown Crypto	No	•	ISUP Body Handling	Transparent	¥
La construction de la constructi			ISUP Variant	ltu92	•
SBC EARLY MEDIA			Max Call Duration [min]	0	
Remote Early Media	Supported	•			
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	•			
Remote RFC 3960 Support	Not Supported	•	SBC FORWARD AND TRANSFER		
Remote Can Play Ringback	Yes	•	Remote REFER Mode •	Handle Locally	T
Generate RTP	None	•	Remote Replaces Mode •	Handle Locally	T
			Play RBT To Transferee •	Yes	v



IP Profile:	s [PSTNGW_Profile]				– ×
5	SBC MEDIA		Remote 3xx Mode	Transparent	٣
1	Mediation Mode	RTP Mediation			
	Extension Coders Group		SBC HOLD		
	Allowed Audio Coders •	#1 [AllowedAudioCodersGroup_PSTNGW]	Remote Hold Format	Transparent	•
	Allowed Coders Mode	Restriction	Reliable Held Tone Source	Yes	<b>v</b>
	Allowed Video Coders		Play Held Tone	No	•
	Allowed Media Types				
1	Direct Media Tag		SBC FAX		
	RFC 2833 Mode	As Is	Fax Coders Group	**	•
1	RFC 2833 DTMF Payload Type •	101	Fax Mode	As Is	Ŧ
	Alternative DTMF Method	As Is	Fax Offer Mode	All coders	٣
:	Send Multiple DTMF Methods	Disable	Fax Answer Mode	Single coder	٣
	Adapt RFC2833 BW to Voice coder BW	Disabled	Remote Renegotiate on Fax Detecti	on Transparent	٣
:	SDP Ptime Answer	Preferred Value	Fax Rerouting Mode	Disable	٧

Figure 65 – IP Profile – PSTN Gateway – Contd.

iles [PSTNGW_Profile]					
Preferred PTime	• 20				
Use Silence Suppression	<ul> <li>Add</li> </ul>	•	MEDIA		
RTP Redundancy Mode	As Is	•	Broken Connection Mode	Disconnect	
RTCP Mode	Generate Always	*	Media IP Version Preference	Only IPv4	
Jitter Compensation	Disable	*	RTP Redundancy Depth	Disable	
ICE Mode	Disable	*			
SDP Handle RTCP	Don't Care	Ŧ	GATEWAY		
RTCP Mux	Not Supported	¥	Coders Group	#0 [AudioCodersGroups 0]	•
RTCP Feedback	Feedback Off	*			
Voice Quality Enhancement	Disable	*	LOCAL TONES		
Max Opus Bandwidth	0				
Generate No-op	No	•	Local RingBack Tone Index	•1	
Enhanced PLC	Disable	Ψ	Local Held Tone Index	-1	

Figure 66 – IP Profile – PSTN Gateway – Contd.

Profiles [PSTNGW_Profile]			
QUALITY OF SERVICE			
RTP IP DiffServ	46		
Signaling DiffServ	24		
JITTER BUFFER			
Dynamic Jitter Buffer Minimum I	Delay [msec]	10	
Dynamic Jitter Buffer Optimizatio	on 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		
		Can	cel APPLY

Figure 67 – IP Profile – PSTN Gateway

Configure the IP Profile for the Avaya as shown below.

IP Prof	iles [AVAYA_Profile]					– x
	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	•
				History-Info Header Mode	As Is	•
	MEDIA SECURITY			Session Expires Mode	Supported	•
	SBC Media Security Mode	RTP T	1	Remote Update Support	Supported	•
	Symmetric MKI	Disable 🔻		Remote re-INVITE	Supported	•
	MKI Size	0		Remote Delayed Offer Support	Supported	•
	SBC Enforce MKI Size	Don't enforce		Remote Representation Mode	According to Operation Mode	•
	SBC Media Security Method	SDES 🔻		Keep Incoming Via Headers	According to Operation Mode	•
	Reset SRTP Upon Re-key	Disable 🔻		Keep Incoming Routing Headers	According to Operation Mode	•
	Generate SRTP Keys Mode	Only If Required		Keep User-Agent Header	According to Operation Mode	•

Figure 68 – IP Profile – Avaya.

IP Prof	iles [AVAYA_Profile]				- x
	SBC Remove Crypto Lifetime in SDP N	0	T	Handle X-Detect	No
	SBC Remove Unknown Crypto	0	Ŧ	ISUP Body Handling	Transparent 🔻
				ISUP Variant	Itu92
	C EARLY MEDIA			Max Call Duration [min]	0
	Remote Early Media	Supported	•		
	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	e By Signaling	•		
	Remote RFC 3960 Support	Not Supported	•	SBC FORWARD AND TRANS	FER
	Remote Can Play Ringback	Yes	Ŧ	Remote REFER Mode •	Handle Locally
	Generate RTP	None	T	Remote Replaces Mode 🔹	Handle Locally
				Play RBT To Transferee •	Yes 🔻

Figure 69 – IP Profile – Avaya – Contd.

IP Profiles [AVAYA_Profile]							– ×
SBC MEDIA			Remote 3xx Mode	Transpa	irent	۳	
Mediation Mode	RTP Mediation	,					
Extension Coders Group			SBC HOLD				
Allowed Audio Coders •	#1 [AllowedAudioCodersGroup_PSTNGW] 🔻	-	Remote Hold Format	Transp	parent	•	
Allowed Coders Mode	Restriction		Reliable Held Tone Source	Yes		•	
Allowed Video Coders		1	Play Held Tone	No		•	
Allowed Media Types							
Direct Media Tag		į I	SBC FAX				
RFC 2833 Mode	As Is		Fax Coders Group			•	
RFC 2833 DTMF Payload Type	0		Fax Mode		As Is	•	
Alternative DTMF Method	As Is		Fax Offer Mode		All coders	•	
Send Multiple DTMF Methods	Disable		Fax Answer Mode		Single coder	•	
Adapt RFC2833 BW to Voice coder BW	Disabled		Remote Renegotiate on Fax De	tection	Transparent	•	
SDP Ptime Answer	Remote Answer		Fax Rerouting Mode		Disable	•	

Figure	70 -	IP	Profile	– Avava –	Contd
riguio	10		1 101110	7 Traya	conta.

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 <b>v</b>
ICE Mode	Disable		
SDP Handle RTCP	Don't Care	GATEWAY	
RTCP Mux	Not Supported	Coders Group	#0 [AudioCodersGroups_0]
RTCP Feedback	Feedback Off		#0 [nadiocodci sel odb2_0]
Voice Quality Enhancement	Disable	LOCAL TONES	
Max Opus Bandwidth	0	LOCAL TONES	
Generate No-op	No	Local RingBack Tone Index	-1
Enhanced PLC	Disable	Local Held Tone Index	-1

Figure 71 – IP Profile – Avaya – Contd.

[AVAYA_Profile]				
QUALITY OF SERVICE				
RTP IP DiffServ	46			
Signaling DiffServ	24			
JITERBOILER				
Dynamic Jitter Buffer Minir	num Delay [msec]	10		
litter Buffer Max Delay Ims	ecl	300		
,, ,, ,				
VOICE				
Echo Canceler	Line	T		
Input Gain (-32 to 31 dB)	0			
Voice Volume (-32 to 31 dB	i) 0			
		Canc	el APPLY	

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

← → C ☆ ③ Not secure   10.64.3.10					Q 🕁	0 3	: 🍪
	MONITOR TROUBLESHOOT			Save	Reset Actions -	4 <mark>.</mark>	Admin 🔻
MEDIANT VE SBC IP NETWORK SIGNALING &	MEDIA ADMINISTRATION				,⊖ Em	tity, paramete	er, value
SRD All							
	SIP Definitions General Settings						
	GENERAL			SBC SETTINGS			
SPI Interfaces (5) Media Realms (2) Proxy Sets (5) IP Groups (5) CODERS & PROFILES SBC SIP DEFINITIONS Accounts (0) SIP Definitions General Settings	Send Reject (503) upon Overload Retry-After Time Fake Retry After Remote Management by SIP NOTIFY	Enable 60 60 Disable	¥	Subscribe Trying Minimum Session-Expires [sec] Session-Expires [sec] DISCONNECT SUPERVISION Broken Connection Mode Broken Connection Timeout [100 msec]	Disable 90 • 1800 Disconnect 100		
Message Structure Transport Settings Proxy & Registration Priority and Emergency Call Setup Pules (0) > Least Cost Routing Dial Plan (0)				MICROSOFT PRESENCE Presence Publish IP Group ID Microsoft Presence Status	-1 Disable		
MESSAGE MANIPULATION			Cancel	APPLY			

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.

← → C ☆ ③ Not secure   10.64.3.10					Q	☆ ⓒ	0	: چ
	OR TROUBLESHOOT			Save	Reset	Actions <del>-</del>	<b>ل</b> ها	Admin
MEDIANT VE SBC IP NETWORK SIGNALING & MEDIA	ADMINISTRATION					© Entit	y, parame	ter, value
📀 💿 SRD All 👻								
	SBC General Settings							
	GENERAL							
SIP Interfaces (5)	Direct Media	Disable	T					
Media Realms (2) Proxy Sets (5)	Unclassified Calls	Reject	Ŧ					
IP Groups (5)	Forking Handling Mode	Sequential	Ŧ					
CODERS & PROFILES	No Answer Timeout [sec]	600						
⊿ SBC	BroadWorks Survivability Feature	Disable	¥					
Classification (2)	Max Forwards Limit	70						
▲ Routing	Max Call Duration [min]	0						
Routing Policies (1) IP-to-IP Routing (9)	No RTP Timeout After Connect [ms]	0						
Alternative Routing Reasons (0)	Keep original user in Register	Do not keep user; Override with	ıur 🔻					
IP Group Set (0)	SBC Performance Profile	Optimized for transcoding	<b>v 5</b>					
SBC General Settings	Routing Timeout [sec]	10						
Call Admission Control Profile (0)								
Malicious Signature (12) External Media Source (0)	FORWARD & TRANSFER							
	SPC Pafer Pahavior	Degular						
Accounts (0) SIP Definitions General Settings	SBC 3xx Behavior	Transparent	Ŧ					
Message Structure Transport Settings			Cancel APPLY					

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  $\rightarrow$  SBC menu  $\rightarrow$  Routing  $\rightarrow$  IP-to-IP Routing Table.

#### Click **Add**.

## Calls from Teams to PSTN Gateway

louting [TEAMS -> PSTN]				
	Routing Policy #0 [/	Default_SBCRoutingPolicy]		
GENERAL		ACTION		
Index	4	Destination Type	IP Group	
Name	TEAMS -> PSTN	Destination IP Group	• #1 [PSTNGW]	✓ View
Alternative Route Options	Route Row 🔻	Destination SIP Interface	• #1 [PSTNGW]	✓ View
		Destination Address		
MATCH		Destination Port	0	
Source IP Group	• #0 [TEAMS]	Destination Transport Type		•
Request Type	All	IP Group Set		- View
Source Username Pattern	*	Call Setup Rules Set ID	-1	
Source Host	*	Group Policy	Sequential	•
Source Tag		Cost Group		✓ View

Figure 75 – Teams to PSTN – Contd.

Destination Username Pattern	*		Routing Tag Name	default	
Destination Host	*		Internal Action		Editor
Destination Tag					
Message Condition		N			
Call Trigger	Any				
ReRoute IP Group	Any 👻 View	v			
	Ca	ncel AP	PLY		

Figure 76 – Teams to PSTN

#### Calls from PSTN Gateway to Teams

IP-to-IP Routing [PSTNGW_to_TEAMS]					-
	Routing Policy	#0 [Defau	t_SBCRoutingPolicy]		
GENERAL			ACTION		
Index	6		Destination Type	IP Group	*
Name	PSTNGW_to_TEAMS		Destination IP Group	• #0 [TEAMS]	✓ View
Alternative Route Options	Route Row	•	Destination SIP Interface	• #0 [TEAMS]	✓ View
			Destination Address		
MATCH			Destination Port	0	
Source IP Group	#1 [PSTNGW]	▼ View	Destination Transport Type		•
Request Type	All	•	IP Group Set		✓ View
Source Username Pattern	*		Call Setup Rules Set ID	-1	
Source Host	*		Group Policy	Sequential	•
Source Tag			Cost Group		✓ View
Destination Username Pattern	*		Routing Tag Name	default	

Figure 77 – PSTN to Teams – Contd.

Destination Username Pattern	*	Routing Tag Name	default	
Destination Host	*	Internal Action		Editor
Destination Tag				
Message Condition	Viev	1		
Call Trigger	Any			
ReRoute IP Group	Any View	(		
	Ca			



### Calls from Teams to Avaya

IP-to-IP Routing [Teams -> Avaya]					– x
	Routing Policy	#0 [Def	fault_SBCRoutingPolicy]		
GENERAL			ACTION		
Index	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
			Destination Address		
MATCH			Destination Port	0	
Source IP Group	• #0 [TEAMS] •	View	Destination Transport Type		•
Request Type	All	•	IP Group Set		View
Source Username Pattern	*		Call Setup Rules Set ID	-1	
Source Host	*		Group Policy	Sequential	Ŧ
Source Tag			Cost Group		View
	Figure 7	'9 –Tea	ams to Avaya.		
Destination Username Pattern	7		Pouting Tag Name	default	
Destination Host	*		Internal Action		Editor
Destination Tag			incernal Accord		Laitor
Message Condition		View			
Call Trigger	Any	•			
ReRoute IP Group	Any	View			
		1			
		Cancel	APPLY		

Figure 80 – Teams to Avaya Contd.

IP Routing <b>[Avaya -&gt; Team</b>	5]		
	Routing Policy #0 [De	efault_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
		Destination Address	
MATCH		Destination Port	0
Source IP Group	• #3 [AVAYA] 👻 View	Destination Transport Type	Ţ
Request Type	All	IP Group Set	view
Source Username Pattern	*	Call Setup Rules Set ID	-1
Source Host	*	Group Policy	Sequential <b>v</b>
Source Tag		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			
		Cance	APPLY		

Figure 82 – Avaya to Teams Contd.

### 4.4.16 IP Group

### IP Group – Teams

pups <b>[TEAMS]</b>					
		SRD #0 [Def	faultSRD]		
GENERAL			QUALITY OF EXPERIENCE		
Index	0		QoE Profile		▼ View
Name	TEAMS		Bandwidth Profile		▼ View
Topology Location	Down	•			
Туре	Server	•	MESSAGE MANIPULATION		
Proxy Set	<ul> <li>#0 [TEAMS]</li> </ul>	▼ View	Inbound Message Manipulation Set	• 1	
IP Profile	<ul> <li>#1 [TEAMS_Profile]</li> </ul>	▼ View	Outbound Message Manipulation Set	• 2	
Media Realm	<ul> <li>#0 [TEAMS]</li> </ul>	▼ View	Message Manipulation User-Defined S	String 1	
Contact User			Message Manipulation User-Defined S	tring 2	
SIP Group Name	<ul> <li>sbc4.tekvizionlabs.com</li> </ul>		Proxy Keep-Alive using IP Group settin	igs = Enable	Ŧ
Created By Routing Server	No				

Figure 83 – IP Groups Teams – Contd.

IP Groups [TEAMS]					- X
Used By Routing Server	Not Used	v	SBC REGISTRATION AND AUTHENTI	CATION	
Proxy Set Connectivity	Connected		Max. Number of Registered Users	4	
			Registration Mode	User Initiates Registration	
SBC GENERAL			User Stickiness	Disable 🔻	
Classify By Proxy Set	Disable	Ŧ	User UDP Port Assignment	Disable ¥	
SBC Operation Mode	Not Configured	•	Authentication Mode	User Authenticates	
SBC Client Forking Mode	Sequential	•	Authentication Method List		
CAC Profile		View	SBC Server Authentication Type	According to Global Parameter	
			OAuth HTTP Service	View	
ADVANCED			Username	e Admin	
Local Host Name	sbc4.tekvizionlabs.com		Password	8	
UUI Format	Disable	v	GW GROUP STATUS		
Always Use Src Address	No	٣	GW Group Registered IP Address		

Figure 84 – IP Groups Teams – Contd.

9	SBC ADVANCED			
	Source URI Input		٣	1
	Destination URI Input		•	'
	SIP Connect	No	•	'
	SBC PSAP Mode	Disable	۳	,
	Route Using Request URI Port	Disable	۳	/
	DTLS Context	#1 [Teams] 🔻	View	w
	Keep Original Call-ID	No	•	/
	Dial Plan		View	w
	Call Setup Rules Set ID	-1		
	Tags			
			Canc	ance

Figure 85 – IP Groups Teams

#### IP Group – PSTN Gateway

IP Group	os [PSTNGW]									- x
			SRE		#0	) [Defau	litSRD]			
	GENERAL						QUALITY OF EXPERIENCE			
	Index		1				QOE Profile		✓ View	
	Name	•	PSTNGW				Bandwidth Profile		✓ View	
	Topology Location	•	Up		•					
	Туре		Server		۳		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 Str	ing 1		
	Contact User						Message Manipulation User-Defined Str	ing 2		
	SIP Group Name	•	10.64.1.72				Proxy Keep-Alive using IP Group setting	s e	Enable V	
	Created By Routing Server		No							

Figure 86 – IP Groups PSTN – Contd.

IP Groups [PSTNGW]					– x
Used By Routing Server	Not Used	¥	SBC REGISTRATION AND AUTHENTIC	CATION	
Proxy Set Connectivity	Connected		Max. Number of Registered Users	-1	
			Registration Mode	User Initiates Registration	•
SBC GENERAL			User Stickiness	Disable	•
Classify By Proxy Set	Enable	٣	User UDP Port Assignment	Disable	•
SBC Operation Mode	Not Configured	٣	Authentication Mode	User Authenticates	•
SBC Client Forking Mode	Sequential	T	Authentication Method List		
CAC Profile	-	- View	SBC Server Authentication Type	According to Global Parameter	•
			OAuth HTTP Service		w
ADVANCED			Username	Admin	· · ·
			Password		
Local Host Name					
UUI Format	Disable	v	GW GROUP STATUS		
Always Use Src Address	No	•	GW Group Registered IP Address		

Figure 87 – IP Groups PSTN – Contd.

SBO	C ADVANCED		
So	ource URI Input		•
De	estination URI Input		•
SIF	P Connect	No	۳
SB	3C PSAP Mode	Disable	۳
Ro	oute Using Request URI Port	Disable	•
DT	TLS Context	#0 [default]	View
Ke	eep Original Call-ID	No	•
Dia	al Plan		View
Ca	all Setup Rules Set ID	-1	
Ta	ıgs		
			Cancr

Figure 88 – IP Groups PSTN

### IP Group – Avaya

IP Grou	ps [AVAYA]						– x
		SRD	#0 [Defa	ultSRD]			
	GENERAL			QUALITY OF EXPERIENCE			
	Index	3		QoE Profile		•	View
	Name •	AVAYA		Bandwidth Profile		•	View
	Topology Location	Down	•				
	Туре	Server	•	MESSAGE MANIPULATION			
	Proxy Set •	#3 [AVAYA]	View	Inbound Message Manipulatio	on Set 🔹 6		
	IP Profile •	#4 [AVAYA_Profile]	View	Outbound Message Manipula	tion Set • 7		_
	Media Realm •	#1 [TEKVLAN]	View	Message Manipulation User-D	efined String 1		
	Contact User			Message Manipulation User-D	efined String 2		
	SIP Group Name	10.64.5.57		Proxy Keep-Alive using IP Grou	up settings Dis	able	•
	Created By Routing Server	No					

Figure 89 – IP Groups Avaya.

Groups [AVAYA]				
Used By Routing Server	Not Used	Ŧ	SBC REGISTRATION AND AUTHE	NTICATION
Proxy Set Connectivity	NA		Max. Number of Registered Users	-1
			Registration Mode	User Initiates Registration
SBC GENERAL			User Stickiness	Disable <b>v</b>
Classify By Proxy Set	Enable	•	User UDP Port Assignment	Disable 🔻
SBC Operation Mode	Not Configured	•	Authentication Mode	User Authenticates
SBC Client Forking Mode	Sequential	•	Authentication Method List	
CAC Profile	vi	ew	SBC Server Authentication Type	According to Global Parameter
			OAuth HTTP Service	view
ADVANCED			Username	Admin
			Password	•
Local Host Name				
UUI Format	Disable	•	GW GROUP STATUS	
Always Use Src Address	No	v	GW Group Registered IP Address	

Figure 90 – IP Groups Avaya – Contd.

5	BC ADVANCED		
	Source URI Input		Ŧ
	Destination URI Input		•
	SIP Connect	No	Ŧ
	SBC PSAP Mode	Disable	Ŧ
	Route Using Request URI Port	Disable	¥
	DTLS Context	#0 [default]	▼ View
	Keep Original Call-ID	No	T
	Dial Plan		▼ View
	Call Setup Rules Set ID	-1	
	Tags		
			Can

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  $\rightarrow$  **Message Manipulations** menu  $\rightarrow$  **Message Manipulations**.

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

Index	1				_
			Action Subject		Editor
Name			Action Type	Add	•
Manipulation Set ID	0		Action Value		Editor
Row Role	Use Current Condition	•			
MATCH					
Message Type		Editor			
Condition		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

age Manipulations [Filter Priv	acy ID except for Anonymous]				
GENERAL					
Index	28		Action Subject	• header.privacy	Editor
Name	Filter Privacy ID except for Anonymous		Action Type	Remove	•
Manipulation Set ID	• 1		Action Value		Editor
Row Role	Use Current Condition	*			
MATCH					
Message Type	Invite.Request	Editor			
Condition	Header.From.URL.Host contains '.com'	Editor			
		Cancel	APPLY		

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

Message	e Manipulations [modify pai host t	towards teams]				- x
	GENERAL			ACTION		
	Index	21		Action Subject	header.P-Asserted-Identity.URL.Host     Edit	or
	Name	modify pai host towards teams		Action Type	Modify	]
	Manipulation Set ID	2		Action Value	'sbc4.tekvizionlabs.com'     Edit	or
	Row Role	Use Current Condition	•			
	MATCH					
	Message Type	• Invite	Editor			
	Condition		Editor			
			Cancel	APPLY		

Figure 94 – SIP Message Manipulation – PAI

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

ge Manipulations <b>[modify t</b> d	o towards teams]				
GENERAL			ACTION		
Index	19		Action Subject	<ul> <li>header.to.url.host</li> </ul>	Editor
Name	modify to towards teams		Action Type	Modify	•
Manipulation Set ID	• 2		Action Value	<ul> <li>'slp.pstnhub.mlcrosoft.com'</li> </ul>	Editor
Row Role	Use Current Condition	•			
MATCH					
Message Type	Invite.request	Editor			
Condition		Editor			
		Cancel	APPLY		

Figure 95 – SIP Message Manipulation - To

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

GENERAL			ACTION	
Index Name Manipulation Set ID	0  Towards Teams FROM  2		Action Subject Action Type Action Value	Header.From.URL     Editor     Modify      'sip.admin@stc4.tekvt2ionlabs.com'     Editor
MATCH	use current condition	Ť		
Message Type Condition	Options     param.message.address.dst.sipinterface==0'	Editor Editor		

Figure 96 – SIP Message Manipulation - From

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

e Manipulations <b>[towards</b>	Teams Contact]			
GENERAL		ACTION		
Index	1	Action Subject	e Header.Contact.URL.Host	Editor
Name	towards Teams Contact	Action Type	Modify	¥
Manipulation Set ID	• 2	Action Value	'sbc4.tekvizionlabs.com'	Editor
Row Role	Use Current Condition		-	
MATCH				
Message Type	Options     Editor			
Condition	param.Message.Address.Dst.SIPInterface=='0'     Editor			
	Cancel	APPLY		

Figure 97 – SIP Message Manipulation - Contact

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

Message Manipulations [Toward	ds Teams]			- x
GENERAL		ACTION		
Index	2	Action Subject	Header.From.URL.host	Editor
Name	Towards Teams	Action Type	Modify	•
Manipulation Set ID	• 2	Action Value	<ul> <li>'sbc4.tekvizionlabs.com'</li> </ul>	Editor
Row Role	Use Current Condition	T		
MATCH				
Message Type	Invite.Request	Editor		
Condition		Editor		
		Cancel APPLY		

Figure 98 – SIP Message Manipulation - From

Manipulation to PSTN

• To Modify "TO" header: To display an IP for an PSTN Gateway

e Manipulations <b>[towards</b> ]	PSTNGW TOJ				
GENERAL			ACTION		
Index	З		Action Subject	header.to.url.host	Editor
Name	towards PSTNGW TO		Action Type	Modify	•
Manipulation Set ID	• 3		Action Value	e '10.64.3.10'	Editor
Row Role	Use Current Condition	•			
MATCH					
Message Type	Options	Editor			
Condition	<ul> <li>Param.Message.Address.dst.SIPInterface=='1</li> </ul>	' Editor			
			10011		

Figure 99 – SIP Message Manipulation – To

• To Modify "FROM" header: To display an IP for an AudioCodes

Messa	ge Manipulations <b>[Towards</b>	PSTNGW FROM]					- x
	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	e 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

age Manipulations [Referred	By to PSTNGW]			
GENERAL		ACTIO	N	
Index	5	Action	Subject e Header.Referred-By.url.host	Editor
Name	Referred-By to PSTNGW	Action	Type Modify	Ŧ
Manipulation Set ID	• 3	Action	Value e '10.64.3.10'	Editor
Row Role	Use Current Condition	¥		
MATCH				
Message Type	• Invite	Editor		
Condition	Header.Referred-By exists	Editor		

Figure 101 – SIP Message Manipulation – Referred – By

• To Modify "FROM" header: To display an IP for an AudioCodes in From

Messag	e Manipulations <b>[Toward</b> s	s PSTNGW Invite]			- x
	GENERAL		ACTION		
	Index	6	Action Subj	ect Header.From.URI	L.Host Editor
	Name	Towards PSTNGW Invite	Action Type	Modify	T
	Manipulation Set ID	• 3	Action Valu	e '10.64.3.10'	Editor
	Row Role	Use Current Condition	Ŧ		
	MATCH				
	Message Type	Invite.Request	Editor		
	Condition		Editor		
			Cancel APPLY		

Figure 102 – SIP Message Manipulation – From

Manipulation to Avaya

• To Modify "Diversion" header: To display AudioCodes IP

age Manipulations <b>[Te</b>	ams -> Avaya Modify Diversion header]			-
GENERAL		ACTION		
Index Name Manipulation Set ID Row Role	22 ■ Teams -> Avaya Modify Diversion header ■ 7 Use Current Condition ▼	Action Subject Action Type Action Value	header.Diversion.url.host     Add     '10.64.3.10'	Editor Editor
MATCH				
Message Type Condition	invite.request     Editor     Header.Diversion exists     Editor			

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	<ul> <li>Modify</li> </ul>	•
Manipulation Set ID	7		Action Value	• '10.64.3.10'	Editor
Row Role	Use Current Condition	•			
MATCH					
Message Type	Invite.Request	ditor			
Condition	Ec	ditor			
	Ca	ancel 🗾	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]				– x
GENERAL			ACTION		
Index	17		Action Subject	Header.Referred-By.url.host	Editor
Name	<ul> <li>Referred-By Teams -&gt; Avaya</li> </ul>		Action Type	<ul> <li>Modify</li> </ul>	•
Manipulation Set I	D • 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 AF	PPLY		

Figure 105 – SIP Message Manipulation – Referred By

• To Modify "FROM" header: To display an IP for an AudioCodes in From

age Manipulations [Fro	m header Teams -> Avaya]			
GENERAL		ACTION		
Index Name Manipulation Set ID Row Role	15       From header Teams -> Avaya       7       Use Current Condition	Action Subject Action Type Action Value	<ul> <li>Header.From.URLhost</li> <li>Modify</li> <li>'10.64.3.10'</li> </ul>	Editor
MATCH				
Message Type Condition	Options     Editor     Param.Message.Address.dst.SIPInterface==     Editor			
	Cance	APPLY		

Figure 106 – SIP Message Manipulation – From

• To Modify "TO" header: To display an IP for an AudioCodes in to

Message Manipulations [To	o header Teams -> Avaya]			– x
GENERAL		ACTION		
Index Name	16 To header Teams -> Avaya	Action Subject Action Type	Header.To.URL.host     Modify	Editor
Manipulation Set ID Row Role	e 7 Use Current Condition ▼	Action Value	• '10.64.3.10'	Editor
MATCH				
Message Type Condition	Options     Editor     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

B		10.89.33.4	4 - PuT	τγ	<b>_</b> D X
admin@lab133-cm80> admin@lab133-cm80> swve Operating system: Built:	rsion Linux 3.1 Dec 19 10	0.0-957.5.1.e 0:46 2018	17.x86	_64 x86_64 x86_64	<u>^</u>
Contains: CM Reports as: CM Release String: RTS Version: Publication Date: VMwaretools version: App Deployment: VM Environment:	00.0.822. R018x.00. vcm-018-0 CM 8.0.1. 09 May 20 10.1.5.59 Virtual M VMware	0 0.822.0 00.0.822.0 1.0.822.25183 018 0732 (build-50 Nachine	955683)		
UPDATES: Update ID		Status	Туре	Update description	
00.0.822.0-25183		activated	cold	8.0.1.1.0-FP1SP1	
KERNEL-3.10.0-957.5.1.e	17	activated	cold	kernel patch KERNEL-3.10.0	)-
Platform/Security ID		Status	Туре	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.

B		10.89.33.4 - PuTTY		x
change node-names i	р		Page 1 of 2	^
		IP NODE NAMES		
Name	IP Address			
Lab133-SM80	10.89.33.7			
Vodafone				
Votenoin				
acmm	10.89.26.25			
detault	0.0.0.0			
gateway	10.89.33.1			
procr	10.09.55.4			
procro				
(8 of 8 admini	stered node-na	ames were displayed )		
Use 'list node-name	s' command to	see all the administered n	iode-names	
Use 'change node-na	mes ip xxx' to	o change a node-name 'xxx'	or add a node-name	
F1=Cancel F2=Refres	h F3=Submit F4	4=Cir Fld F5=Help F6=Update	F7=Nxt Pg F8=Prv Pg	
				$\mathbf{x}$
		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

ß		10.89	).33.4 - PuTTY	_ □	x
change ip-codec-s	set 1		Page	1 of	2 ^
Codec Set: 1	IP	MEDIA PAR	AMETERS		
Audio Codec 1: <mark>G.711MU</mark> 2: <u>G.711A</u> 3: <u>G.729</u> 4: 5: 6: 7:	Silence Suppression <u>n</u> - - - - -	Frames <u>Per Pkt</u> <u>2</u> <u>2</u>   	Packet Size(ms) 20 20 20		
Media Encryp 1: 1-srtp-aescm1	otion 178-bmac80		Encrypted SRTCP: <u>best-effort</u>	:	
2: <u>2-srtp-aescm</u> 3: 4: 5:	128-hmac32				=
F1=Cancel F2=Refr	resh F3=Submi	t F4=Clr	Fld F5=Help F6=Update F7=Nxt F	g F8=Prv	Pg 🗸

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

B	10.89.33.4 - PuTTY	_ □	x
change ip-network-region 1	Pa	ge 1 of	20 ^
	IP NETWORK REGION		
Region: 1 NR Group: <mark>1</mark>			
Location: <u>1</u> Authoritative	Domain: <u>lab.tekvizion.com</u>		
Name: Lab133	Stub Network Region: n		_
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: y	25	
Codec Set: 1	Inter-region IP-IP Direct Audio: y	25	
UDP Port Min: 2048	IP Audio Hairpinning? <u>n</u>		
UDP Port Max: 65535			
DIFFSERV/TOS PARAMETERS			
Call Control PHB Value: 46			
Audio PHB Value: 46			
Video PHB Value: <u>26</u>			
602.1P/Q PARAMETERS	~		
Call Control 602.1p Priority:			
Audio 602.1p Priority:		DAMETERS	
H 333 TO ENDOTINTS	S AUDIO RESOURCE RESERVATION P	led2 n	
H 222 Link Rounce Decovery) y	KSVF LIND.	reu: <u>n</u>	
Idle Traffic Interval (sec): 2	a		
Keen-Alive Interval (sec): 5	<u>v                                    </u>		
Keep-Alive Count: 5			
Keep Arrive counter 5			
F1=Cancel F2=Refresh F3=Submit	F4=Clr Fld F5=Help F6=Update F7=Nxt	Pg E8=Prv	Pg

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                                                                                                                        | _ □                | Х          | ۲ ( |
|---------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|-----|
| change signaling-group 5 Page                                                                                                               | 1 of               | 2          | ^   |
| SIGNALING GROUP                                                                                                                             |                    |            |     |
| Group Number: 5<br>IMS Enabled? n<br>Q-SIP? n                                                                                               |                    |            |     |
| IP Video? n Enforce SIPS URI f                                                                                                              | or SRTP            | ۲ Y        |     |
| Peer Detection Enabled? y Peer Server: SM Cl                                                                                                | ustered            | <u>n</u>   |     |
| Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public<br>Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected | Numbers<br>Numbers | Ру<br>Рп   |     |
| Alert Incoming SIP Crisis Calls? n                                                                                                          |                    |            |     |
| Near-end Node Name: procr Far-end Node Name: Lab13                                                                                          | <u>3-SM80</u>      | -1         |     |
| Far-end Listen Port: <u>5060</u><br>Far-end Network Region: 2                                                                               |                    |            |     |
|                                                                                                                                             |                    |            |     |
| Far-end Domain: lab.tekvizion.com                                                                                                           |                    |            |     |
| Bypass If IP Threshold E                                                                                                                    | xceeded            | <u>n</u>   |     |
| Incoming <u>Dialog Loopbacks: eliminate</u> <u>RFC 3389 Comfor</u>                                                                          | t Noise            | <u>, u</u> |     |
| DTMF over IP: rtp-payload Direct IP-IP Audio Conn                                                                                           | ections            | <u>n</u>   |     |
| Session Establishment Timer(min): <u>3</u> IP Audio Hair                                                                                    | pinning            | <u>n</u>   |     |
| Enable Layer 3 Test? y                                                                                                                      |                    |            | ∎   |
| Alternate Route Tim                                                                                                                         | er(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 reated 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

10.89.33.4 - PuTTY – 🗖 🗙	
change trunk-group 5       Page 1 of 4         TRUNK GROUP         Group Number: 5       Group Type: sip       CDR Reports: v         Group Name: Crestron Teams       COR: 1       TN: 1       TAC: #005         Direction: two-way       Outgoing Display? n       Dial Access? n       Night Service:       Queue Length: Ø         Service Type: public-ntwrk       Auth Code? n       Member Assignment Method: auto       Signaling Group: 5         Number of Members: 5       Service Type: public Service       Signaling Group: 5       Number of Members: 5	
F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg ✓	

### 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

Putty 10.89.33.4 - Putty	- 🗆 X
change route-pattern 5Page	1 of 4 ^
Pattern Number: 5 Pattern Name: <u>to ASM7</u> SCCAN? <mark>n</mark> Secure SIP? <u>n</u> Used for SIP stations? <u>n</u>	
Grp FRL NPA Pfx Hop Toll No. Inserted No       Inserted Digits         1: 5       0       -       -       -         2:	DCS/ IXC QSIG Intw <u>n user</u> <u>n user</u> <u>n user</u> <u>n user</u> <u>n user</u> <u>n user</u>
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM Sub Numbe 012M4W Request Dgts Forma 1: y y y y n n rest unk-u	ering LAR at unk <u>none</u>
2: y y y y n n       n       rest	none none none none none
F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg	F8=Prv Pg

#### 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

B	1	0.89.33.4 -	PuTTY				x
change aar analysis 8					Page	1 of	2 ^
	AAR D	IGIT ANALY	SIS TABL	.Е			
		Location:	all		Percent Fi	111: 3	
Dialed	Total	Route	Call	Node	ANI		
String	Min Max	Pattern	Туре	Num	Reqd		
R.	7 7	254	aar		<u>n</u>		
800	<u> </u>	254	aar		<u>n</u>		
<u> </u>	<u> </u>	2.34	<u>aai</u>		<u>"</u>		
					<u>n</u>		
					<u>n</u>		
					<u>n</u>		
					<u>n</u>		
					<u>"</u>		
					n		
					<u>n</u>		
					<u>n</u>		
					<u>n</u>		
					<u>ш</u>		=
F1=Cancel F2=Refresh F3=	Submit F4=	Clr Fld F5	=Help F6	5=Updat	e F7=Nxt Pg	F8=Prv	Pg
							$\checkmark$

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 - P	PuTTY	_ □	x
change private-numb	ering 1		Рад	e 1 of	2 ^
	NOM	DERING - PRIVAT	E FURMAT		
Ext Ext Len Code 4 26 4 265 4 0982 4 0988 4 0989 4 0991 4 0992 4 0992 4 7500 5 7500 4 7501	Trk Grp(s) 2 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	Private Prefix 043207 	Total Len <u>4</u> Total Administr <u>10</u> Maximum Ent <u>10</u> <u>10</u> <u>10</u> <u>10</u> <u>10</u> <u>4</u> <u>4</u> <u>4</u>	ered: 16 ries: 540	
<u>5</u> 7501 <u>4</u> 7503 <u>5</u> 70988 <u>7</u> 0988	<u>5</u> <u>5</u>	7501 7503	$ \frac{4}{4}$ 		
7 2149177 7 2149177 7 5980100	9 5 5				=
F1=Cancel F2=Refres	sh 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

← → C 🏠 🔺 Not secure   10.89.33.3/network-login/	☆ ⓒ ♀   🎯 🗄
Recommended access to System Manager is via FQDN.	
Go to central login for Single Sign-On	User ID: admin
If IP address access is your only option, then note that authentication will fail in the following cases:	Password:
First time login with "admin" account     Expired/Reset passwords	Log On Cancel
Use the "Change Password" hyperlink on this page to change the password manually, and then login.	Change Password
Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.	<b>OSupported Browsers:</b> Internet Explorer 11.x or Firefox 59.0, 60.0 and 61.0.
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.	
Unauthorized users are subject to company disciplinary procedures and or	

Figure 117 - Log into Avaya Aura System Manager

#### ← → C ☆ ▲ Not secure | 10.89.33.3/SMGR/ ☆ 🕝 🔾 🅞 avaya 🔔 🗮 | admin Services v | Widgets v Shortcuts v 🔒 Users 🗸 🔑 Elements 🗸 ra® Syster System Resource Utilization Notifications Application State 28 License Status Active 21-Deployment Type VMware 14-Multi-Tenancy DISABLED OOBM State DISABLED 7 Hardening Mode Standard 0 opt var emdata tmp perfdata swlibrary home pgsql 📕 Critical 🔛 Warning 📕 Normal 📃 Free Alarms Information Shortcuts Critical Major Indeterminate Minor Warning Elements Count Sync Status Drag shortcuts here Severity СМ 1 SourceIP Description Session Manager A scheduled job CRLExpirationChe 10.89.33.3 System Manager Job failed to execute.Please see lo or more details. UCM Applications 8 A scheduled job sys\_ConfRefresh( Current Usage: 10.89.33.3 g failed to execute.Please see logs more details. 12/250000 USERS A scheduled job sys\_ConfRefresh 10.89.33.3 g failed to execute.Please see logs 1/50

### Navigate to Elements → Routing

Figure 118 - Routing

## 4.6.1 Version

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

Αναγα	×
System Manager 8.0.1.1 Build No 8.0.0.0.931077 Software Update Revision No: 8.0.1.1.039340	
> Details	
> Third Party Terms for RHEL	
	Cancel

Figure 119 – Version

### 4.6.2 Domains

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

Aura® System Manager 8.0	🛔 Users 🗸 🌾 Elements 🗸 🏟 Services 🗸 📗 Widge	ets v Shortcuts v	Search 🐥 🚍 🛛 admin
Home Routing			
Routing ^	Domain Management		Help ?
Domains	New Edit Delete Duplicate More Actions		
Locations	1 Item @		Filter: Enable
Conditions	Name	Type Notes	
Adaptations 🗸	Select : All, None	sip Lab113	

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**

Avra® System	m Manager 8.0	)	Users v	🗲 Elements 🗸	🔅 Services 🗸	Wid	gets v Shortcut	s ~	Search	🜲 🗮   admin
Home	Routing									
Routing		^	Dom	ain Manage	ment				Commit Cancel	Help ?
Doma	ains									
Locat	ions		1 Item	æ						Filter: Enable
Cond	itions		Name				Туре	Notes		
Adap	tations	~	* lab.t	ekvizion.com			sip ▼	Lab113		
SIP E	ntities									
Entity	/ Links								Commit Cancel	-

Figure 121 - Domain

## 4.6.3 Locations

- 1. Navigate to **Routing**  $\rightarrow$  **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**

Avra® System	m Manager 8.0	🛓 Users 🗸 🌾 Elements 🗸 🏘 Services 🗸   Widgets 🗸 Shortcuts 🗸	Search 🔔 🗮 🛛 admin	
Home	Routing			
Routing		Location Details	Help ? A	
Doma	ains	General	_	
Locati	ions	* Name: Lab133-Plano		
Condi	itions	Notes: Lab133		ļ
Adapt	tations Y	Dial Plan Transparency in Survivable Mode		
SIP En	ntities	Enabled:		1
Entity	Links	Listed Directory Number:		
		Associated CM SIP Entity:		
Time f	Ranges			
Routir	ng Policies	Overall Managed Bandwidth		
Dial P	atterns v	Managed Bandwidth Units: Kbit/sec 🔻		
		Total Bandwidth:		
Regula	ar Expressions	Multimedia Bandwidth:		
Defau	ilts	<ul> <li>Audio Calls Can Take Multimedia Bandwidth:</li> </ul>		

Figure 122- Add Location

Avra® System Manager 8.0	Users ∨ 🖌 Elements ∨ 🌣 Services ∨	Widgets v Shortcuts v Search	🜲 🚍   admin
Home Routing <			
Routing ^	Overall Managed Bandwidth		•
Domains	Managed Bandwidth Units:	Kbit/sec 🔻	
	Total Bandwidth:		
Locations	Multimedia Bandwidth:		
Conditions	Audio Calls Can Take Multimedia Bandwidth:	✓	
Adaptations 🗸	Per-Call Bandwidth Parameters		
SIP Entities	Maximum Multimedia Bandwidth (Intra- Location):	2000 Kbit/Sec	
Entity Links	Maximum Multimedia Bandwidth (Inter- Location):	2000 Kbit/Sec	
Time Ranges	* Minimum Multimedia Bandwidth:	64 Kbit/Sec	
Routing Policies	* Default Audio Bandwidth:	80 Kbit/sec 🔻	
Dial Patterns 🗸 🗸	Alarm Threshold		
Regular Expressions	Overall Alarm Threshold:	80 • %	
Dafaulte	Multimedia Alarm Threshold:	80 <b>v</b> %	
<	* Latency before Overall Alarm Trigger:	5 Minutes	
	* Latency before Multimedia Alarm Trigger:	5 Minutes	*

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

Aura® System Manager 8.0	sers 🗸 🎤 Elements 🗸	🔅 Servic	es v   Wid	lgets v Shor	tcuts v	Search	_ ▲ ≡	adm	nin
Home Routing									
Routing ^	Adaptation Detai	ls				Commit Canc	el	Help ?	*
Domains	Ganaral						_		L
Locations	*	Adaptatior	<b>Name:</b> Adapt	ation_for_ACM					L
Conditions	* Module	Name: D	igitConversionA	dapter 🔻					
Conditions	Module Paramete	r Type: N	lame-Value Para	meter 🔻					
Adaptations ^		6							
Adaptations		Ľ	Add Remove		Value				
Regular Expressi			fromto	-	true				
		s	elect : All. None					/	
SIP Entities	Egross	IIPT Dara	motors:						
Entity Links	Lgres.	, on i un	Notes:						
Time Ranges									
	Digit Conversion for I	ncoming	g Calls to SM	1					
Kouting Policies	Add Remove								
Dial Patterns V	0 Items 🛛 🍣						Filter:	Enable	
	Matching Pattern Mi	in Max F	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes	+
Adaptations	Digit Conversion for I	ncoming	g Calls to SN	1					
Regular Expressi	Add Remove								
	0 Items 👌				-		Filter	: Enable	
SIP Entities	Matching Pattern Mi	n Max F	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes	
Entity Links	Digit Conversion for C	Outgoing	) Calls from	SM					
Time Ranges	Add Remove								
Routing Policies	0 Items 🛛 🥲						Filter	Enable	
	Matching Pattern Mi	n Max F	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes	
Dial Patterns V						Commit Cano	el		+

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

Aura © System Manager 8.0	Users 🗸 🌾 Elements 🗸 🏶 Services 🗸 📔 Widge	ts v Shortcuts v		Search	📄 🐥 🗮 🛛 admin
Home Routing					
Routing	SIP Entity Details	Com	nmit Cancel		Help ? 🔺
Domains	General				
Locations	* Name:	Lab133-SM80			
Conditions	* IP Address:	10.89.33.7			
Conditions	SIP FQDN:				
Adaptations ^	Туре:	Session Manager 🔻			
Adaptations	Notes:	Lab133			
	Location:	Lab133-Plano 🔻			
Regular Expres	Outbound Proxy:	▼			
SIP Entities	Time Zone:	America/Chicago 🔻			
Entity Links	Minimum TLS Version:	Use Global Setting 🔻			
	Credential name:				
Time Ranges	Manitanian				
Routing Policies	SIP Link Monitoring	Use Session Manager Configuration V			
- Dial Patterns	CRLF Keep Alive Monitoring:	Use Session Manager Configuration V			
	Entity Links				
Regular Expressions	Add Remove				
Defaults	9 Items				Filter: Enable
-	Name SIP Entity 1 Pr	otocol Port SIP Entity 2	Port	Connection Policy	Deny New Service
<		TCP ▼ * 5060 AMM	▼ * 5060	trusted V	
	* Lab133-5M80_Corp_Gy Lab133-5M80 V (	LS ▼ * 5061 IPC	▼ * 5061	trusted V	

Figure 125 - SIP Entity: Avaya Aura Session Manager

Adaptations	Entity Links
Regular Expres	Add Remove
	9 Items 💩 Filter: Enable
SIP Entities	Name         SIP Entity 1         Protocol         Port         SIP Entity 2         Port         Connection Policy         Dany New Service
	■ * Lab133-SM80_Lab133 Lab133-SM80 ▼ TCP ▼ * 5060 Lab133CM_SIP_TCP ▼ * 5060 trusted ▼
Entity Links	■ *Lab133-5M80_Lab133 Lab133-5M80 ▼ TLS ▼ *5061 Lab133CM_SIP_TLS ▼ *5061 trusted ▼
	Lab133-SM80_Nokia_S Lab133-SM80 V UDP V * 5060 Nokia_SBC V * 5068 trusted V
Time Ranges	□ * ToAmazonCVCAvayaSB Lab133-SM80 ▼ UDP ▼ * 5060 AmazonCVC_AvayaSBC ▼ * 5060 trusted ▼ □
Routing Policies	Select : All, None
Dial Patterns v	Failover Ports       TCP Failover port:       5060
Regular Expressions	TLS Failover port: 5061
Defaults	Add Remove
<	3 Items 🖓 Filter: Enable
	Listen Ports Protocol Default Domain Endpoint Notes
	5060 TCP V lab.tekvizion.com V

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**

AVAYA Aura © System Manager 8.0	🛦 Users 🗸 🌾 Elements 🗸 🌩 Services 🗸   Widgets 🗸 Shortcuts 🗸	Search 💄 🗮 🛛 adm	iin
Home Routing			
Routing ^	<ul> <li>SIP Entity Details</li> </ul>	Commit Cancel	
Demains	General	-	
Domains	* Name: Lab133CM_SIP_TCP	]	
Locations	* FQDN or IP Address: 10.89.33.4	]	
Conditions	Type: CM V		
	Notes:	]	
Adaptations ^	Adaptation: Adaptation_for_ACM V		
Adaptations	Location: V	-	
Regular Expres	Time Zone: America/Fortaleza		
	* SIP Timer B/F (in seconds): 4		
SIP Entities	Minimum TLS Version: Use Global Setting V		
Entity Links	Credential name:		
Time Panger	Securable:		
Time hanges	Call Detail Recording: none <b>T</b>		
Routing Policies	Loop Detection		
Dial Patterns v	Loop Detection Mode: On V		
	Loop Count Threshold: 5		
Regular Expressions	Loop Detection Interval (in msec): 200		
Defaults	Monitoring		
	▼ SIP Link Monitoring: Use Session Manager Configuration ▼		
	CRLF Keep Alive Monitoring: Use Session Manager Configuration V		
	Supports Call Admission Control:		•

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

Regular Expres	Entity Links
SIP Entities	Override Port & Transport with DNS SRV:
Entity Links	Add Remove
	1 Item 😨 Filter: Enable
Time Ranges	Name SIP Entity 1 Protocol Port SIP Entity 2 Port Connection Policy Deny New Service
	*Lab133-SM80_Lab133 Lab133-SM80 V TCP V * 5060 Lab133CM_SIP_TCP V * 5060 trusted V
Routing Policies	Select : All, None
Dial Patterns v	SIP Responses to an OPTIONS Request
Regular Expressions	Add Remove
	0 Items 💩 Filter: Enable
Defaults	Response Code & Reason Phrase Hark Entity Notes
<	
	Commit Cancel

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**

Aura® System Manager 8.0	Users 🗸 🎤 Elements 🗸 🌞 Se	ervices ~   Widget	s × Shortcuts ×	Search 🔷 🌲 🗏   admin
Home Routing				
Routing ^	SIP Entity Details		Commit Cancel	A
Domains	General			
		* Name:	AvayaSBC	
Locations		* FQDN or IP Address:	10.89.33.13	
Conditions		Туре:	Other V	
Adaptations ^		Notes:		
A destadance		Adaptation:	Adaptation_for_SBC V	
Adaptations		Location:	Lab133-Plano V	
Regular Expres		Time Zone:	America/Fortaleza	
SIP Entities	* SIP T	imer B/F (in seconds):	4	
		Minimum TLS Version:	Use Global Setting 🔻	
Entity Links		Credential name:		
Time Ranges		Securable:		
Routing Policies	CommP	rofile Type Preference:		
Dial Patterns ^	Loop Detection	Loop Dataction Mode	On V	
Dial Patterns		Loop Count Threshold:	5	
Origination Dia	Loop Detect	ion Interval (in msec):	200	
-				
Regular Expressions	Monitoring	CTD Link Marile	Link Monitoring Enabled	
	* Droactive Monitoring	SIP Link Monitoring:		
	Proactive Monitoring	interval (in seconds):	200	Ŧ

Figure 129 - SIP Entity: Avaya SBCE

SIP Entities	Entity Links Override Port & Transport with DNS SRV:
Entity Links	Add Remove
Time Ranges	1 Item 🖉 Filter: Enable
	Name SIP Entity 1 Protocol Port SIP Entity 2 Port Connection Policy Deny New Service
Routing Policies	* To_AvayaSBC     Lab133-SM80 ▼ UDP ▼ * 5060     AvayaSBC ▼ * 5060     trusted ▼
	Select : All, None
Dial Patterns 🔨	

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**

Aura® System Manager 8.0	lsers v 🖋 Elements v 🌢 Services v   Widgets v Shortcuts v	Search	ㅣ 🐥 🗮   admin
Home Routing			
Routing ^	Routing Policy Details	Commit Cancel	Help ?
Domains	General		
Locations	* Name: to_CM(TCP)		
Conditions	Disabled:		
	* Retries: 0		
Adaptations ^	Notes:		
Adaptations	SIP Entity as Destination		
Regular Expres	Select		
	Name FQDN or IP Address	Туре	lotes
SIP Entities	Lab133CM_SIP_TCP 10.89.33.4	СМ	
Entity Links	Time of Day		
Time Ranges	Add Remove View Gaps/Overlaps		
	1 Item 🧔		Filter: Enable
Routing Policies	Ranking A Name Mon Tue Wed Thu Fri Sat	Sun Start Time End Time Notes	
Dial Patterns 🗸 🗸		✓ 00:00 23:59 Time Rail	nge 24/7
	Select : All, None		
Regular Expressions	Dial Patterns		
Defaults	Add Remove		
•	3 Items 🖓		Filter: Enable
<	Pattern Min Max Emergency Call SIP Doma	ain Originating Location	Notes
	2137 4 12 -ALL- 750 4 12 -Δ11-	Lab133-Plano	
			1.

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

Aura® System Manager 8.0	🛔 Users 🗸 🎤 Elements 🗸 🏘 Services	√   Widgets ✓	Shortcuts v				Sear	ch 🔰 🐥 🗏	admin
Home Routing									
Routing ^	Routing Policy Details				Comm	it Cancel			Help ?
Domains									
Locations	General	* Name: To_	ASBC						- 1
Conditions		Disabled:							
Adaptations ^		* Retries: 0 Notes:							- 1
Adaptations	SIP Entity as Destination								- 1
Regular Expres	Select								
SIP Entities	Name AvayaSBC	FQDN or IP Addres 10.89.33.13	55				Type Other	Notes	
Entity Links	Time of Day								
Time Ranges	Add Remove View Gaps/Overlaps								
	1 Item 🛛							Filter	: Enable
Routing Policies	Ranking A Name Mon	Tue Wed	Thu Fri	Sat	Sun	Start Time	End Time	Notes	
Dial Patterns 🔨	Select : All, None	V V	<u>v</u>		2	00:00	23:59	Time Range 24/7	

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**

AVAYA Aura © System Manager 8.0	Jsers 🗸 🌶 Elements 🗸 🌣 Services 🗸 🏻	Nidgets Y Shortcuts Y		Search	🜲 🗮   admin
Home Routing					
Routing	Dial Pattern Details		Commit Cancel		Help ?
Domains	General				
Locations	*1	Pattern: 750			
Conditions		* Min: 4			
Adaptations ^	Emerger	* Max: 12			
Adaptations	SIP	omain: -ALL-			
Regular Expres		Notes:			
SIP Entities	Originating Locations and Routing Poli	cies			
Entity Links	1 Item 2				Filter: Enable
Time Ranges	Originating Location Name 🔺 Originating Lo	cation Notes Routing Policy Name R	ank Routing P Disable	olicy Routing Policy Destination	Routing Policy Notes
	Lab133-Plano Lab133	to_CM(TCP)	0	Lab133CM_SIP_TCP	
Routing Policies	Select : All, None				
Dial Patterns 🔨	Denied Originating Locations				
Dial Patterns	Add Remove				
Origination Dia	Originating Location			Notes	
Ransılar Fynnassinne			Commit Cancel		

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**

Avra © Syste	aya a em Manager 8.0	Users v	🗲 Elements 🗸 🔅 Serv	rices ~   Widgets ~	Shortcuts 🗸			Se	earch	🜲 🗮   adr	min
Home	Routing										
Routing	^ ^	Dial	Pattern Details			Commit 0	Cancel			He	lp ?
Dom	nains	Gener	ral								
Loca	itions			* Pattern: 800	9						
Cond	ditions			* Min: 5							
Adar	ntations A			* Max: 12							
- Coop				Emergency Call:							
1.00	Adaptations			SIP Domain: -AL	L- V						
	Regular Expres			Notes:							
cin c		Origin	nating Locations and R	outing Policies							
SIPE	indues	Add	Remove								
Entit	ty Links	1 Item	2							Filter: Enab	le
Time	Ranges		Originating Location Name 🔺	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy	Destination	Routing Policy Note	es
	-		Lab133-Plano	Lab133	To_ASBC	0		AvayaSBC			
Rout	Routing Policies Select : All, None										
Dial	Patterns ^	Denie	d Originating Location	15							
	Dial Pattome	Add	Remove								
	Dial Patterns	0 Item	s 🥲								
	Origination Dia	0 OI	riginating Location					Note	5		
Regu	ular Expressions					Commit 0	Cancel				

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 V Diagnostics	Users Settings • Help • Log Out
EMS Lab126-ASBCE	er Controller for	Enterprise	AVAYA
EMS Dashboard	Dashboard		A
Device Management	Information		Installed Devices
<ul> <li>System Parameters</li> </ul>	System Time	10:09:22 AM Refresh	EMS
Configuration Profiles	Version	8.0.0.0-19-16991	Lab126-ASBCE
<ul> <li>Services</li> <li>Domain Policies</li> </ul>	Build Date	Sat Jan 26 21:58:11 UTC 2019	
TLS Management	License State	Ø OK	
<ul> <li>Network &amp; Flows</li> <li>DMZ Services</li> </ul>	Aggregate Licensing Overages	s 0	
<ul> <li>Monitoring &amp; Logging</li> </ul>	Peak Licensing Overage Coun	nt O	
5 55 5	Last Logged in at	10/24/2019 10:00:18 CDT	
	Failed Login Attempts	0	
	Active Alarms (past 24 hours)	_	Incidents (past 24 hours)
	None found.		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
			Lah126 ACDCE: Canazal Mathed pat allowed Out Of Dialaz

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

Session Borde	er Controlle	r for Enterprise	9	Αναγα
EMS Dashboard Device Management	Interworking Pr     Add	rofiles: avaya-ru		Clone
Backup/Restore		Clone Profile		x einstead.
Configuration Profiles	Profile Name	avaya-ru		Tan Advanced
Domain DoS Server	Clone Name	Lab126ASM		Advanced
Interworking Media Forking		Finish		
Routina	Comcast	Iou Handling	None	
Topology Hiding	Avaya_SM_to	181 Handling	None	
Signaling	Vodafone_NL	182 Handling	None	
Manipulation	Vodafone	183 Handling	None	
URI Groups	Lab126ASM	Refer Handling	No	
Time of Day Rules	To AmazonCVC	URI Group	None	
FGDN Groups	- AudioCodes	Send Hold	No	
Reverse Proxy		Delayed Offer	No	
Policy		3xx Handling	No	

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

Property of tekVizionLabs - 95



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@ ping@10.89.33.13, **To URI** as ping@10.89.33.7

Device: Lab126-ASBCE 🗸	Alarms Incidents S	tatus 🛩 Logs 🛩 Diagno: Edit SIP Server Profile - He	stics Users artbeat	Settings ❤ Help ❤ Log Out X
Session Borde	Enable Heartbeat			Αναγα
	Method	OPTIONS V		
Routing	Frequency	30	seconds	
Topology Hiding	From URI	ping@10.89.33.1	3	Rename Clone Delete
Signaling Manipulation	To URI	ping@10.89.33.7		ivanced
URI Groups		Finish		
SNMP Traps		1 11131		
Time of Day Rules	CNoIP	Frequency	30 seconds	
FGDN Groups	GENBAND			
Reverse Proxy Policy	Comcast	From URI	ping@10.89.33.13	
<ul> <li>Services</li> </ul>	Vodafone		ping@10.89.33.7	
SIP Servers	IPC		Edit	
LDAP	Avaya_SM			, ,
RADIUS	AudioCodesSi			
<ul> <li>TLS Management</li> </ul>	AmazonCVC			
A Network & Flows				
Network				
Management				
Media Interface	-			
				e

Figure 139 - Add SIP Server – Avaya SM

### 15. Select Ping

16. Keep the parameters at default values

Device: Lab126-ASBCE ∽ A	Alarms Incidents	Status 🗸 🛛 Logs 🗸	Diagnostics	Users	Settings 🗸	Help 🖌 Log Out
Session Borde	r Controlle	er for Ente	erprise			Αναγα
Routing	SIP Servers: A	waya_SM				
Topology Hiding	Add				Rename	Clone Delete
Signaling Manipulation	Server Profiles	General Authe	ntication Heart	beat Registration Pin	Advanced	
URI Groups	QLIEX	Enable Ping				
SNMP Traps	VoV					
Time of Day Rules	CNoIP			Edit		
FGDN Groups	GENBAND					
Reverse Proxy Policy	Comcast					
<ul> <li>Services</li> </ul>	Vodafone					
SIP Servers	IPC					
LDAP	Avava SM					
RADIUS	Avaya_Sim					
Domain Policies	AudioCodesSi					
▶ TLS Management	AmazonCVC					
A Network & Flows						
Network Management						
Media Interface						

Figure 140 - Add SIP Server – Avaya SM

# 17. Select **Advanced**

18. Keep the parameters at default values

Device: Lab126-ASBCE 🗸	Alarms Incidents	Status 🗙 Logs 🖌 Diagnostics	Users	Settings 🗸	Help 🖌 Log Out
Session Borde	er Controlle	r for Enterprise			AVAYA
Routing	SIP Servers: A	vaya_SM			
Topology Hiding	Add			Rename	Clone Delete
Signaling Manipulation	Server Profiles	General Authentication Heartb	eat Registration Ping	Advanced	
URI Groups		Enable DoS Protection			
SNMP Traps	VoV	Enable Grooming			
Time of Day Rules	CNoIP	Lindble Grooming			
FGDN Groups	GENBAND	Interworking Profile	None		
Reverse Proxy	Comcast	Signaling Manipulation Script	None		
<ul> <li>Services</li> </ul>	Vodafone	Securable			
SIP Servers	IPC	Enable FGDN			
LDAP	Avava SM	Tolerant			
RADIUS	AudioCodesCi				
Domain Policies	AudioCodesSI	URI Group	None		
TLS Management	AmazonCVC		Edit		
<ul> <li>Network &amp; Flows</li> </ul>					
Network Management					
Media Interface	•				

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



Figure 142 - Add SIP Server – AudioCodes

### 9. Select Authentication

10. Keep the parameters at default values

Device: Lab126-ASBCE 🗸	Alarms	Incidents	Status 🗸	Logs 🗸	Diagnos	tics Us	sers	Settin	gs 🗸	Help 🗸	Log Out
EMS	or Co	ontroll	or for	Ento	rnrie	0				Δ\	/^//
LaD120-ASDCE		JIIIOII		Line	ihua	C				<i>2</i> \v	<i>F</i> (y <i>F</i> (
EMS Dashboard	SIF	Servers:	AudioCo	desSipS	erver						
Device Management		Add							Rename	Clone	Delete
Backup/Restore System Parameters	Ser	ver Profiles	General	Authentie	cation H	leartbeat	Registration	Ping	Advance	d	
Configuration Profiles			Server	Туре		Tr	unk Server				
<ul> <li>Services</li> </ul>			SID Do	main		la la	h tekvizien eem				
SIP Servers			SIP D0	main		Ia	D.tekvizion.com				
LDAP			DNS Q	uery Type		N	ONE/A				
RADIUS			IP Add	ress / FQDN			Port		Trar	isport	
Domain Policies			10.64.3	3.10			5064		UDF	)	
TLS Management							Edit				
Network & Flows							Edit				
<ul> <li>DIMZ Services</li> <li>Magitaring &amp; Lagging</li> </ul>	Au	dioCodes									
	Ava	ava SM									
		/									
	1										

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 🗸	Diagnosti	cs U	sers	Setting	gs <b>∨</b> H	elp 🗸	Log Out
EMS											
Lab126-ASBCE	ler Co	ontroll	er for	Ente	rprise	•				A۷	ΆYA
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	Ser Ser Au	Servers: Add ver Profiles	AudioCo General Enable Met Fre Fro To I	desSipSo Authentic Heartbeat hod quency m URI JRI	erver ation He	artbeat O 30 pi	Registration PTIONS D seconds ng@10.64.5.57 ng@10.64.3.10 Edit	Ping	Rename Advanced	Clone	Delete

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

Device: Lab126-ASBCE ✔	Alarms	Incidents	Status 🗸	Logs 🗸	Diagnos	stics U	lsers	Settin	gs 🗸	Help 🗸	Log Out
Session Bord	ler Co	ontroll	er for	Ente	rpris	e				A	/AYA
EMS Dashboard	SIF	Servers:	AudioCo	desSipS	erver						
Device Management		Add							Renan	ne Clone	Delete
Backup/Restore	0.	Deeflee									
System Parameters	Se	rver Profiles	General	Authentic	cation	leartbeat	Registration	Ping	Advan	ced	
Configuration Profiles			Enable	DoS Protecti	ion	ſ					
<ul> <li>Services</li> </ul>							_				
SIP Servers			Enable	Grooming		6	✓				
LDAP			Interwo	orking Profile		N	lone				
RADIUS			Signali	ng Manipulati	ion Script	N	lone				
Domain Policies			0	5 I			_				
TLS Management			Secura	DIE		l					
Network & Flows			Enable	FGDN		ĺ					
DMZ Services	Au	dioCodes	Tolerar	ıt		ſ	-				
Monitoring & Logging			1101.0								
			URIG	oup		N	lone				
	Av	aya_SM					Edit				

#### 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.

Session Border Controller for Enterprise         Evis Lasribuard         Device Management         Backup/Restore         • System Parameters         • Configuration Profiles         Domain DoS         Server Intervorking         Media Forking         Routing         Topology Hiding         Signaling         Manipulation         URI Groups         SNMP Traps         Time of Day Rules         FOD Norphice         FOD Norphice         Domain DoS         Signaling         Manipulation         URI Groups         SNMP Traps         Time of Day Rules         FOD Norphice         FOD Norphice         Downin Day         Severe Proxy         Policy	Log Out
ENVS Dasribuoard         Device Management         Backup/Restore         System Parameters         Configuration Profiles         Domain DoS         Server Interworking         Media Forking         Routing         Signaling         Manipulation         URI Groups         SNMP Traps         Time of Day Rules         FGDN Groups         Reverse Proxy         Policy	/AYA
It is not recommended to edit the defaults. Try cloning or adding a new profile instead.         It is not recommended to edit the defaults. Try cloning or adding a new profile instead.         It is not recommended to edit the defaults. Try cloning or adding a new profile instead.         Domain DoS         Server Interworking         Media Forking         Routing         Topology Hiding         Signaling         Manipulation         URI Groups         SNMP Traps         Time of Day Rules         FGDN Groups         Reverse Proxy         Policy	
Server Interworking Media Forking RoutingHeaderCriteriaReplace ActionOverwrite ValueTopology Hiding Signaling ManipulationToIP/DomainAutoViaIP/DomainAutoIP/DomainAutoURI Groups SNMP Traps Time of Day Rules FGDN Groups Reverse Proxy PolicyIP/DomainAutoRecord-RouteIP/DomainAutoIP/DomainSDPIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoRecord-RouteIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAutoSupportIP/DomainAuto <t< td=""><td></td></t<>	
Media Forking       To       IP/Domain       Auto          Routing       From       IP/Domain       Auto          Topology Hiding       Signaling       IP/Domain       Auto          Signaling       IP/Domain       Auto        IP/Domain         URI Groups       Referred-By       IP/Domain       Auto          SNMP Traps       Referred-By       IP/Domain       Auto          Refer-To       IP/Domain       Auto          Record-Route       IP/Domain       Auto          SDP       IP/Domain       Auto          SDP       IP/Domain       Auto	
RoutingFromIP/DomainAutoTopology HidingSignalingRequest-LineIP/DomainAutoSignalingIP/DomainAutoIP/DomainAutoIP/DomainURI GroupsReferred-ByIP/DomainAutoIP/DomainSNMP TrapsReferred-ByIP/DomainAutoIP/DomainTime of Day RulesRefer-ToIP/DomainAutoIP/DomainReverse ProxySDPIP/DomainAutoIP/DomainPolicyIP/DomainAutoIP/DomainIP/Domain	
Topology Hiding Signaling ManipulationRequest-LineIP/DomainAutoURI GroupsViaIP/DomainAutoSNMP Traps Time of Day RulesReferred-ByIP/DomainAutoFGDN GroupsRefer-ToIP/DomainAutoReverse Proxy PolicySDPIP/DomainAuto	
Signaling ManipulationViaIP/DomainAutoURI GroupsReferred-ByIP/DomainAutoSNMP TrapsIP/DomainAutoTime of Day RulesRefer-ToIP/DomainAutoFGDN GroupsRecord-RouteIP/DomainAutoReverse Proxy PolicySDPIP/DomainAuto	
URI Groups     Referred-By     IP/Domain     Auto        SNMP Traps     Refer-To     IP/Domain     Auto        Time of Day Rules     Record-Route     IP/Domain     Auto        FGDN Groups     SDP     IP/Domain     Auto        Olicy     SDP     IP/Domain     Auto	
SNMP Traps     Refer-To     IP/Domain     Auto        Time of Day Rules     Record-Route     IP/Domain     Auto        FGDN Groups     SDP     IP/Domain     Auto        SDP     IP/Domain     Auto	
Time of Day Rules     Record-Route     IP/Domain     Auto        FGDN Groups     SDP     IP/Domain     Auto        Policy     Policy     SDP     IP/Domain     Auto	
FGDN Groups     SDP     IP/Domain     Auto       Policy     Figure 1000     Figure 1000     Figure 1000	
Policy SUP IP/Domain Auto	
Policy	
Edit	
SIF Servers	

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 Bord	der Co	ontroll	er for	Ente	rprise			A۷	/AYA
EMS Dashboard Device Management	- Тој	oology Hid	ling Profile	es: Avay	/a_SM		Rena	ame Clone	Delete
Backup/Restore ▶ System Parameters	Το	pology Hiding			Clic	k here to add a des	cription.		
Configuration Profiles     Domain DoS	Pr	onies	Topology	' Hiding					
Server Interworking			Header		Criteria	Replac	ce Action (	Overwrite Value	e
Media Forking			То		IP/Domain	Overw	rite I	ab.tekvizion.cc	m
Routing			From		IP/Domain	Overw	rite I	ab.tekvizion.cc	om
Topology Hiding			Reques	t-Line	IP/Domain	Overw	rite I	ab.tekvizion.co	om
Signaling Manipulation	15		· ·			Edit			
URI Groups	Av	aya_SM							
SNMP Traps									
Time of Day Rules									
FGDN Groups									
Reverse Proxy Policy									
<ul> <li>Services</li> </ul>									
010 0	•								

# 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**

	Prot	file : Avaya_SM - Edit Rule	X
URI Group	* •	Time of Day	default ▼
Load Balancing	Priority •	NAPTR	
Transport	None V	LDAP Routing	
LDAP Server Profile	None T	LDAP Base DN (Search)	None T
Matched Attribute Priority		Alternate Routing	
Next Hop Priority		Next Hop In-Dialog	
Ignore Route Header			
ENUM		ENUM Suffix	
			Add
Priority LDAP Search / Attribute Weight	LDAP Search Regex Pattern	LDAP Search SIP Server Regex Result Profile	Next Hop Address Transport
1		Avaya_S 🔻	10.89.33.7:5060  None  Delete
		Finish	

Figure 149 - Routing Profile – Avaya SM

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

	Profile :	AudioCodes_RP - Edit Ru	le			Х
URI Group	* •	Time of Da	ý	default <b>T</b>		
Load Balancing	Priority •	NAPTR				
Transport	None *	LDAP Rout	ing			
LDAP Server Profile	None <b>*</b>	LDAP Base	DN (Search)	None <b>T</b>		
Matched Attribute Priority		Alternate R	outing			
Next Hop Priority		Next Hop Ir	n-Dialog			
Ignore Route Header						
ENUM		ENUM Suff	ix			
						Add
Priority / 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 V	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 **defaul**t 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 Sta	atus 🗙 🛛 Lo	gs 🗸 🛛 Diagnos	tics Use	ers		Setti	ngs 🗸	Help 🛰	<ul> <li>Log Out</li> </ul>
EMS	or Controller	for E	ntornric	•					^	\//\//
			Interpris	C					-	.v <i>F</i> \y <i>F</i> \
EMS Dashboard	Signaling Rules:	Avaya_S	SM							
Device Management	Add							Rename	Clor	e Delete
Backup/Restore	Signaling Rules				Click here to ad	d a description				
System Parameters	default				Olick Here to ad	d a description.				
Configuration Profiles		General	Requests Res	sponses	Request Headers	Response H	leaders	Signaling Q	lo <b>S</b> l	JCID
<ul> <li>Services</li> <li>Demain Policies</li> </ul>	No-Content-Type					Add In Head	ler Control	Add Out H	leader (	Control
Application Rules	Comcast Crestron	Row H	leader Name	Method Name	Header Criteria	Action I	Proprietary	Direction		
Media Rules	Avaya_SM	1 A	V-Global-Session- )	ALL	Forbidden	Remove , Header	Yes	IN	Edit	Delete
Security Rules Signaling Rules	test	2 E	ndpoint-View	ALL	Forbidden	Remove , Header	Yes	IN	Edit	Delete
Charging Rules End Point Policy		3 P	-AV-Message-Id	ALL	Forbidden	Remove , Header	Yes	IN	Edit	Delete
Groups Session Policies		4 P	-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
<ul> <li>TLS Management</li> <li>Network &amp; Flows</li> </ul>		5 P	-Location	ALL	Forbidden	Remove , Header	Yes	IN	Edit	Delete
<ul> <li>DMZ Services</li> </ul>		6 F	leason	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
Monitoring & Logging		7 A	lert-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 <u>Incidents</u> Sta | atus 🗸 | Logs 🗸 🛛 Diag            | nostics U        | sers           |                    |                  | Setti        | ings 🗸      | Help   | 🗙 Lo    | g Out |
|-----------------------------------------------------------------|-----------------------------|--------|--------------------------|------------------|----------------|--------------------|------------------|--------------|-------------|--------|---------|-------|
| Session Borde                                                   | er Controller               | for    | Enterpr                  | ise              |                |                    |                  |              |             | 4      |         | γA    |
| EMS Dashboard<br>Device Management                              | Signaling Rules:            | Avaya  | _SM                      |                  |                |                    |                  |              | Renam       | e Clo  | ne De   | lete  |
| Backup/Restore                                                  | Signaling Rules             |        |                          |                  | Click          | here to add        | a descriptio     | 1.           |             |        |         |       |
| Configuration Profiles                                          | default                     | Genera | al Requests              | Responses        | Reques         | st Headers         | Response         | e Headers    | Signaling ( | QoS    | UCID    |       |
| <ul> <li>Services</li> <li>Domain Policies</li> </ul>           | No-Content-Type             |        |                          |                  | -              |                    | Add In He        | ader Control | Add Out     | Header | Control |       |
| Application Rules                                               | Crestron                    | Row    | Header Name              | Response<br>Code | Method<br>Name | Header<br>Criteria | Action           | Proprietary  | Direction   |        |         |       |
| Media Rules                                                     | Avaya_SM                    | 1      | P-Location               | 1XX              | ALL            | Forbidden          | Remove<br>Header | Yes          | IN          | Edit   | Delete  |       |
| Security Rules Signaling Rules                                  | test                        | 2      | Endpoint-View            | 1XX              | ALL            | Forbidden          | Remove<br>Header | Yes          | IN          | Edit   | Delete  |       |
| Charging Rules<br>End Point Policy                              |                             | 3      | P-Location               | 2XX              | ALL            | Forbidden          | Remove<br>Header | Yes          | IN          | Edit   | Delete  |       |
| Groups<br>Session Policies                                      |                             | 4      | AV-Global-<br>Session-ID | 1XX              | ALL            | Forbidden          | Remove<br>Header | Yes          | IN          | Edit   | Delete  |       |
| <ul> <li>TLS Management</li> <li>Network &amp; Flows</li> </ul> |                             | 5      | AV-Global-<br>Session-ID | 2XX              | ALL            | Forbidden          | Remove<br>Header | Yes          | IN          | Edit   | Delete  |       |
| <ul> <li>DMZ Services</li> </ul>                                |                             | 6      | P-AV-Message-<br>Id      | 1XX              | ALL            | Forbidden          | Remove<br>Header | Yes          | IN          | Edit   | Delete  |       |
| Monitoring & Logging                                            |                             | 7      | P-AV-Message-<br>Id      | 2XX              | ALL            | Forbidden          | Remove<br>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.

Device: Lab126-ASBCE 🗸 Ala	arms Incidents S	Status 🗸 🛛 Lo	gs 🗸 🛛 Diagn	ostics U	sers			Settings 🗸	Help 🗸	Log Out
Session Border	Controlle	r for E	nterpri	se					A۱	/AYA
<ul> <li>Services</li> <li>Domain Policies</li> </ul>	Policy Groups default-low				Click her Hover over a	e to add a deso row to see its (	cription. description.			_
Border Rules Media Rules	default-low-enc default-med	Policy Gro	oup						Sum	mary
Security Rules Signaling Rules Charging Rules	default-med-enc default-high default-high-enc	Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
End Point Policy Groups Session Policies	avaya-def-low-enc avaya-def-high-s	1	default	default	default- low-med	default-low	Crestron	None	Off	Edit
<ul> <li>TLS Management</li> <li>Network &amp; Flows</li> </ul>	avaya-def-high-s Avaya_SM									
Management Media Interface Signaling Interface	Vodafone Comcast									
End Point Flows Session Flows	IPC AmazonCVC									
Advanced Options	Crestron_PG									•

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

	Alarms Inclue	nts Status 🗸	Logs 🗸	Diagnostic	Users			Settings V	Help 🗸	Log Out
Session Bord	er Contr	oller for	Ente	rprise					A	VAYA
EMS Dashboard Device Management Backup/Restore	<ul> <li>Policy Gr</li> </ul>	oups: Avaya	_SM					Renam	ne Clone	Delete
<ul> <li>System Parameters</li> <li>Configuration Profiles</li> <li>Services</li> </ul>	Policy Grou default-low default-low-	enc Polic	y Group		Click I Click he	nere to add a des re to add a row d	cription. escription.			
Domain Policies     Application Rules     Border Rules     Media Rules	default-med default-med default-high	enc	ler App	lication Bor	er Media	Security	Signaling	Charging	Sum RTCP Mon Gen	mary
Security Rules Signaling Rules Charging Rules	default-high avaya-def-lo	enc 1	defa	ault defa	ult default- low-me	d default-low	Avaya_SM	None	Off	Edit
End Point Policy Groups Session Policies	avaya-def-h	gh-s								
<ul> <li>TLS Management</li> <li>Network &amp; Flows Network Management Media Interface</li> </ul>										

Figure 154 - End Point Policy Group – Avaya SM

#### 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

Device: Lab126-ASBCE	<ul> <li>Alarms</li> </ul>	Incidents S	Status 👻 Logs 🗸	Diagnostics	Users	Sett	ings 🗸	Help 🗸	Log Out
Session Bor	Session Border Controller for Enterprise								
Domain Policies     Application Rules     Border Rules     Media Rules     Security Rules	^ M	edia Interface	e						
Signaling Rules									Add
Charging Rules		Name		Media IP Network		Port Range			
End Point Policy Groups		Med_LAN		<b>10.89.33</b> LAN-A1 (A1	.13 1. VLAN 0)	35000 - 40000		Edit	Delete
Session Policies		Med_WAN		192.65.7 WAN-B1 (В	9.204 11, VLAN 0)	35000 - 40000		Edit	Delete
<ul> <li>Network &amp; Flows</li> <li>Network</li> <li>Management</li> <li>Media Interface</li> </ul>	•								

#### 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 ∽	Alarm	s Incidents	Status 🗸	Logs 🗸	Diagnostics	Users			Sett	tings 🗸	Help 🗸	Log Out
EMS Lab126-ASBCE	ler C	ontroll	er for	Ente	rprise						A۱	/AYA
<ul> <li>Domain Policies</li> <li>Application Rules</li> <li>Border Rules</li> <li>Media Rules</li> </ul>	^ S	ignaling Inte	erface									
Security Rules												Add
Charging Rules		Name		Signaling IP		TCP Port	UDP Port	TLS Port	TLS Profile			
End Point Policy Groups		SIG_LAN		10.89.33.13 LAN-A1 (A1, V	LAN 0)		5060		None		Edit	Delete
Session Policies TLS Management		SIG_WAN		192.65.79.2 WAN-B1 (B1, \	04 /LAN 0)		5060		None		Edit	Delete
<ul> <li>Network &amp; Flows Network Management Media Interface Signaling Interface End Point Flows</li> </ul>	•											

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**

Device: Lab126-ASBCE V Alarms	Incidents Status 🗙 Logs 🗸	Diagnostics Users Edit Elour Avava SM	Settings 🕶 Help 👻 Log Out 🔺
		Luction. Avaya Sm	
Session Border C	Flow Name	Avaya SM	AVAYA
	SIP Server Profile	Avaya_SM 🔻	
Media Rules	URI Group	× •	
Security Rules	Transport	UDP V	
Signaling Rules Charging Rules	Remote Subnet	*	
End Point Policy	Received Interface	SIG_WAN V	Add
Session Policies	Signaling Interface	SIG_LAN •	
TLS Management	Media Interface	Med_LAN •	
<ul> <li>Network &amp; Flows</li> <li>Network</li> </ul>	Secondary Media Interface	None •	na
Management	End Point Policy Group	Avaya_SM 🔻	e
Media Interface	Routing Profile	AudioCodes_RP V	a_SM View Clone Edit Delete
End Point Flows	Topology Hiding Profile	Avaya_SM 🔻	
Session Flows	Signaling Manipulation Script	None 🔻	ofile
Advanced Options DMZ Services	Remote Branch Office	Any <b>v</b>	s_RP View Clone Edit Delete
▹ Monitoring & Logging	Link Monitoring from Peer		·····································

Figure 157 - Server Flow

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

Device: Lab126-ASBCE V Alarms	s Incidents Status ∽ Loqs ∽ E	Diagnostics Users dit Flow: AudioCodes	Settings ❤ H	elp 👻 Log Out 🔶
Session Border C	Flow Name	AudioCodes		AVAYA
Media Rules E Security Rules	URI Group Transport			
Signaling Rules Charging Rules End Point Policy	Remote Subnet Received Interface	SIG_LAN •		Add
Groups Session Policies > TLS Management	Signaling Interface Media Interface	SIG_WAN • Med_WAN •		
<ul> <li>Network &amp; Flows</li> <li>Network</li> <li>Management</li> </ul>	Secondary Media Interface End Point Policy Group	None  Crestron_PG	ng e	
Signaling Interface	Routing Profile Topology Hiding Profile	Avaya_SM    default	a_SM View Clone	
Advanced Options <ul> <li>DMZ Services</li> </ul>	Signaling Manipulation Script Remote Branch Office	None   Any	ofile s_RP View Clone	Edit Delete
Monitoring & Logging	Link Monitoring from Peer			

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> <li>Make a voice call from Teams user to PBX A user</li> <li>Teams user hears Ring back Tone</li> <li>PBX A user answers the call</li> <li>Verify two way audio</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> <li>Repeat steps 1 to 4</li> <li>PBX A user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is connected with bi-directional audio, voice is clear, no echo</li> <li>Call is disconnected</li> </ol>	PASSED	
2	Teams user Calls PBX B user	<ol> <li>Make a voice call from Teams user to PBX B user</li> <li>Teams user hears Ring back Tone</li> <li>PBX B user answers the call</li> <li>Verify two way audio</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> <li>Repeat steps 1 to 4</li> <li>PBX B user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is connected with bi-directional audio, voice is clear, no echo</li> <li>Call is disconnected</li> </ol>	NOT APPLICABLE	This testing is for only one PBX with Teams
3	Teams user Calls PSTN user	<ol> <li>Make a voice call from Teams user to PSTN user</li> <li>Teams user hears Ring back Tone</li> <li>PSTN user answers the call</li> </ol>	1. Call is connected with bi-directional audio, voice is clear, no echo	PASSED	

External	Title	Procedure	Expected Results	Status	Comments
ID					
		4. Verify two way audio	2. Call is		
		5. Teams user hangs up the call	disconnected		
		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			
4	Teams user	1. Make a voice call from Teams user to	1. Call is		
	Calls PBX A	PBX A user	disconnected before		
	user and	2. PBX A user starts ringing	answer		
	hangs up	3. Teams user hears Ring back Tone			
	before	4. Teams user hangs up the call while		PASSED	
	answer	PBX A user is ringing			
		5. PBX A user stops ringing			
		6. Verify call is cleared successfully			
5	Teams user	1. Make a voice call from Teams user to	1. Call is		This testing is for
	Calls PBX B	PBX B user	disconnected before		only one PBX with
	user and	2. PBX B user starts ringing	answer		Teams
	hangs up	3. Teams user hears Ring back Tone		NOT	
	before	4. Teams user hangs up the call while		APPLICABLE	
	answer	PBX B user is ringing			
		5. PBX B user stops ringing			
		6. Verify call is cleared successfully			

External	Title	Procedure	Expected Results	Status	Comments
ID C	Teamsuser	1. Make a vision call from Teams upor to	1 Callia		
0		DSTN user	I. Call IS		
	Lalis PSTN	2 DSTN user starts ringing	answor		
		2. Tooms user boors Ding back Topo	aliswei		
	hangs up	4. Teams user hangs up the call while		PASSED	
	Delore	A. Teams user hangs up the call while			
	answei	5 DSTN user stops ringing			
		6. Verify call is cleared successfully			
	DDV Augor	1. Make a voice call from DBX A user to	1 Call is connected		
/	PDA A USEI		with hi directional		
		2 DBX A user bears Ding back Tone			
	user	2. PBA A user field's Ring back folle	audio, voice is clear,		
		4. Vorify two way audio			
		4. Verify two way audio	Z. Call IS	PASSED	
		6. Verify call is cleared successfully	disconnected		
		7. Depend stops 1 to 4			
		7. Repeat steps 1 to 4			
		0. Verify call is cleared successfully			
		9. Verify call is cleared successfully			
8	PBX B user	T. Make a voice call from PBX B user to	1. Call is connected		This testing is for
	Calls reams	2 DBX D year bears Ding back Tana	with bi-directional		only one PBX with
	user	2. PBX B user nears Ring back Tone	audio, voice is clear,		reams
		3. Teams user answers the call	no ecno	NOT	
		4. Verify two way audio	2. Call is		
		5. PBX B user hangs up the call	disconnected	APPLICABLE	
		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			

External ID	Title	Procedure	Expected Results	Status	Comments
9	PSTN user Calls Teams user	<ol> <li>Make a voice call from PSTN user to Teams user</li> <li>PSTN user hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>PSTN user hangs up the call</li> <li>Verify call is cleared successfully</li> <li>Repeat steps 1 to 4</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is connected with bi-directional audio, voice is clear, no echo</li> <li>Call is disconnected</li> </ol>	PASSED	
10	PBX A user Calls Teams user and hangs up before answer	<ol> <li>Make a voice call from PBX A user to Teams user</li> <li>Teams user starts ringing</li> <li>PBX A user hears Ring back Tone</li> <li>PBX A user hangs up the call while</li> <li>Teams user is ringing</li> <li>Teams user stops ringing</li> <li>Verify call is cleared successfully</li> </ol>	1. Call is disconnected before answer	PASSED	
11	PBX B user Calls Teams user and hangs up before answer	<ol> <li>Make a voice call from PBX B user to Teams user</li> <li>Teams user starts ringing</li> <li>PBX B user hears Ring back Tone</li> <li>PBX B user hangs up the call while</li> <li>Teams user is ringing</li> <li>Teams user stops ringing</li> <li>Verify call is cleared successfully</li> </ol>	1. Call is disconnected before answer	NOT APPLICABLE	This testing is for only one PBX with Teams

External	Title	Procedure	Expected Results	Status	Comments
12	PSTN user Calls Teams user and hangs up before answer	<ol> <li>Make a voice call from PSTN user to Teams user</li> <li>Teams user starts ringing</li> <li>PSTN user hears Ring back Tone</li> <li>PSTN user hangs up the call while</li> <li>Teams user is ringing</li> <li>Teams user stops ringing</li> <li>Verify call is cleared successfully</li> </ol>	1. Call is disconnected before answer	PASSED	
13	Teams user Calls PBX A user and performs hold/resume	<ol> <li>Make a voice call from Teams user to PBX A user</li> <li>Teams user hears Ring back Tone</li> <li>PBX A user answers the call</li> <li>Verify two way audio</li> <li>Teams user initiates call hold</li> <li>Verify no audio is present while call is on hold</li> <li>Teams user resumes the call</li> <li>Verify two way audio is re-established between the two end points</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is placed on hold successfully</li> <li>No audio present during hold</li> <li>Call is resumed successfully</li> <li>Two way audio present after call is resumed</li> </ol>	PASSED	
14	Teams user Calls PBX B user and performs hold/resume	<ol> <li>Make a voice call from Teams user to PBX B user</li> <li>Teams user hears Ring back Tone</li> <li>PBX B user answers the call</li> <li>Verify two way audio</li> <li>Teams user initiates call hold</li> <li>Verify no audio is present while call is</li> </ol>	<ol> <li>Call is placed on hold successfully</li> <li>No audio present during hold</li> <li>Call is resumed successfully</li> <li>Two way audio</li> </ol>	NOT APPLICABLE	This testing is for only one PBX with Teams

External	Title	Procedure	Expected Results	Status	Comments
ID 15	Teams user Calls PSTN user and performs hold/resume	<ul> <li>on hold</li> <li>7. Teams user resumes the call</li> <li>8. Verify two way audio is re-established between the two end points</li> <li>9. Teams user hangs up the call</li> <li>10. Verify call is cleared successfully</li> <li>1. Make a voice call from Teams user to PSTN user</li> <li>2. Teams user hears Ring back Tone</li> <li>3. PSTN user answers the call</li> <li>4. Verify two way audio</li> <li>5. Teams user initiates call hold</li> <li>6. Verify no audio is present while call is on hold</li> <li>7. Teams user resumes the call</li> <li>8. Verify two way audio is re-established between the two end points</li> <li>9. Teams user hangs up the call</li> </ul>	present after call is resumed 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	
16	PBX A user Calls Teams user and Teams user performs hold/resume	<ol> <li>Verify call is cleared successfully</li> <li>Make a voice call from PBX A user to Teams user</li> <li>PBX A user hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user initiates call hold</li> <li>Verify no audio is present while call is on hold</li> <li>Teams user resumes the call</li> </ol>	<ol> <li>Call is placed on hold successfully</li> <li>No audio present during hold</li> <li>Call is resumed successfully</li> <li>Two way audio present after call is resumed</li> </ol>	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	Title	Procedure	Expected Results	Status	Comments
		<ul><li>8. Verify two way audio is re-established</li><li>between the two end points</li><li>9. PBX A user hangs up the call</li><li>10. Verify call is cleared successfully</li></ul>			receiver or speaker button.
17	PBX B user Calls Teams user and Teams user performs hold/resume	<ol> <li>Make a voice call from PBX B user to Teams user</li> <li>PBX B user hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user initiates call hold</li> <li>Verify no audio is present while call is on hold</li> <li>Teams user resumes the call</li> <li>Verify two way audio is re-established between the two end points</li> <li>PBX B user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is placed on hold successfully</li> <li>No audio present during hold</li> <li>Call is resumed successfully</li> <li>Two way audio present after call is resumed</li> </ol>	NOT APPLICABLE	PBX B is not tested with this cycle
18	PSTN user Calls Teams user and Teams performs hold/resume	<ol> <li>Make a voice call from PSTN user to Teams user</li> <li>PSTN user hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user initiates call hold</li> <li>Verify no audio is present while call is on hold</li> <li>Teams user resumes the call</li> <li>Verify two way audio is re-established between the two end points</li> </ol>	<ol> <li>Call is placed on hold successfully</li> <li>No audio present during hold</li> <li>Call is resumed successfully</li> <li>Two way audio present after call is resumed</li> </ol>	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	Title	Procedure	Expected Results	Status	Comments
ID					
		9. PSTN user hangs up the call			
		10. Verify call is cleared successfully			
19	Teams user	1. Make a voice call from Teams user to	1. Call is transferred		
	Calls PBX A	PBX A user 1	successfully		
	user, Teams	2. Teams user hears Ring back Tone	2. Two way audio		
	user	3. PBX A user 1 answers the call	present after call is		
	performs	4. Verify two way audio	transferred		
	Attended	5. Teams user places a consultation call			
	Transfer to	to PBX A user 2			
	PBX A user	6. Verify PBX A user 1 is placed on hold		PASSED	
		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 nangs up the call			
20	Teeree	12. Verify call is cleared successfully	1 Collistropoformod		This testing is for
20		I. Make a voice call from reams user to			This testing is for
		2 Tooms user boors Ding back Topo	2 Two way audio		
	user, reams	2. PBY A user apswers the call	2. Two way audio		Teams
	nerforms	A Verify two way audio	transferred		
	Attended	5 Teams user places a consultation call	transierreu	NOT	
	Transfer to	to PBX Buser		APPLICABLE	
	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			

External	Title	Procedure	Expected Results	Status	Comments
ID					
		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	1. Make a voice call from Teams user to	1. Call is transferred		
		PBX A user	successfully		
	user, Teams	2. Teams user hears Ring back Tone	2. Two way audio		
	user	3. PBX A user answers the call	present after call is		
	performs	4. Verify two way audio	transferred		
	Attended	5. Teams user places a consultation call			
	Transfer to	to PSIN user		DAGGED	
	PSTN user	6. Verify PBX A user is placed on hold		PASSED	
		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 PSIN user			
		11. PBX A user hangs up the call			
	<b>.</b>				
22	Teams user	1. Make a voice call from Teams user to	1. Call is transferred		I his testing is for
		PBX B user 1	SUCCESSTUIIY		only one PBX with
	user, Teams	2. Teams user nears Ring back Tone	2. Two way audio		Teams
	user	3. PBX B user 1 answers the call	present after call is	NOT	
	performs	4. verify two way audio	transferred	APPLICABLE	
	Attended	5. Teams user places a consultation call			
	Transfer to	to PBX B user 2			
	PBX B user	6. Verity PBX B user 1 is placed on hold			
		7. PBX B user 2 answers the call			

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

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

External	Title	Procedure	Expected Results	Status	Comments
ID	Attanded	E. Teams user places a consultation call			
	Transfor to	5. Teams user places a consultation call			
		6 Vorify PSTN user is placed on hold			
	F DA A USEI	7 PRX A usor answers the call			
		8. Vorify two way audio			
		0. Tooms user completes the transfer			
		10. Vorify two way audio botwoon PSTN			
		Its verify two way addio between F31N			
		11 PSTN user bangs up the call			
		12 Verify call is cleared successfully			
27	Toomsusor	1 Make a voice call from Teams user to	1 Call is transforred		
21	Calle PCTN 1	PSTN user 1	successfully		
	LISER Teams	2 Teams user hears Ring back Tone	2 Two way audio		
	user	3 PSTN user 1 answers the call	nresent after call is		
	nerforms	4 Verify two way audio	transferred		
	Attended	5 Teams user places a consultation call	aansiened		
	Transfer to	to PSTN user 2			
	PSTN 2 user	6 Verify PSTN user 1 is placed on hold		PASSED	
		7. PSTN user 2 answers the call		17(3320	
		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			
28	PBX A user	1. Make a voice call from PBX A user 1	1. Call is transferred		
	Calls Teams	to Teams user	successfully	PASSED	
	user, Teams	2. PBX A user 1 hears Ring back Tone	2. Two way audio		

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

External	Title	Procedure	Expected Results	Status	Comments
30	PBX A user Calls Teams user, Teams user performs Attended Transfer to PSTN user	<ol> <li>Make a voice call from PBX A user to Teams user</li> <li>PBX A user hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user places a consultation call to PSTN user</li> <li>Verify PBX A user is placed on hold</li> <li>PSTN user answers the call</li> <li>Verify two way audio</li> <li>Teams user completes the transfer</li> <li>Verify two way audio between PBX A user and PSTN user</li> <li>PBX A user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is transferred successfully</li> <li>Two way audio present after call is transferred</li> </ol>	PASSED	
31	PBX B user Calls Teams user, Teams user performs Attended Transfer to PBX B user	<ol> <li>Make a voice call from PBX B user 1 to Teams user</li> <li>PBX B user 1 hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user places a consultation call to PBX B user 2</li> <li>Verify PBX B user 1 is placed on hold</li> <li>PBX B user 2 answers the call</li> <li>Verify two way audio</li> <li>Teams user completes the transfer</li> <li>Verify two way audio between PBX B user 1 and PBX B user 2</li> </ol>	<ol> <li>Call is transferred successfully</li> <li>Two way audio present after call is transferred</li> </ol>	NOT APPLICABLE	This testing is for only one PBX with Teams

External	Title	Procedure	Expected Results	Status	Comments
ID				Statas	
		11. PBX B user 1 hangs up the call			
		12. Verify call is cleared successfully			
32	PBX B user	1. Make a voice call from PBX B user to	1. Call is transferred		This testing is for
	Calls Teams	Teams user	successfully		only one PBX with
	user, Teams	2. PBX B user hears Ring back Tone	2. Two way audio		Teams
	user	3. Teams user answers the call	present after call is		
	performs	4. Verify two way audio	transferred		
	Attended	5. Teams user places a consultation call			
	Transfer to	to PBX A user		NOT	
	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			
33	PBX B user	1. Make a voice call from PBX B user to	1. Call is transferred		This testing is for
	Calls Teams	Teams user	successfully		only one PBX with
	user, Teams	2. PBX B user hears Ring back Tone	2. Two way audio		Teams
	user	3. Teams user answers the call	present after call is		
	performs	4. Verify two way audio	transferred	NOT	
	Attended	5. Teams user places a consultation call			
	Transfer to	to PSTN user			
	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			

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

External	Title	Procedure	Expected Results	Status	Comments
ID				Statas	
		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	1. Make a voice call from PSTN user 1 to	1. Call is transferred		
	Calls Teams	Teams user	successfully		
	user, Teams	2. PSTN user 1 hears Ring back Tone	2. Two way audio		
	user	3. Teams user answers the call	present after call is		
	performs	4. Verify two way audio	transferred		
	Attended	5. Teams user places a consultation call			
	Transfer to	to PSTN user 2			
	PSTN 2 user	6. Verify PSTN user 1 is placed on hold		PASSED	
		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			
37	Teams user	1. Make a voice call from Teams user to	1. Call is transferred		
	Calls PBX A	PBX A user 1	successfully		
	user, Teams	2. Teams user hears Ring back Tone	2. Two way audio		
	user	3. PBX A user 1 answers the call	present after call is	PASSED	
	performs	4. Verify two way audio	transferred		
	Unattended	5. Teams user transfers the call to PBX			
		A user 2			

External ID	Title	Procedure	Expected Results	Status	Comments
	Transfer to PBX A user	<ul> <li>6.PBX A user 2 starts ringing</li> <li>7. PBX A user 1 hears Ring back Tone</li> <li>8. PBX A user 2 answers the call</li> <li>9. Verify two way audio between PBX A user 1 and PBX A user 2</li> <li>10. PBX A user 1 hangs up the call</li> <li>11. Verify call is cleared successfully</li> </ul>			
38	Teams user Calls PBX A user, Teams user performs Unattended Transfer to PBX B user	<ol> <li>Make a voice call from Teams user to PBX A user</li> <li>Teams user hears Ring back Tone</li> <li>PBX A user answers the call</li> <li>Verify two way audio</li> <li>Teams user transfers the call to PBX</li> <li>B user</li> <li>PBX B user starts ringing</li> <li>PBX A user hears Ring back Tone</li> <li>PBX B user answers the call</li> <li>Verify two way audio between PBX A user and PBX B user</li> <li>PBX A user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is transferred successfully</li> <li>Two way audio present after call is transferred</li> </ol>	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> <li>Make a voice call from Teams user to PBX A user</li> <li>Teams user hears Ring back Tone</li> <li>PBX A user answers the call</li> <li>Verify two way audio</li> <li>Teams user transfers the call to PSTN user</li> <li>PSTN user starts ringing</li> <li>PBX A user hears Ring back Tone</li> <li>PSTN user answers the call</li> <li>Verify two way audio between PBX A user and PSTN user</li> <li>PBX A user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is transferred successfully</li> <li>Two way audio present after call is transferred</li> </ol>	PASSED	
40	Teams user Calls PBX B user, Teams user performs Unattended Transfer to PBX B user	<ol> <li>Make a voice call from Teams user to PBX B user 1</li> <li>Teams user hears Ring back Tone</li> <li>PBX B user 1 answers the call</li> <li>Verify two way audio</li> <li>Teams user transfers the call to PBX B user 2</li> <li>PBX B user 2 starts ringing</li> <li>PBX B user 1 hears Ring back Tone</li> <li>PBX B user 2 answers the call</li> <li>Verify two way audio between PBX B user 1 and PBX B user 2</li> <li>PBX B user 1 hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is transferred successfully</li> <li>Two way audio present after call is transferred</li> </ol>	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> <li>Make a voice call from Teams user to PBX B user</li> <li>Teams user hears Ring back Tone</li> <li>PBX B user answers the call</li> <li>Verify two way audio</li> <li>Teams user transfers the call to PBX</li> <li>A user</li> <li>PBX A user starts ringing</li> <li>PBX B user hears Ring back Tone</li> <li>PBX A user answers the call</li> <li>Verify two way audio between PBX B user and PBX A user</li> <li>PBX B user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is transferred successfully</li> <li>Two way audio present after call is transferred</li> </ol>	NOT APPLICABLE	This testing is for only one PBX with Teams
42	Teams userCalls PBX B user, Teams user performs Unattended Transfer to PSTN user	<ol> <li>Nake a voice call from Teams user to PBX B user</li> <li>Teams user hears Ring back Tone</li> <li>PBX B user answers the call</li> <li>Verify two way audio</li> <li>Teams user transfers the call to PSTN user</li> <li>PBX B user starts ringing</li> <li>PBX B user hears Ring back Tone</li> <li>PSTN user answers the call</li> <li>Verify two way audio between PBX B user and PSTN user</li> <li>PBX B user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is transferred successfully</li> <li>Two way audio present after call is transferred</li> </ol>	NOT APPLICABLE	This testing is for only one PBX with Teams

External	Title	Procedure	Expected Results	Status	Comments
43	Teams user Calls PSTN	1. Make a voice call from Teams user to PSTN user	1. Call is transferred successfully		This testing is for only one PBX with
	user, Teams user performs Unattended Transfer to PBX B user	<ul> <li>2. Teams user hears Ring back Tone</li> <li>3. PSTN user answers the call</li> <li>4. Verify two way audio</li> <li>5. Teams user transfers the call to PBX</li> <li>B user</li> <li>6.PBX B user starts ringing</li> <li>7. PSTN user hears Ring back Tone</li> <li>8. PBX B user answers the call</li> <li>9. Verify two way audio between PSTN user and PBX B user</li> </ul>	2. Two way audio present after call is transferred	NOT APPLICABLE	Teams
		10. PSTN user hangs up the call 11. Verify call is cleared successfully			
44	Teams user Calls PSTN user, Teams user performs Unattended Transfer to PBX A user	<ol> <li>Make a voice call from Teams user to PSTN user</li> <li>Teams user hears Ring back Tone</li> <li>PSTN user answers the call</li> <li>Verify two way audio</li> <li>Teams user transfers the call to PBX</li> <li>A user</li> <li>PBX A user starts ringing</li> <li>PSTN user hears Ring back Tone</li> <li>PBX A user answers the call</li> <li>Verify two way audio between PSTN user and PBX A user</li> <li>PSTN user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is transferred successfully</li> <li>Two way audio present after call is transferred</li> </ol>	PASSED	

External	Title	Procedure	Expected Results	Status	Comments
ID					
45	Teams user Calls PSTN 1 user, Teams user performs Unattended Transfer to PSTN 2 user	<ol> <li>Make a voice call from Teams user to PSTN user 1</li> <li>Teams user hears Ring back Tone</li> <li>PSTN user 1 answers the call</li> <li>Verify two way audio</li> <li>Teams user transfers the call to PSTN user 2</li> <li>PSTN user 2 starts ringing</li> <li>PSTN user 1 hears Ring back Tone</li> <li>PSTN user 2 answers the call</li> <li>Verify two way audio between PSTN user 1 and PSTN user 2</li> <li>PSTN user 1 hangs up the call</li> </ol>	<ol> <li>Call is transferred successfully</li> <li>Two way audio present after call is transferred</li> </ol>	PASSED	
46	PBX A user Calls Teams user, Teams user performs Unattended Transfer to PBX A user	<ol> <li>1. Werny can be cleared successfully</li> <li>1. Make a voice call from PBX A user 1 to Teams user</li> <li>2. PBX A user 1 hears Ring back Tone</li> <li>3. Teams user answers the call</li> <li>4. Verify two way audio</li> <li>5. Teams user transfers the call to PBX</li> <li>A user 2</li> <li>6.PBX A user 2 starts ringing</li> <li>7. PBX A user 1 hears Ring back Tone</li> <li>8. PBX A user 2 answers the call</li> <li>9. Verify two way audio between PBX A user 1 and PBX A user 2</li> <li>10. PBX A user 1 hangs up the call</li> <li>11. Verify call is cleared successfully</li> </ol>	<ol> <li>Call is transferred successfully</li> <li>Two way audio present after call is transferred</li> </ol>	PASSED	

External	Title	Procedure	Expected Results	Status	Comments
ID					
47	PBX A user	1. Make a voice call from PBX A user to	1. Call is transferred		This testing is for
	Calls Teams	Teams user	successfully		only one PBX with
	user, Teams	2. PBX A user hears Ring back Tone	2. Two way audio		Teams
	user	3. Teams user answers the call	present after call is		
	performs	4. Verify two way audio	transferred		
	Unattended	5. Teams user transfers the call to PBX			
	Transfer to	B user		NOT	
	PBX B user	6.PBX B user starts ringing		APPLICABLE	
		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			
48	PBX A user	1. Make a voice call from PBX A user to	1. Call is transferred		
	Calls Teams	Teams user	successfully		
	user, Teams	2. PBX A user hears Ring back Tone	2. Two way audio		
	user	3. Teams user answers the call	present after call is		
	performs	4. Verify two way audio	transferred		
	Unattended	5. Teams user transfers the call to PSTN			
	Transfer to	user		PASSED	
	PSTN user	6.PSTN user starts ringing		TASSED	
		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			

External	Title	Procedure	Expected Results	Status	Comments
49	PBX B user Calls Teams user, Teams user performs Unattended Transfer to PBX B user	<ol> <li>Make a voice call from PBX B user 1 to Teams user</li> <li>PBX B user 1 hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user transfers the call to PBX</li> <li>B user 2</li> <li>PBX B user 2 starts ringing</li> <li>PBX B user 1 hears Ring back Tone</li> <li>PBX B user 2 answers the call</li> <li>Verify two way audio between PBX B user 1 and PBX B user 2</li> <li>PBX B user 1 hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is transferred successfully</li> <li>Two way audio present after call is transferred</li> </ol>	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> <li>1. Make a voice call from PBX B user to Teams user</li> <li>2. PBX B user hears Ring back Tone</li> <li>3. Teams user answers the call</li> <li>4. Verify two way audio</li> <li>5. Teams user transfers the call to PBX</li> <li>A user</li> <li>6.PBX A user starts ringing</li> <li>7. PBX B user hears Ring back Tone</li> <li>8. PBX A user answers the call</li> <li>9. Verify two way audio between PBX B user and PBX A user</li> <li>10. PBX B user hangs up the call</li> <li>11. Verify call is cleared successfully</li> </ol>	<ol> <li>Call is transferred successfully</li> <li>Two way audio present after call is transferred</li> </ol>	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> <li>Make a voice call from PBX B user to Teams user</li> <li>PBX B user hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user transfers the call to PSTN user</li> <li>PSTN user starts ringing</li> <li>PBX B user hears Ring back Tone</li> <li>PSTN user answers the call</li> <li>Verify two way audio between PBX B user and PSTN user</li> <li>PBX B user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is transferred successfully</li> <li>Two way audio present after call is transferred</li> </ol>	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> <li>Make a voice call from PSTN user to Teams user</li> <li>PSTN user hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user transfers the call to PBX</li> <li>B user</li> <li>PBX B user starts ringing</li> <li>PSTN user hears Ring back Tone</li> <li>PBX B user answers the call</li> <li>Verify two way audio between PSTN user and PBX B user</li> <li>PSTN user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is transferred successfully</li> <li>Two way audio present after call is transferred</li> </ol>	NOT APPLICABLE	This testing is for only one PBX with Teams

External	Title	Procedure	Expected Results	Status	Comments
ID F2	DCTN		1 Call is two softwards		
53	PSTN user	T. Make a voice call from PSTN user to	1. Call is transferred		
		2 DSTN user bears Ding back Topo	2 Two way audio		
	user, reams	2. Tooms user answers the call	2. Two way audio		
	norforms	4. Verify two way audio	transforred		
	Unattended	5. Teams user transfers the call to PBX	li ansien eu		
	Transfer to	A user			
	PRX A user	6 PBX A user starts ringing		PASSED	
	1 BAA doct	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			
54	PSTN 1 user	1. Make a voice call from PSTN user 1 to	1. Call is transferred		
	Calls Teams	Teams user	successfully		
	user, Teams	2. PSTN user 1 hears Ring back Tone	2. Two way audio		
	user	3. Teams user answers the call	present after call is		
	performs	4. Verify two way audio	transferred		
	Unattended	5. Teams user transfers the call to PSTN			
	Transfer to	user 2		PASSED	
	PSTN 2 user	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			

External ID	Title	Procedure	Expected Results	Status	Comments
55	PSTN user calls Teams user, Teams user performs Unattended Transfer to second Teams user	<ol> <li>Make a voice call from PSTN user to Teams user 1</li> <li>PSTN user hears Ring back Tone</li> <li>Teams user 1 answers the call</li> <li>Verify two way audio</li> <li>Teams user 1 transfers the call to Teams user 2</li> <li>Teams user 2 starts ringing</li> <li>Teams user 2 answers the call</li> <li>Verify two way audio between PSTN user and Teams user 2</li> <li>PSTN user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Call is transferred successfully</li> <li>Two way audio present after call is transferred</li> </ol>	PASSED	
56	Teams user Calls PBX A user, Teams user adds PBX A user to the ongoing call	<ol> <li>Make a voice call from Teams user to PBX A user 1</li> <li>Teams user hears Ring back Tone</li> <li>PBX A user 1 answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PBX A user 2 to the ongoing call</li> <li>PBX A user 2 starts ringing</li> <li>PBX A user 2 answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Third user is added to the call successfully</li> <li>All three users are able to hear each other</li> </ol>	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 user Calls PBX A user, Teams user adds PBX B user to the ongoing call	<ol> <li>Make a voice call from Teams user to PBX A user</li> <li>Teams user hears Ring back Tone</li> <li>PBX A user answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PBX B user to the ongoing call</li> <li>PBX B user starts ringing</li> <li>PBX B user answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Third user is added to the call successfully</li> <li>All three users are able to hear each other</li> </ol>	NOT APPLICABLE	This testing is for only one PBX with Teams

External	Title	Procedure	Expected Results	Status	Comments
58	Teams user user Calls PBX A user, Teams user adds PSTN user to the ongoing call	<ol> <li>Make a voice call from Teams user to PBX A user</li> <li>Teams user hears Ring back Tone</li> <li>PBX A user answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PSTN user to the ongoing call</li> <li>PSTN user starts ringing</li> <li>PSTN user answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Make a voice call from Teams user to PBX B user 1</li> <li>Teams user hears Ring back Tone</li> <li>PBX B user 1 answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PBX B user 2 to the ongoing call</li> <li>PBX B user 2 starts ringing</li> <li>PBX B user 2 answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Third user is added to the call successfully</li> <li>All three users are able to hear each other</li> </ol>	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> <li>Make a voice call from Teams user to PBX B user</li> <li>Teams user hears Ring back Tone</li> <li>PBX B user answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PBX A user to the ongoing call</li> <li>PBX A user starts ringing</li> <li>PBX A user answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Third user is added to the call successfully</li> <li>All three users are able to hear each other</li> </ol>	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> <li>Make a voice call from Teams user to PBX B user</li> <li>Teams user hears Ring back Tone</li> <li>PBX B user answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PSTN user to the ongoing call</li> <li>PSTN user starts ringing</li> <li>PSTN user answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Third user is added to the call successfully</li> <li>All three users are able to hear each other</li> </ol>	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> <li>Make a voice call from Teams user to PSTN user</li> <li>Teams user hears Ring back Tone</li> <li>PSTN user answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PBX B user to the ongoing call</li> <li>PBX B user starts ringing</li> <li>PBX B user answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Third user is added to the call successfully</li> <li>All three users are able to hear each other</li> </ol>	NOT APPLICABLE	This testing is for only one PBX with Teams

External	Title	Procedure	Expected Results	Status	Comments
63	Teams user user Calls PSTN user, Teams user adds PBX A user to the ongoing call	<ol> <li>Make a voice call from Teams user to PSTN user</li> <li>Teams user hears Ring back Tone</li> <li>PSTN user answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PBX A user to the ongoing call</li> <li>PBX A user starts ringing</li> <li>PBX A user answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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

64    Teams user    1. Make a voice call from Teams user to    1. Third user is	us Comments
user CallsPSTN user 1added to the call successfullyPSTN 1 user, Teams user adds PSTN 22. 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 successfully2. All three users added to the call successfully 2. All three users are able to hear each otherImage: Display the call 11. Verify call is cleared successfullyFAILI	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 ED 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

External	Title	Procedure	Expected Results	Status	Comments
65	PBX A user Calls Teams user, Teams user adds PBX A user to the ongoing call	<ol> <li>Make a voice call from PBX A user 1 to Teams user</li> <li>PBX A user 1 hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PBX A user 2 to the ongoing call</li> <li>PBX A user 2 starts ringing</li> <li>PBX A user 2 answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Make a voice call from PBX A user to Teams user</li> <li>PBX A user hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PBXB user to the ongoing call</li> <li>PBX B user starts ringing</li> <li>PBX B user answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Third user is added to the call successfully</li> <li>All three users are able to hear each other</li> </ol>	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> <li>Make a voice call from PBX A user to Teams user</li> <li>PBX A user hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PSTN user to the ongoing call</li> <li>PSTN user starts ringing</li> <li>PSTN user answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Third user is added to the call successfully</li> <li>All three users are able to hear each other</li> </ol>	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
68	DBY B usor	1 Make a voice call from PBY B user 1	1 Third user is		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> <li>Make a voice call from PBX B user 1 to Teams user</li> <li>PBX B user 1 hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PBX B user 2 to the ongoing call</li> <li>PBX B user 2 starts ringing</li> <li>PBX B user 2 answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Make a voice call from PBX B user to Teams user</li> <li>PBX B user hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PBX A user to the ongoing call</li> <li>PBX A user starts ringing</li> <li>PBX A user answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Third user is added to the call successfully</li> <li>All three users are able to hear each other</li> </ol>	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> <li>Make a voice call from PBX B user to Teams user</li> <li>PBX B user hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PSTN user to the ongoing call</li> <li>PSTN user starts ringing</li> <li>PSTN user answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Third user is added to the call successfully</li> <li>All three users are able to hear each other</li> </ol>	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> <li>Make a voice call from PSTN user to Teams user</li> <li>PSTN user hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PBX B user to the ongoing call</li> <li>PBX B user starts ringing</li> <li>PBX B user answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Third user is added to the call successfully</li> <li>All three users are able to hear each other</li> </ol>	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> <li>Make a voice call from PSTN user to Teams user</li> <li>PSTN user hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Teams user adds PBX A user to the ongoing call</li> <li>PBX A user starts ringing</li> <li>PBX A user answers the call</li> <li>Verify all three users are able to hear each other</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Third user is added to the call successfully</li> <li>All three users are able to hear each other</li> </ol>	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	Title	Procedure	Expected Results	Status	Comments
ID					
73	PSTN 1 user	1. Make a voice call from PSTN user 1 to	1. Third user is		Crestron phone
		leams user	added to the call		does not have an
	user, Teams	2. PSTN user 1 hears Ring back Tone	successfully		option to add a
	user adds	3. Teams user answers the call	2. All three users are		user into
	PSTN 2 user	4. Verify two way audio	able to hear each		conference when
	to the	5. Teams user adds PSTN user 2 to the	other		its Teams user is
	ongoing call	ongoing call			assigned with E5
		6. PSTN user 2 starts ringing			without Audio
		7. PSTN user 2 answers the call			Conferencing
		9. Verify all three users are able to hear			license. Only on
		each other			E5 without A/C
		10. Teams user hangs up the call			license, audio
		11. Verify call is cleared successfully			conferencing a
				FAILED	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

74PSTN user1. Make a voice call from PSTN user to Calls Teams1. Third user is added to the callCalls TeamsTeams user 1added to the calluser, Teams2. PSTN user hears Ring back Tonesuccessfullyuser adds3. Teams user 1 answers the call2. All three users are	Crestron phone does not have an option to add a user into
two or more users to the ongoing call4. Verify two way audio 5. Teams user 1 adds Teams user 2 to otherable to hear each otherongoing call 6. Verify Teams user 2 is added successfully to the call 7. Teams user 1 adds PBX A user to the ongoing call 	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

External ID	Title	Procedure	Expected Results	Status	Comments
75	PBX A user Calls Teams user, Teams user CFA to PBX A user	<ol> <li>Teams user sets call forwarding all to PBX A user 2</li> <li>Make a voice call from PBX A user 1 to Teams user</li> <li>PBX A user 2 starts ringing</li> <li>PBX A user 2 answers the call</li> <li>Verify two way audio</li> <li>PBX A user 1 hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets call forwarding all to PBX B user</li> <li>Make a voice call from PBX A user to Teams user</li> <li>PBX B user starts ringing</li> <li>PBX B user answers the call</li> <li>Verify two way audio</li> <li>PBX A user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets call forwarding all to PSTN user</li> <li>Make a voice call from PBX A user to Teams user</li> <li>PSTN user starts ringing</li> <li>PSTN user answers the call</li> <li>Verify two way audio</li> <li>PBX A user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets call forwarding all to PBX B user 2</li> <li>Make a voice call from PBX B user 1 to Teams user</li> <li>PBX B user 2 starts ringing</li> <li>PBX B user 2 answers the call</li> <li>Verify two way audio</li> <li>PBX B user 1 hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets call forwarding all to PBX A user</li> <li>Make a voice call from PBX B user to Teams user</li> <li>PBX A user starts ringing</li> <li>PBX A user answers the call</li> <li>Verify two way audio</li> <li>PBX B user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets call forwarding all to PSTN user</li> <li>Make a voice call from PBX B user to Teams user</li> <li>PSTN user starts ringing</li> <li>PSTN user answers the call</li> <li>Verify two way audio</li> <li>PBX B user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets call forwarding all to PBX B user</li> <li>Make a voice call from PSTN user to Teams user</li> <li>PBX B user starts ringing</li> <li>PBX B user answers the call</li> <li>Verify two way audio</li> <li>PSTN user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets call forwarding all to PBX A user</li> <li>Make a voice call from PSTN user to Teams user</li> <li>PBX A user starts ringing</li> <li>PBX A user answers the call</li> <li>Verify two way audio</li> <li>PSTN user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets call forwarding all to PSTN user 2</li> <li>Make a voice call from PSTN user 1 to Teams user</li> <li>PSTN user 2 starts ringing</li> <li>PSTN user 2 answers the call</li> <li>Verify two way audio</li> <li>PSTN user 1 hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets call forwarding no answer to PBX A user 2</li> <li>Make a voice call from PBX A user 1 to Teams user</li> <li>Teams user starts ringing</li> <li>Teams user does not answer the call</li> <li>Call gets forwarded after the no answer timeout value is reached</li> <li>PBX A user 2 starts ringing</li> <li>PBX A user 2 answers the call</li> <li>Verify two way audio</li> <li>PBX A user 1 hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets call forwarding no answer to PBX B user</li> <li>Make a voice call from PBX A user to Teams user</li> <li>Teams user starts ringing</li> <li>Teams user does not answer the call</li> <li>Call gets forwarded after the no answer timeout value is reached</li> <li>PBX B user starts ringing</li> <li>PBX B user answers the call</li> <li>Verify two way audio</li> <li>PBX A user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets call forwarding no answer to PSTN user</li> <li>Make a voice call from PBX A user to Teams user</li> <li>Teams user starts ringing</li> <li>Teams user does not answer the call</li> <li>Call gets forwarded after the no answer timeout value is reached</li> <li>PSTN user starts ringing</li> <li>PSTN user answers the call</li> <li>Verify two way audio</li> <li>PBX A user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets call forwarding no answer to PBX B user 2</li> <li>Make a voice call from PBX B user 1 to Teams user</li> <li>Teams user starts ringing</li> <li>Teams user does not answer the call</li> <li>Call gets forwarded after the no answer timeout value is reached</li> <li>PBX B user 2 starts ringing</li> <li>PBX B user 2 answers the call</li> <li>Verify two way audio</li> <li>PBX B user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets call forwarding no answer to PBX A user</li> <li>Make a voice call from PBX B user to Teams user</li> <li>Teams user starts ringing</li> <li>Teams user does not answer the call</li> <li>Call gets forwarded after the no answer timeout value is reached</li> <li>PBX A user starts ringing</li> <li>PBX A user answers the call</li> <li>Verify two way audio</li> <li>PBX B user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets call forwarding no answer to PSTN user</li> <li>Make a voice call from PBX B user to Teams user</li> <li>Teams user starts ringing</li> <li>Teams user does not answer the call</li> <li>Call gets forwarded after the no answer timeout value is reached</li> <li>PSTN user starts ringing</li> <li>PSTN user answers the call</li> <li>Verify two way audio</li> <li>PBX B user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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	Title	Procedure	Expected Results	Status	Comments
90	PSTN user Calls Teams user, Teams user CFNA to PBX B user	<ol> <li>Teams user sets call forwarding no answer to PBX B user</li> <li>Make a voice call from PSTN user to Teams user</li> <li>Teams user starts ringing</li> <li>Teams user does not answer the call</li> <li>Call gets forwarded after the no answer timeout value is reached</li> <li>PBX B user starts ringing</li> <li>PBX B user answers the call</li> <li>Verify two way audio</li> <li>PSTN user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets call forwarding no answer to PBX A user</li> <li>Make a voice call from PSTN user to Teams user</li> <li>Teams user starts ringing</li> <li>Teams user does not answer the call</li> <li>Call gets forwarded after the no answer timeout value is reached</li> <li>PBX A user starts ringing</li> <li>PBX A user answers the call</li> <li>Verify two way audio</li> <li>PSTN user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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	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> <li>Make a voice call from PSTN user 1 to Teams user</li> <li>Teams user starts ringing</li> <li>Teams user does not answer the call</li> <li>Call gets forwarded after the no answer timeout value is reached</li> <li>PSTN user 2 starts ringing</li> <li>PSTN user 2 answers the call</li> <li>Verify two way audio</li> <li>PSTN user 1 hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Teams user sets simultaneous ringing to PBX A user and PBX B user</li> <li>Make a voice call from PSTN user to Teams user</li> <li>Teams user, PBX A user and PBX B user starts ringing</li> <li>PBX A user answers the call</li> <li>Verify two way audio</li> <li>PSTN user hangs up</li> <li>Verify call is cleared successfully</li> <li>Repeat steps 2 to 6 where PBX B user answers the call</li> </ol>		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> <li>Make a voice call from Teams user with restricted caller ID to PBX A user</li> <li>Teams user hears Ring back Tone</li> <li>PBX A user starts ringing</li> <li>Verify caller ID displayed on PBX A user is Unavailable/Private/Anonymous</li> <li>PBX A user answers the call</li> <li>Verify two way audio</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Teams user is able to dial an outbound call with restricted caller ID</li> <li>Call is successful with two way audio</li> </ol>	PASSED	
95	Teams user with restricted Caller ID Calls PBX B user	<ol> <li>Make a voice call from Teams user with restricted caller ID to PBX B user</li> <li>Teams user hears Ring back Tone</li> <li>PBX B user starts ringing</li> <li>Verify caller ID displayed on PBX B user is Unavailable/Private/Anonymous</li> <li>PBX B user answers the call</li> <li>Verify two way audio</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Teams user is able to dial an outbound call with restricted caller ID</li> <li>Call is successful with two way audio</li> </ol>	NOT APPLICABLE	This testing is for only one PBX with Teams
96	Teams user with restricted Caller ID Calls PSTN user	<ol> <li>Make a voice call from Teams user with restricted caller ID to PSTN user</li> <li>Teams user hears Ring back Tone</li> <li>PSTN user starts ringing</li> <li>Verify caller ID displayed on PSTN user is Unavailable/Private/Anonymous</li> </ol>	<ol> <li>Teams user is able to dial an outbound call with restricted caller ID</li> <li>Call is successful with two way audio</li> </ol>	PASSED	

External ID	Title	Procedure	Expected Results	Status	Comments
		<ol> <li>5. PSTN user answers the call</li> <li>6. Verify two way audio</li> <li>7. Teams user hangs up the call</li> <li>8. Verify call is cleared successfully</li> </ol>			
97	PBX A user with restricted Caller ID Calls Teams user	<ol> <li>Make a voice call from PBX A user with restricted caller ID to Teams user</li> <li>PBX A user hears Ring back Tone</li> <li>Teams user starts ringing</li> <li>Verify caller ID displayed on Teams user is Unavailable/Private/Anonymous</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>PBX A user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Teams user is able to receive an inbound call with restricted caller ID</li> <li>Call is successful with two way audio</li> </ol>	PASSED	
98	PBX B user with restricted Caller ID Calls Teams user	<ol> <li>Make a voice call from PBX B user with restricted caller ID to Teams user</li> <li>PBX B user hears Ring back Tone</li> <li>Teams user starts ringing</li> <li>Verify caller ID displayed on Teams user is Unavailable/Private/Anonymous</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>PBX B user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Teams user is able to receive an inbound call with restricted caller ID</li> <li>Call is successful with two way audio</li> </ol>	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> <li>Make a voice call from PSTN user with restricted caller ID to Teams user</li> <li>PSTN user hears Ring back Tone</li> <li>Teams user starts ringing</li> <li>Verify caller ID displayed on Teams user is Unavailable/Private/Anonymous</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>PSTN user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	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> <li>Make a voice call from PBX A user to Teams user</li> <li>Teams user does not answer the call</li> <li>Allow the call to get forwarded to voicemail</li> <li>PBX A user successfully leaves voicemail</li> <li>Teams user receives voicemail notification</li> <li>Teams user successfully retrieves voicemail</li> </ol>	1. Teams user is able to receive and retrieve voicemail successfully	PASSED	
101	PBX B user Calls Teams	1. Make a voice call from PBX B user to Teams user	1. Teams user is able to receive and	NOT	This testing is for only one PBX with
	user and	<ol> <li>Teams user does not answer the call</li> <li>Allow the call to get forwarded to</li> </ol>	retrieve voicemail successfully	APPLICABLE	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			
102	PSTN user Calls Teams user and leaves voicemail	<ol> <li>Make a voice call from PSTN user to Teams user</li> <li>Teams user does not answer the call</li> <li>Allow the call to get forwarded to voicemail</li> <li>PSTN user successfully leaves voicemail</li> <li>Teams user receives voicemail notification</li> <li>Teams user successfully retrieves voicemail</li> </ol>	1. Teams user is able to receive and retrieve voicemail successfully	PASSED	
103	Teams user Calls PBX A user and leaves voicemail	<ol> <li>Make a voice call from Teams user to PBX A user</li> <li>PBX A user does not answer the call</li> <li>Allow the call to get forwarded to voicemail</li> <li>Teams user successfully leaves voicemail and navigates voicemail menu using DTMF</li> </ol>	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> <li>Make a voice call from Teams user to PBX B user</li> <li>PBX B user does not answer the call</li> <li>Allow the call to get forwarded to voicemail</li> <li>Teams user successfully leaves voicemail and navigates voicemail menu using DTMF</li> </ol>	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> <li>Make a voice call from Teams user to PBX A user</li> <li>PBX A returns 486 Busy</li> <li>Verify Teams user gets appropriate notification or announcement and the call is cleared</li> <li>Repeat steps 1 to 3 where PBX A returns 480, 404, 503 SIP responses</li> <li>Document the observation on Teams user side</li> </ol>	1. Teams user handles the failure response successfully	PASSED	
106	Teams user Calls PBX A user using SIP URI	<ol> <li>Make a voice call from Teams user to PBX A user using SIP URI</li> <li>PBX A user starts ringing</li> <li>PBX A user answers the call</li> <li>Verify two way audio</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>	<ol> <li>Teams user is able to call using SIP URI</li> <li>Call is connected with two way audio successfully</li> </ol>	NOT TESTED	SIP URI Not tested for this PBX
107	Teams user Calls PBX B	<ol> <li>Make a voice call from Teams user to PBX B user using SIP URI</li> <li>PBX B user starts ringing</li> </ol>	<ol> <li>Teams user is able to call using SIP URI</li> <li>Call is connected</li> </ol>	NOT APPLICABLE	This testing is for only one PBX with Teams

External ID	Title	Procedure	Expected Results	Status	Comments
	user using	3. PBX B user answers the call	with two way audio		
	SIP URI	4. Verify two way audio	successfully		
		5. Teams user hangs up the call			
		6. Verify call is cleared successfully			
108	PBX A user	1. Make a voice call from PBX A user to	1. Teams user is able		SIP URI Not tested
	Calls Teams	Teams user using SIP URI	to call using SIP URI		for this PBX
	user using	2. PBX A user starts ringing	2. Call is connected	NOT	
	SIP URI	3. PBX A user answers the call	with two way audio		
		4. Verify two way audio	successfully	TESTED	
		5. PBX A user hangs up the call			
		6. Verify call is cleared successfully			
109	PBX B user	1. Make a voice call from PBX B user to	1. Teams user is able		This testing is for
	Calls Teams	Teams user using SIP URI	to call using SIP URI		only one PBX with
	user using	2. PBX B user starts ringing	2. Call is connected	NOT	Teams
	SIP URI	3. PBX B user answers the call	with two way audio		
		4. Verify two way audio	successfully		
		5. PBX B user hangs up the call			
		6. Verify call is cleared successfully			
110	Teams user	1. Make a voice call from Teams user to			Not applicable for
	calls Skype	Skype for Business user			this topology
	for Business	2. Teams user hears Ring back Tone			
	user	3. Skype for Business user answers the		NOT	
		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			

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> <li>Make a voice call from Skype for Business user to Teams user</li> <li>Skype for Business user hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Skype for Business user hangs up the call</li> <li>Verify call is cleared successfully</li> <li>Verify the same scenario where</li> <li>Skype for Business user is internal and external</li> </ol>		NOT APPLICABLE	Not applicable for this topology
112	Teams user calls Skype for Business External Mobile user	<ol> <li>Skype for business user is an External Mobile user</li> <li>Make a voice call from Teams user to Skype for Business user</li> <li>Teams user hears Ring back Tone</li> <li>Skype for Business user answers the call</li> <li>Verify two way audio</li> <li>Teams user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>		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> <li>Skype for business user is an External Mobile user</li> <li>Make a voice call from Skype for Business user to Teams user</li> <li>Skype for Business user hears Ring back Tone</li> <li>Teams user answers the call</li> <li>Verify two way audio</li> <li>Skype for Business user hangs up the call</li> <li>Verify call is cleared successfully</li> </ol>		NOT APPLICABLE	Not applicable for this topology
114	Teams user call other tenant users	<ol> <li>Make a voice call from Teams user to another tenant users (Teams desktop client user, Teams mobile user, Skype for Business Online user)</li> <li>Verify call is successful</li> <li>Make one call to each different user one by one</li> </ol>		NOT APPLICABLE	Not applicable for this topology
115	Teams users joins a meeting scheduled by Skype for business On- premises user	<ol> <li>Skype for business user schedules a meeting and invites Teams user 1 and Teams user 2</li> <li>Teams user 1 joins the meeting using the Join button</li> <li>Teams user 2 joins the meeting using the dial-in conferencing number</li> <li>Verify Teams users are able to join the meeting successfully</li> <li>Verify all three users are able to hear</li> </ol>		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	<ol> <li>Teams user schedules a meeting and invites Skype for Business user 1 and Skype for Business user 2</li> <li>Skype for Business user 1 joins the meeting using the Meeting link</li> <li>Skype for Business user 2 joins the meeting using the dial-in conferencing number</li> <li>Verify all three users are able to hear each other</li> <li>Teams user ends the meeting</li> </ol>		NOT APPLICABLE	Not applicable for this topology