Mitel Technical Configuration Notes – HO3272

July 29, 2019

Microsoft Teams Direct Routing with MiVoice Office 400 6.0 SP2 using AudioCodes Mediant Virtual Edition (VE) 7.20A.252.011 as SBC

Description: This document provides a reference to Mitel Authorized Solutions providers for configuring the Mitel MiVO400 to connect to Microsoft Teams Direct Routing using AudioCodes Median Virtual Edition.

Environment: MiVoice Office 400 6.0 SP2 (8947c1), Mediant SW/v.7.20A.252.011

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.
No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

TRADEMARKS

Mitel is a trademark of Mitel Networks Corporation.

Windows and Microsoft are trademarks of Microsoft Corporation.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

Mitel Technical Configuration Notes – Configure MiVO400 for use with AudioCodes.

July 2019 – HO3272

Table of Contents

Overview

This document provides a reference to Mitel Authorized Solutions providers for configuring the Mitel MiVO400 to connect to Teams using AudioCodes as SBC. The different devices can be configured in various configurations depending on your VoIP solution. This document covers a basic setup with required option setup.

Interop History

Version	Date	Reason
1	July, 2019	Configure MiVoice Office 400 6.0 SP2 for use with Microsoft Teams Direct Routing using AudioCodes Mediant Virtual Edition (VE) SW/v. 7.20A.252.011 as SBC

Interop Status

The Interop of Microsoft Teams Direct Routing with MiVO400 using AudioCodes Mediant Virtual Edition has been given a Certification status. This will be included in the Mitel Interoperability Reference Guide (IRG). The status Microsoft Teams Direct Routing achieved is:

COMPATIBLE	The most common certification which means Microsoft Teams Direct Routing with MiVO400 using AudioCodes as SBC has been tested and/or validated by the Mitel Third-Party Interop Team. Mitel Product Support will provide all necessary support related to the interop, but issues unique or specific to the 3rd party will be referred to the 3rd party as appropriate.

Deployment Considerations

1. Simulated PSTN (with SIP trunks to another MiVB) is used for this testing. This testing doesn't intend to certify any SIP provider, and hence one must exercise their own diligence before using SIP carrier with AudioCodes in Teams Direct routing context

2. According to AudioCodes Teams Direct Routing guide, all three Microsoft proxies need to be listed under the same Proxy Set. As this configuration had some issues in interop lab, each proxy set was setup with a dedicated Proxy Address. And subsequently IP Group was setup corresponding to each IP proxy set. Eventually, Destination Type is configured as IP Group set under IP-to-IP routing, and this IP Group set has all three IP Groups listed which point to three different proxies. One must assess their requirements, and consult with AudioCodes in case any routing issues are noticed with this configuration

3. In the lab deployment, Destination Username Pattern is used to route the calls to destination. Any four-digit dialing from MiVO400 is routed to Teams, and 10-digit dialing goes to PSTN. It's suggested that other options be evaluated and the appropriate one be chosen which would be more applicable for a specific deployment

4. Teams prefixes the country code (+91 in lab testing) for all outbound dialing. SIP Message Manipulation has been used on AudioCodes to remove the prefix. SIP Manipulation has also been used to modify SIP host name.

5. All DIDs (that belong to both MiVO400 and Teams users) are provisioned on MiVO 400. Any inbound call to DID is mapped to appropriate extension. And if an extension turns out to be Teams, the call gets forwarded to Teams through MiVO 400. PSTN call to Teams is always routed via MiVO 400. One can directly route PSTN call to Teams, but it needs to properly be provisioned on Teams to accept inbound PSTN call and map it to Teams extension.

6. Due to SRTP compatibility issues with AudioCodes, media is confined to RTP between MiVO400 and AudioCodes.

7. Hold INVITE from MiVO400 doesn't have SDP. Microsoft doesn't accept any INVITEs with out SDP. IP profile needs to be properly setup on AudioCodes in order to have SDP in all outbound INVITEs to Teams. See the configuration details.

8. MIVO400 uses the same SIP trunk to reach Teams as well as PSTN user.

9. TLS and SRTP are mandatory between AudioCodes and Teams. See the configuration details.

10. Media by-pass hasn't been tested it's largely a feature specific to SBC and Phone system. This is expected to have already been tested as part of SBC certification with Phone System Direct Routing.

Software & Hardware Setup

This was the test setup to generate a basic SIP call between Teams and MIVO400 with AudioCodes Mediant Virtual Edition as SBC

Note – Although this testing was performed on the below tested variants, the scope of this testing can be extended to other product variants that work with the same firmware. The list of components for which this testing can be considered applicable is given in the "Additional Applicable Variants" column of the following table –

Manufacturer	Tested Variants	Software Version	Additional Applicable Variants
Mitel	MiVoice Office 400	Release 6.0 SP2 (8947c1)	NA
Mitel	69XX SIP 68XX SIP	5.1.0.1032	NA
Mitel	SIP-DECT RFP 48	SIP-DECT 8.0-DI16	RFP 4X
Mitel	DECT Handsets 650c/622d	[650,602: 7.2] [602v2: 7.2]	NA
AudioCodes	Mediant Virtual Edition	v.7.20A.252.011	Mediant 500L/500/800/1000
Microsoft	Office 365 Phone System	NA	NA

Tested Features

This is an overview of the features tested during the Interop test cycle and not a detailed view of the test cases.

Feature	Feature Description	Issues
Basic Call	Placing calls between Teams Client and Mitel SIP Phone, call holding, transferring, conferencing, busy calls, long calls durations, variable codec.	☑
Packetization	Forcing the Mitel MiVO400 to stream RTP packets through its E2T card at different intervals, from 10ms to 90ms	☑
MiCollab	Placing calls between MiCollab and Teams users. Call Hold, transfer, Call forward etc	☑
PSTN	Placing calls between PSTN and Teams through MiVO400. Call hold, transfer, Call forward etc	☑
Voice Mail	PSTN and MiVO400 leaving voice message for Teams. Teams retrieves the call.	☑
Auto-Attendant	PSTN and MiVO400 calling Teams Auto-attendant. Transferring the call to other internal extensions	⚠
Longevity Calls	Long calls between Teams and MiVO400. Long calls between PSTN and Teams through MiVO400	☑

☑ - No issues found ✗ - Issues found, cannot recommend to use ⚠ - Issues found

Device Limitations and Known Issues

This is a list of problems or unsupported features when AudioCodes Mediant Virtual Edition connected with MiVO 400.

Feature	Problem Description
TLS/SRTP	With SRTP enabled between MiVO400 and AudioCodes, in case of Call hold scenario, AudioCodes sends duplicate Crypto tag to Teams which results in 488 Not Acceptable from Office 365 Phone system. **Recommendation:** Disable SRTP between MiVO400 and AudioCodes. UDP has been used for both SIP and RTP for call leg between MiVO400 and AudioCodes. Please contact AudioCodes for more information.
INVITE without SDP	INVITE without SDP from AudioCodes are rejected by Teams. Need to advertise SDP always in INVITE. This is more important when MiVO400 places the call on hold as MiVO400 doesn't include any SDP in hold invite. **Recommendation:** Follow the configuration specified in this guide. Contact Mitel or AudioCodes for more details
Teams Auto-Attendant	During the testing, MiVO400 has been able to reach Teams Auto-Attendant, but the calls are not transferred to other Teams users. **Recommendation:** This is due to configuration error on Office 365 tenant. Contact Microsoft Support as to how to setup Auto-Attendant on Teams.
Call Transfer	Teams transferring MiVO400/PSTN call to another teams user is not working. While transferring the call the 'Refer-to' address is not populated with right destination details. **Recommendation:** Contact Microsoft team for more details.
Call Hold/Resume	Teams client is initiating SIP REFER when Teams places the call on hold. REFER doesn't go well with MiVO400 due to which the user can't resume the call further **Recommendation:** Ticket #***617080*** has been logged with Microsoft. Contact Microsoft for more details. As a work-around 'Operator console' option needs to be disabled on MiVO400.
Call Receive	Immediately answering an incoming call at team's user end will not enable the ***'More action'*** option. One should wait for minimum 2-3 rings and then call should

	be answered. **Recommendation:** Contact Microsoft for more details.

Network Topology

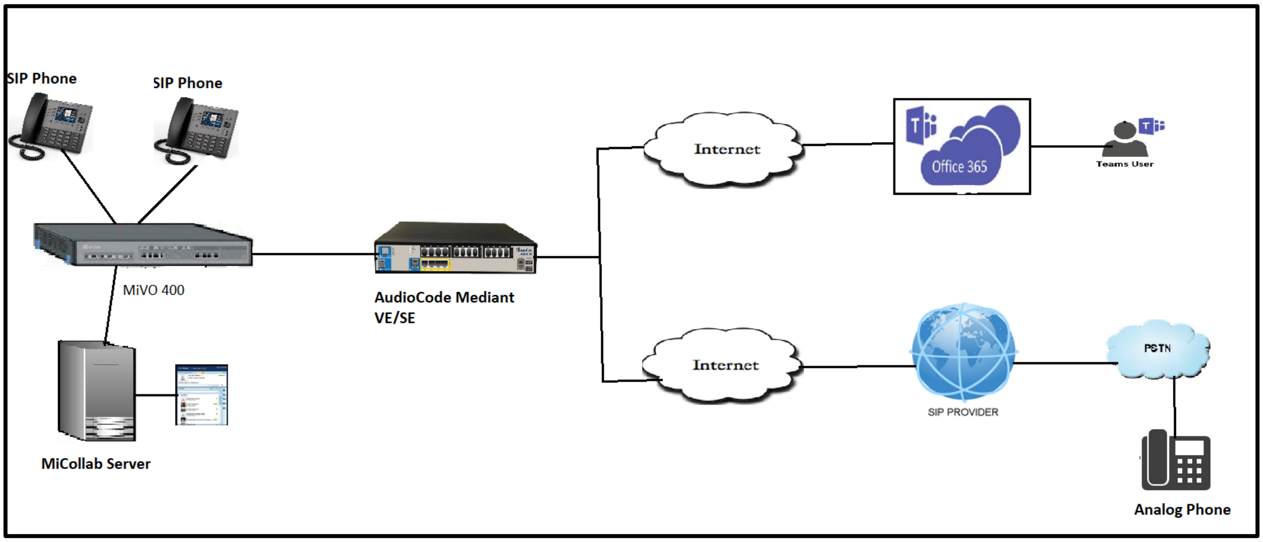


Figure 1 – Network Topology

Configuration Notes

This section is a description of how the SIP Interop was configured. These notes should give a guideline how a device can be configured in a customer environment and how AudioCodes Mediant Virtual Edition with MiVO400 programming was configured in our test environment.

Disclaimer: Although Mitel has attempted to setup the interop testing facility as closely as possible to a customer premise environment, implementation setup could be different onsite. YOU MUST EXERCISE YOUR OWN DUE DILIGENCE IN REVIEWING, planning, implementing, and testing a customer configuration.

MiVO400 Configuration Notes

The following steps show how to program a MiVO400 to interconnect with Teams using AudioCodes SBC.

Configuration Template

A configuration template can be found in the same Mitel Knowledge Management System (KMS) article as this document. The template is a Microsoft Excel spreadsheet (.csv format) **solely** consisting of the SIP Peer profile option settings used during Interop testing. All other forms should be programmed as indicated below. Importing the template can save you considerable configuration time and reduce the likelihood of data-entry errors. Refer to the MiVO400 documentation on how the Import functionality is used.

Network Requirements

- There must be adequate bandwidth to support the voice over IP. As a guide, the Ethernet bandwidth is approx. 85 Kb/s per G.711 voice session and 29 Kb/s per G.729 voice session (assumes 20ms packetization). As an example, for 20 simultaneous SIP sessions, the Ethernet bandwidth consumption will be approx. 1.7 Mb/s for G.711 and 0.6Mb/s. Almost all Enterprise LAN networks can support this level of traffic without any special engineering. Please refer to the MiVO400 Engineering guidelines for further information.
- For high quality voice, the network connectivity must support a voice-quality grade of service (packet loss <1%, jitter < 30ms, one-way delay < 80ms).

Assumptions for M Programming

The SIP signaling connection uses UDP on Port 5060.

Licensing and Option Selection – SIP Licensing

Ensure that MiVoice Office 400 is equipped with enough SIP Access Channel licenses for the connection to service provider SIP trunk. Up to 30 SIP voice channels are available for each SIP provider. For each

SIP voice channel, you need a SIP Access Channels license.

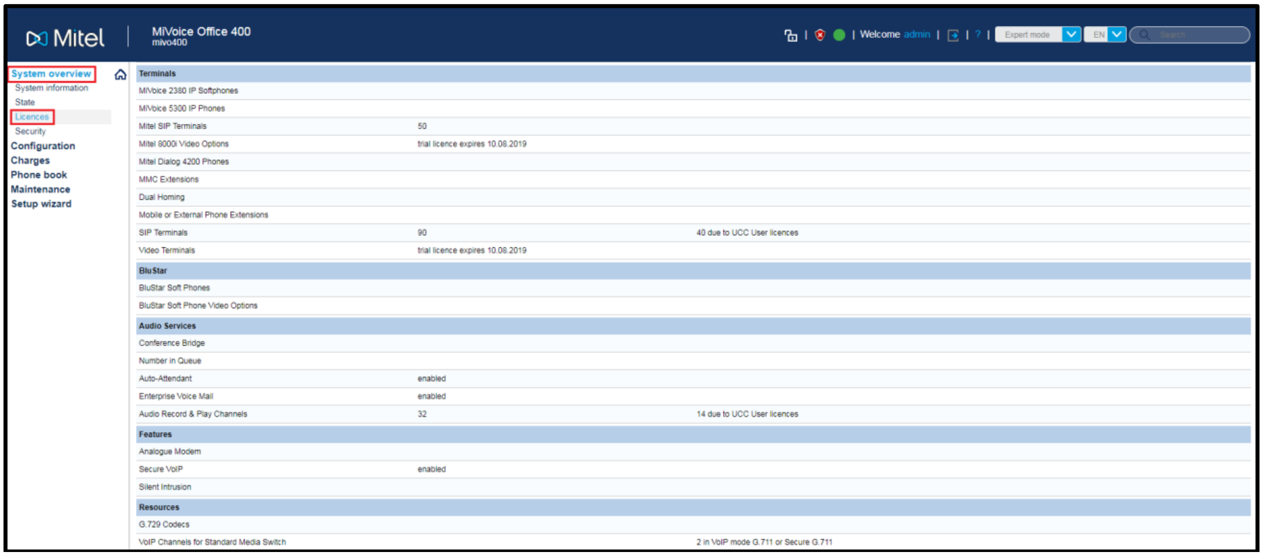


Figure 2 – License

Network Interfaces

Create a network interface for AudioCodes. In this example, AudioCodes is reachable using an IP address as entered in the “Registrar IP address” field. Your configuration may be different depending on the type and configuration of the SBC you are using.

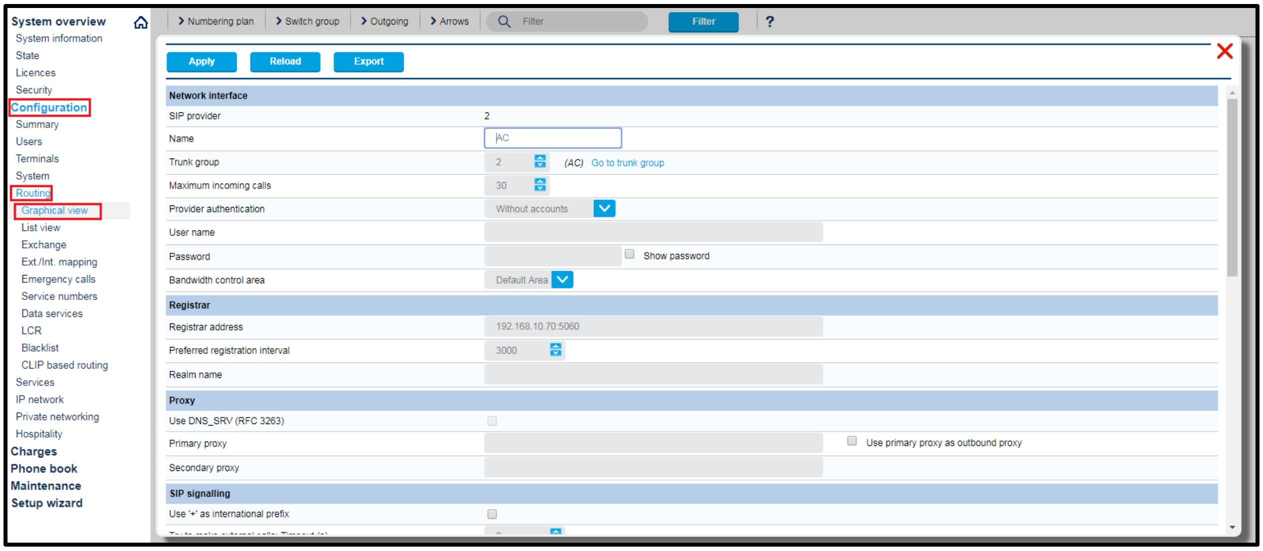


Figure 3 – Network Interface Creation

Network Interface Settings

The following 2 figures show the settings that were used for establishing a connection to AudioCodes SIP trunk. Most of the settings were left at their default values. You may want to specify a preferred codec.

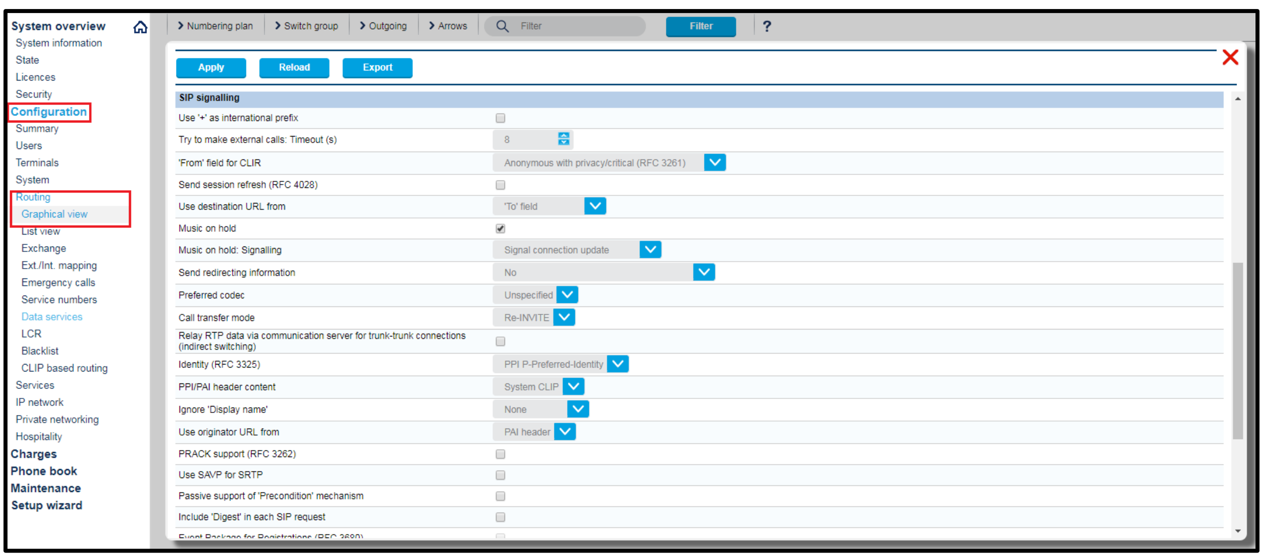


Figure 4 – Network Interface Settings

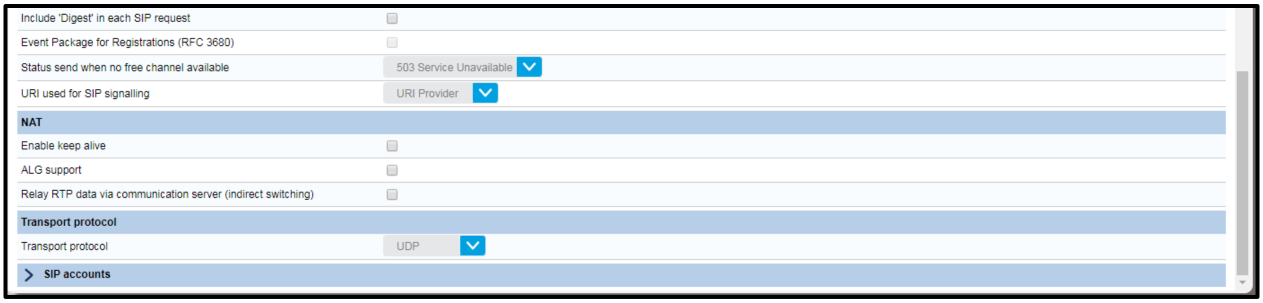


Figure 5 – Network Interface Setting (Continued)

Outgoing Call Routing

Create a route to handle your outgoing calls. In the test setup route 40 was used for outgoing calls to AudioCodes with a call number of 470. This will route all calls that begin with the digit 470 to the AudioCodes interface, **See figure 6**.

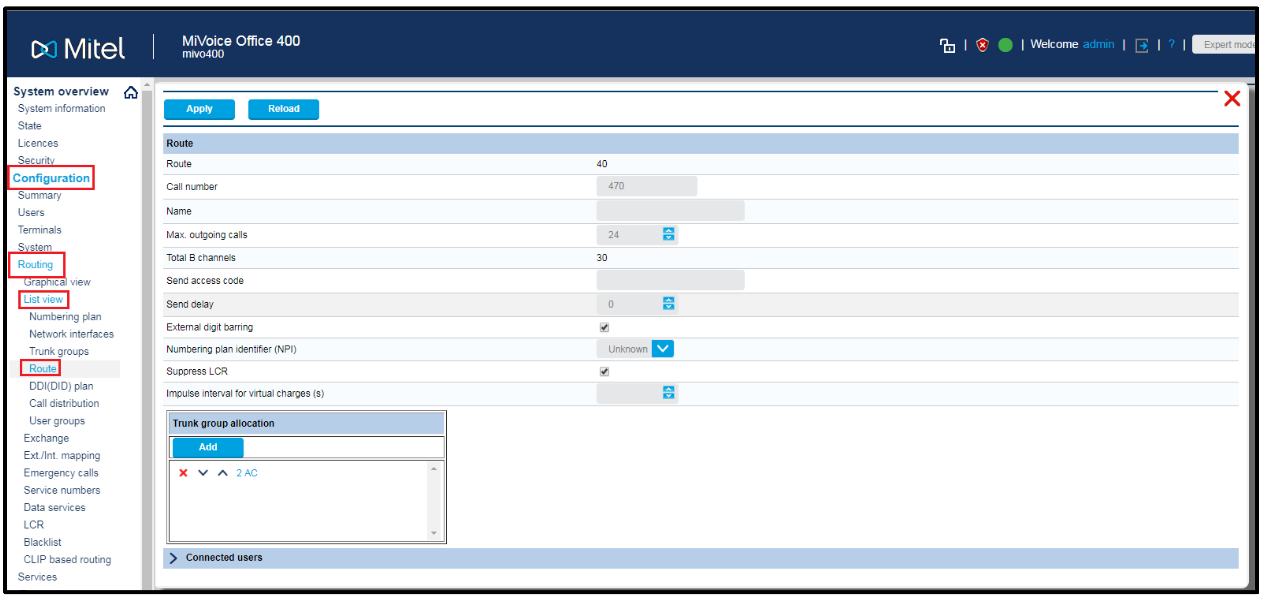


Figure 6 – Trunk Service Assignment

Incoming Call Route

There are several different ways to route inbound calls to a destination answer point. Inbound calls were tested using a DDI plan and a Call Distribution Element. As well, calls were routed to both a User Group and individual users. Calls can be directed to a DDI plan or a CDE via the Trunk Group we created when the Network interface was created.

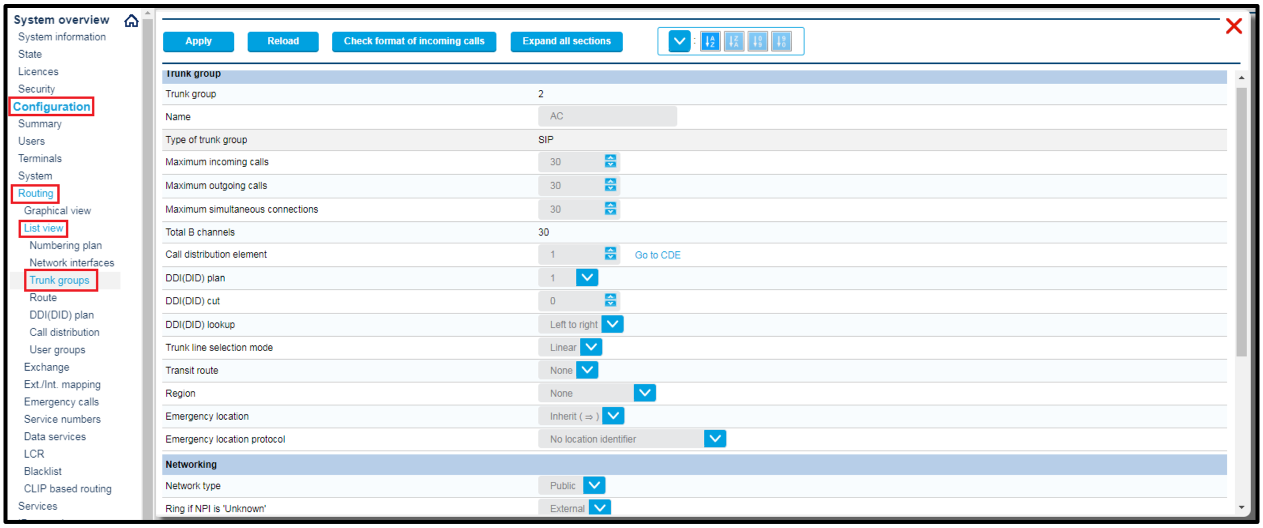


Figure 7: Trunk Group

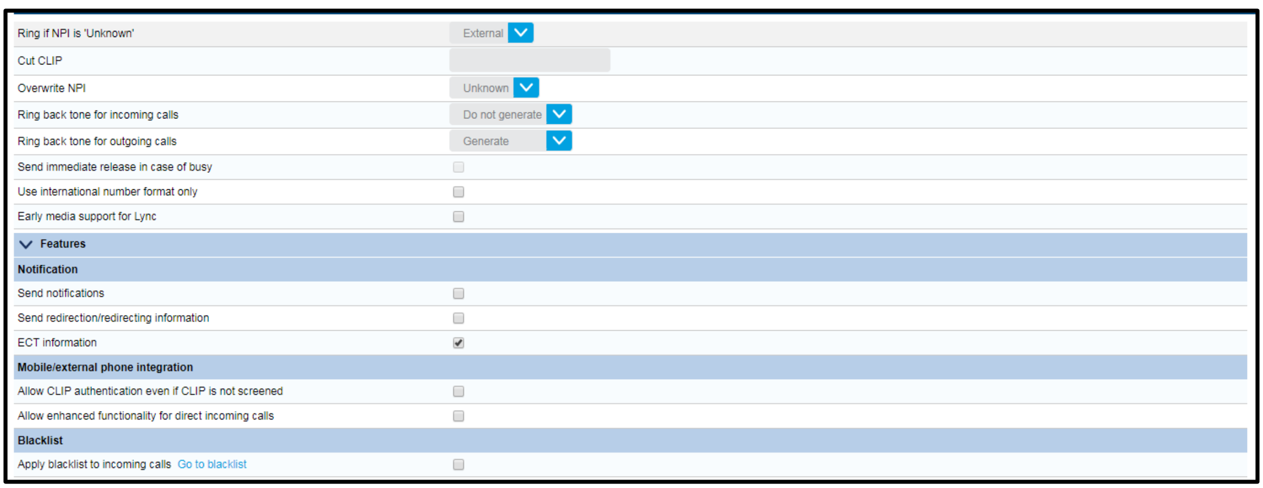


Figure 8: Trunk Group (Continued)

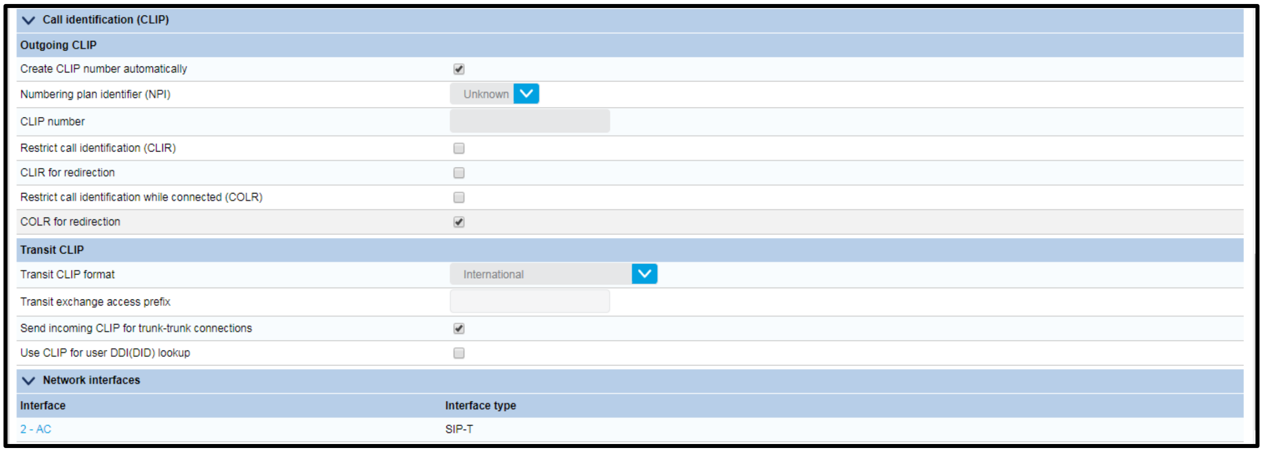


Figure 9: Trunk Group (Continued)

DDI Plan

The DDI Plan is where you can assign individual called numbers to specific Users or User Groups etc. In the example bellow Figure 10 two incoming numbers were created to route calls to individual destinations. These called numbers were then routed to destinations using the Call Distribution Elements as depicted in Figure 11 below.

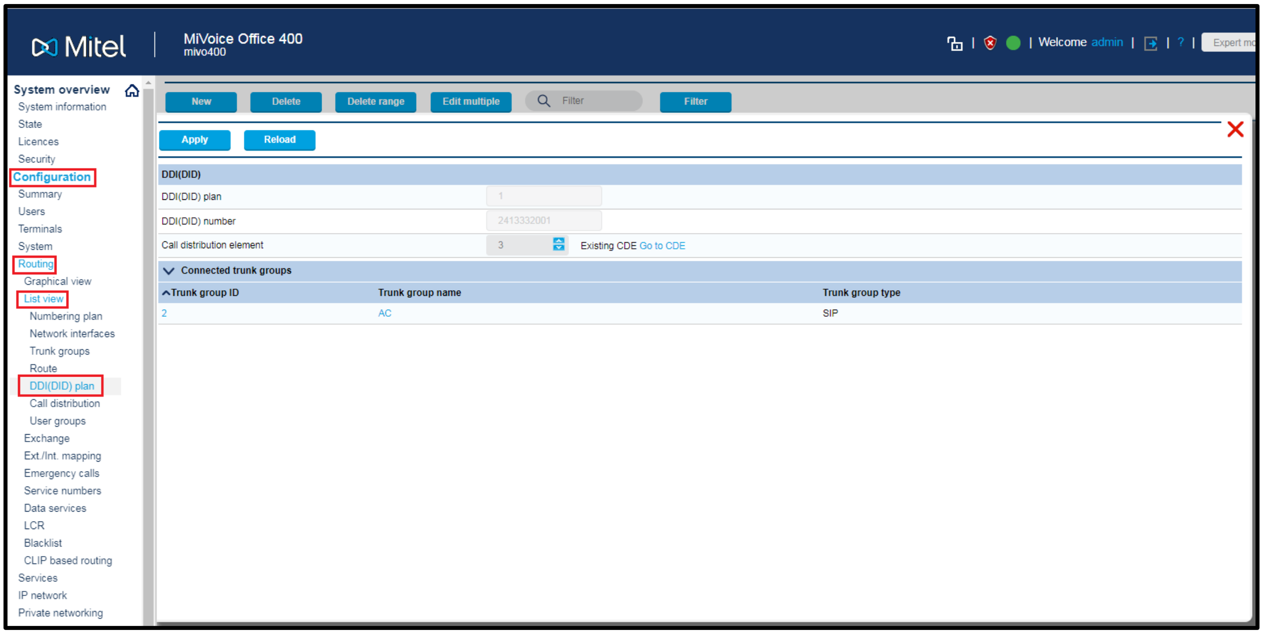


Figure 10: DDI Creation

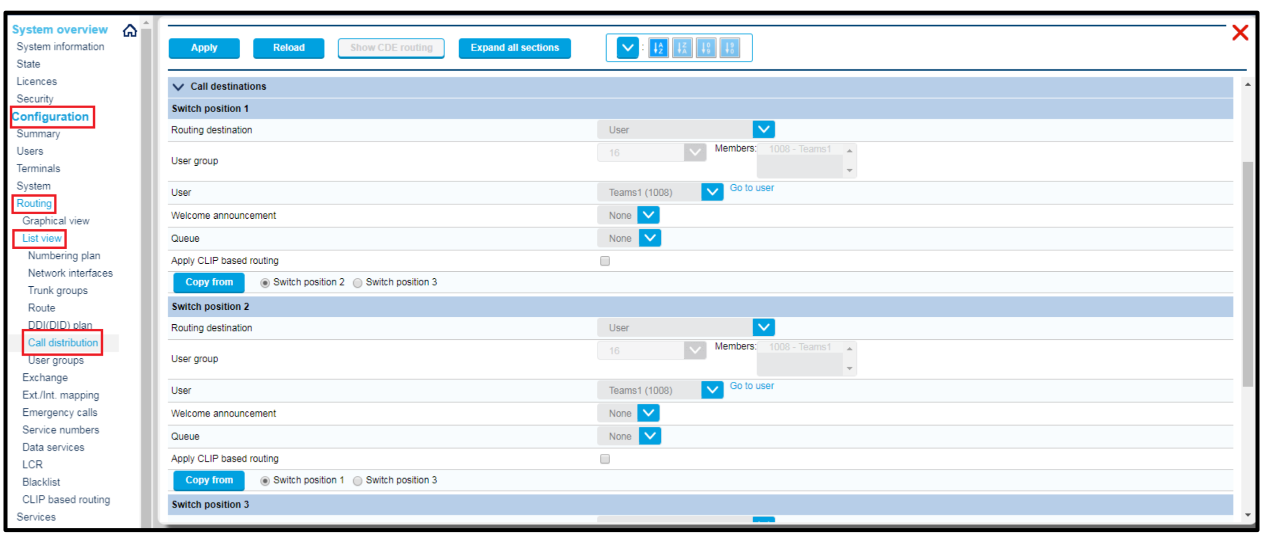
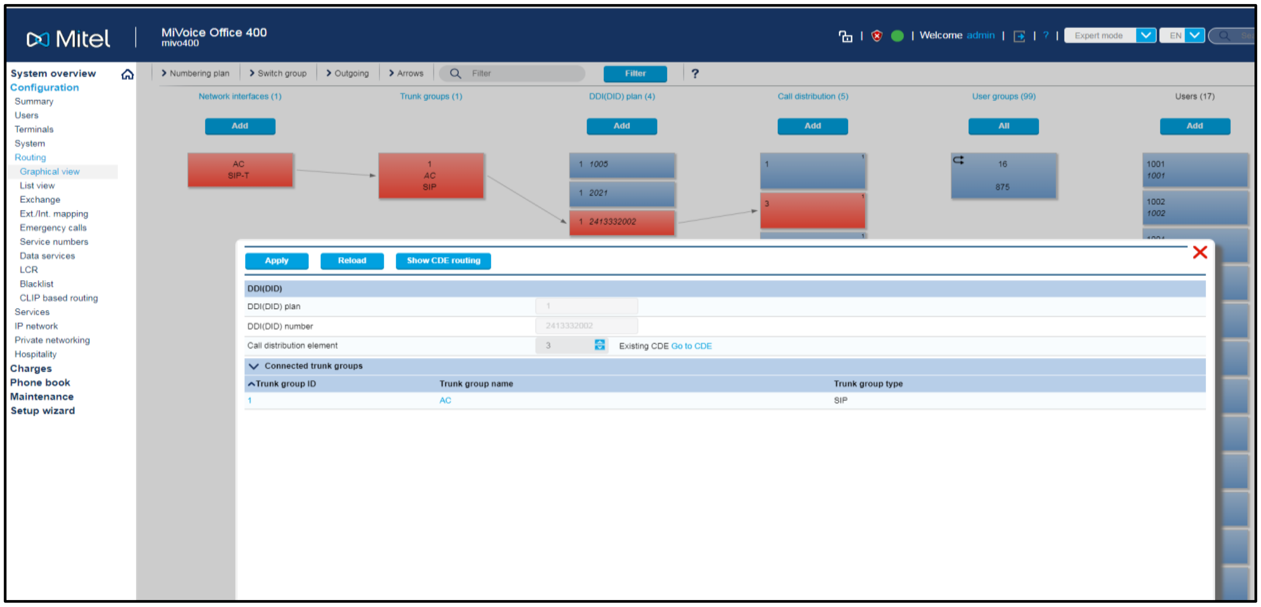
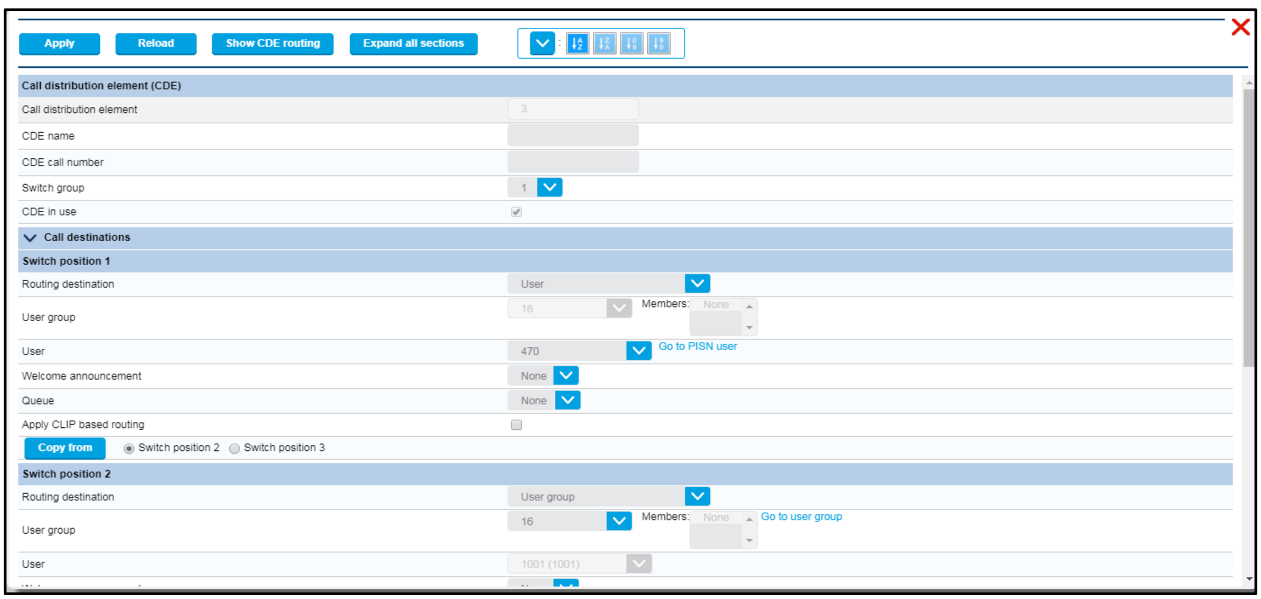


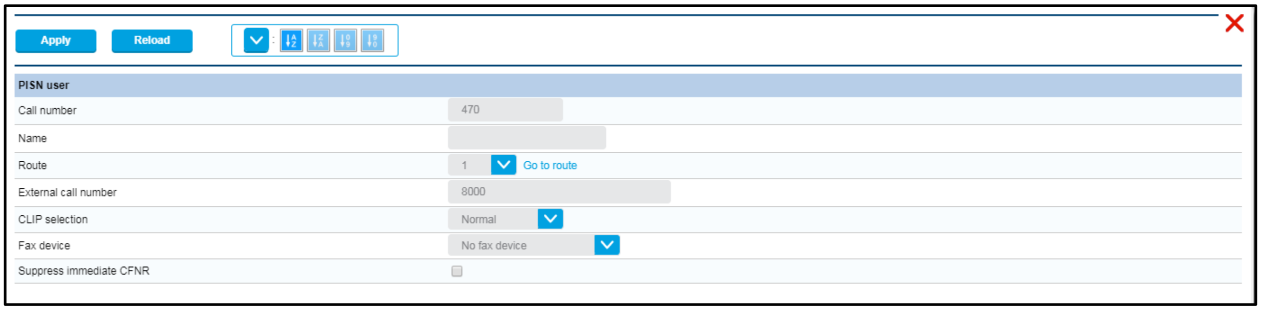
Figure 11: CDE

PSTN calls Team's USER via 400 – Routing Configuration

Need to create a PISN user in MiVO400 to route call when PSTN calls teams user. Below are the configuration details for the same.

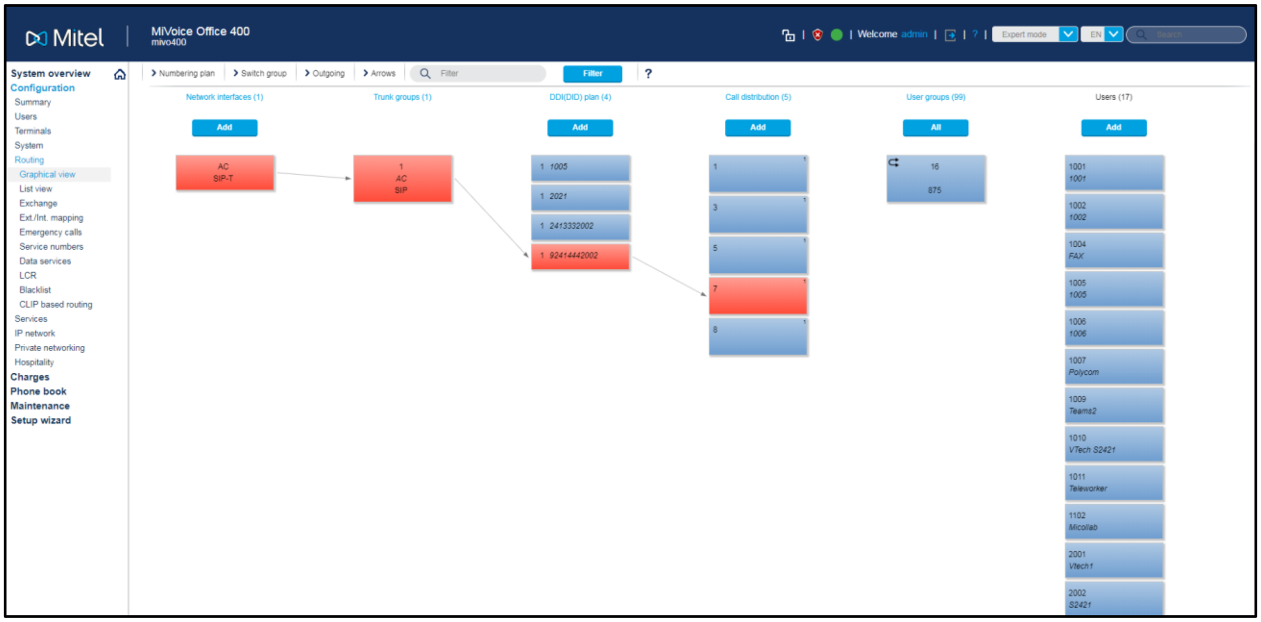


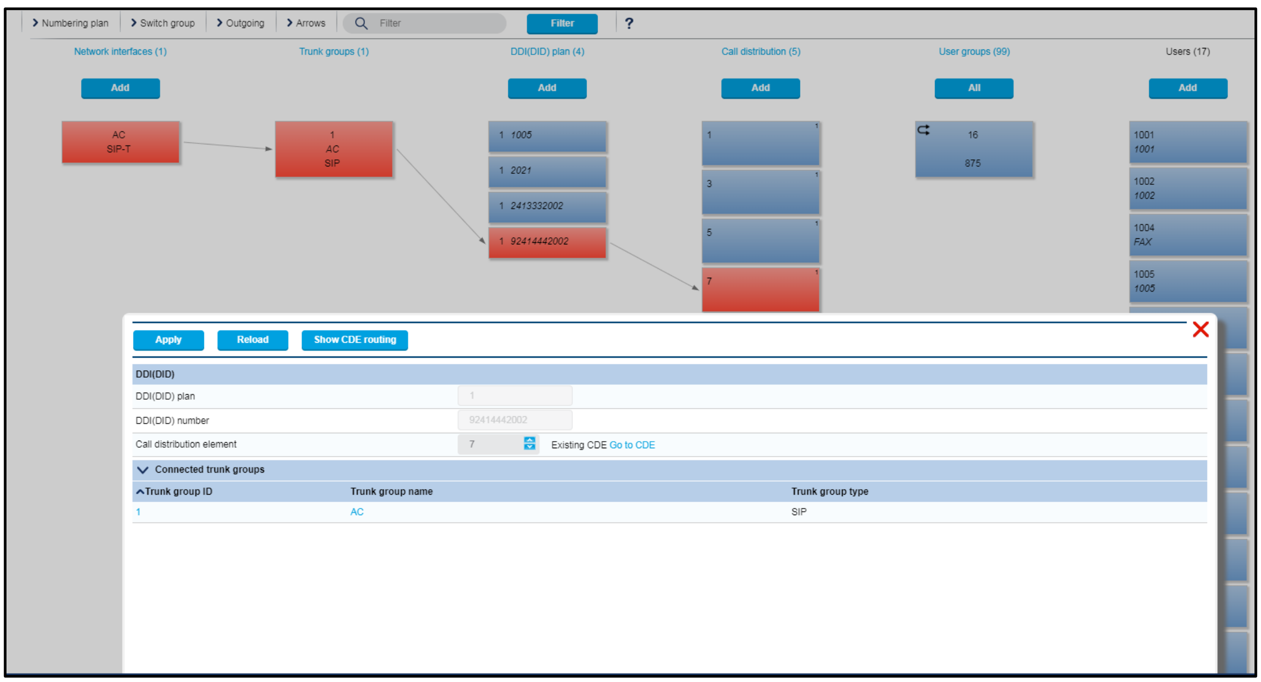


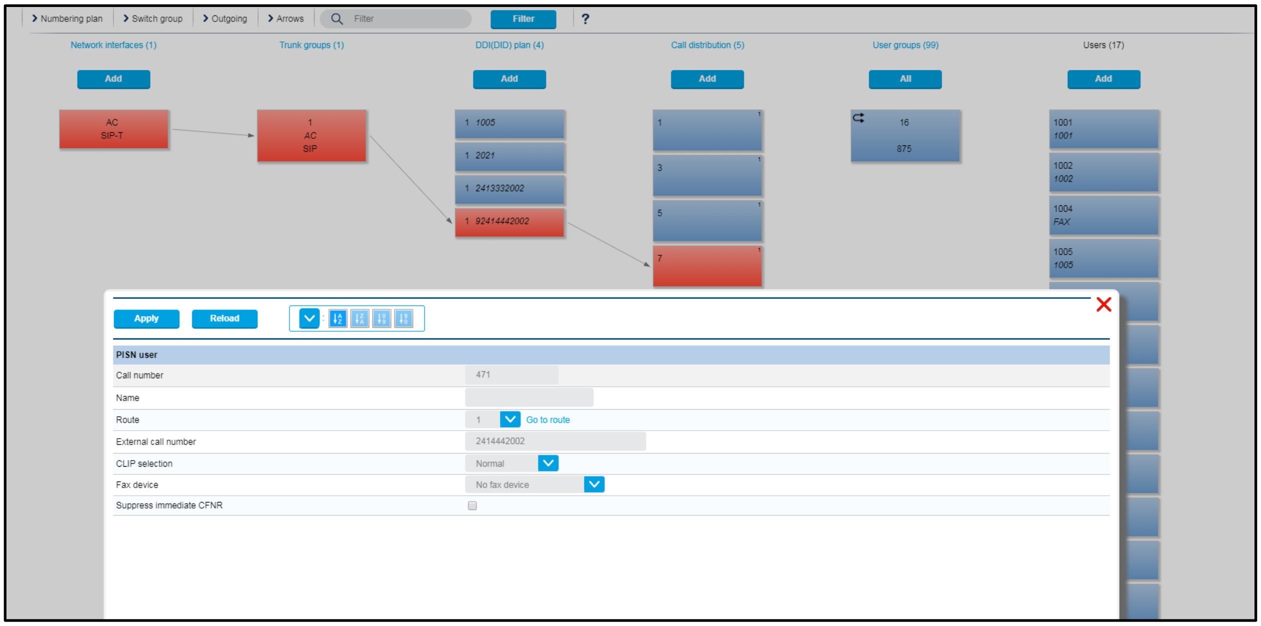


PSTN calls Team USER via 400

Team's USER call PSTN via 400 – Routing Configuration







Team USER call PSTN via 400

Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes Mediant Virtual Edition for interworking between MIVO400 and the Service provider SIP Trunk. These configuration procedures are based on the interoperability test and includes the following main areas:

- E-SBC WAN interface – Service provider SIP Trunking environment
- E-SBC LAN interface – MIVO 400

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

Note:
For Interop Testing we have set the default configuration

IP Network Interfaces Configuration

This step describes how to configure the E-SBC's IP network interfaces. There are several ways to deploy the E-SBC; however, scenario exemplified in this document employs the following deployment method:

- E-SBC interfaces with the following IP entities:
  - MIVO400, located on the LAN
  - Service provider SIP Trunk located on the WAN
- Physical connection: The type of physical connection to the LAN depends on the method used to connect to the Enterprise's network.

- E-SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - WAN (VLAN ID 2)

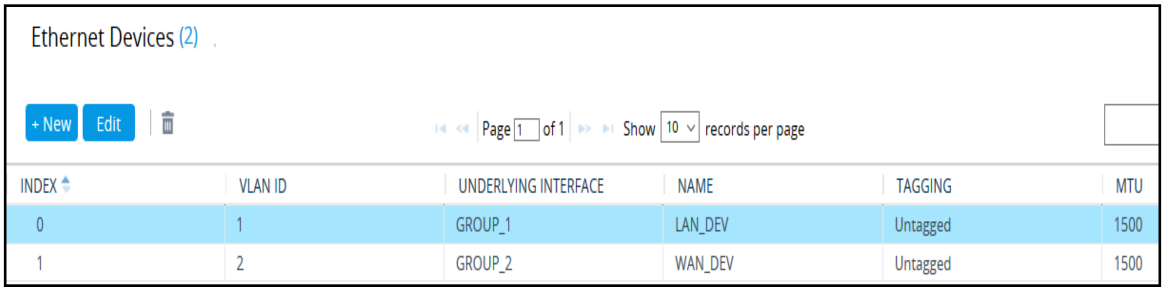
Configure VLANs

This step describes how to define VLANs for each of the following interfaces:

- LAN VoIP (assigned the name "LAN_IP")
- WAN VoIP (assigned the name "WAN_IP")

Open the Ethernet Device table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Devices**).

The existing row for VLAN ID 1 and VLAN ID 2. Check Figure 12


Ethernet Devices (2)

+ New | Edit | Page 1 of 1 | Show 10 records per page

INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING	MTU
0	1	GROUP_1	LAN_DEV	Untagged	1500
1	2	GROUP_2	WAN_DEV	Untagged	1500

Figure 12 - Configured VLAN IDs in Ethernet Device

Configure IP Network Interfaces for LAN and WAN

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

LAN VoIP (assigned the name "LAN_IF")

WAN VoIP (assigned the name "WAN_IF")

Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).

Modify the existing LAN network interface:

Select the 'Index' radio button of the **OAMP + Media + Control** table row, and then click **Edit**.

Configure the interface as follows and Click Apply

Parameter	Example Setting for IPv4
Name	LAN_IF (arbitrary descriptive name)
Application Type	OAMP + Media + Control
Interface Mode	See IPv4 in the SBC documentation.
IP Address	192.168.10.70 (LAN IP address of E-SBC)
Prefix Length	24 (subnet mask in bits for 255.255.255.0)
Default Gateway	192.168.10.1
Primary DNS	192.168.10.111
Ethernet Device	LAN_DEV

Add a network interface for the WAN side

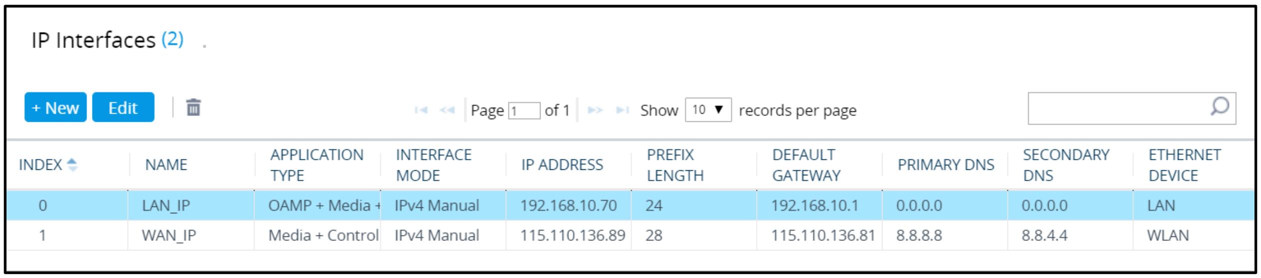
Click New.

Configure the interface as follows and Click Apply

Parameter	Example Setting for IPv4
Name	WAN_IF (arbitrary descriptive name)
Application Type	Media + Control
Interface Mode	See IPv4 in the SBC documentation.
IP Address	WAN IP address of E-SBC

Prefix Length	subnet mask
Default Gateway	Default Gateway of WAN IP
Primary DNS	Primary DNS of WAN IP
Ethernet Device	WAN_DEV

The configured IP network interfaces are shown below in Figure 13


IP Interfaces (2)

+ New Edit Page 1 of 1 Show 10 records per page

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	LAN_IP	OAMP + Media +	IPv4 Manual	192.168.10.70	24	192.168.10.1	0.0.0.0	0.0.0.0	LAN
1	WAN_IP	Media + Control	IPv4 Manual	115.110.136.89	28	115.110.136.81	8.8.8.8	8.8.4.4	WLAN

Figure 13 - Configured Network Interfaces in IP Interfaces Table

Configure Media Realms

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

To configure Media Realms:

Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).

Add a Media Realm for the LAN interface. You can use the default Media Realm (Index 0), however modify it as shown below in figure 14 and Click Apply

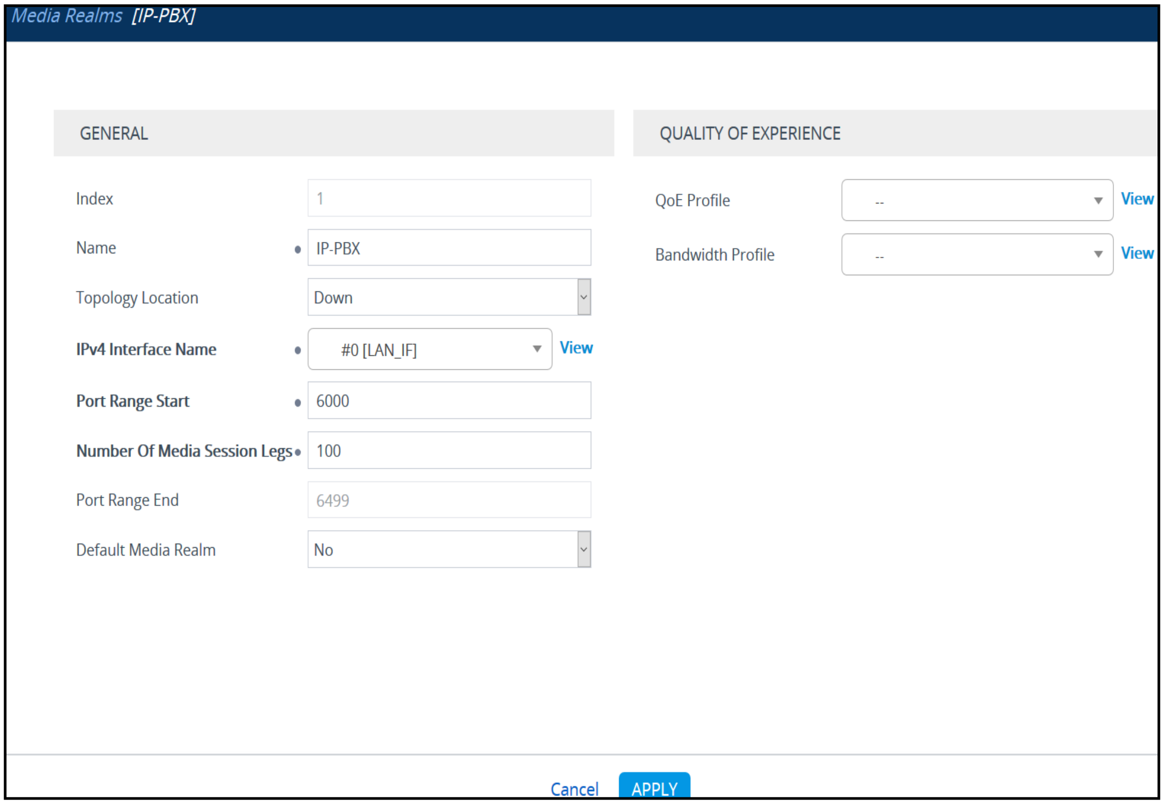


Figure 14 - Configuring Media Realm for LAN

Configure a Media Realm for WAN traffic as shown in Figure 15 and Click Apply

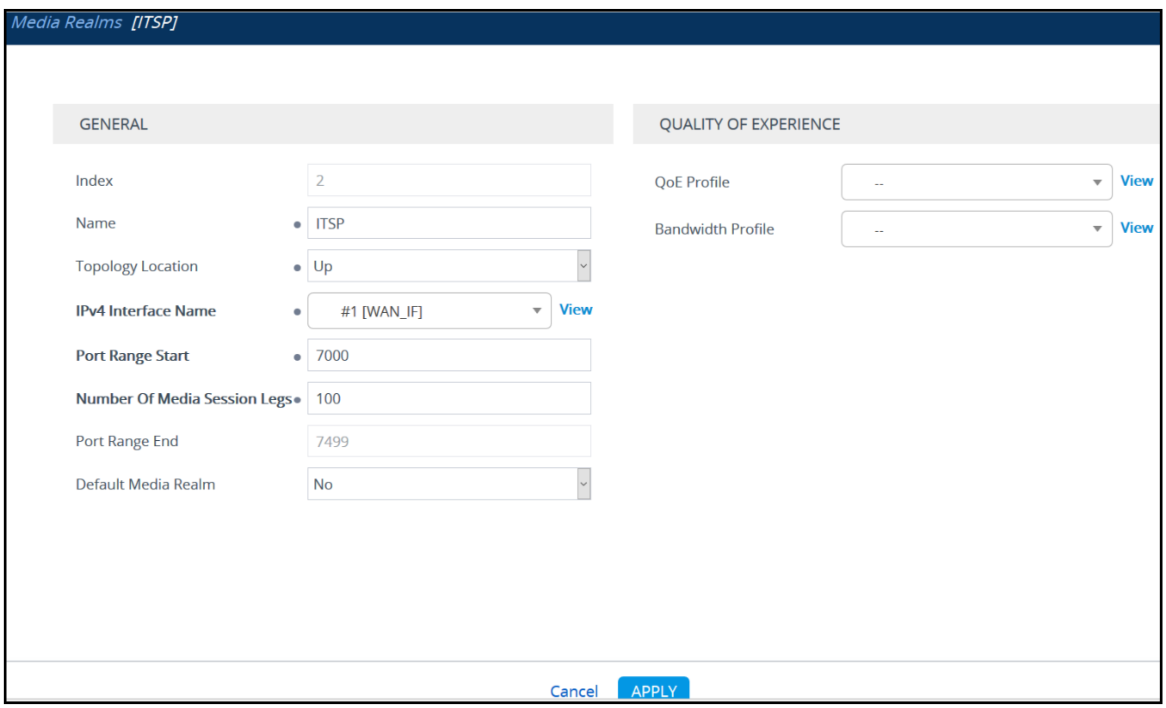


Figure 15 - Configuring Media Realm for WAN

The configured Media Realms are shown in the figure 16 below

Media Realms (2)

+ New Edit Page 1 of 1 Show 10 records per page

INDEX	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	IP-PBX	LAN_IP	6000	100	6499	No
1	ITSP	WAN_IP	7000	100	7499	No

Figure 16 - Configured Media Realms in Media Realm Table

Configure Media Security

This step describes how to enable Media Encryption

To Configure Media Encryption

Open the Media Security (Setup menu > Signaling & Media tab > Media folder > Media Security).

The Configured Media Security in Below Figure

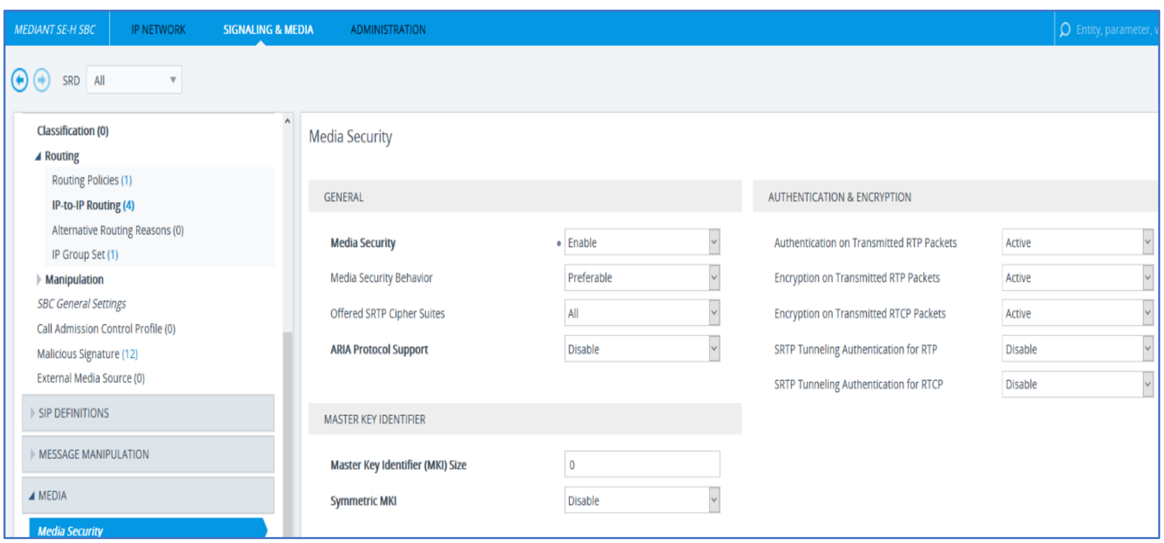


Figure 17 - Configured Media Security

Configure SIP Interfaces

This step describes how to configure SIP Interfaces. In the example scenario, an internal and external SIP Interface must be configured for the E-SBC

To configure SIP Interfaces:

Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).

Add a SIP Interface for the LAN interface. You can use the default SIP Interface (Index 0), but modify it as shown below and Click Apply

Parameter	Value
Index	1
Name	LAN SIP IFC
Network Interface	LAN_IP
Application Type	SBC
UDP	5060
TCP and TLS Port	0
Media Realm	IP-PBX

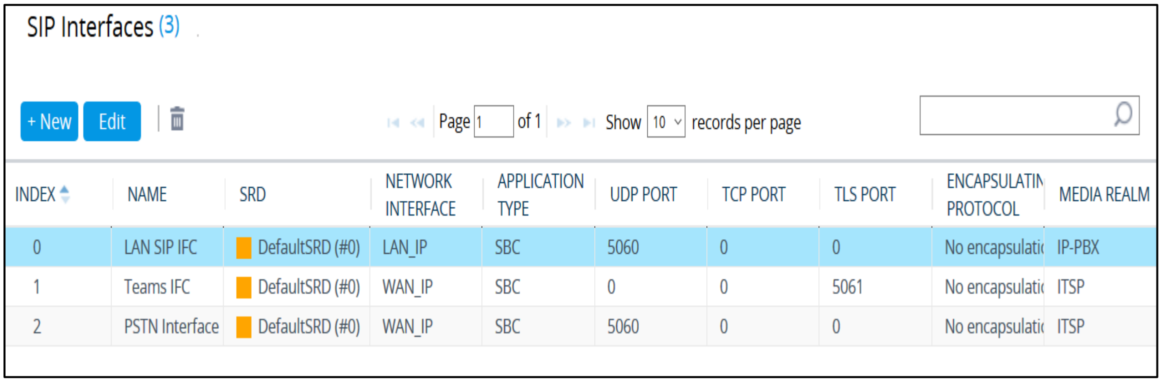
Configure a SIP Interface for the WAN for Teams and Click Apply

Parameter	Value
Index	2
Name	sipInterface2
Network Interface	WAN_IP
Application Type	SBC
UDP and TCP Port	0
TLS Port	5061
Media Realm	ITSP

Configure a SIP Interface for the WAN for PSTN and Click Apply

Parameter	Value
Index	2
Name	sipInterface2
Network Interface	WAN_IF
Application Type	SBC
UDP	5060
TCP and TLS Port	0
Media Realm	ITSP

The configured SIP Interfaces are shown in the figure 18


SIP Interfaces (3)

+ New | Edit | Page 1 of 1 | Show 10 records per page

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATIN PROTOCOL	MEDIA REALM
0	LAN SIP IFC	DefaultSRD (#0)	LAN_IP	SBC	5060	0	0	No encapsulati	IP-PBX
1	Teams IFC	DefaultSRD (#0)	WAN_IP	SBC	0	0	5061	No encapsulati	ITSP
2	PSTN Interface	DefaultSRD (#0)	WAN_IP	SBC	5060	0	0	No encapsulati	ITSP

Figure 18 - Configured SIP Interfaces in SIP Interface Table

Configure Proxy Sets

This step describes how to configure Proxy Sets. The Proxy Set defines the destination address (IP address or FQDN) of the IP entity server. Proxy Sets can also be used to configure load balancing between multiple servers.
In the example scenario, two Proxy Sets need to be configured for the following IP entities

MiVO400
Teams

Service provider SIP Trunk

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

To configure Proxy Sets:

Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder >**Proxy Sets**).

Add a Proxy Set for the MIVO400 as shown below in Figure 19 and Click Apply

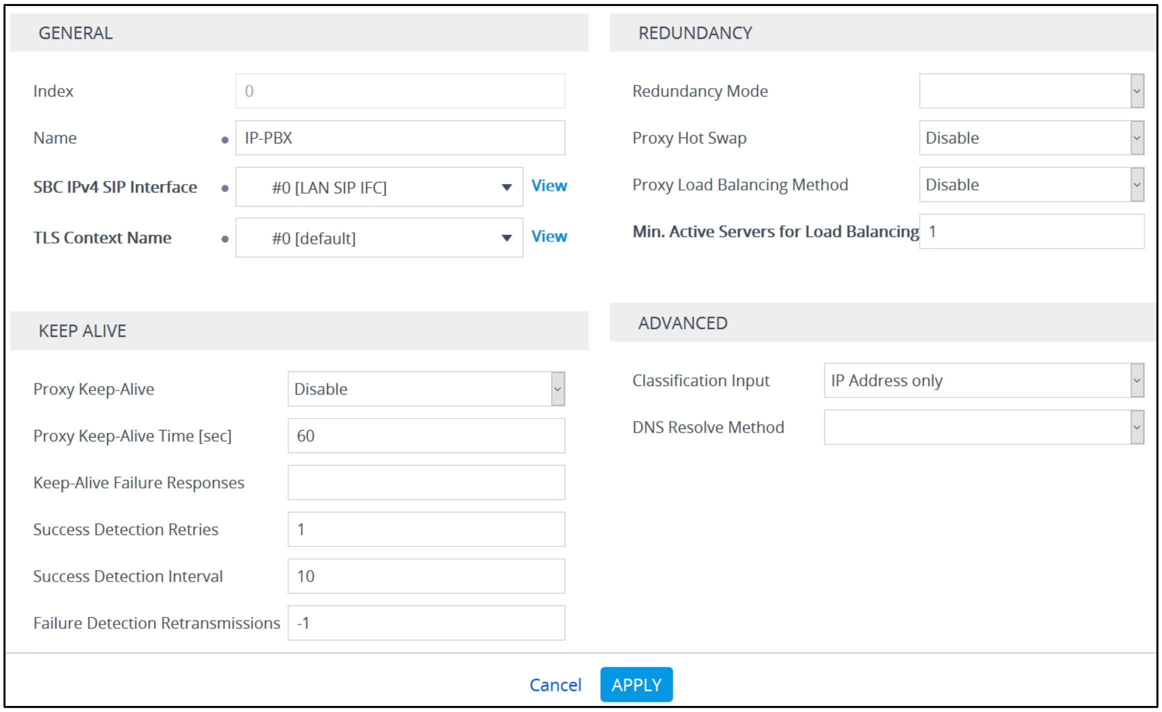


Figure 19 - Configuring Proxy Set for MIVO400

Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
Click **New**; the following dialog box appears as in Figure 20 and Configure the address of the Proxy Set according to the parameters and Click Apply

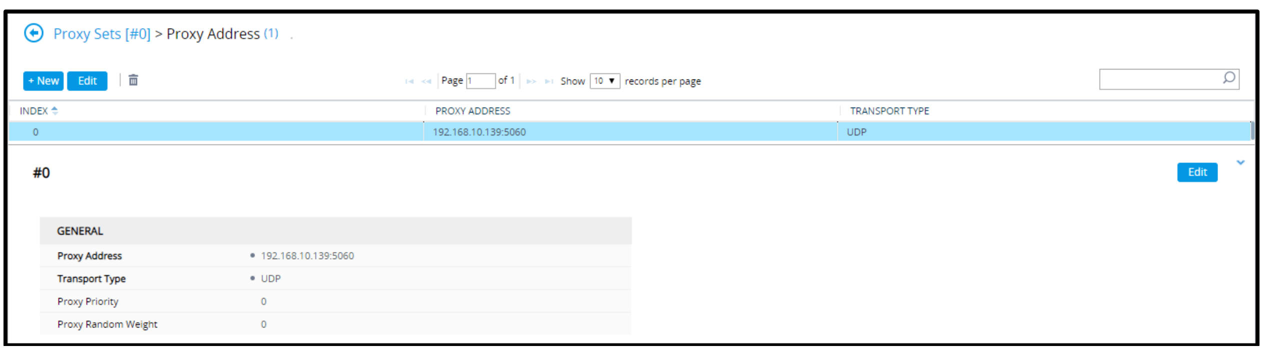


Figure 20 - Configuring Proxy Address for MIVO400

Add a Proxy Set for the Teams as shown below in Figure 21 and Click Apply

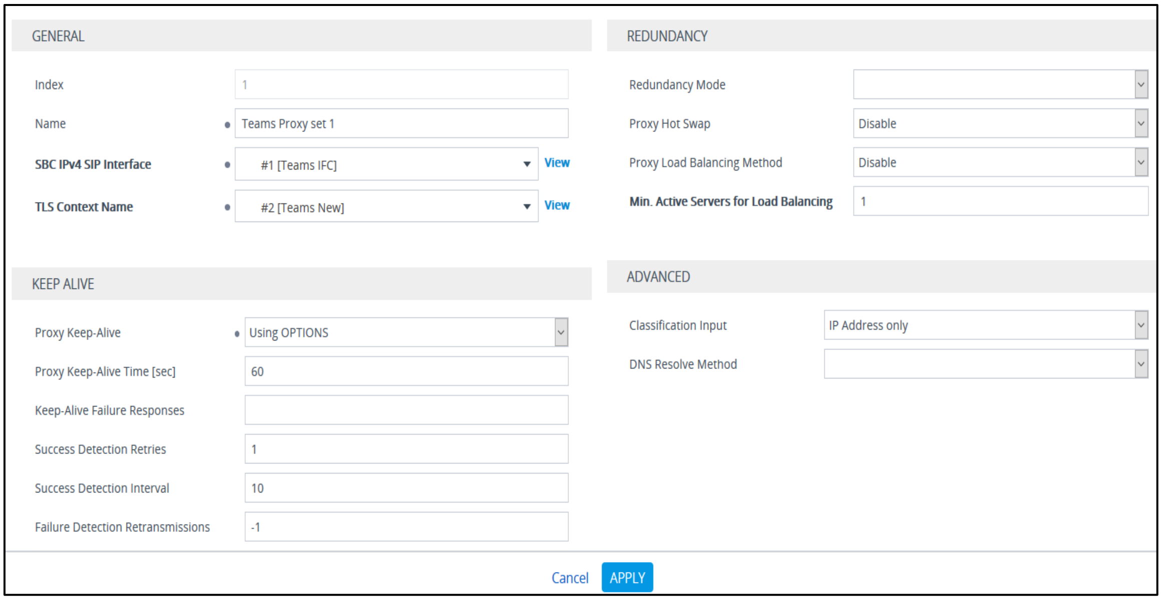


Figure 21 - Configuring Proxy Set for Teams

Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
Click **New**; the following dialog box appears as in Figure 21 and Configure the address of the Proxy Set according to the parameters and Click Apply

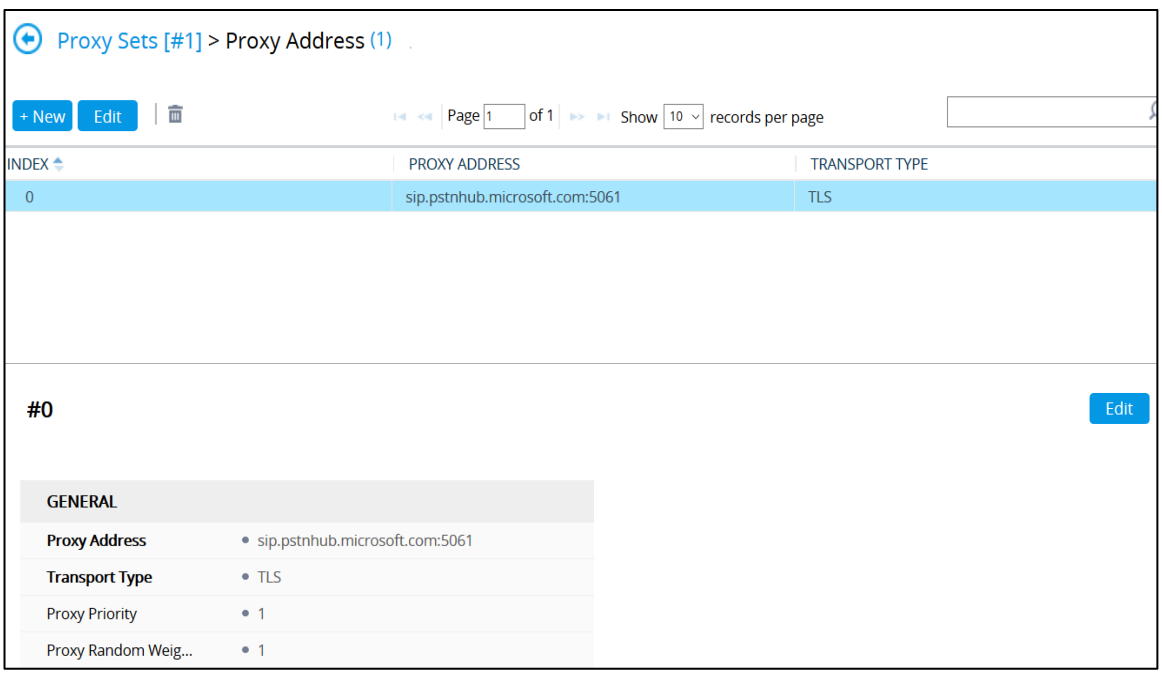


Figure 21A - Configuring Proxy Address for Teams

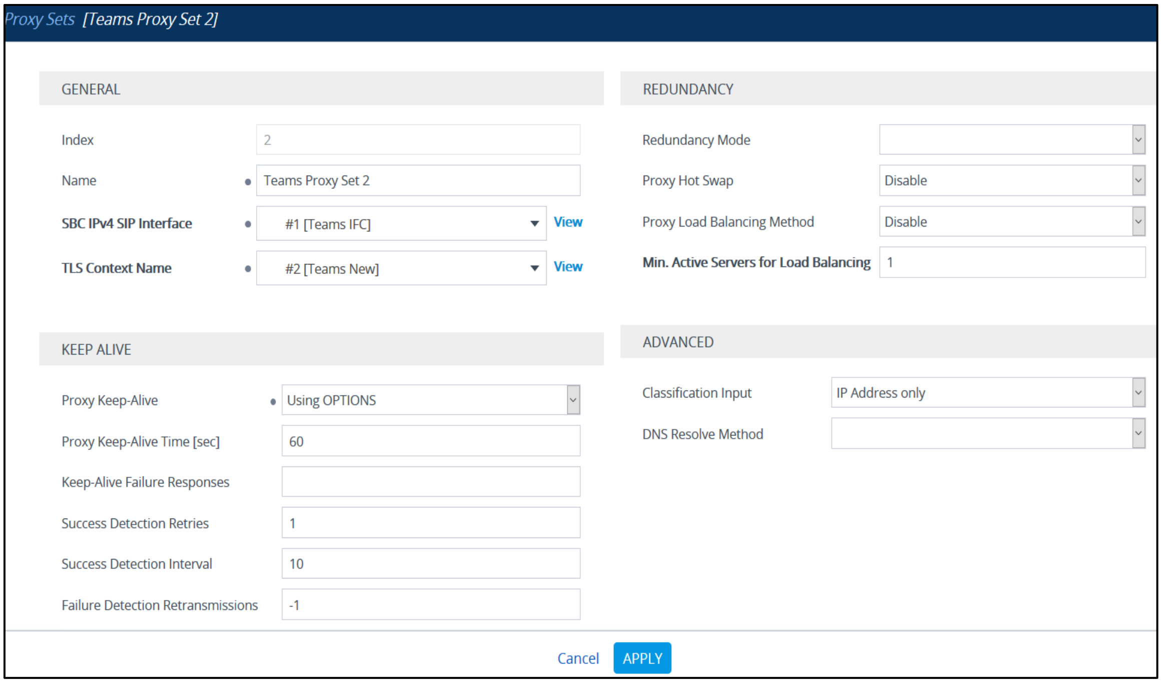


Figure 21C - Configuring Proxy Set for Teams

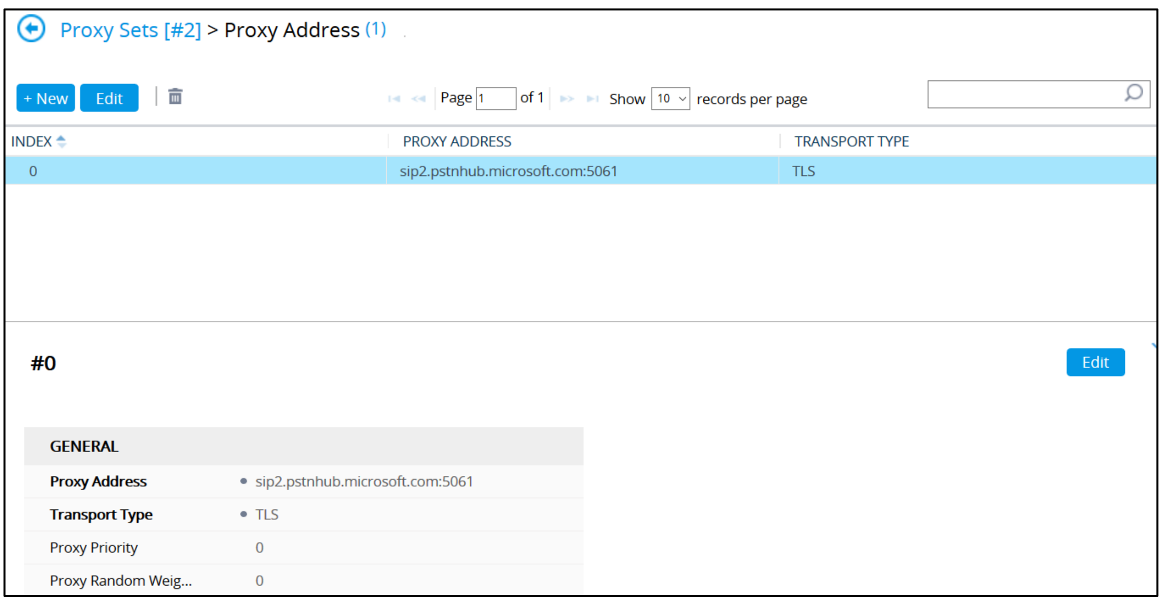


Figure 21D - Configuring Proxy Address for Teams

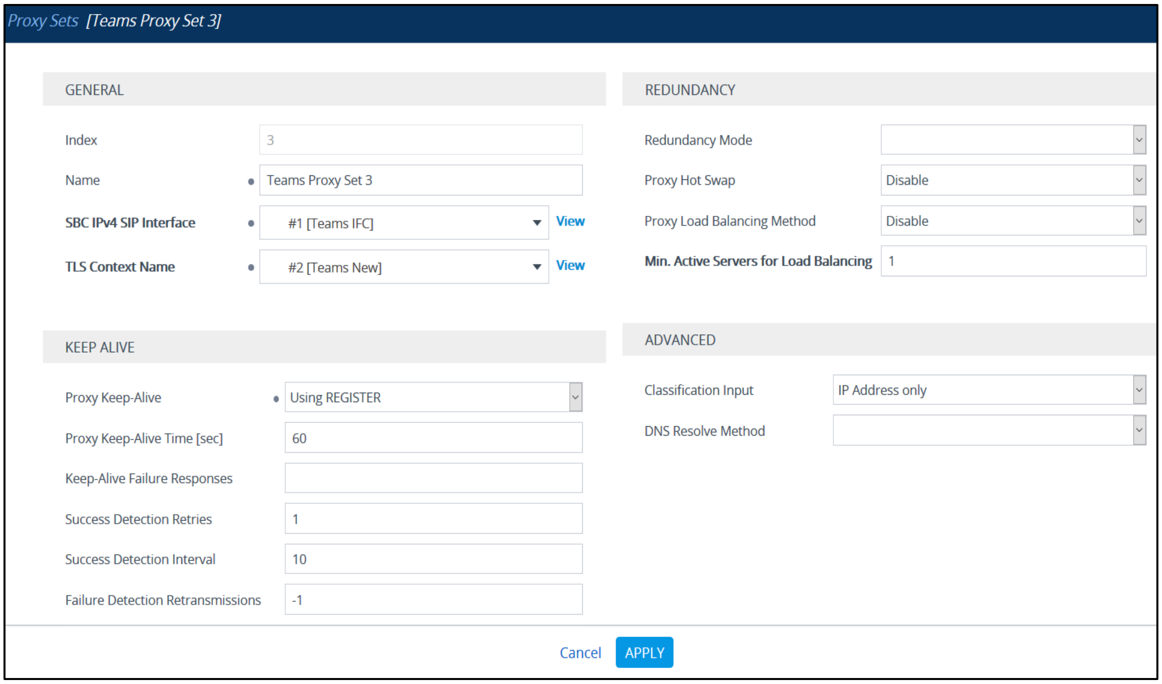


Figure 21E - Configuring Proxy Set for Teams

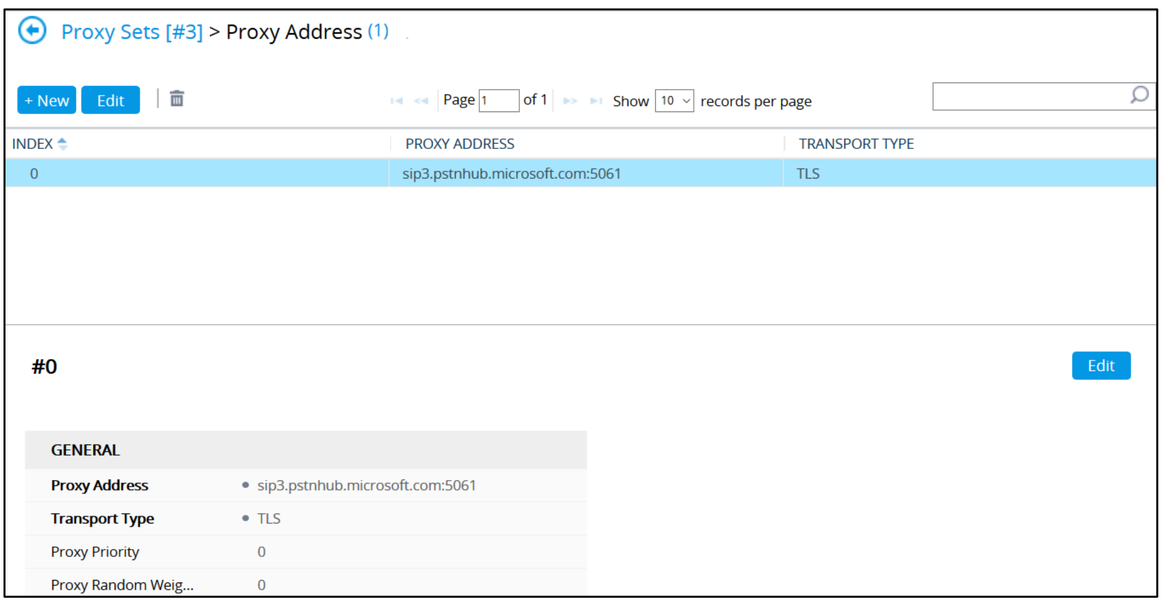


Figure 21F - Configuring Proxy Address for Teams

Add a Proxy Set for the Service Provider as shown below in Figure 22 and Click Apply

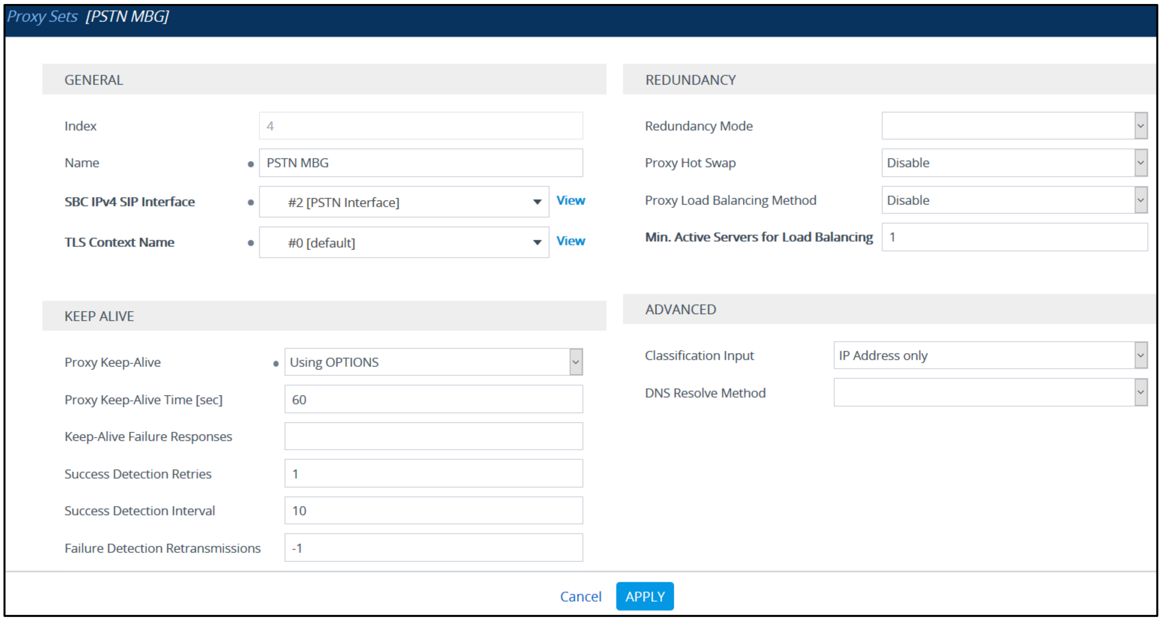


Figure 22 - Configuring Proxy Set for PSTN

Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
Click **New**; the following dialog box appears as in Figure 22A and Configure the address of the Proxy Set according to the parameters and Click Apply

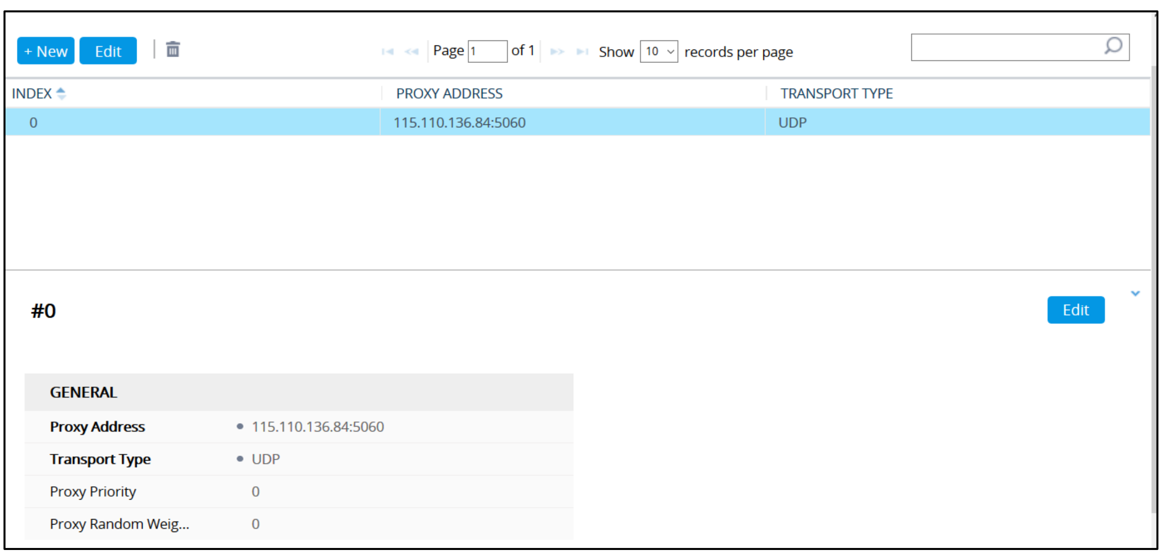
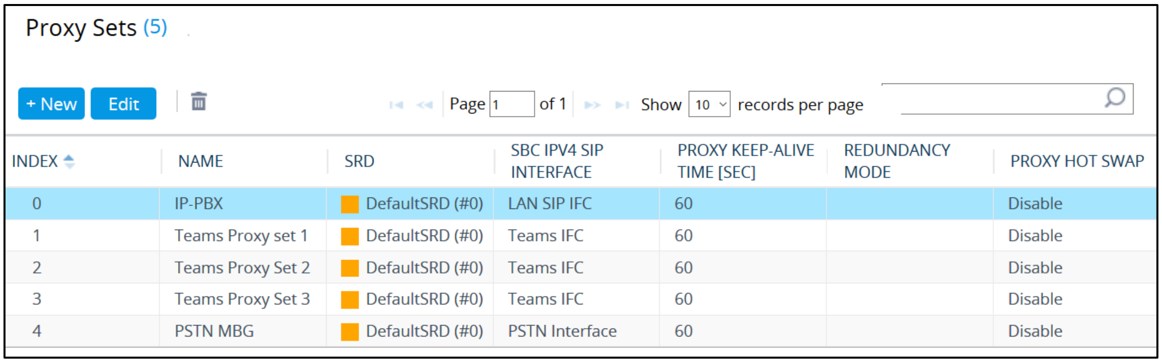


Figure 22A - Configuring Proxy Address for PSTN

The configured Proxy Sets are shown in the below Figure 23



Proxy Sets (5)

+ New | Edit | Page 1 of 1 | Show 10 records per page

INDEX	NAME	SRD	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	IP-PBX	DefaultSRD (#0)	LAN SIP IFC	60		Disable
1	Teams Proxy set 1	DefaultSRD (#0)	Teams IFC	60		Disable
2	Teams Proxy Set 2	DefaultSRD (#0)	Teams IFC	60		Disable
3	Teams Proxy Set 3	DefaultSRD (#0)	Teams IFC	60		Disable
4	PSTN MBG	DefaultSRD (#0)	PSTN Interface	60		Disable

Figure 23 - Proxy Sets

Configure Coder Groups

This step describes how to configure coders (termed *Coder Group*).
Note that Coder Group ID for this entity will be assign to its corresponding IP Profile in the next step.
Refer AudioCodes Config Guide for Details Explanations about use of Coders Group

To configure Coder Groups:

Open the Coder Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Coder Groups**).

Configure a Coder Group (We can configure multiple Coder Group and assign to different IP Profiles. See Figure 24

Click Apply

Parameter	Value
Coder Group ID	1
Coder Name	G.711 U-Law G.711 A-Law
Silence Suppression	**Enable** (for both coders)

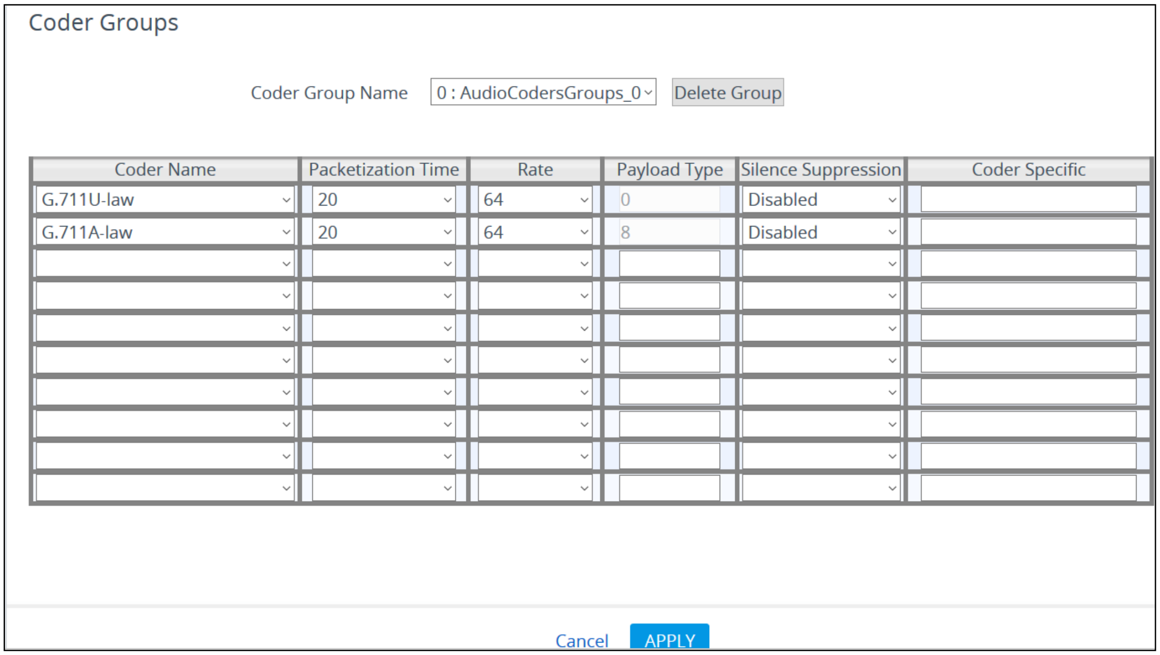


Figure 24 - Configuring Coder Group

Note:
For Interop Testing we didn't configure any Coder Group. We have allowed SBC to use Same codec from Teams to PBX and PBX to Teams

To configure Media Setting

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

Click Apply (Default Configuration). See Figure 25

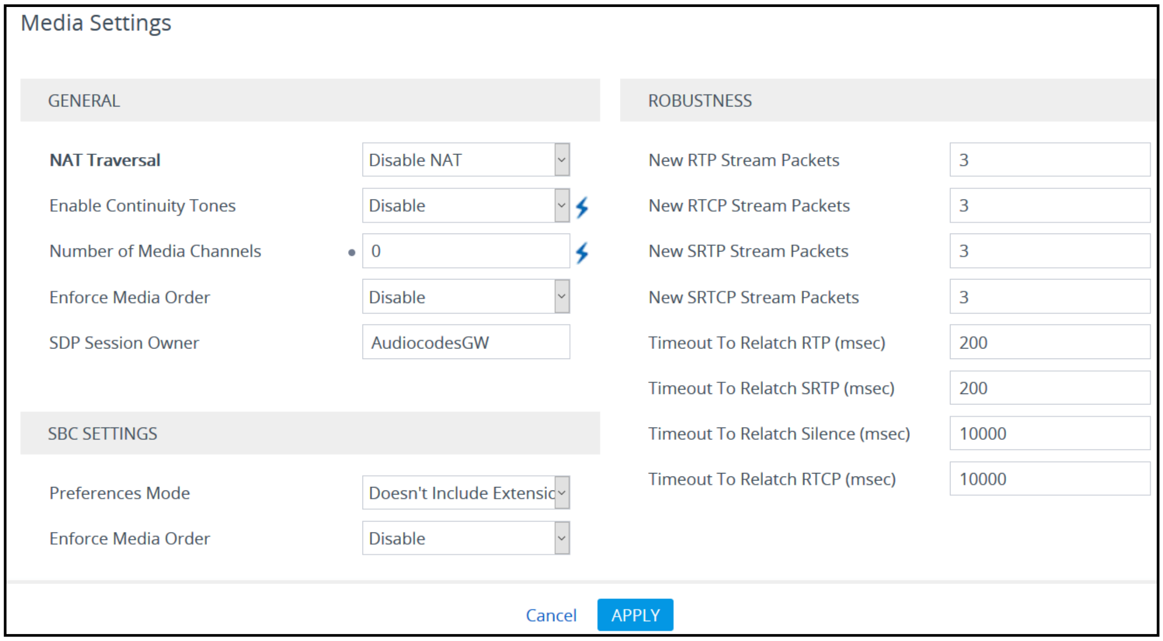


Figure 25 – Media Settings

Configure IP Profiles

This step describes how to configure IP Profiles. The IP Profile defines a set of call capabilities relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder and transcoding method). In the example scenario, IP Profiles need to be configured for the following IP entities:

MIVO400
Service provider SIP Trunk

To configure IP Profiles for MIVO400

Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).

Click **New**

Give Name and Click Apply (Default Configuration is applied for the IP Profiles for Interop Testing). See Figure 26,27,28,29,30

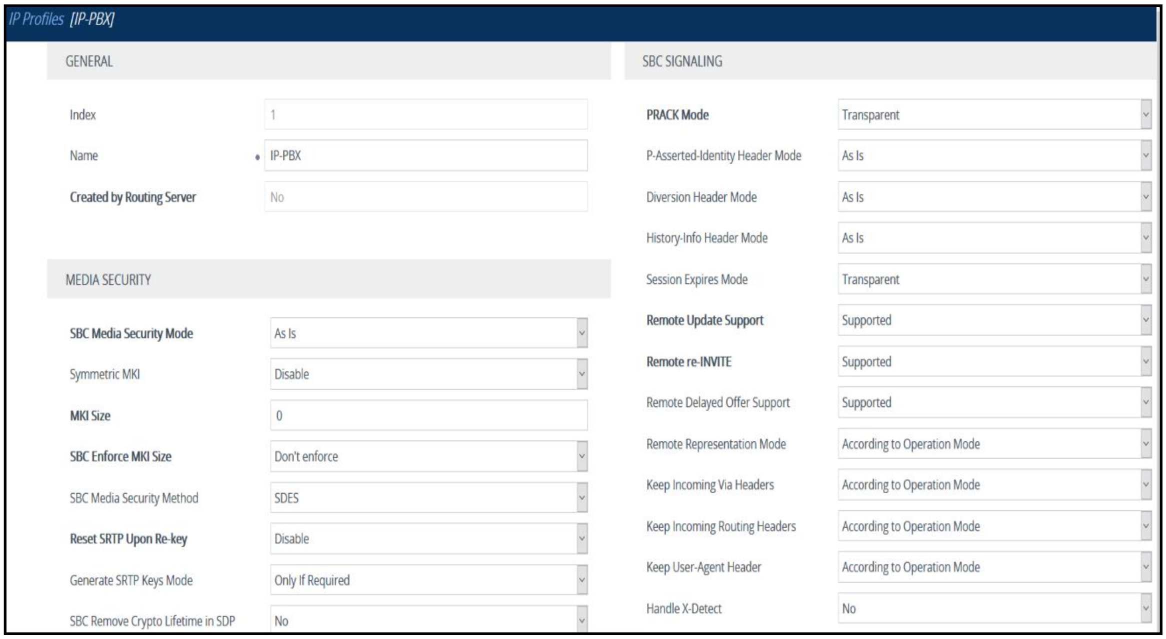


Figure 26 – IP Profiles (MIVO400)

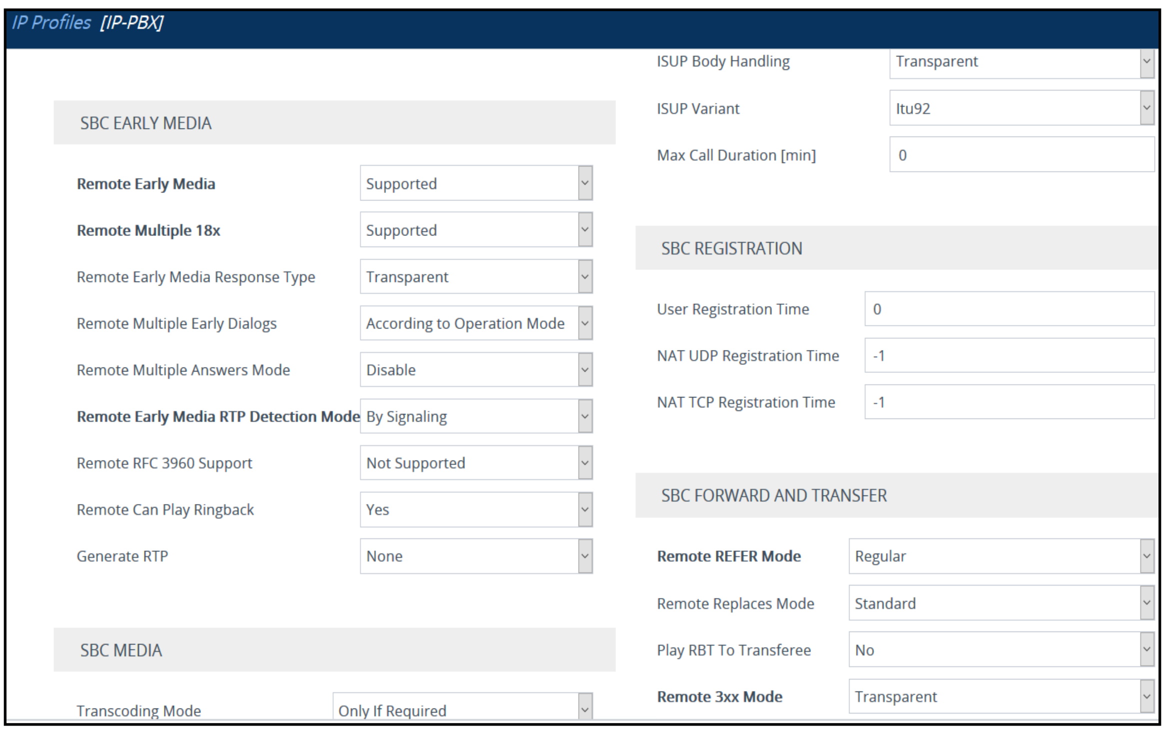


Figure 27 – IP Profiles (MIVO400)

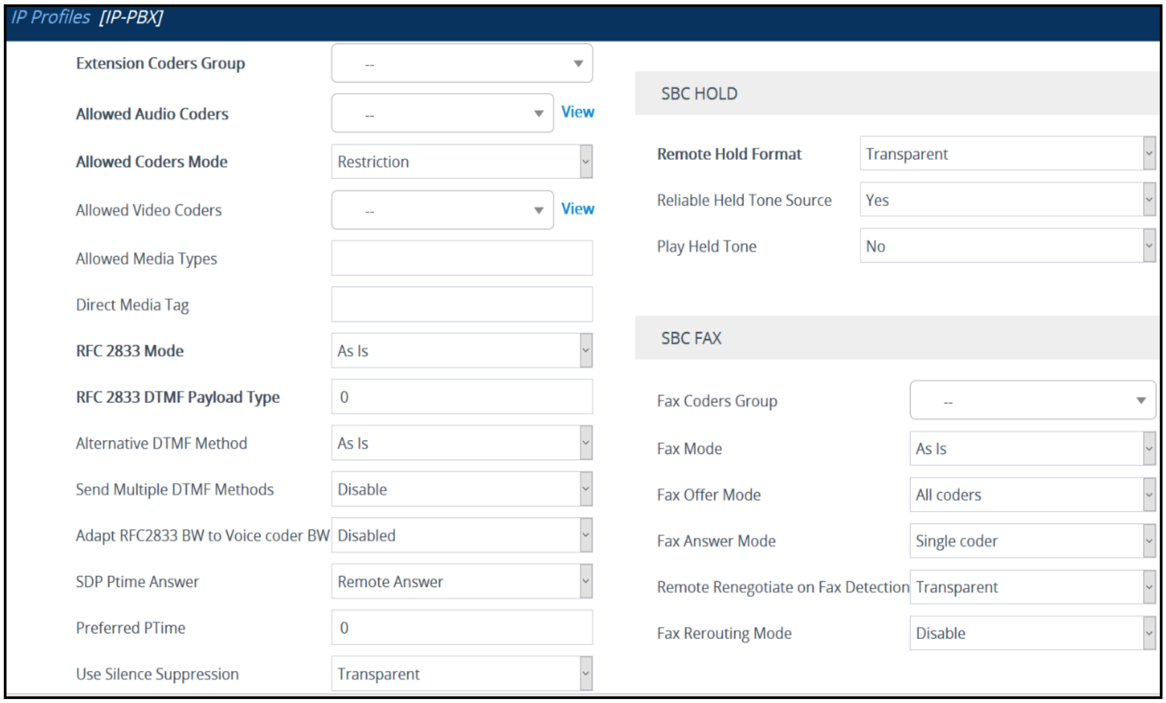


Figure 28 – IP Profiles (MIVO400)

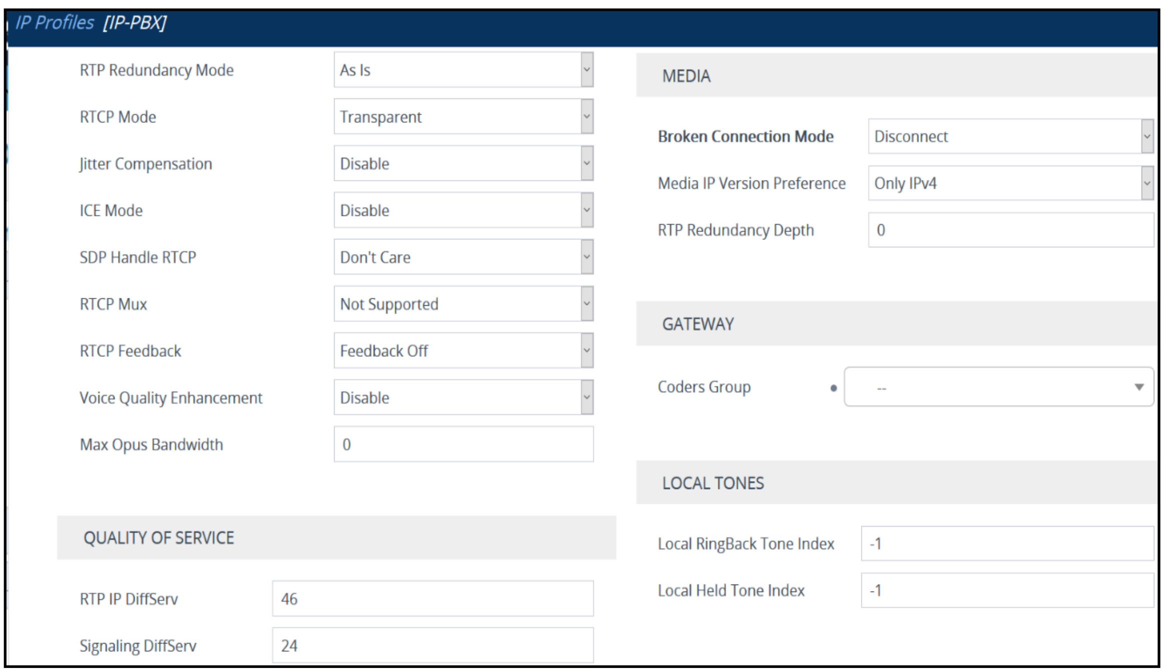


Figure 29 – IP Profiles (MIVO400)

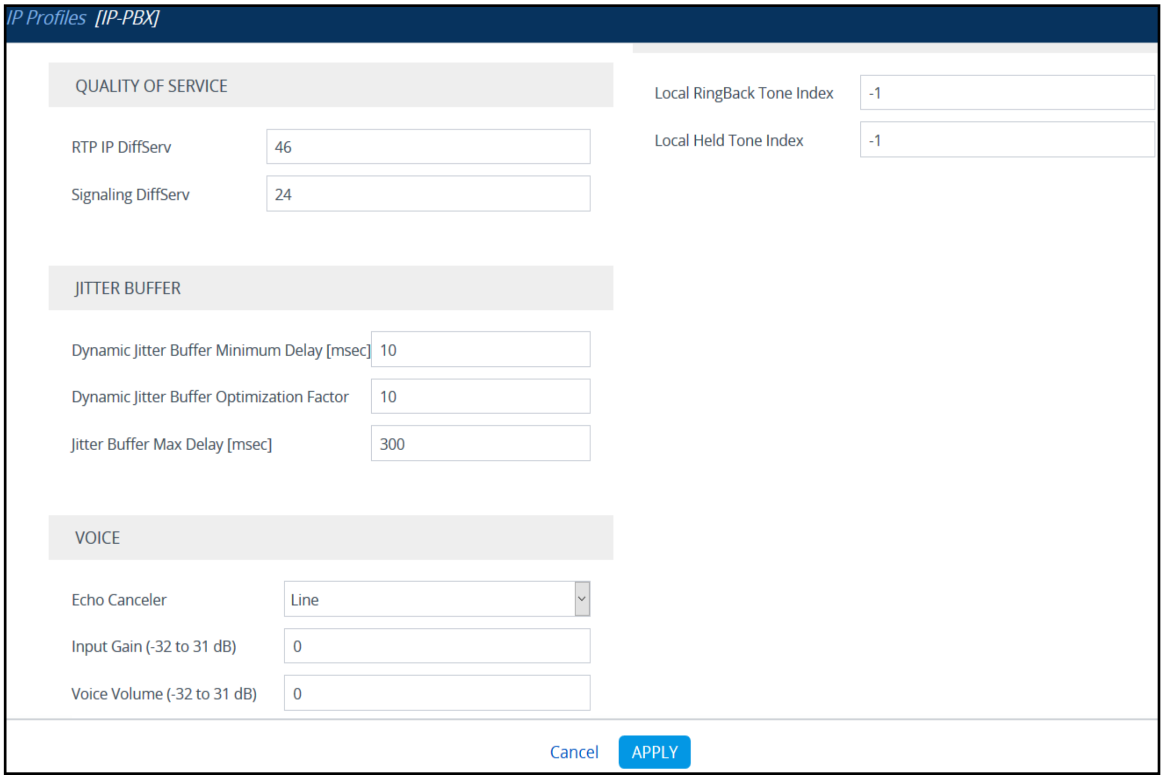


Figure 30 – IP Profiles (MIVO400)

To configure IP Profiles for Teams and Service Provider SIP Trunk

Click **New**

Give Name and Click Apply (Default Configuration is applied for the IP Profiles for Interop Testing). See Figure 31,32,33,34,35,35A,35B,35C

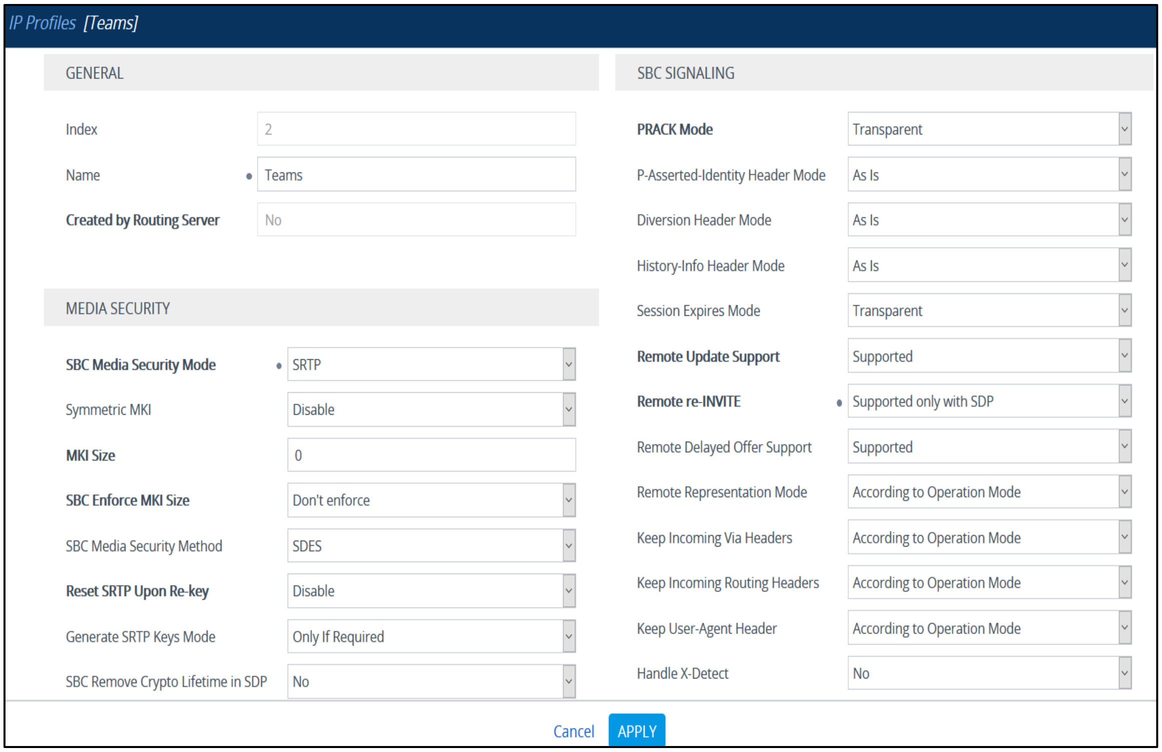


Figure 31 – IP Profiles (Teams)

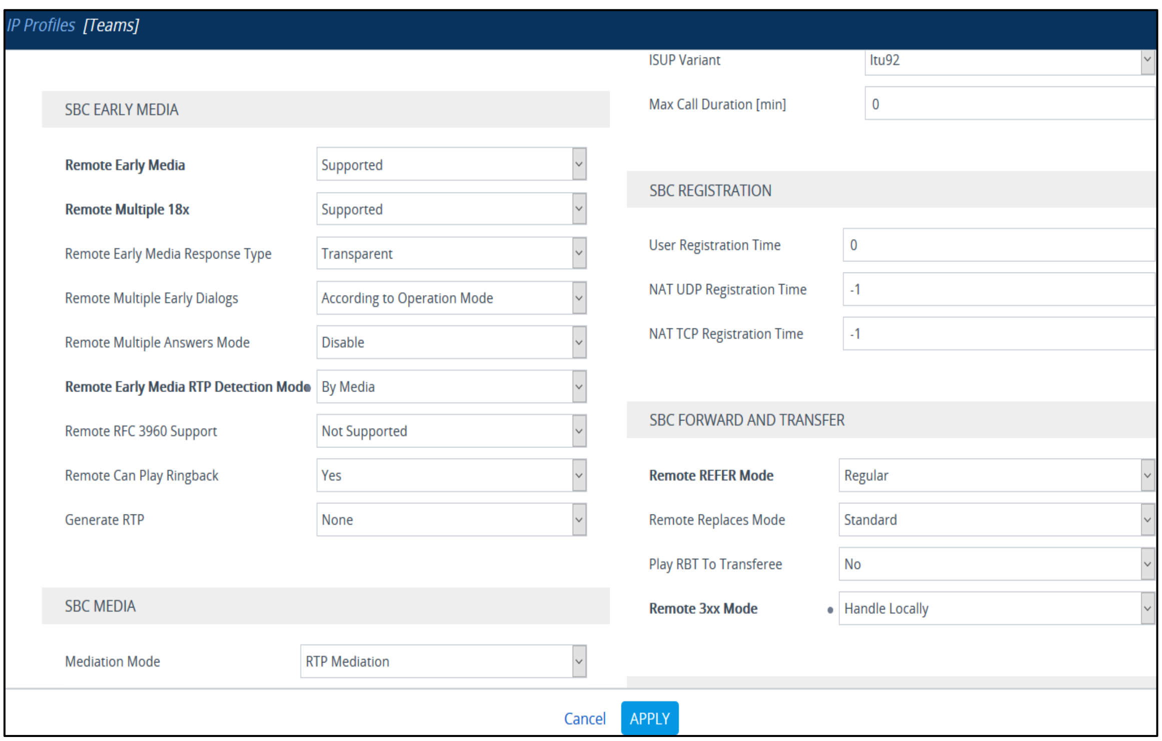


Figure 32 – IP Profiles (Teams)

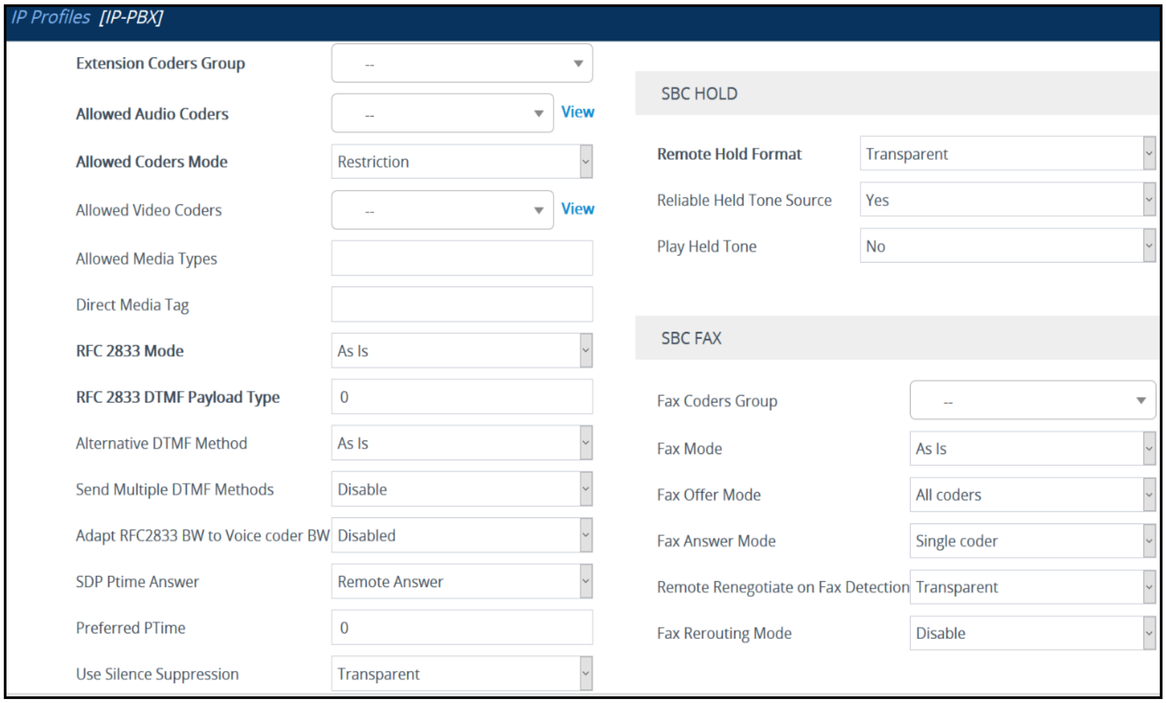


Figure 33 – IP Profiles (Teams)

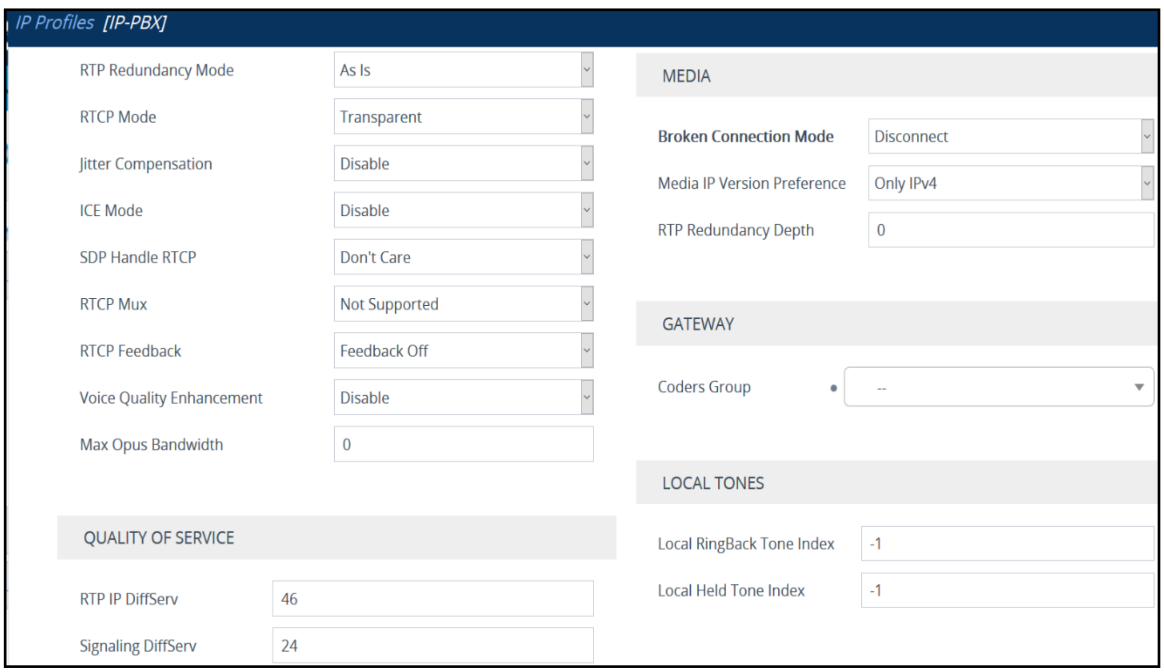


Figure 34 – IP Profiles (Teams)

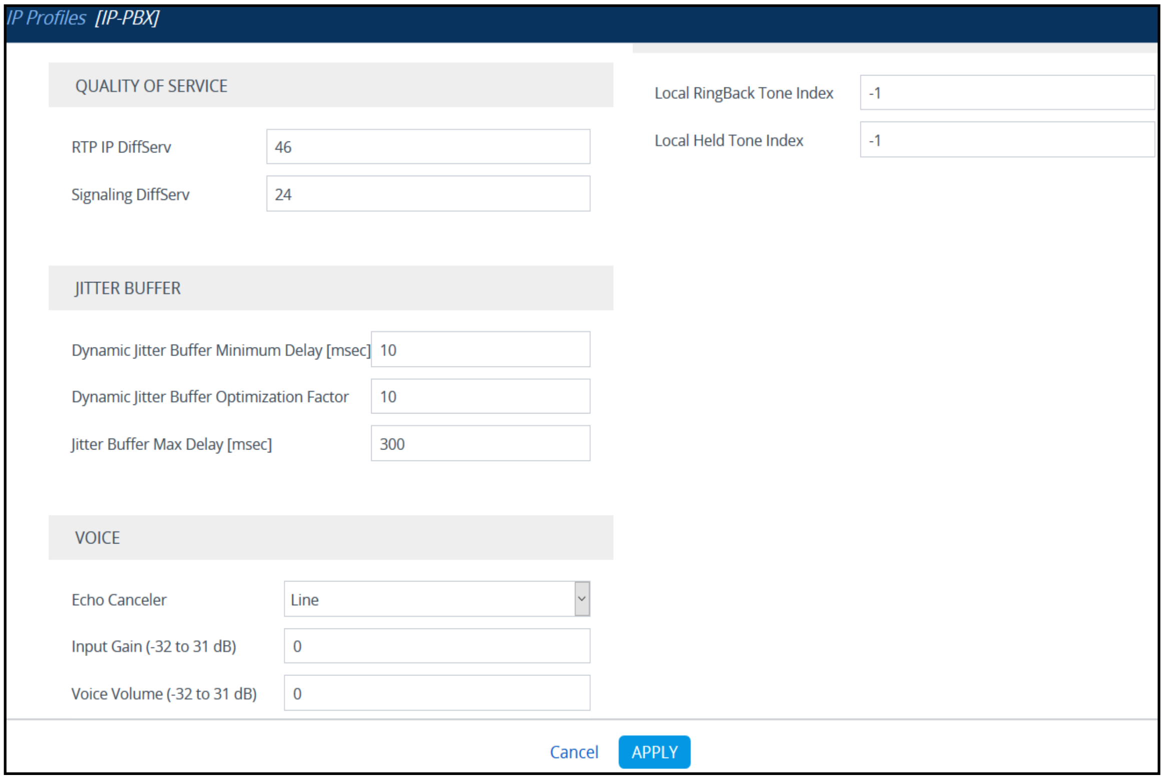


Figure 35 – IP Profiles (Teams)

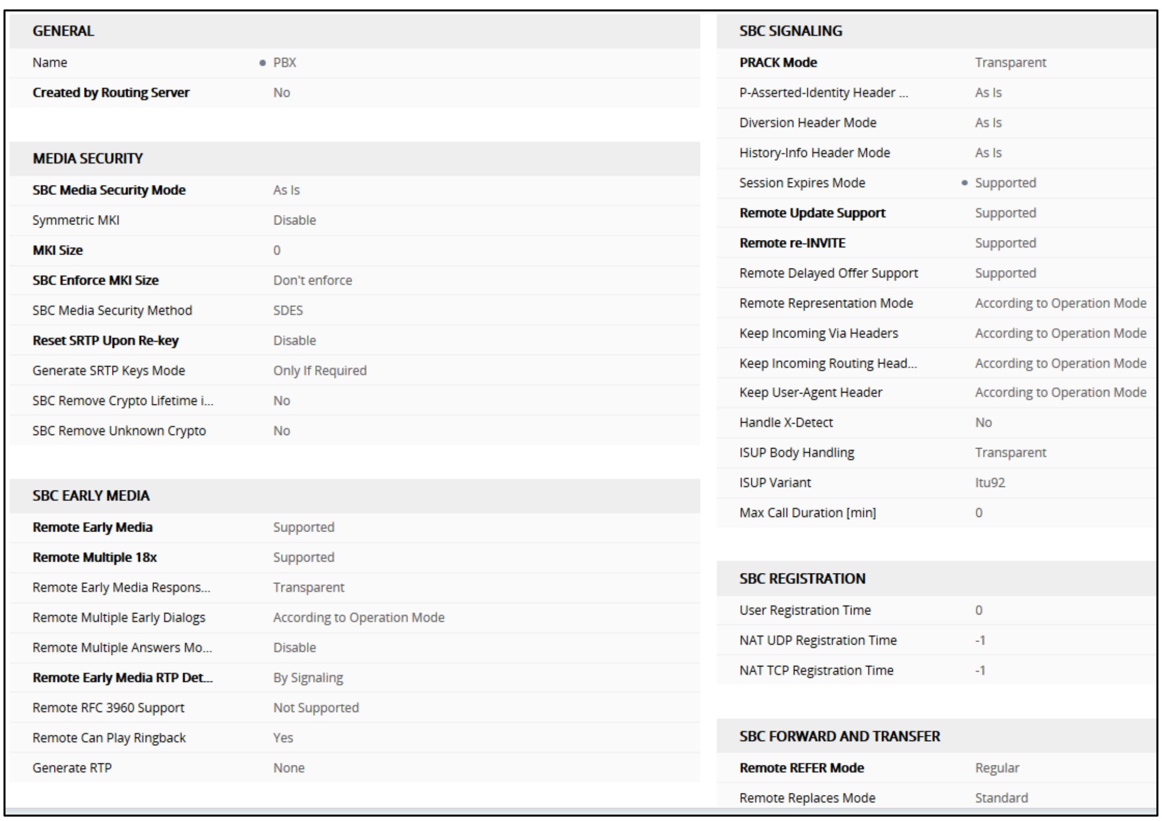


Figure 35A – IP Profiles (Service Provider)

SBC MEDIA		
Mediation Mode	RTP Mediation	
Extension Coders Group	• AudioCodersGroups_1	
Allowed Audio Coders	--	View
Allowed Coders Mode	Restriction	
Allowed Video Coders	--	View
Allowed Media Types		
Direct Media Tag		
RFC 2833 Mode	As Is	
RFC 2833 DTMF Payload Type	• 101	
Alternative DTMF Method	As Is	
Send Multiple DTMF Methods	Disable	
Adapt RFC2833 BW to Voice c...	Disabled	
SDP Ptime Answer	Remote Answer	
Preferred PTime	• 20	
Use Silence Suppression	Transparent	
RTP Redundancy Mode	As Is	
RTCP Mode	Transparent	
Jitter Compensation	Disable	
ICE Mode	Disable	
SDP Handle RTCP	Don't Care	
RTCP Mux	Not Supported	
RTCP Feedback	Feedback Off	
Voice Quality Enhancement	Disable	
Max Opus Bandwidth	0	
Generate No-op	No	

Play RBT To Transferee	No
Remote 3xx Mode	Transparent

SBC HOLD	
Remote Hold Format	Transparent
Reliable Held Tone Source	Yes
Play Held Tone	No

SBC FAX	
Fax Coders Group	--
Fax Mode	As Is
Fax Offer Mode	All coders
Fax Answer Mode	Single coder
Remote Renegotiate on Fax ...	Transparent
Fax Rerouting Mode	Disable

MEDIA	
Broken Connection Mode	Disconnect
Media IP Version Preference	Only IPv4
RTP Redundancy Depth	Disable

LOCAL TONES	
Local RingBack Tone Index	-1
Local Held Tone Index	-1

Figure 35B – IP Profiles (Service Provider)

Generate No-op	No
Enhanced PLC	Disable

QUALITY OF SERVICE	
RTP IP DiffServ	46
Signaling DiffServ	24

JITTER BUFFER	
Dynamic Jitter Buffe...	10
Dynamic Jitter Buffe...	10
Jitter Buffer Max De...	300

VOICE	
Echo Canceler	Line
Input Gain (-32 to 3...	0
Voice Volume (-32 t...	0

Figure 35B – IP Profiles (Service Provider)

Configure IP Groups

This step describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the E- SBC communicates. This can be a server (e.g., IP PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

In the example scenario, IP Groups must be configured for the following IP entities:

MIVO400 located on LAN

Teams and Service provider SIP Trunk located on WAN

To configure IP Groups:

Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).

Add an IP Group for the MIVO400 with following values and rest all are default values

Parameter	Value
Index	1
Name	IP-PBX
Type	Server
Proxy Set	IP-PBX
IP Profile	IP-PBX
Media Realm	IP-PBX
SIP Group Name	AudioCodes WAN FQDN which Configured in Teams
SBC Operation Mode	B2BUA
Outbound Message Manipulation Set	As per Manipulation Configuration
Inbound Message Manipulation Set	As per Manipulation Configuration

Configure an IP Group for the Teams/ ITSP SIP Trunk

Parameter	Value
Index	1
Name	ITSP
Type	Server
Proxy Set	ITSP
IP Profile	ITSP
Media Realm	ITSP
SIP Group Name	Provider IP / FQDN
SBC Operation Mode	B2BUA
Outbound Message Manipulation Set	As per Manipulation Configuration
Inbound Message Manipulation Set	As per Manipulation Configuration

The configured IP Groups are shown in the Figure 36

IP Groups (5)

+ New Edit Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
0	PBX	DefaultSRD (	Server	B2BUA	IP-PBX	IP-PBX	IP-PBX	sbc.thesipcoe.c	Enable	-1	0
1	TeaMS IP Group 1	DefaultSRD (	Server	B2BUA	Teams Proxy set 1	Teams	ITSP	sip.pstnhub.mic	Enable	0	-1
2	Teams IP Group 2	DefaultSRD (	Server	B2BUA	Teams Proxy Set 2	Teams	ITSP	sip2.pstnhub.m	Enable	-1	-1
3	Teams IP Group 3	DefaultSRD (	Server	B2BUA	Teams Proxy Set 3	Teams	ITSP	sip3.pstnhub.m	Enable	-1	-1
4	PSTN MBG	DefaultSRD (	Server	B2BUA	PSTN MBG	PBX	ITSP	115.110.136.84	Enable	0	-1

Figure 36 - Configured IP Groups

Configure Message Manipulations

SIP Message Manipulation has been applied on the lab system to change the host part for inbound calling in to MiVO400. One should carefully assess all the possible options and identify SIP Message Manipulation requirements in a specific deployment

To configure Message Manipulations:

Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** > **Message Manipulations**).

The configured Message Manipulations are shown in below Figure

Message Manipulations (8)

+ New Edit Insert Page 1 of 1 Show 10 records per page

INDEX	NAME	MANIF SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	Team1	2	OPTIONS	param.message.address.dst.sipinterface=='1'	header.contact.url.host	Modify	'sbc.thesipcoe.com'	Use Curren
1	Change From Header towards PBX	0	Any	Header.Request-URI contains 'sbc.thesipcoe.com'	Header.From.URL.Host	Modify	'192.168.10.70:5060'	Use Curren
2	Change To Header towards PBX	0	Any	Header.Request-URI contains 'sbc.thesipcoe.com'	Header.To.URL.Host	Modify	'192.168.10.125'	Use Curren
3	Change Req URI Towards PBX	0	Any	Header.Request-URI contains 'sbc.thesipcoe.com'	Header.Request-URI.URL.Host	Modify	'192.168.10.125'	Use Curren
4	Remove Prefix +91 in Req URI	0	Any	header.Request-URI.URL contains '+91'	Header.Request-URI.URL.User	Remove Prefix	'+91'	Use Curren
5	Change Refer To Header	0	Refer	header.Refer-To.URL contains '+91'	Header.Refer-To.URL.User	Remove Prefix	'+91'	Use Curren
6	Remove + in From	0	Any	Header.from.URL contains '+'	Header.From.URL.User	Remove Prefix	'+'	Use Curren
7	Remove +91 in To Header	0	Any	header.to.URL contains '+91'	Header.to.URL.User	Remove Prefix	'+91'	Use Curren

#0[Team1]

Figure - Configured Message Manipulations

Configure IP-to-IP Call Routing Rules

This step describes how to configure IP- to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-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

In the example scenario, the following IP-to-IP routing rules need to be configured to route calls between MIVO400 (LAN) and Service provider SIP Trunk (WAN):

Calls from MIVO400 to PSTN
Calls from MIVO400 to Teams
Calls from Teams to MIVO400
Calls from PSTN to MIVO400

To configure IP-to-IP routing rules:

Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).

Click **New**, and then configure the parameters as follows for MIVO400 to Service provider, See Figure 37

Click Apply

Parameter	Value
Index	0
Name	IP-PBX -> PSTN
Source IP Group	PBX
Destination Type	IP Group
Destination IP Group	PSTN MBG
Destination SIP Interface	
Destination Port	5060
Destination Transport Type	udp

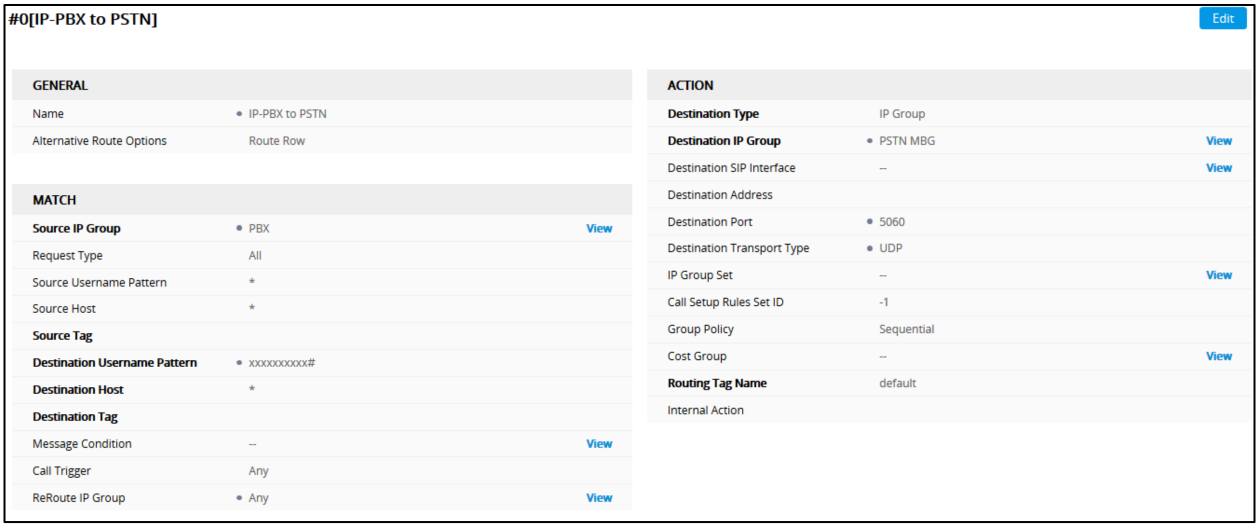


Figure 37 - Configuring IP-to-IP Routing Rule for MIVO400 to Service provider

Click **New**, and then configure the parameters as follows for PSTN to MIVO400, See Figure 37A

Click Apply

Parameter	Value
Index	3
Name	PSTN to PBX
Source IP Group	PSTN MBG
Destination Type	IP Group
Destination IP Group	PBX
Destination SIP Interface	
Destination Port	5060
Destination Transport Type	udp

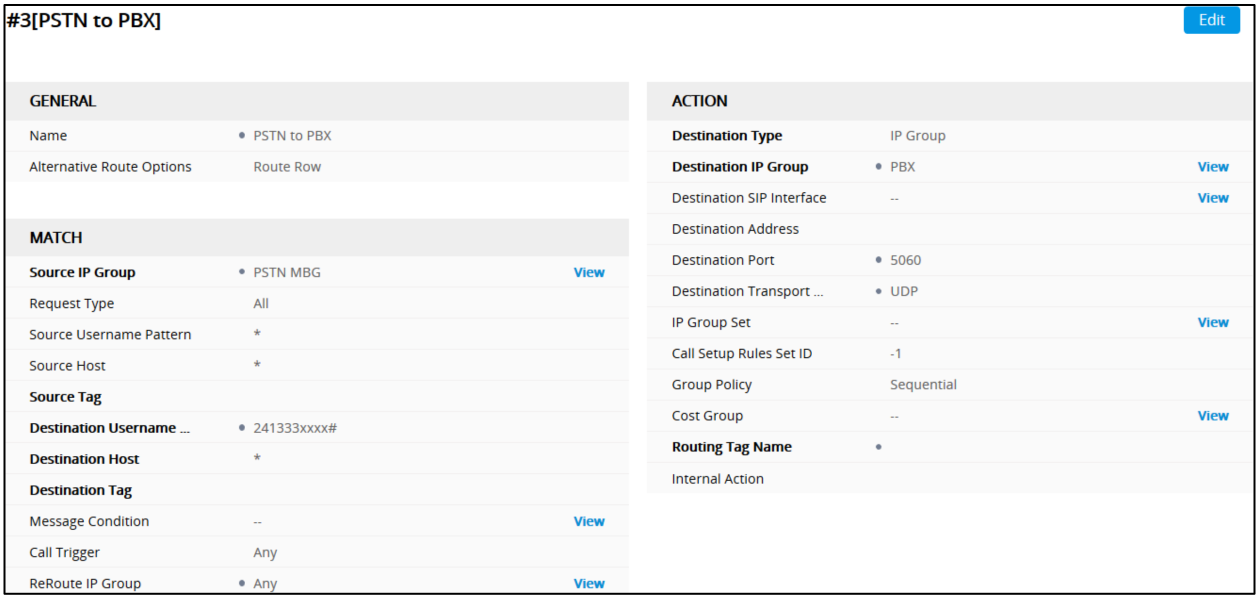


Figure 37A - Configuring IP-to-IP Routing Rule for PSTN to MIVO400

Click New, and then configure the parameters as follows for MIVO400 to Teams, See Figure 37A

Click Apply

Parameter	Value
Index	1
Name	IP-PBX to Teams
Source IP Group	PBX
Destination Type	IP Group Set
Destination IP Group	Teams IP Group
Destination SIP Interface	
Destination Port	5061
Destination Transport Type	TLS

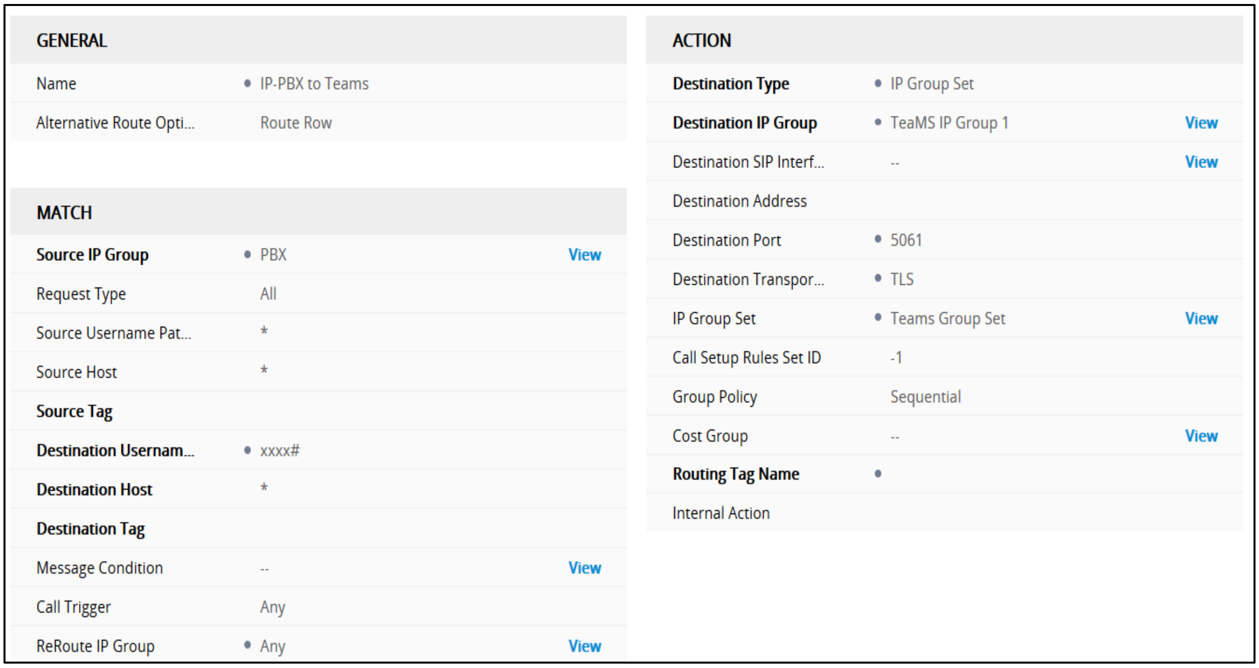


Figure 38 - Configuring IP-to-IP Routing Rule for MIVO400 to Teams

Click **New**, and then configure the parameters as follows for MIVO400 to Teams, See Figure 38A

Click Apply

Parameter	Value
Index	2
Name	Teams to IP-PBX
Source IP Group	Teams IP Group
Destination Type	IP Group
Destination IP Group	PBX
Destination SIP Interface	
Destination Port	5060
Destination Transport Type	UDP

The configured routing rules are shown in the Figure 38A

IP Groups (5)

+ New Edit

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATIC SET	OUTBOUND MESSAGE MANIPULATI SET
0	PBX	DefaultSRD	Server	B2BUA	IP-PBX	IP-PBX	IP-PBX	sbc.thesipcoe.	Enable	-1	0
1	TeaMS IP Grou	DefaultSRD	Server	B2BUA	Teams Proxy s	Teams	ITSP	sip.pstnhub.m	Enable	0	-1
2	Teams IP Grou	DefaultSRD	Server	B2BUA	Teams Proxy S	Teams	ITSP	sip2.pstnhub.r	Enable	-1	-1
3	Teams IP Grou	DefaultSRD	Server	B2BUA	Teams Proxy S	Teams	ITSP	sip3.pstnhub.r	Enable	-1	-1
4	PSTN MBG	DefaultSRD	Server	B2BUA	PSTN MBG	PBX	ITSP	115.110.136.8	Enable	0	-1

Figure 38A - Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

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

Configure IP Group Sets

IP Group Set - the destination can be based on multiple IP Groups for load balancing, where each call may be sent to a different IP Group within the IP Group Set depending on the IP Group Set's definition

The IP Group Sets will be later applied to the IP-IP Call Routing

To configure IP Group Sets:

Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP Group Set**).

Add a Proxy Set for the MIVO400 as shown below in Figure 39 and 39A

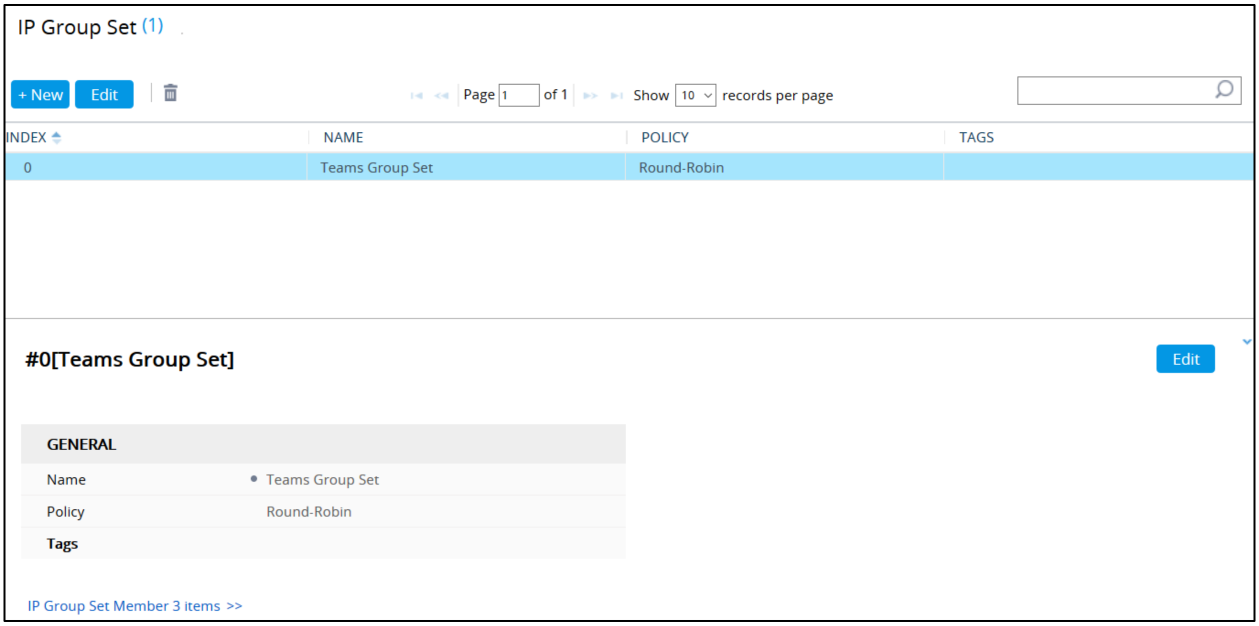


Figure 39 -Configuring IP Group Set for Teams

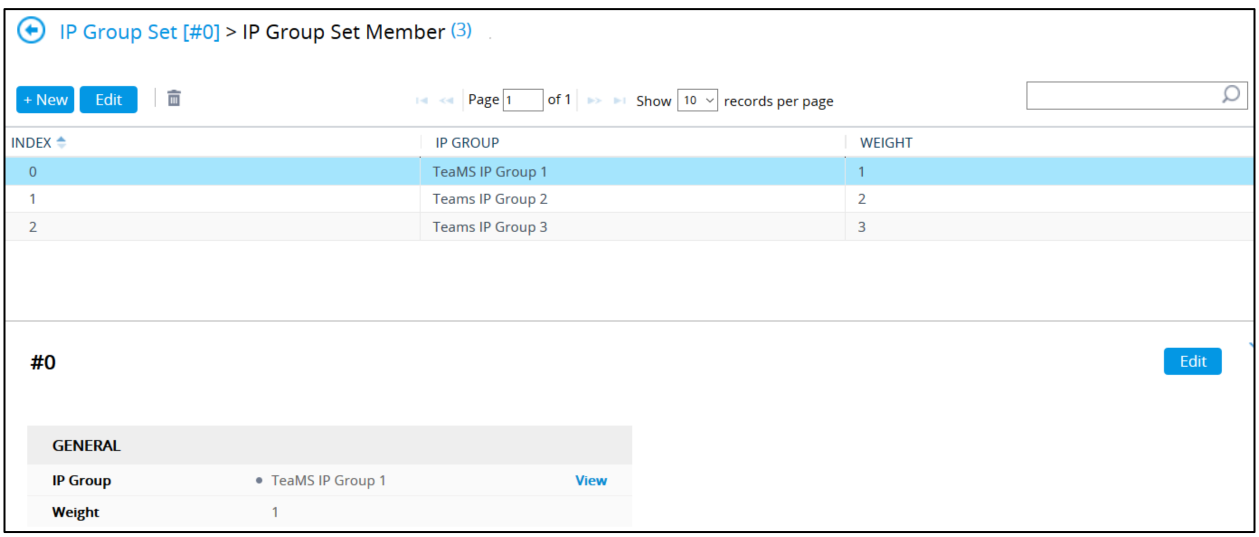


Figure 39A-Configuring IP Group Set Members for Teams

Configure Registration Accounts

This step describes how to configure SIP registration accounts. This is required so that the E-SBC can register with the Service provider SIP Trunk on behalf of MIVO400. The Service provider SIP Trunk requires registration and authentication to provide service.

In the interoperability test topology, the Served IP Group is MIVO400 IP Group and the Serving IP Group is Service provider SIP Trunk IP Group.

To configure a registration account:

Open the Accounts table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**).

Click **New**.

Configure the account according to the provided information from, for example as See in Figure 40

Parameter	Value
Served IP Group	**IP-PBX**
Application Type	**SBC**
Serving IP Group	**ITSP**
Host Name	As provided by the SIP Trunk provider
Register	**Regular**
Contact User	**1234567890** (trunk main line)
User Name	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

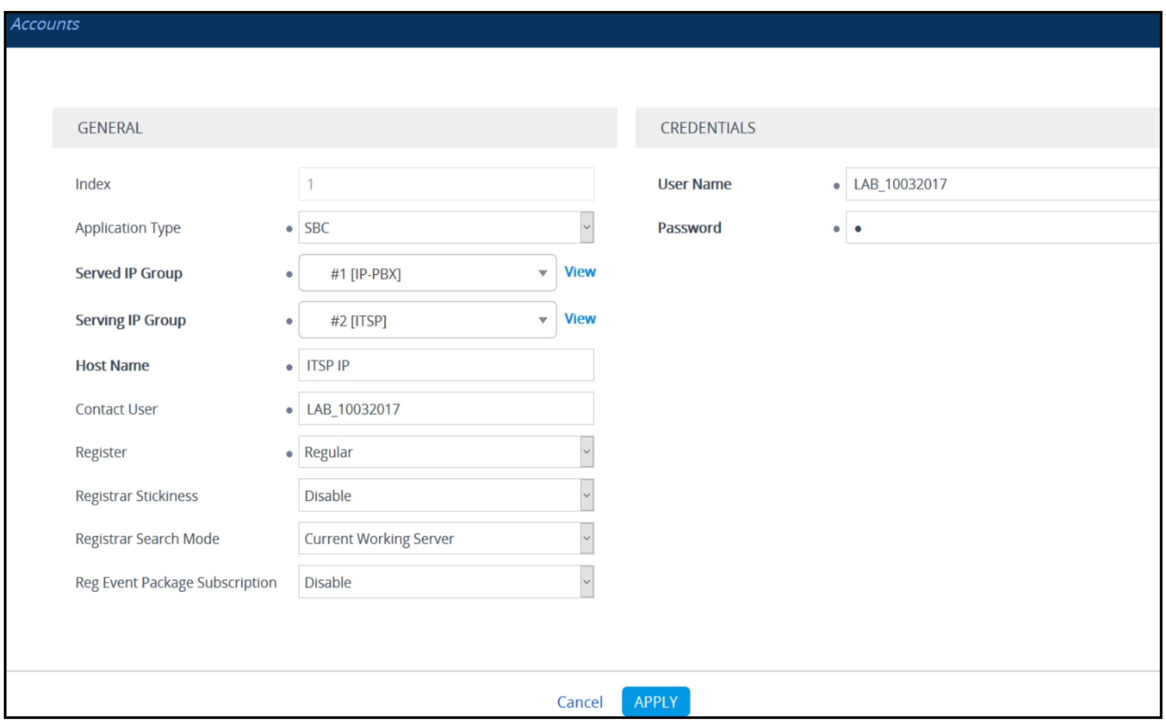


Figure 40 - Configuring a SIP Registration Account

TLS Configuration

Microsoft Phone System only allows TLS connections from SBCs for SIP traffic with a certificate signed by one of the trusted Certificate Authorities

This involves the following steps –

- Create a TLS Context
- Generate a Certificate Signing Request (CSR) and get that signed from supported Certificate Authority
- Upload the SBC and Root/Intermediate certificates

<u>Create a TLS Context</u>

Open TLS Context Page (Setup Menu -> IP Network tab -> Security Folder -> TLS contexts)

Create a New TLS Context (Teams New in this example)

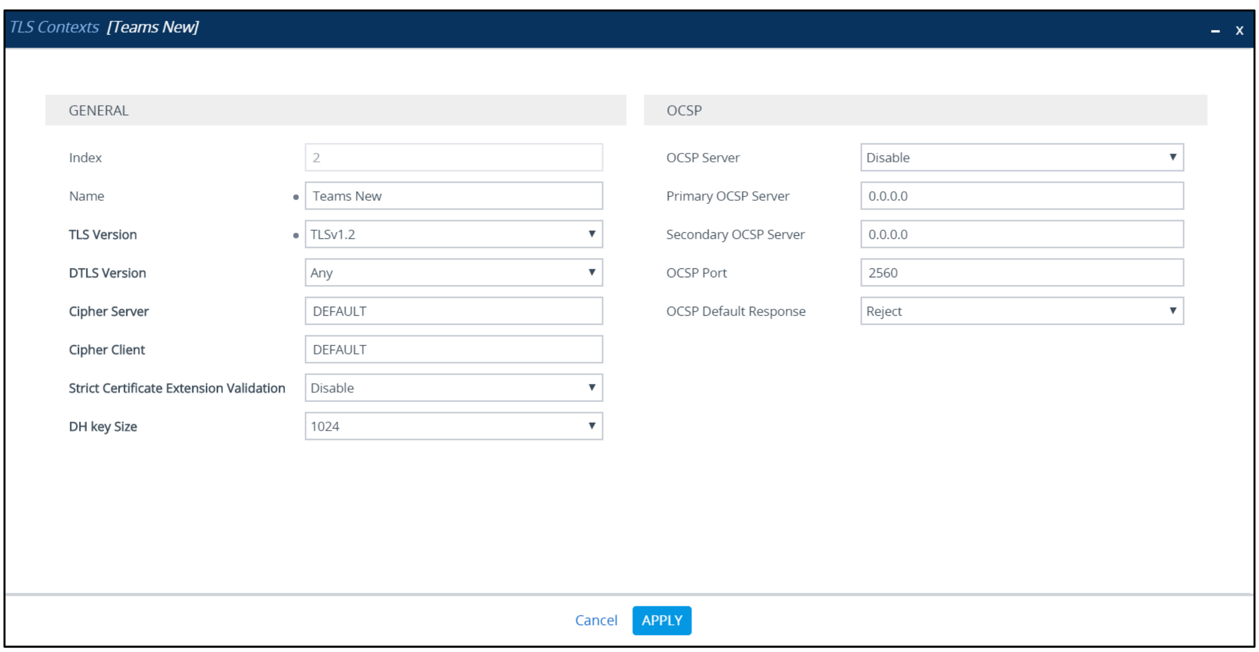


Figure 41 – Adding TLS Context for Teams

<u>Generate a CSR and Obtain the Certificate from a Supported CA</u>

In the TLS Contexts page, select the Teams TLS Context index row, and then click the Change Certificate link located below the table; the Context Certificates page appears

Under the Certificate Signing Request group, do the following –

Subject Name (CN) field – Enter SBC FQDN name (sbc.thesipcoe.com) (Ensure A record is created for this record on Domain Server)

Change the 'Private Key Size' based on the requirements of your Certification Authority. Many CAs do not support private key of size 1024. In this case, you must change the key size to 2048.

Fill in the rest of the request fields according to your security provider's instructions.

Click the Create CSR button; a textual certificate signing request is displayed in the area below the button

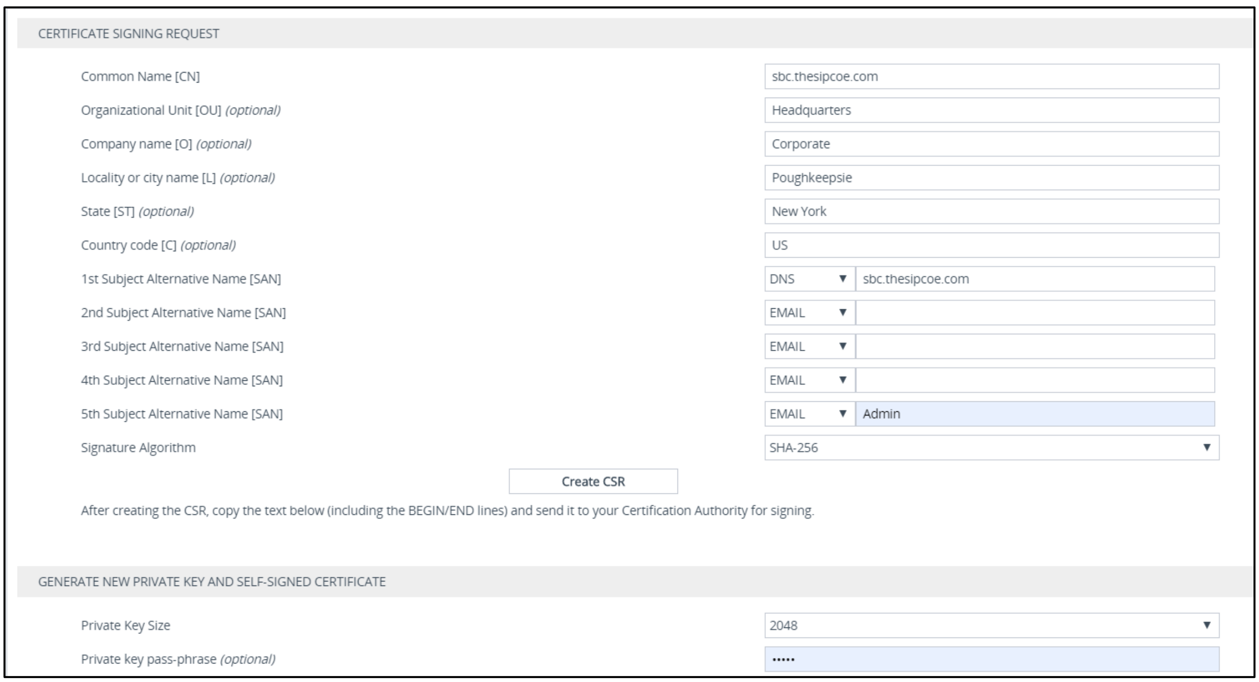


Figure 42 – Generating CSR

Deploy the SBC and the Root/Intermediate Certificates on the SBC

After obtaining the SBC signed and Trusted Root/Intermediate Certificate from the CA, install the following –

- SBC certificate
- Root and Intermediate certificates

To install the SBC certificate:

In the SBC's Web interface, return to the TLS Contexts page and do the following

- In the TLS Contexts page, select the required TLS Context index row, and then click the Change Certificate link located below the table; the Context Certificates page appears.

- Scroll down to the Upload certificates files from your computer group, click the Choose File button corresponding to the 'Send Device Certificate...' field, navigate to the certificate file obtained from the CA, and then click Load File to upload the certificate to the SBC.

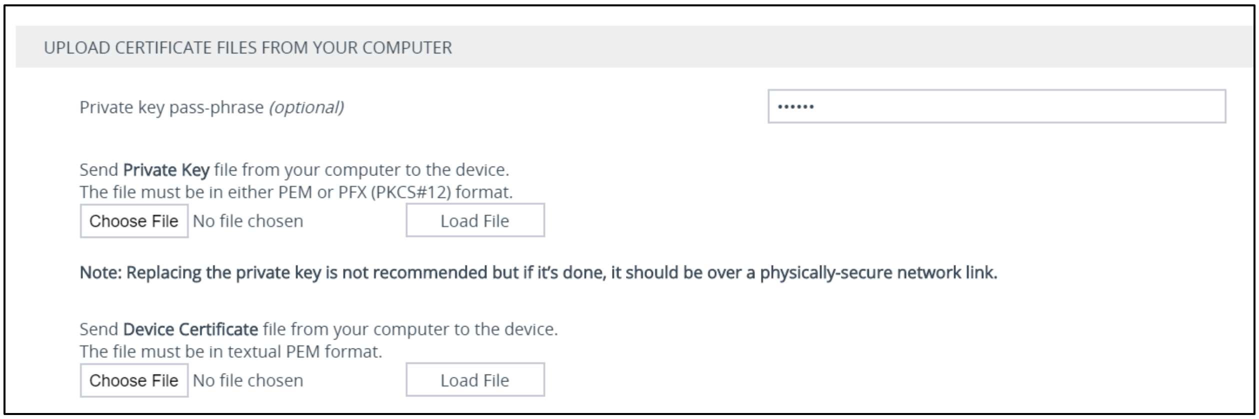
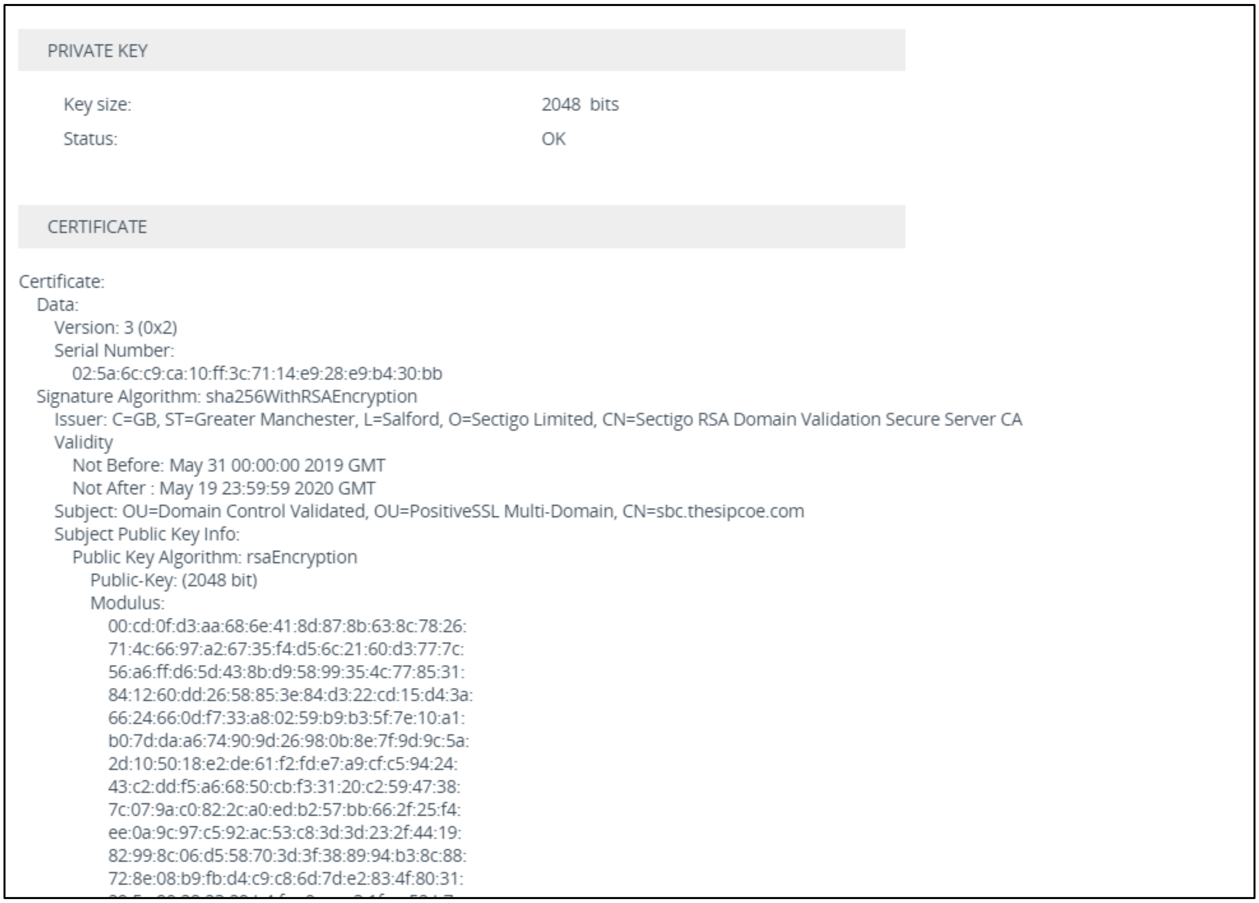


Figure 43 – Upload Device Certificate

In the SBC's Web interface, return to the TLS Contexts page, select the required TLS Context index row, and then click the Certificate Information link, located at the bottom of the TLS. Then validate the Key size, certificate status and Subject Name:


PRIVATE KEY

Key size: 2048 bits
Status: OK

CERTIFICATE

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      02:5a:6c:c9:ca:10:ff:3c:71:14:e9:28:e9:b4:30:bb
  Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
    Validity
      Not Before: May 31 00:00:00 2019 GMT
      Not After : May 19 23:59:59 2020 GMT
    Subject: OU=Domain Control Validated, OU=PositiveSSL Multi-Domain, CN=sbc.thesipcoe.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
          00:cd:0f:d3:aa:68:6e:41:8d:87:8b:63:8c:78:26:
          71:4c:66:97:a2:67:35:f4:d5:6c:21:60:d3:77:7c:
          56:a6:ff:d6:5d:43:8b:d9:58:99:35:4c:77:85:31:
          84:12:60:dd:26:58:85:3e:84:d3:22:cd:15:d4:3a:
          66:24:66:0d:f7:33:a8:02:59:b9:b3:5f:7e:10:a1:
          b0:7d:da:a6:74:90:9d:26:98:0b:8e:7f:9d:9c:5a:
          2d:10:50:18:e2:de:61:f2:fd:e7:a9:cf:c5:94:24:
          43:c2:dd:f5:a6:68:50:cb:f3:31:20:c2:59:47:38:
          7c:07:9a:c0:82:2c:a0:ed:b2:57:bb:66:2f:25:f4:
          ee:0a:9c:97:c5:92:ac:53:c8:3d:3d:23:2f:44:19:
          82:99:8c:06:d5:58:70:3d:3f:38:89:94:b3:8c:88:
          72:8e:08:b9:fb:d4:c9:c8:6d:7d:e2:83:4f:80:31:
```

Figure 44 – Device Certificate Details

To Install Root and Intermediate Certificates –

In the TLS Contexts page, select the required TLS Context index row, and then click the Trusted Root Certificates link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears

Click the Import button, and then select all Root/Intermediate Certificates obtained from your Certification Authority to load.

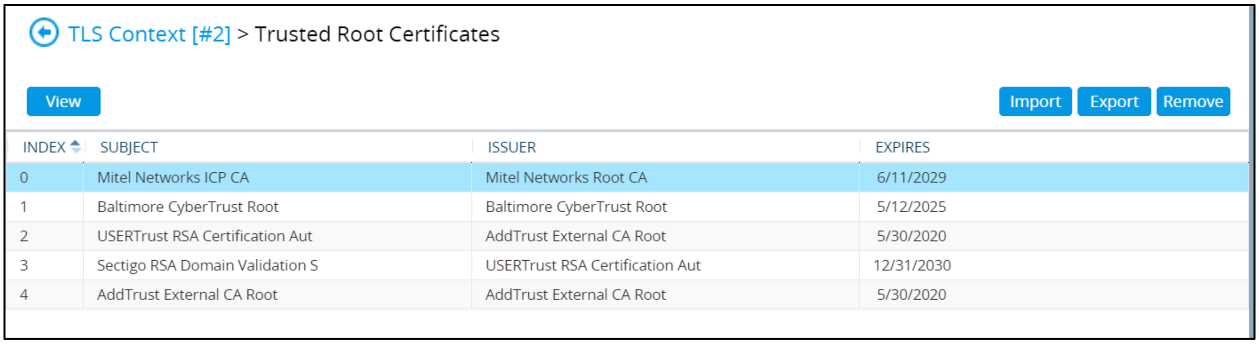


Figure 45 – Import Root and Intermediate Certificates

Reset the SBC by clicking Save To Flash for your settings to take effect.

Reset the E-SBC

After you have completed the configuration of the E-SBC described in this chapter, save ("burn") the configuration to the E-SBC's flash memory with a reset for the settings to take effect.

To reset the device through Web interface:

Open the Maintenance Actions page (**Setup** menu > **Administration** tab > **Maintenance** folder > **Maintenance Actions**)

Ensure that the ' Save To Flash' field is set to **Yes** (default).

Click the **Reset** button; a confirmation message box appears, requesting you to confirm.

Click **OK** to confirm device reset. See Figure 46

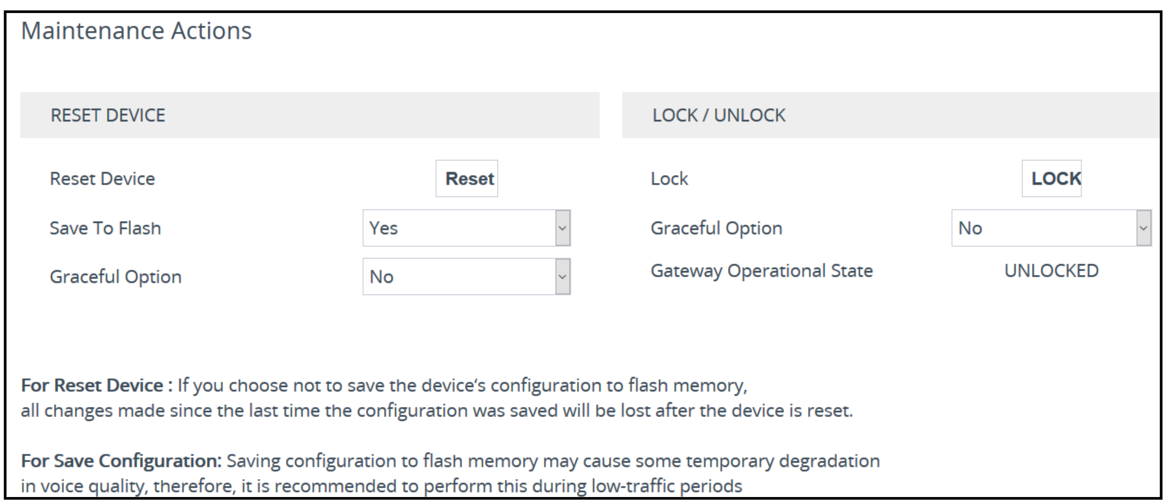


Figure 46 - Resetting the E-SBC

Configuring Office 365 Tenant for Teams Direct Routing

It's clearly illustrated on Microsoft documentation portal as to how to plan and deploy Teams Direct Routing feature. This outlines the configuration that has been used for this testing

Setup Domain – Setting up the domain is one of the important steps, and it's in fact a pre-requisite for creating Office 365 Tenant. Domain used for this testing – thesipcoe.com

Office 365 Tenant – The next step is to create a tenant on Office 365 with valid license. E5 without Audio Conferencing is the licensing used with this tenant.

Adding Domain – Login on to Office 365 as an administrator. Add your domain (thesipcoe.com) on Admin panel (under Setup -> Domains)

Configure Users – Create users on Admin panel and assign the licenses.

Download and install Teams client. Two-way calling between Teams Clients is expected to work with this setup. The coming steps cover how to configure Direct Routing between Teams and AudioCodes

Pair the SBC to the Direct Routing Service of the Phone system –

- Connect to **Skype for Business Online** admin center using PowerShell
- Pair the SBC
- Validate the pairing

To pair the SBC to the tenant, in the PowerShell session type the following and press Enter:
New-CsOnlinePSTNGateway -Fqdn <SBC FQDN> -SipSignallingPort <SBC SIP Port> -MaxConcurrentSessions <Max Concurrent Sessions the SBC can handle> -Enabled $true

Enable users for Direct Routing Service –

- Create a user in Office 365 and assign a phone system license.
- Ensure that the user is homed in Skype for Business Online.
- Configure the phone number and enable enterprise voice and voicemail.
- Configure voice routing. The route is automatically validated.

For more details with respect to the licensing requirements, contact Microsoft. E5 without Audio Conferencing has been used for the lab testing purpose

To Enable Enterprise Voice and Voicemail connect to the powershell and execute the below commands for a specific user –

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

Voice Routing Policy needs to be defined to route the calls towards AudioCodes. One must exercise their own dialling requirement before setting up Voice Policies, Routes, PSTN usages on the Phone System. A simple routing (to dial out 4- and 10-digit numbers) has been configured for the lab testing

Test call should be made between MiVO400 and Teams users to ensure two-way calling is working after setting up Direct Routing configuration

Glossary

MiVoice Office 400	MiVO400
MiCollab	MiCollab
MiNET Interface	MiNET
Mitel Solutions Alliance	MSA
Personal Ring Group	PRG
External Hot Desk User	EHDU
Knowledge Management System	KMS
Class of Service	COS
Automatic Call Distribution	ACD
Automatic Route Selection	ARS