A MITEL
PRODUCT
GUIDE

Unify OpenScape Solution Set V10

OpenScape Voice with MS Teams and AudioCodes SBC, Configuration Guide

OpenScape Voice with MS Teams and AudioCodes SBC, Configuration Guide

Administrator Documentation

07/2024

A31003-S11A0-M120-01-76A9

Mitel

Notices

Trademarks

Table of Contents

History of Change

Version	Date	Description
1	March 6th, 2020	Initial Creation

1. Overview

1.1. Executive Summary

The scope of this document is to detail the Microsoft Direct Routing configuration for the connectivity of Microsoft Teams phone system and AudioCodes SBC with Unify's OpenScape Voice V10 IP-PBX.

1.1.1. Description

Direct Routing allows the integration of Teams infrastructure into existing on-premise telephony system. Teams users are enabled to use on-premises telco lines or SIP trunks to make and receive calls instead of using Microsoft Carrier Services via Calling Plans. Thus, eliminating the need for error prone number porting and eventual down times. Costs are significantly reduced with Direct Routing in comparison to Microsoft's Cloud Voice.
Teams client users can make and receive calls from Unify SIP phones registered to OS Voice IP-PBX.
Successful execution of VoIP telephony features, including a mix of Teams users and OS Voice SIP subscribers, when invoked either from Teams or OS Voice system.
Teams users are accessing PSTN via OS Voice IP-PBX.

Teams web resources:
https://docs.microsoft.com/en-us/MicrosoftTeams/teams-overview
https://docs.microsoft.com/en-us/MicrosoftTeams/direct-routing-landing-page

Refer to Mediant 800B technical documentation on this website:
https://www.audiocodes.com/library/technical-documents?productFamilyGroup=1637&productGroup=1692&versionGroup=Version+7.2
https://www.audiocodes.com/solutions-products/products/products-for-microsoft-365/direct-routing-for-microsoft-teams

1.1.2. Test Equipment

Test Equipment	Software Releases
Virtual OpenScape Voice co-located cluster	OS Voice version: V10
Virtual OpenScape CMP / Media server	OS CMP / Media Server version: V10
Virtual OpenScape Xpressions	OS Xpressions server version: V7 R1 FR5 HF32

Mediatrix 4402plus BRI gateway device	Mediatrix 4402plus firmware: Dgw 44.1.1605
OpenScape Deskphone CP400 & CP600 phones	SIP phones firmware: V1 R6.14.0 SIP
Microsoft Office365 Cloud (with Teams & Phone System)	VMware ESXi v5.5.0 Build 6480324
AudioCodes M800B SBC	Microsoft Teams version: 1.3.00.362 (64-bit)
	AudioCodes SBC firmware: 7.20A.254.376

1.2. Test Network

Microsoft O365 cloud tenant (with Teams & Phone System) is interconnected via internet with a SIP trunk to the WAN interface of AudioCodes M800B SBC. Additionally, the SBC's LAN interface is interconnected with a SIP trunk to OS Voice IP-PBX.

OS UC server provides OS Voice management and media services.

OS Voice is connected (SIP) to a Mediatrix 4402plus BRI gateway, that provides access to PSTN (OTE ITSP).

Voicemail services to OS Voice SIP subscribers are provided by an OS Xpressions server (SIP trunk connectivity with OS Voice)

The diagram of **figure 1** below displays the logical diagram which is used for the certification project testing.

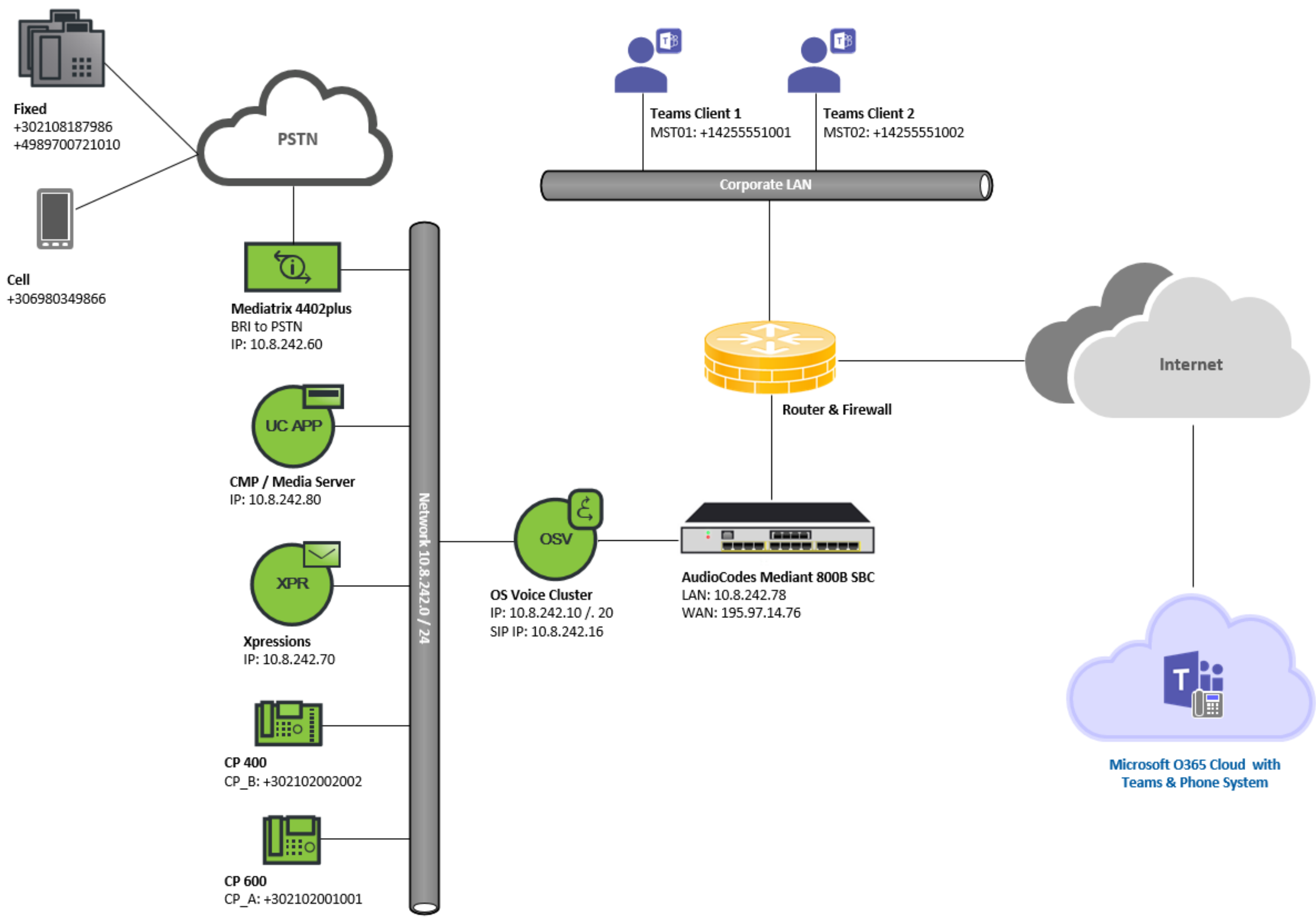


Figure 1 Logical Topology Diagram

2. Limitations and Observations

2.1. Remarks

- **Media clipping behavior in calls**
  With Media Bypass = ON, in a call between a Teams user and an OS Voice subscriber, after call establishment, if the Teams user talks first, then speechpath isn't properly established; OS Voice subscriber hears the speech from Teams user clipped, until after 5-8secs have elapsed from call establishment. The latter behavior isn't noticed if the OS Voice subscriber talks first, i.e. audio is heard normally (no media clipping) from both sides.

On the other hand, with Media Bypass = OFF, the audio clipping behavior is less noticeable.

This media clipping issue is most probable to be caused by internal lab network hops.

- **Call Hold**

In current Teams version the MOH feature isn't configurable by the administrator (https://docs.microsoft.com/en-us/microsoftteams/here-s-what-you-get-with-phone-system).

- **RTCP sender and receiver reports**

CP phones send only RTCP sender reports and not receiver ones.

When CP phone initiates call hold, it stops sending RTCP (and RTP) packets (direction "inactive" is used).

By default, the SBC doesn't send RTCP packets in the normal call, but only in specific scenarios, for example, call hold. However, if this is required by the customer, the RTCP Mode parameter in the IP Profile of the relevant entity should be configured accordingly. For example, for Teams it's recommended to configure this parameter with value *"Generate Always"* (see 4.2.7).

- **RTP sessions**

For a basic call between a Teams user and an OS Voice subscriber, instead of having 4 RTP sessions, we have 6. The SBC is working in B2BUA operational mode. This mode is implemented for multiple functionalities, required from the SBC in the VoIP network. In this mode SBC terminate session on one leg and setup another (a new one) session on other leg. So, when the audio passes through the SBC, for a basic call, there will be 4 RTP sessions (i.e. 4 SSRC values), instead of 2 RTP sessions (i.e. 2 SSRC values). The extra 2 RTP sessions are for internal SBC use, therefore we have 6 RTP sessions, totally.

- **DTMF**

When in an established call between a Teams user and an OS Voice subscriber, DTMF digits are audible from OS Voice subscriber only. Traces verify that DTMF digits are sent to both sides correctly and are recognized by voicemail systems on opposite side (i.e. Teams Phone System voicemail and OS Xpressions).

The details of M800B SBC configuration for Teams Direct Routing, may be found at: https://www.audiocodes.com/media/13253/connecting-audiocodes-sbc-to-microsoft-teams-direct-routing-enterprise-model-configuration-note.pdf

In this section the SBC configuration steps for Teams Direct Routing, that will be presented, will relate to current project specific settings. Default or non-project specific M800B configuration will not be referenced in subsequent sub-sections.

2.2. Restrictions

- **Name and number display of Teams users on CP phones**

For calls between Teams users and OS Voice subscribers, Unify CP phones, doesn't display the name of the opposite Teams party in the call, but only Teams party number in international format.

When the OS Voice subscriber is the caller, Teams client shows the name and the number of the OS Voice subscriber on incoming call notification and when the call is established, on Teams client, the OS Voice subscriber number is displayed in international format. On the CP phone, only the number of the Teams user is displayed in international format. MS Phone System doesn't send P-Asserted-Identity SIP header in 180 Ringing or 200 OK SIP messages to convey connected party information.

If a Teams user calls an OS Voice subscriber number, in ringing and call connected phase the CP phone of the OS Voice subscriber, displays only the number of the Teams user and not the name and number of the caller. OS Voice doesn't support Teams *"ForwardPAI"* header on Teams tenant. MS Phone System *"ForwardPAI"* setting should be deactivated on MS Phone System, because CP phones will display incoming calls from Teams users with suppressed CID (Number Unavailable).

- **Silence Suppression / Comfort Noise**

  OS Voice SIP devices, such as CP phones, use the parameter *"silenceSupp: on"* for silence suppression, but MS Phone System doesn't support that method. MS Phone System uses comfort noise packets (CN 13) as a method of silence suppression. On the other hand, CP phones do not support the comfort noise codec (i.e. Payload type 13).

  In a call between a Teams user and an OS Voice subscriber, when OS Voice subscriber mutes, with special configuration, the SBC may send CN 13 RTP packets to Teams user (see 4.2.7). If the Teams user mutes the call, the SBC doesn't send CN packets towards CP phone, because in the negotiation process SBC understood that CP phone didn't support CN 13, so the OS Voice subscriber doesn't hear "comfort noise" and has "dead air" that may lead to false assumption that call was disconnected.

- **Early Media**

  MS Phone System doesn't support early media. OS Voice respond with SIP PRACK message only when it receives a 18x response with SDP (early media content).

- **Call Hold**

  In a call between a Teams user and an OS Voice subscriber, when OS Voice subscriber has system MOH activated and holds the call, Teams user doesn't have a held call display on Teams client.

  When OS Voice RTP parameter `Srx/Main/UseSendOnlyForMOH` is set to *"RtpTrue"* (default value), the held party will receive the SDP of the media server with *Attribute (a): sendonly* and an indication is provided to the held party (on the display), while MOH is played. Note that this Hold indication is only displayed on the Unify phones. If it's required for the Teams user to indicate the call as held, the OS Voice MOH feature should be deactivated for OS Voice subscribers.

  The Teams user may hold the call with OS Voice subscriber by:

  1. Clicking the **Hold** option on client while being on a call; this will play MOH for OS Voice subscriber, but "held remotely" indication isn't displayed on the CP phone (appears for a little while and then disappears).

     Usually there is a delay of hold and resume actions about 2-3 seconds. Hold and Resume delay is just design issue and matter of how fast will be the exchange of the information about new session after REFER of the call to Music on Hold source (If Hold is clicked in Teams during the call via Direct Routing the call is transferred to another Teams "user"/object which is playing music to the held party).

  2. Clicking the **Consult then transfer** option on client while being on a call; MOH isn't played for OS Voice subscriber, but *"held remotely"* indication is displayed on the CP phone. Additionally, OS Voice subscriber side is put on hold much faster.

  In double call hold scenarios for calls between Teams users and OS Voice subscribers, it has been observed that if the OS Voice subscriber retrieves first, MOH isn't resumed for the OS Voice subscriber.

  When Teams user holds a call with an OS Voice subscriber and then hangs up, system recall isn't supported by MS Phone System.

- **Call Park**

  Regarding the displays, when a parked call is retrieved from a device registered to another system (MS Phone System or OS Voice), the retrieved device displays the original caller and not the connected-to party.

This behavior is a consequence of PAI restrictions mentioned in *"Name and number display of Teams users on CP phones*" bullet point in current sub-section.

- **Call Transfer**

  In order call transfer scenarios to work, secure media should be deactivated in OpenScape Media Server and in SBC's IP profiles (see 4.2.7& 4.3.5). When secure media is used, transfer fails with a SIP 410 Gone message from Teams with the reason *"Could not parse SDP in order to transform it to an NGC friendly format"*. SBC is adding wrong crypto lines to the 200 OK from Teams, propagated to OS Voice. OS Voice sends re-INVITE with SDP and crypto lines as received from SBC; Teams rejects that INVITE (*a=crypto:2* line twice).

  MS Phone System doesn't send SIP REFER messages when executing "consult then transfer" from Teams client.

  When transferring calls between Teams users and OS Voice subscribers, in certain cases, user devices (CP phones / Teams client) display the original connected party and not the transferred-to party. Additionally, sometimes, the user devices display the number of a user registered to the same system (MS Phone System / OS Voice) with an international format. Various display issues are caused due to PAI restrictions between MS Phone System and OS Voice, mentioned previously in current sub-section (*"Name and number display of Teams users on CP phones"* bullet point).

  In the current Teams version, semi-attended transfer isn't supported from Teams client; only attended and blind transfer are possible.

- **Call Forwarding**

  The MS Phone System doesn't support SIP Diversion header for call forwarding, but History-Info header. On the other hand, OS Voice doesn't support History-Info header.

  For call forwards between Teams users and OS Voice subscribers and vice versa, the forwarded-to party's device won't display "forwarded from" information. Moreover, the original caller won't display "forwarded for" information.

  Furthermore, for cross platform call forwarding, in certain cases, at the caller's side the original called party is displayed and not the forwarded-to party. MS Phone System doesn't send P-Asserted-ID in 180 or 200 SIP messages (OS Voice sends P-Asserted-ID of forwarded-to party in 180 and 200) and Teams PAI isn't supported from OS Voice.

  Call forwarding on busy isn't supported by current Teams implementation.

- **Call Deflect**

  Same as *"Call Forwarding"* bullet point above.

- **Simultaneous Ringing**

  Like *"Call Forwarding"* bullet point above.

- **Conference**

  Large conference (IP-PBX conference) requires the same configuration as call transfer case to work (see 4.2.7 & 4.3.5).

  Teams users participating in large conference display a basic call with conference initiator. Similarly, OS Voice subscribers participating in Teams meeting display original connected-to party. There is no conference / meeting information display across different telephony systems.

2.3. Known Issues

- **Call Toggle**

When Media Bypass = OFF and Teams user alternates between calls with different OS Voice subscribers, when OS Voice subscriber drops call (after second call alteration), Teams user is dropped from call.

- **Conference**

Adding an OS Voice subscriber to an existing Teams meeting isn't possible for the Teams tenant utilized in current project. Issue should be investigated by Microsoft.

3. Configuration Overview

3.1. Microsoft Teams & AudioCodes SBC

For the needs of current certification, Microsoft Teams Direct Routing configuration is utilized to setup the testing environment.

The prerequisites for Direct Routing are:

1. Teams users of Direct Routing must have the following licenses assigned in Office 365: *Office 365 Enterprise E3 (including SfB Online Plan2, Exchange Plan2, and Teams) + Phone System licenses or Office 365 Enterprise E5 (including SfB Online Plan2, Exchange Plan2, Teams, Phone System and Audio Conferencing)*.

2. Teams certified SBC (https://docs.microsoft.com/en-us/microsoftteams/direct-routing-border-controllers).

3. A publicly registered domain name. Public domain name like *onmicrosoft.com* is not a possibility for direct routing.

4. Public trusted certificate for the SBC with a SAN record with the host name of the SBC. The certificate must be from one Microsoft's approved root CAs (https://docs.microsoft.com/en-us/MicrosoftTeams/direct-routing-plan#public-trusted-certificate-for-the-sbc).

5. Public IP address for SBC WAN connection and appropriate firewall rules for signaling.

In certification environment, Office 365 E5 licenses are used, which are applied to the Teams test users:

- MST01@M365x316382.onmicrosoft.com with phone number +14255551001
- MST02@M365x316382.onmicrosoft.com with phone number +14255551002

The AudioCodes M800B, Teams certified SBC, is connected via internet with public IP 195.97.14.76 and public FQDN sbc.drtests.com to Microsoft Phone System in Microsoft O365 cloud. Additionally, a public trusted certificate for the SBC is used, which is issued from AddTrust root CA.

The SBC LAN IP address is 10.8.242.78 and is connected via corporate network to OS Voice IP PBX.

Proper firewall rules in SBC are configured for SIP and RTP traffic (see in detail in 4.2.13).

The Teams tenant SIP trunk connectivity to AudioCodes SBC is tested with and without Media Bypass. In a nutshell, with media bypass activated the audio during speechpath “stays” in corporate LAN, while without media bypass, the media always passes through Microsoft Cloud. More details about media bypass may be found at: (https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan-media-bypass).

3.2. Unify Component Infrastructure

OS Voice is configured for extension dialing between the subscribers. The Office code used is 30 (210) 200 and the subscriber extensions are with 4 digits (e.g. 10xx). Full DN dialing is also possible (3021020010xx) between subscribers.
OS Voice provides access to PSTN (OTE ISDN BRI provider) via a Mediatrix 4402plus BRI gateway. Teams users and OS Voice subscribers dial 9 + number to reach a PSTN subscriber. The digit 9 may be considered a “seizure code” digit which enables call routing to Mediatrix 4402plus and then is stripped away by OS Voice before sending the number to PSTN.
OpenScape UC applications server supplies OS Voice with media services (Media Server) & UI administration services (CMP).
Voicemail functionality is provided by OS Voice through OpenScape Xpressions server (10.8.242.70). OS Voice subscribers may call 302102003001 (direct access number) to access their mailboxes. The number 302102003000 OS Xpressions system (callback) number.

- OS Voice

  10.8.242.10 node 1

  10.8.242.20 node 2

- OS UC (Media Server, CMP-Management)

  10.8.242.80

- OS Xpressions

  10.8.242.70

- SIP phones

  CP_A = 1001 (CP_600 SIP phone device)

  CP_B = 1002 (CP_400 SIP phone device)

- Mediatrix 4402plus

  10.8.242.60

- ISDN BRI number for incoming calls from PSTN

  302106203360

- PSTN

  302108187986 (fixed line)
  4989700721010 (fixed line)
  306980349866 (mobile line)

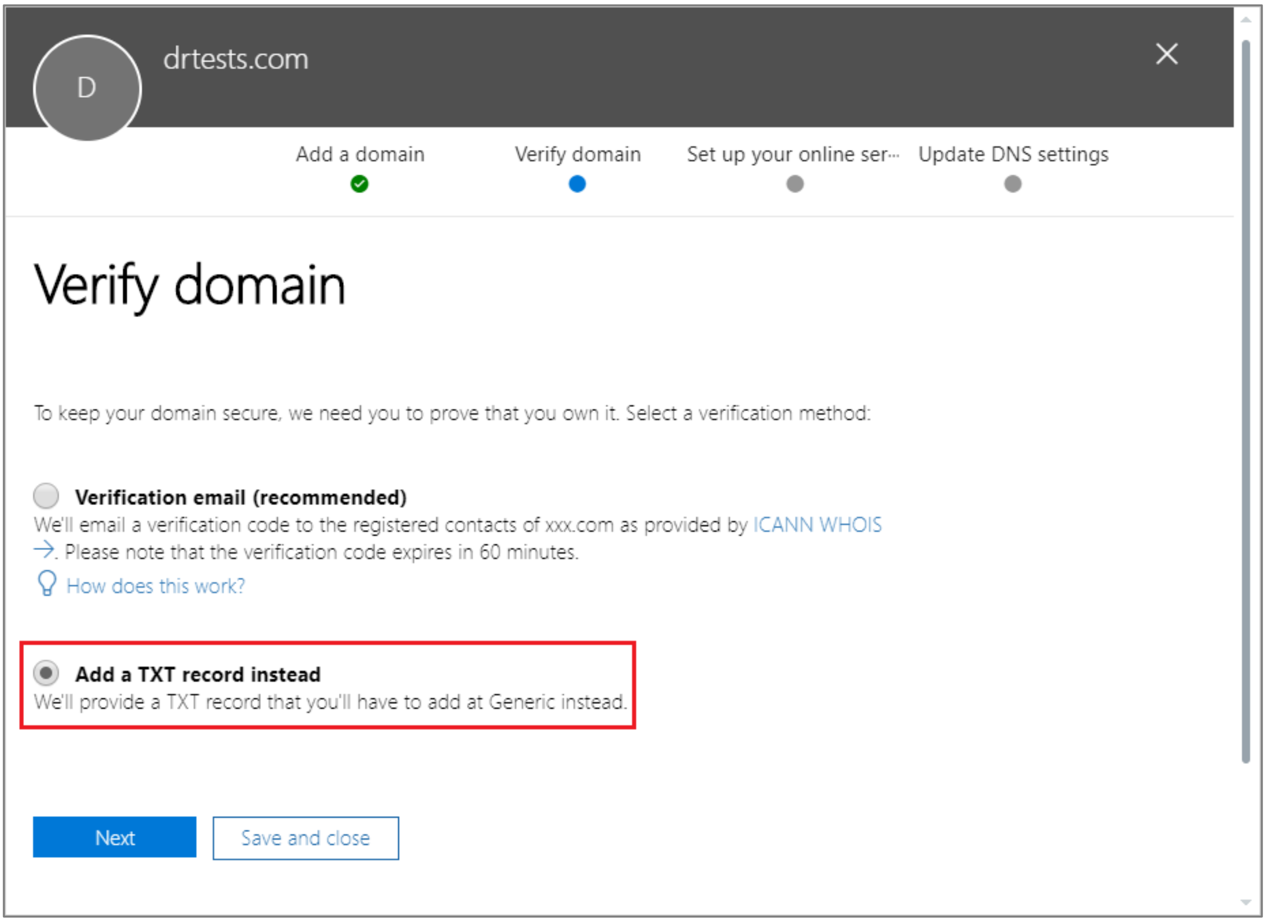
4. Configuration in Detail

The values of many parameters given in this chapter, such as IP addresses, are given as examples and should be treated as such.

4.1. Setting up the Domain

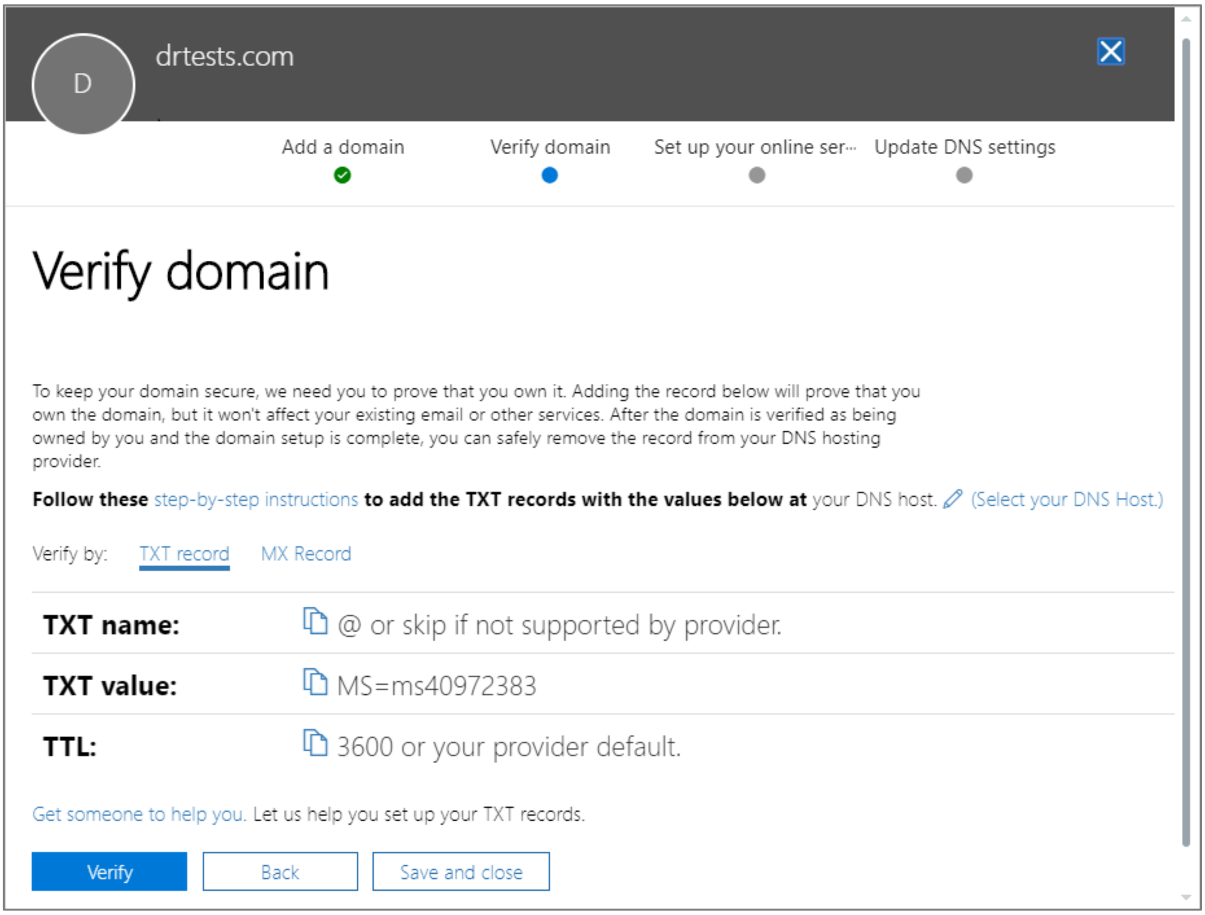
This subsection outlines how to add the SBC domain to the tenant.

Navigate toO365 portal, select on the left menu **Setup >> Domain** and click on **Add domain**.



Enter the SBC domain name, for example *drtests.com* in **Enter a domain you own** box.

Click **Next**.

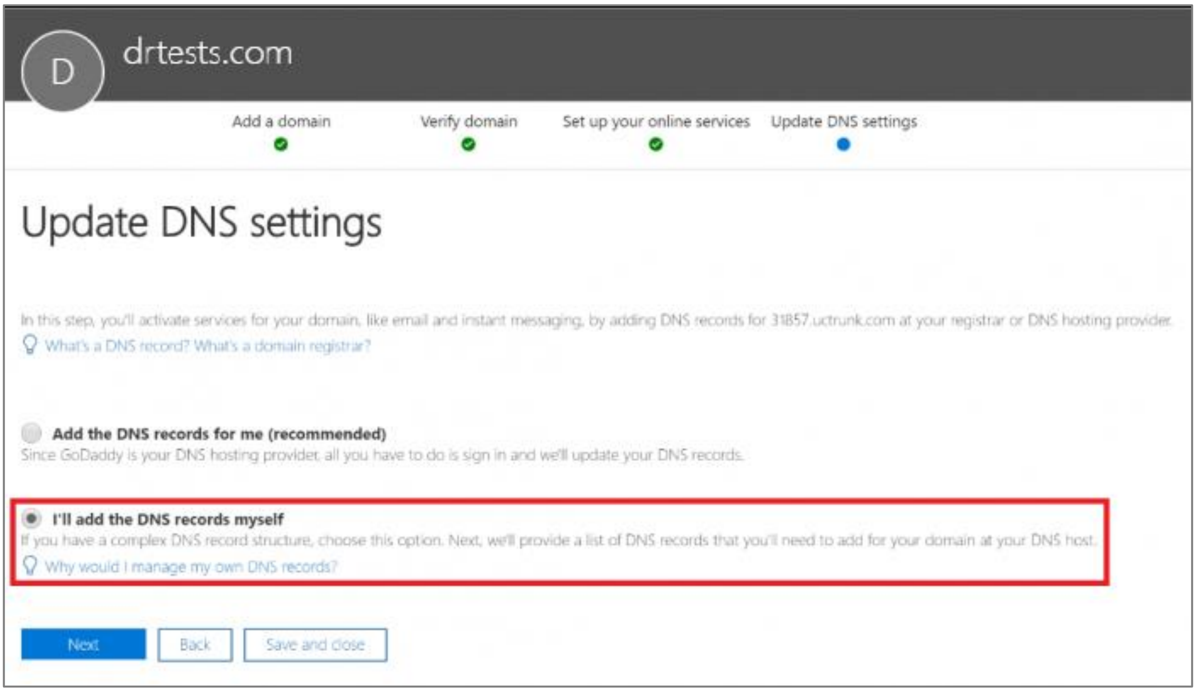


Select **Add a TXT record instead** and click **Next**.

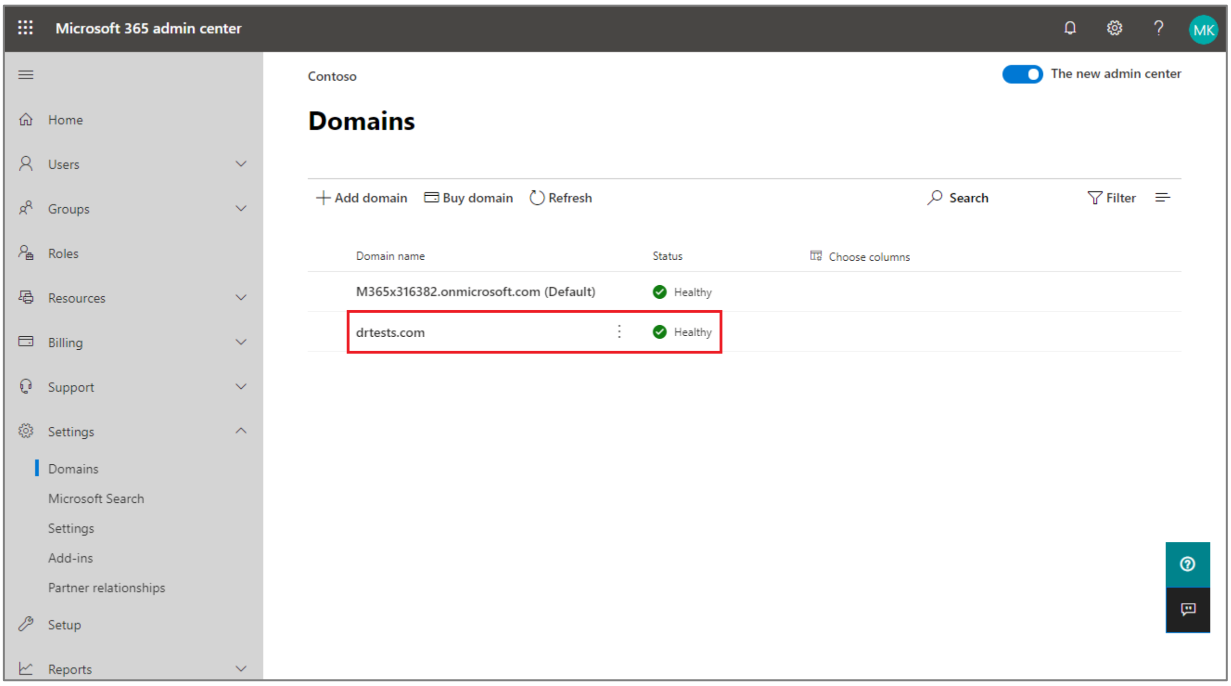
Copy-paste this screen and contact corresponding support organization to validate domain ownership.

When the confirmation that the TXT verification is ready, go back to this domain set up and start the verification process.

Disable all services on the **Setup your online services** window and click **Next**.



Select **I'll add the DNS records myself**.



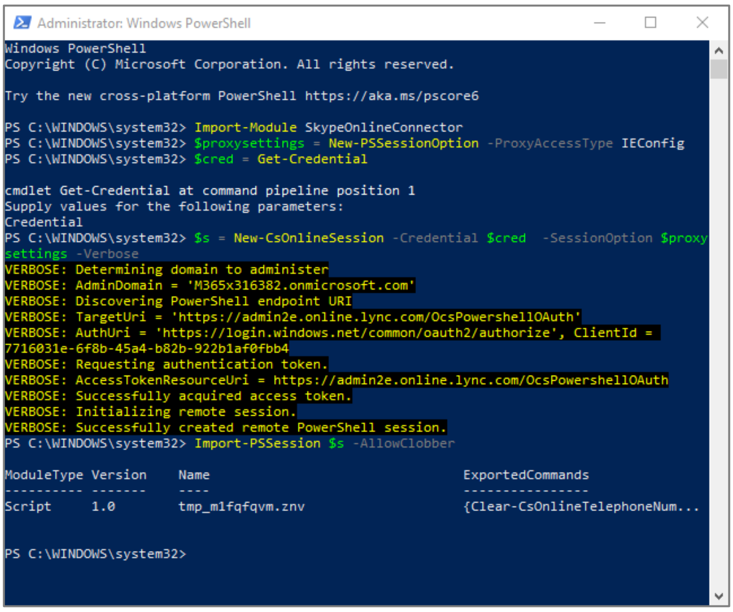
When the SBC's domain setup is completed, the next step is to activate it. For this, a "dummy" user (with a E3 or E5 license) should be added to this specific domain, not the default one. When the setup is completed this "dummy" user could be deleted.

Note: The addition of the default Teams domain *M365x316382.onmicrosoft.com* for the testing activities and the creation of the test Teams test users *MST01 & MST02* with the O365 E5 licensing is out of scope and won't be referenced to, in current document.

4.1.1. Pair the SBC to the Direct Routing Service of MS Phone System

The SBC connection to Microsoft Phone System, routes and routing policies will be configured via PowerShell. Specifically, in the Skype for Business Online PowerShell.

To setup PowerShell in administrator's PC, follow this link: https://docs.microsoft.com/en-us/SkypeForBusiness/set-up-your-computer-for-windows-powershell/set-up-your-computer-for-windows-powershell.



Once PowerShell in administrator's PC is setup, execute below commands to connect to Skype for Business Online:

Import-Module SkypeOnlineConnector

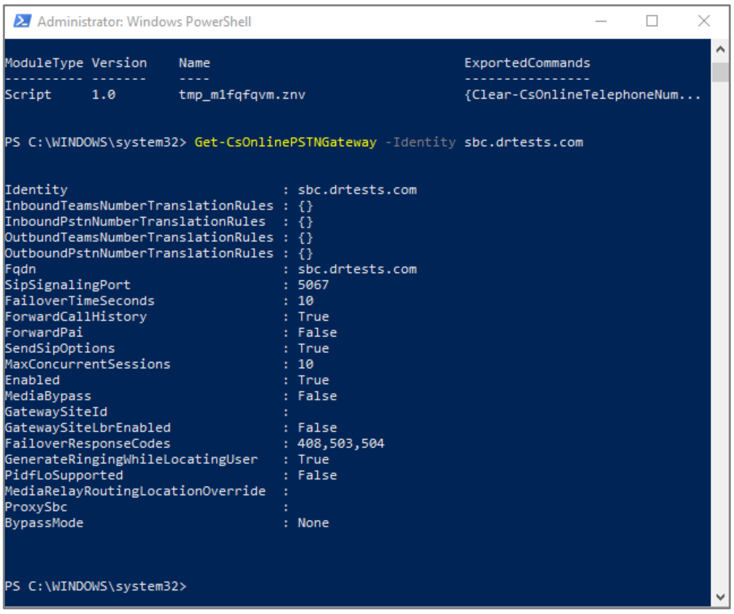
$proxysettings = New-PSSessionOption -ProxyAccessType IEConfig

$cred = Get-Credential

$s = New-CsOnlineSession -Credential $cred -SessionOption $proxysettings -Verbose

Import-PSSession $s -AllowClobber

Provide Tenant Admin credentials to log in.



Create the Gateway and pair with the tenant. Run the command:

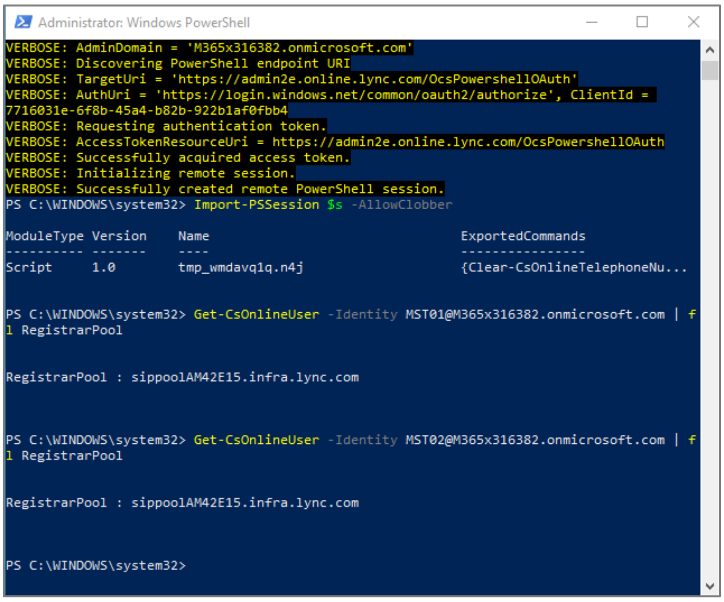
New-CsOnlinePSTNGateway -Identity sbc.drtests.com -SipSignallingPort 5067 -MaxConcurrentSessions 10 -Enabled $true

Parameters that affect the current certification:

- **ForwardCallHistory** True or False. If enabled, MS Phone System sends two SIP headers: History-info and Referred-By (see 2.2).
- **ForwardPai** False. It should be disabled (see 2.2)
- **MediaBypass** True or False, depending the customer requirements.

4.1.2. Enable users for Direct Routing Service

Ensure that the user is homed in Skype for Business Online.



Get-CsOnlineUser -Identity MST01@M365x316382.onmicrosoft.com | fl RegistrarPool

Get-CsOnlineUser -Identity MST02@M365x316382.onmicrosoft.com | *fl RegistrarPool*

Configure the phone number and enable enterprise voice and voicemail.

Set-CsUser -Identity MST01@M365x316382.onmicrosoft.com -EnterpriseVoiceEnabled $true -HostedVoiceMail $true - OnPremLineURI tel:+14255551001

Set-CsUser -Identity MST02@M365x316382.onmicrosoft.com -EnterpriseVoiceEnabled $true -HostedVoiceMail $true - OnPremLineURI tel:+14255551002

The phone numbers used must be configured as a full E.164 phone number with country code.

Verify phone number assignment with:

Get-CsOnlineUser -Identity MST01@M365x316382.onmicrosoft.com

Get-CsOnlineUser -Identity MST01@M365x316382.onmicrosoft.com

4.1.3. Configure Voice Routing

Microsoft Phone System has a routing mechanism that allows a call to be sent to a specific SBC based on:

• Called number pattern.

• Called number pattern + specific user who makes the call.

Call routing is made up of the following elements:

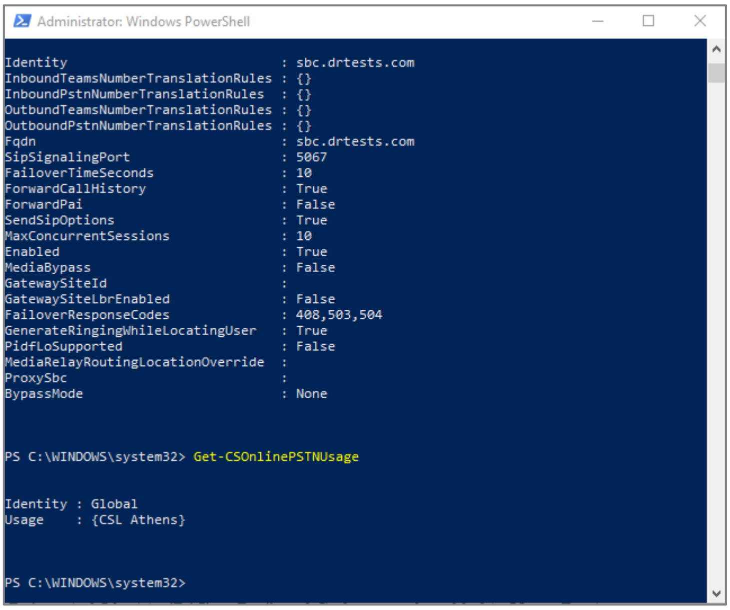
• Voice Routing Policy – container for PSTN Usages; can be assigned to a user or to multiple users.

• PSTN Usages – container for Voice Routes; can be shared in different Voice Routing policies.

• Voice Routes – number pattern and set of Online PSTN Gateways to use for calls where calling number matches the pattern.

• Online PSTN Gateway - pointer to an SBC, also stores the configuration that is applied when call is placed via the SBC, such as forward P-Asserted-Identity (PAI) or Preferred Codecs; can be added to Voice Routes.

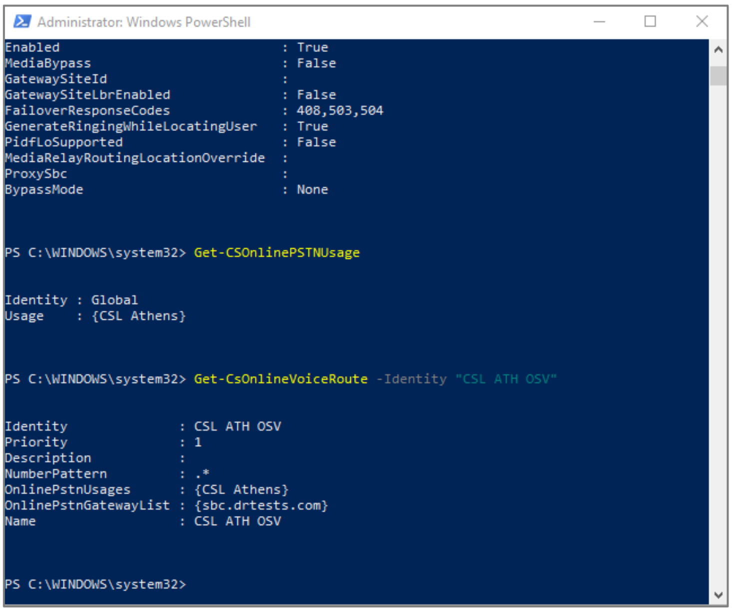
For all other calls, if a user has both licenses (Microsoft Phone System and Microsoft Calling Plan), Automatic Route is used. If nothing matches the number patterns in the administrator-created online voice routes, route via Microsoft Calling Plan. If the user has only Microsoft Phone System, the call is dropped because no matching rules are available.



```
Administrator: Windows PowerShell
Identity                          : sbc.drtests.com
InboundTeamsNumberTranslationRules : {}
InboundPstnNumberTranslationRules  : {}
OutbundTeamsNumberTranslationRules : {}
OutboundPstnNumberTranslationRules : {}
Fqdn                              : sbc.drtests.com
SipSignalingPort                  : 5067
FailoverTimeSeconds               : 10
ForwardCallHistory                : True
ForwardPai                        : False
SendSipOptions                    : True
MaxConcurrentSessions             : 10
Enabled                           : True
MediaBypass                       : False
GatewaySiteId                     :
GatewaySiteLbrEnabled             : False
FailoverResponseCodes             : 408,503,504
GenerateRingingWhileLocatingUser  : True
PidfLoSupported                   : False
MediaRelayRoutingLocationOverride :
ProxySbc                          :
BypassMode                        : None


PS C:\WINDOWS\system32> Get-CSOnlinePSTNUsage


Identity : Global
Usage    : {CSL Athens}


PS C:\WINDOWS\system32>
```

Create the **PSTN Usage**, by executing:

Set-CsOnlinePstnUsage -Identity Global -Usage @{Add="CSL Athens"}



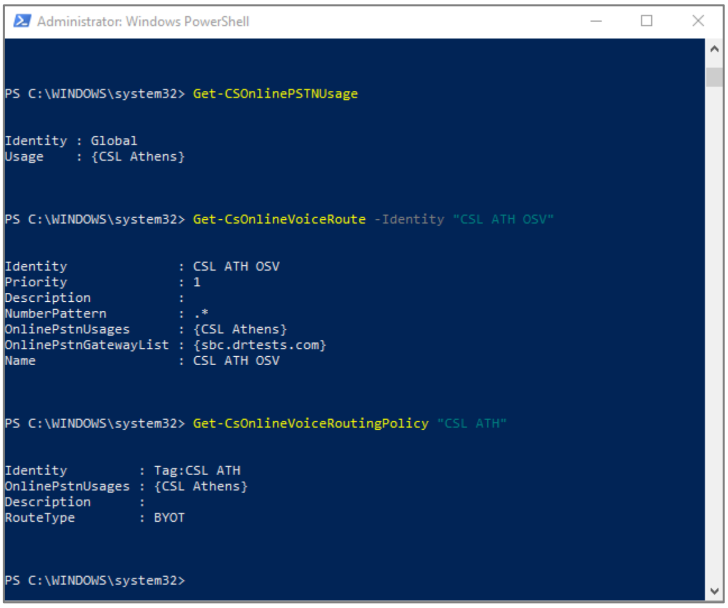
```
Administrator: Windows PowerShell
Enabled                           : True
MediaBypass                       : False
GatewaySiteId                     :
GatewaySiteLbrEnabled             : False
FailoverResponseCodes             : 408,503,504
GenerateRingingWhileLocatingUser  : True
PidfLoSupported                   : False
MediaRelayRoutingLocationOverride :
ProxySbc                          :
BypassMode                        : None


PS C:\WINDOWS\system32> Get-CSOnlinePSTNUsage


Identity : Global
Usage    : {CSL Athens}


PS C:\WINDOWS\system32> Get-CsOnlineVoiceRoute -Identity "CSL ATH OSV"


Identity              : CSL ATH OSV
Priority              : 1
Description           :
NumberPattern         : .*
OnlinePstnUsages      : {CSL Athens}
OnlinePstnGatewayList : {sbc.drtests.com}
Name                  : CSL ATH OSV


PS C:\WINDOWS\system32>
```

Create the **Voice Route** for outgoing calls from Teams users. Route specific numbers to SBC or route all number patterns to SBC:

New-CsOnlineVoiceRoute -Identity "CSL ATH OSV" -NumberPattern "^\+30(2102)(\d{7})$" -OnlinePstnGatewayList sbc.drtests.com -Priority 1 -OnlinePstnUsages "CSL Athens"

or

New-CsOnlineVoiceRoute -Identity "CSL ATH OSV" -NumberPattern "." -OnlinePstnGatewayList sbc.drtests.com -OnlinePstnUsages "CSL Athens"*



Create the **Voice Routing Policy** and add the previously created **PSTN Usage:**

New-CsOnlineVoiceRoutingPolicy "CSL ATH" -OnlinePstnUsages "CSL Athens"

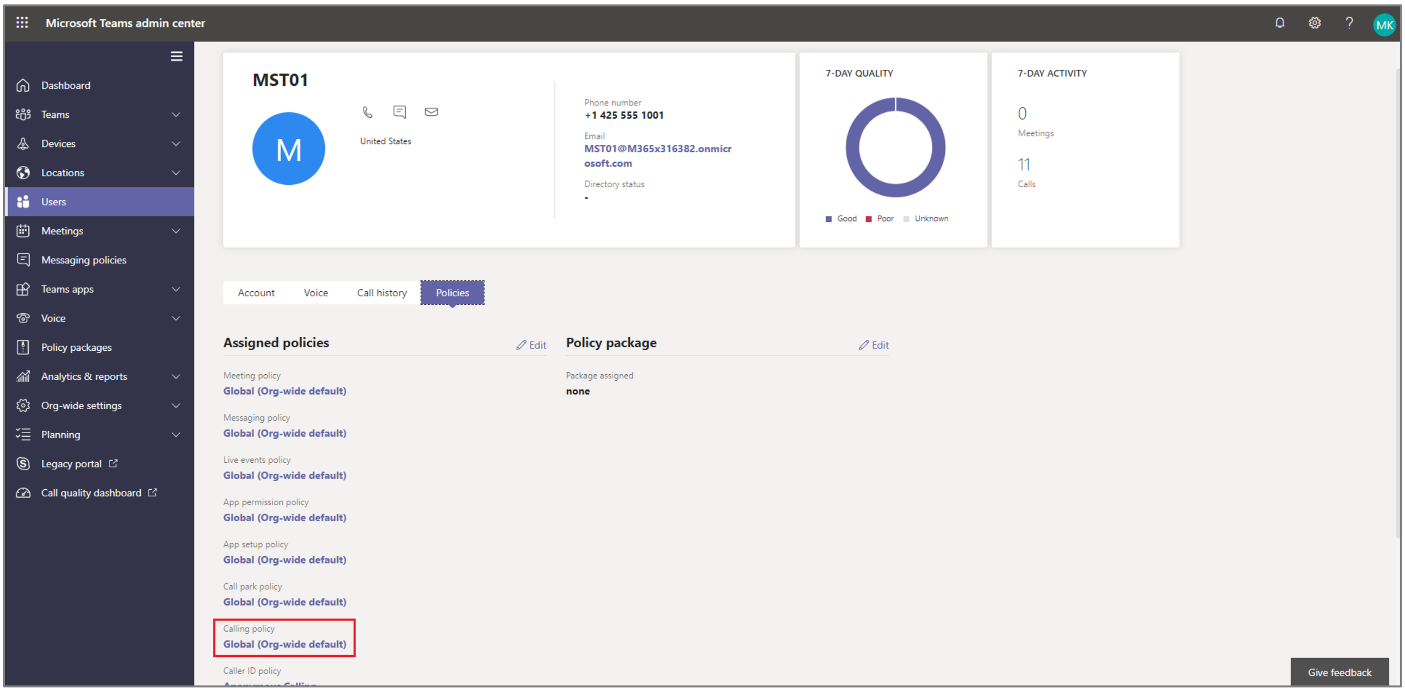
Grant to test users the previously created **Voice Routing Policy** with the commands:

Grant-CsOnlineVoiceRoutingPolicy -Identity MST01@M365x316382.onmicrosoft.com -PolicyName "CSL ATH"

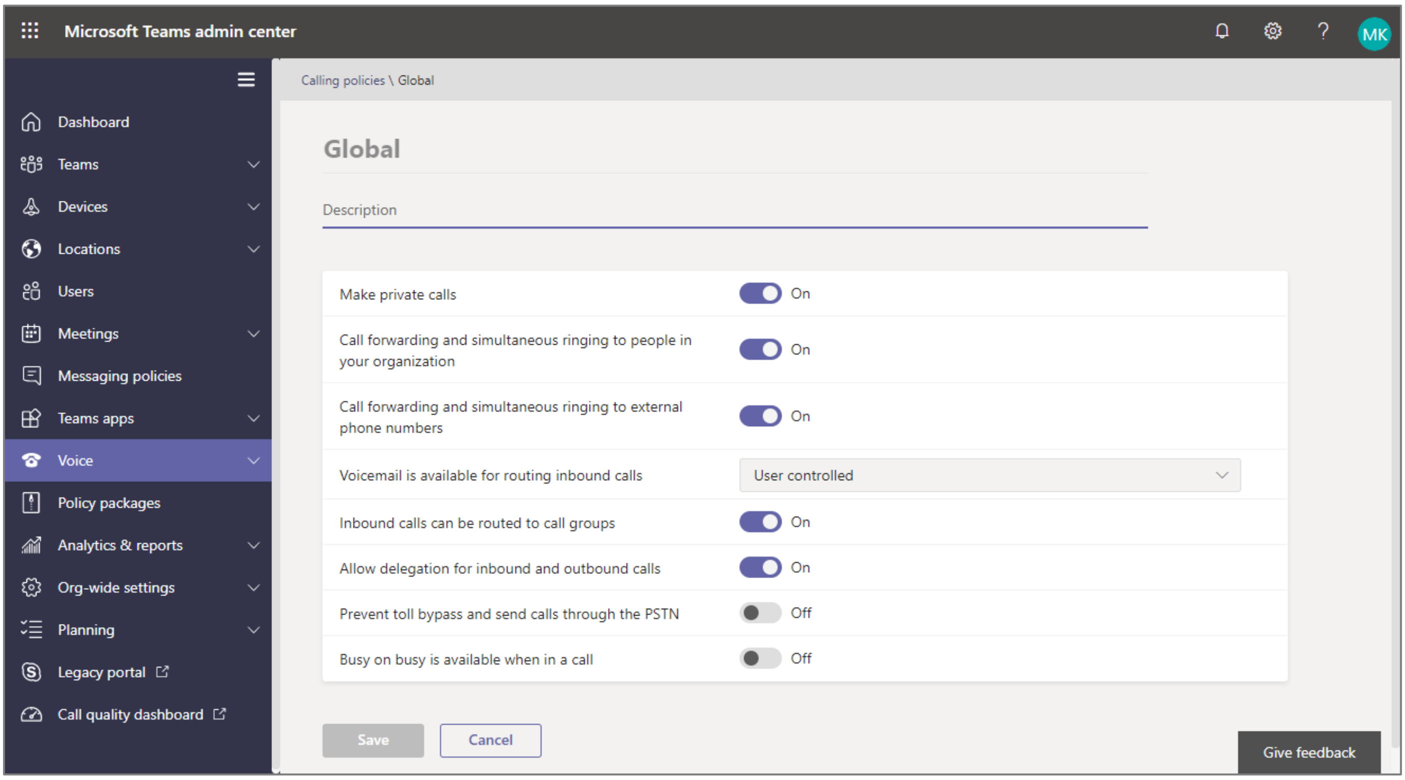
Grant-CsOnlineVoiceRoutingPolicy -Identity MST01@M365x316382.onmicrosoft.com -PolicyName "CSL ATH"

4.1.4. Designate the ability to use the calling functionality within Teams

You should have the Global policy assigned where calling functionality is enabled.



At Teams Admin Center, navigate to **Users,** select a user and click **Policies.** On this window various policies may be assigned to the user by clicking on **Edit**.

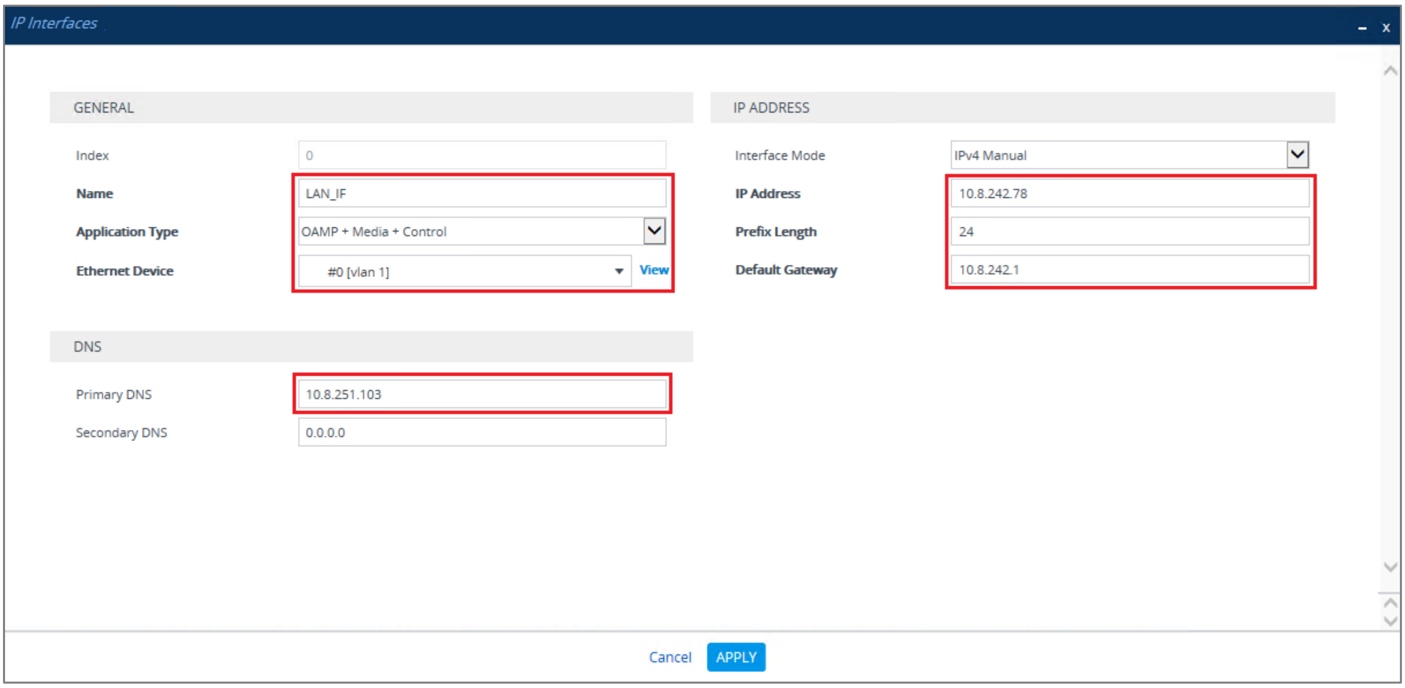


Click **Global (Org-wide default)** under **Calling Policies** to view various policy options.

Instead of Teams Admin Center, PowerShell may be used.

4.2. Configuring the AudioCodes SBC

4.2.1. LAN and WAN IP Interfaces

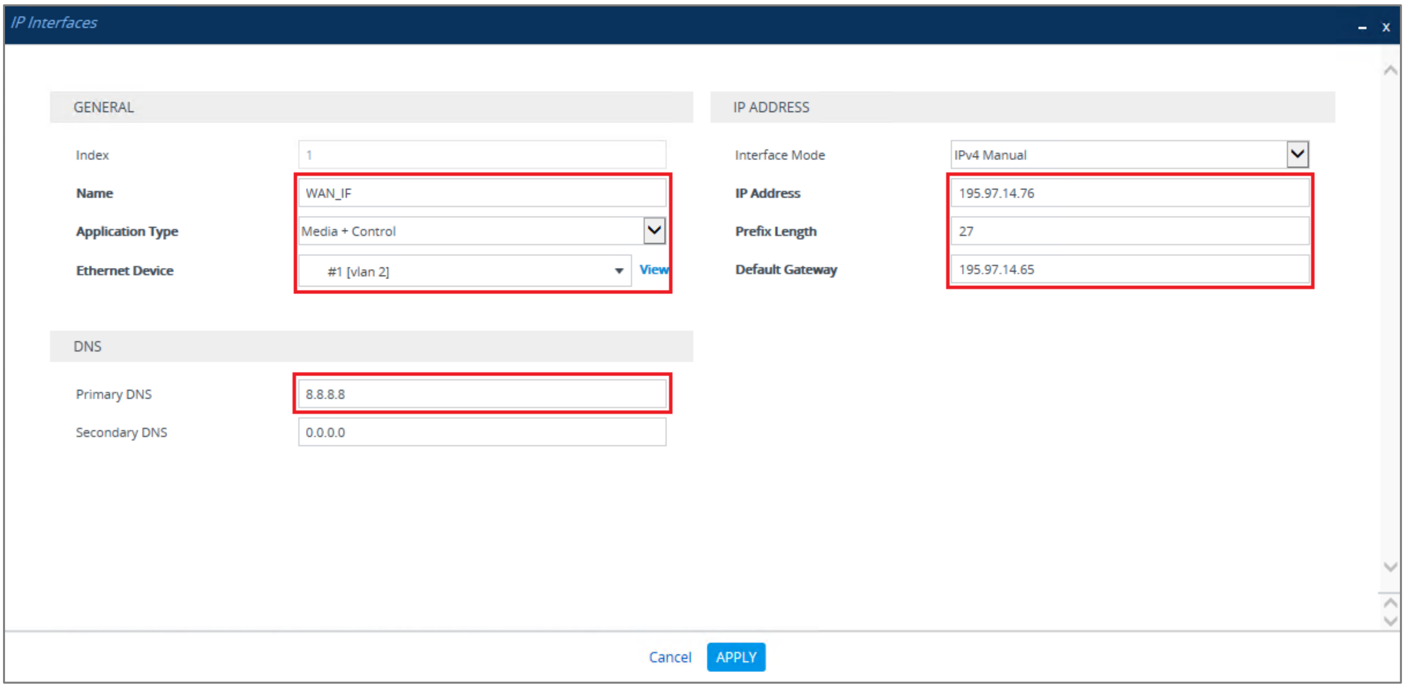


Navigate to: **SETUP >> IP NETWORK >> CORE ENTITIES >> IP Interfaces** and click **New.** To configure the LAN interface (faces to OS Voice), enter the following:

In the new window, configure the following fields:

- **Name**: LAN_IF (LAN interface friendly name)
- **Application Type**: OAMP + Media + Control
- **Ethernet Device**: vlan 1 (dedicated VLAN for LAN interface to OS Voice)
- **Primary DNS**: 10.8.251.103
- **IP Address**: 10.8.242.78 (SBC IP – SBC WBM IP)
- **Prefix Length**: 24
- **Default Gateway**: 10.8.242.1

Click **Apply**.



For the WAN interface (pointing to Teams via internet), navigate to:

SETUP >> IP NETWORK >> CORE ENTITIES >> IP Interfaces, click **New** and configure:

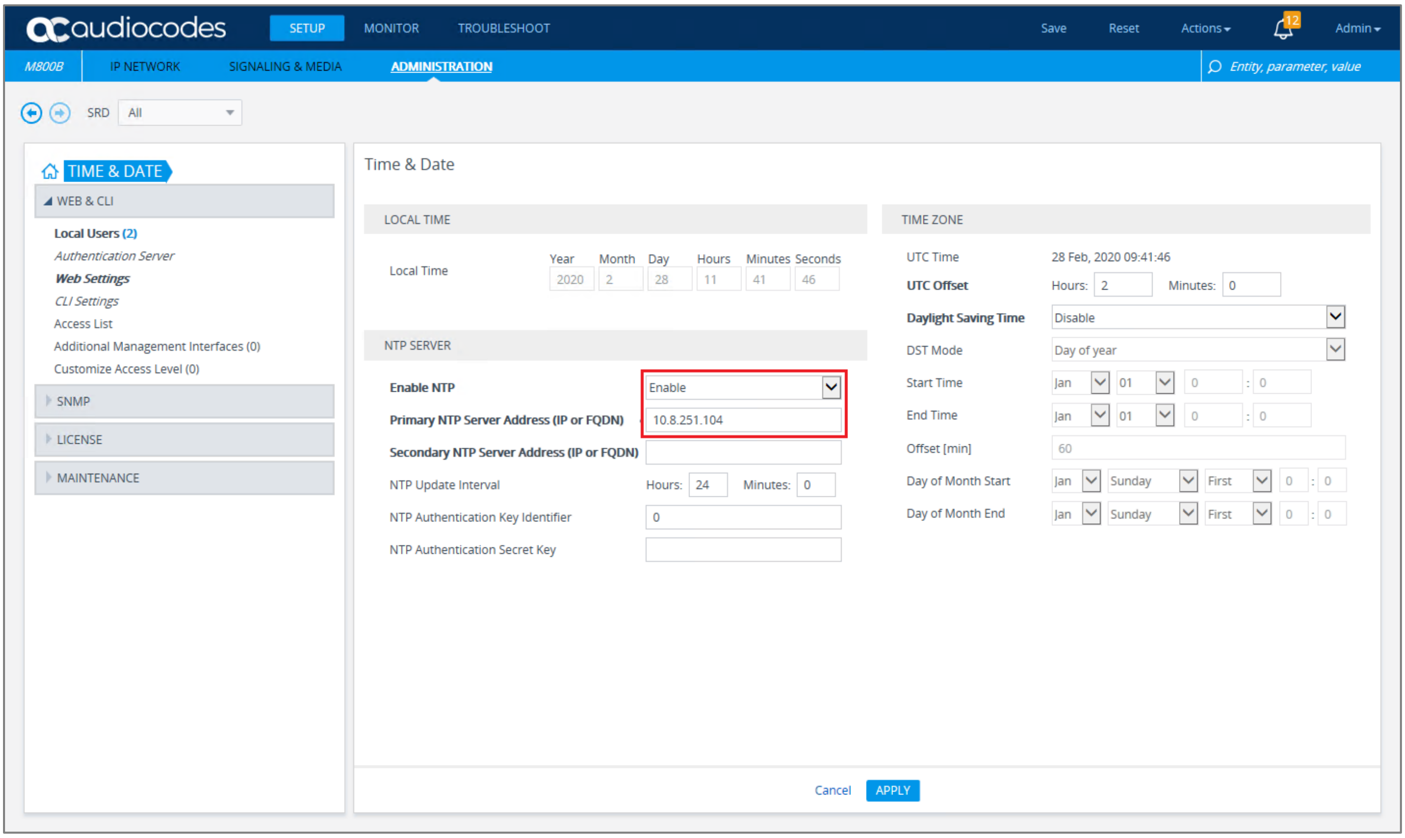
- **Name**: WAN_IF (WAN interface friendly name).
- **Application Type**: Media + Control (not recommended to activate OAMP i.e. SBC WBM on an interface pointing to internet).
- **Ethernet Device**: vlan 2 (dedicated VLAN for WAN interface to Teams).
- **Primary DNS**: 8.8.8.8 (any known public DNS or according to internet provider's instructions).
- **IP Address**: 195.97.14.76 (DMZ IP address of SBC)
- **Prefix Length**: 27
- **Default Gateway**: 195.97.14.65 (router GW IP)

Click **Apply**.

4.2.2. Teams TLS Context

As Microsoft Teams will only use TLS and it's connected over the Internet, a public certificate, issued only by a Microsoft trusted CA must be used in the SBC to establish TLS sessions. The public certificate must contain a SAN record for the SBC

For TLS to work, time synchronization is required. So, NTP configuration is needed on SBC. The NTP used, should be in sync with Microsoft NTP server or any other global server.

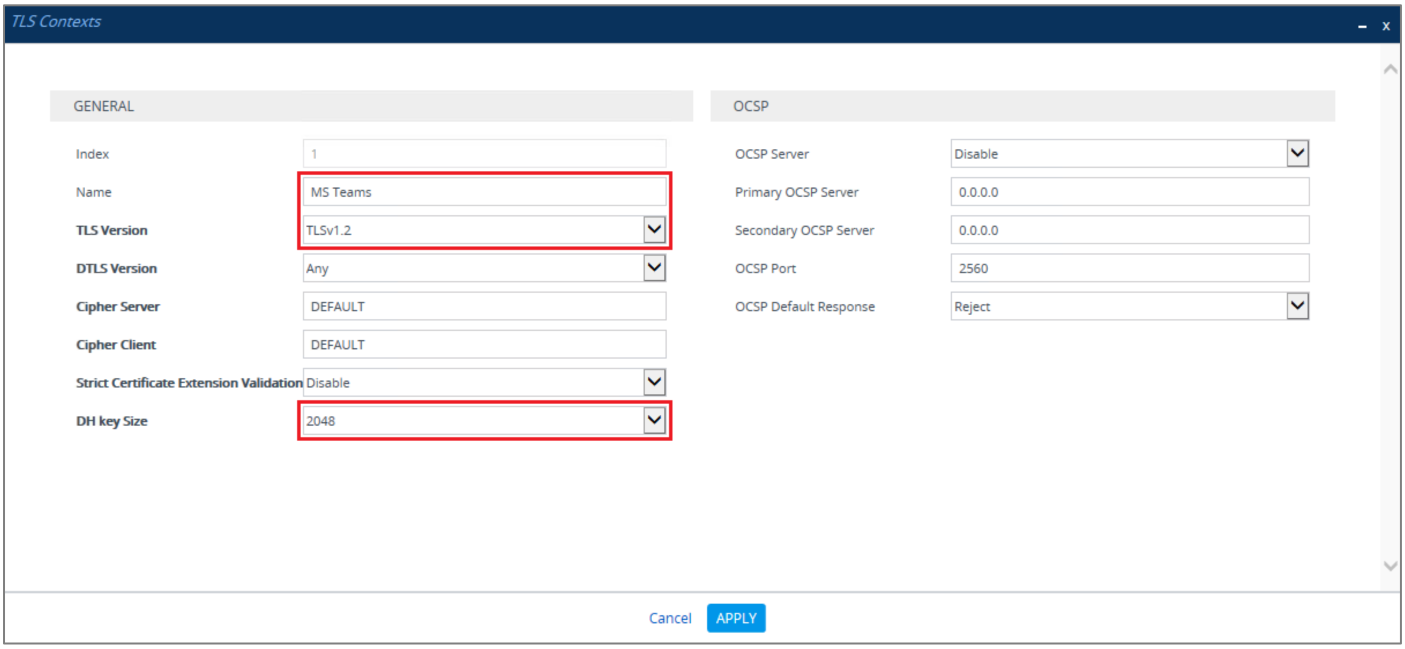


Navigate to: **SETUP >> ADMINISTRATION >> TIME & DATE** and enter the following:

- **Enable NTP:** Enable
- **Primary NTP Server Address**: 10.8.251.104 (reachable from OAMP IP interface, i.e. LAN_IF)
  This NTP is also used by Unify systems in certification environment

Click **Apply**.

Next step is to create a Teams Direct Routing TLS context in SBC.



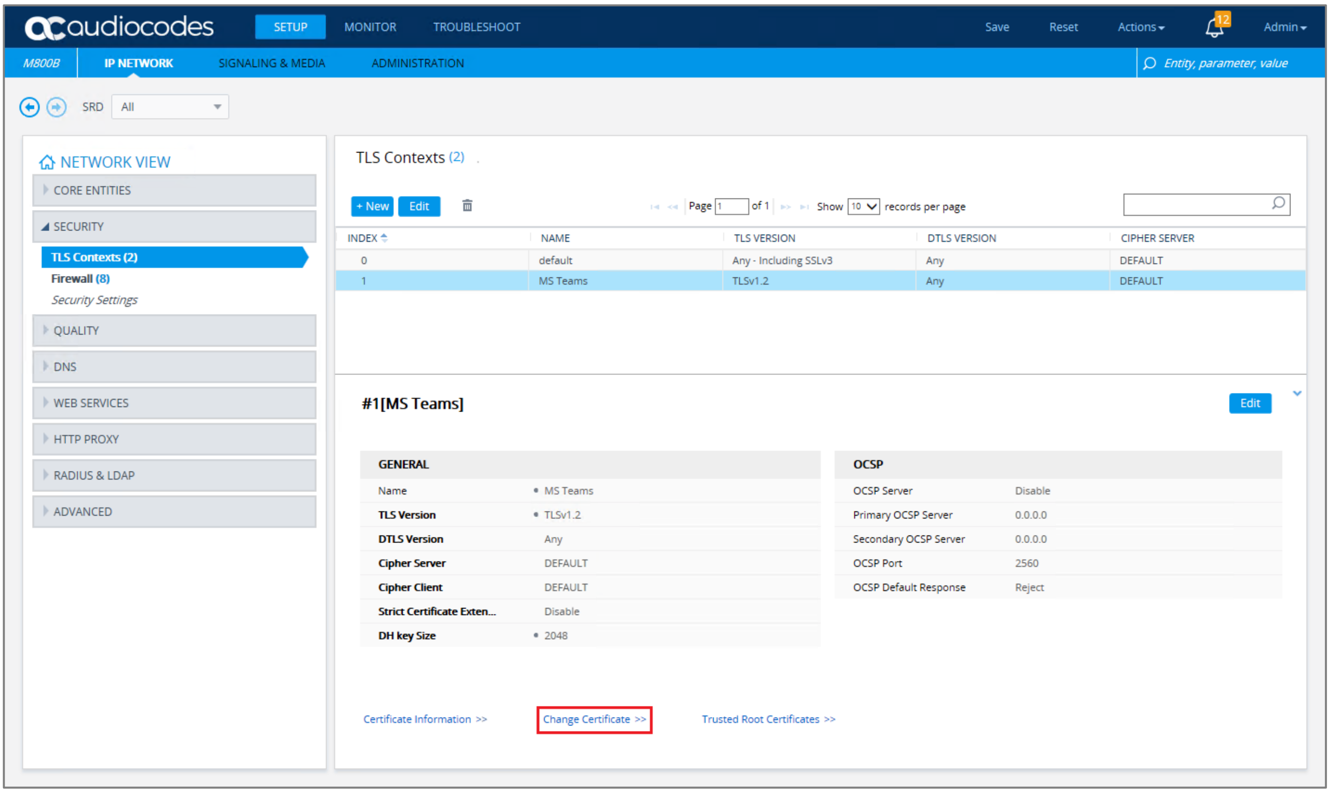
Navigate to: **SETUP >> IP NETWORK >> SECURITY >> TLS Contexts** and click **New.**

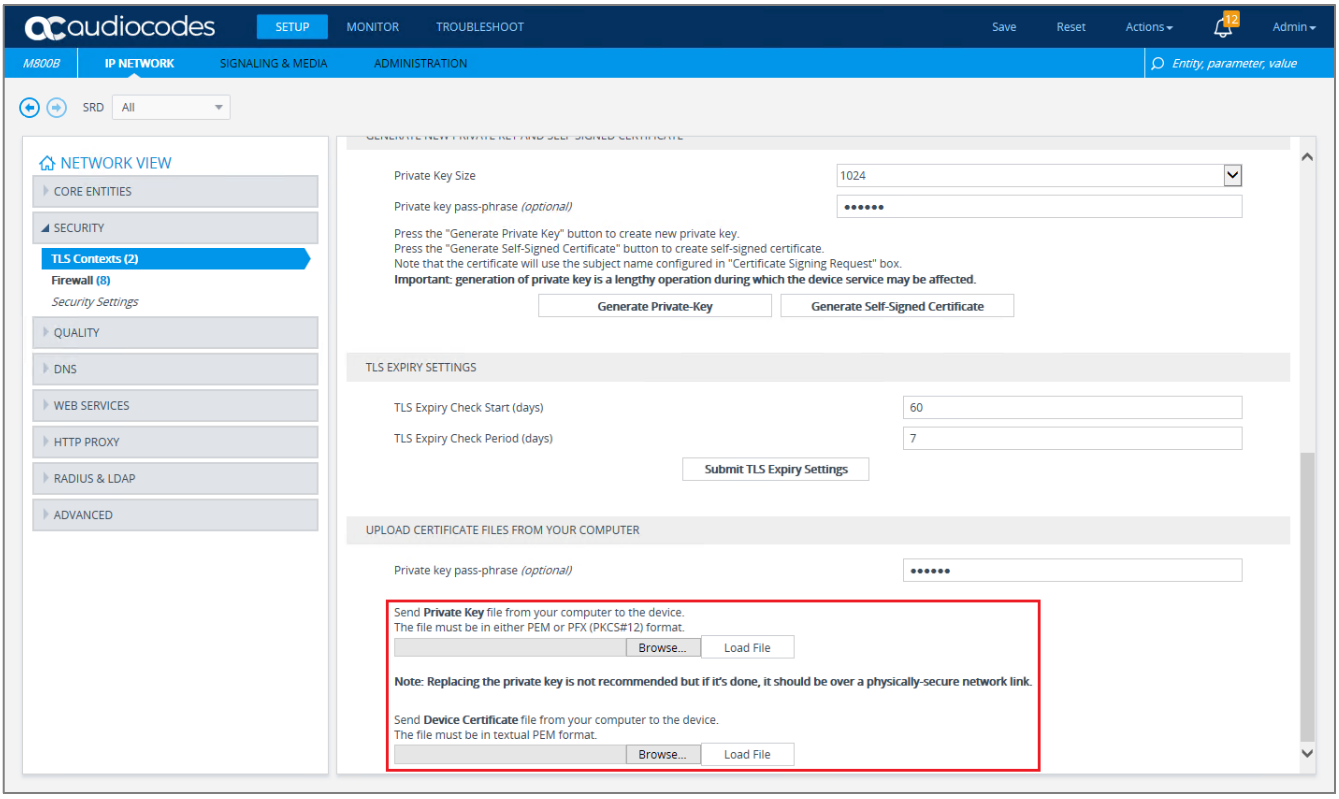
Enter the following:

- **Name:** MS Teams (Teams TLS context friendly name)
- **TLS Version:** TLSv1.2
- **DH key Size:** 2048

Click **Apply**.

After the Teams TLS context has been configured, the public certificate will be assigned to SBC.

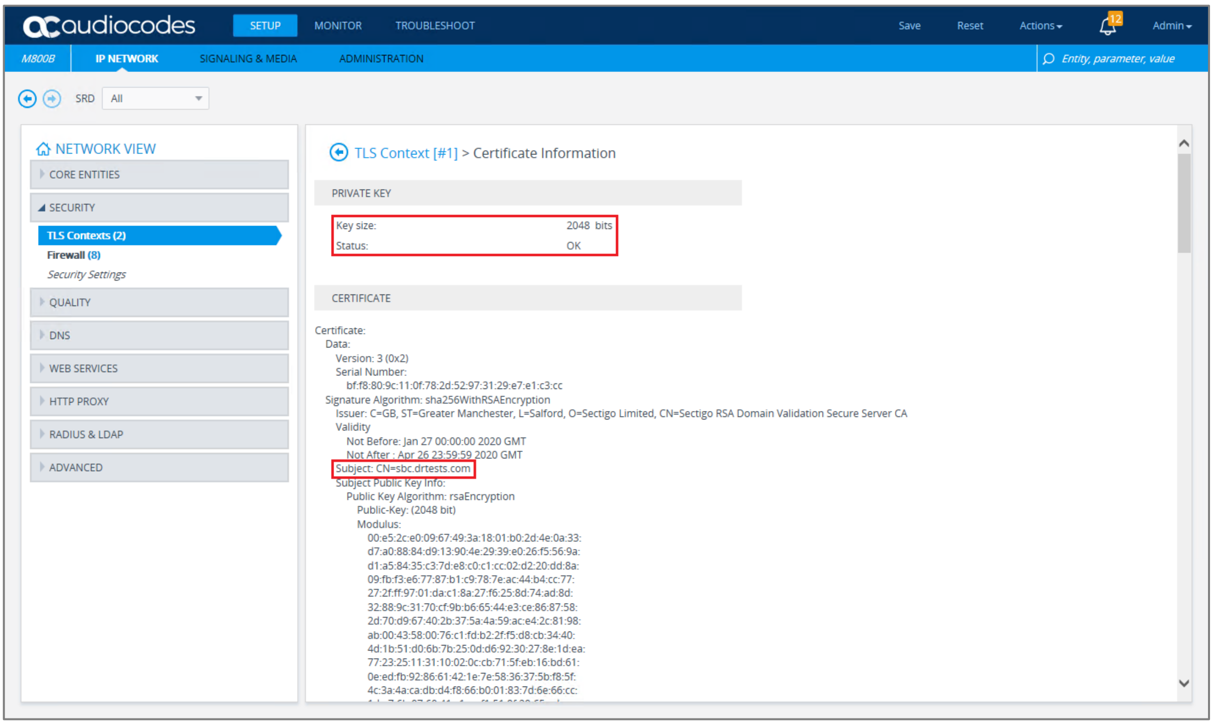




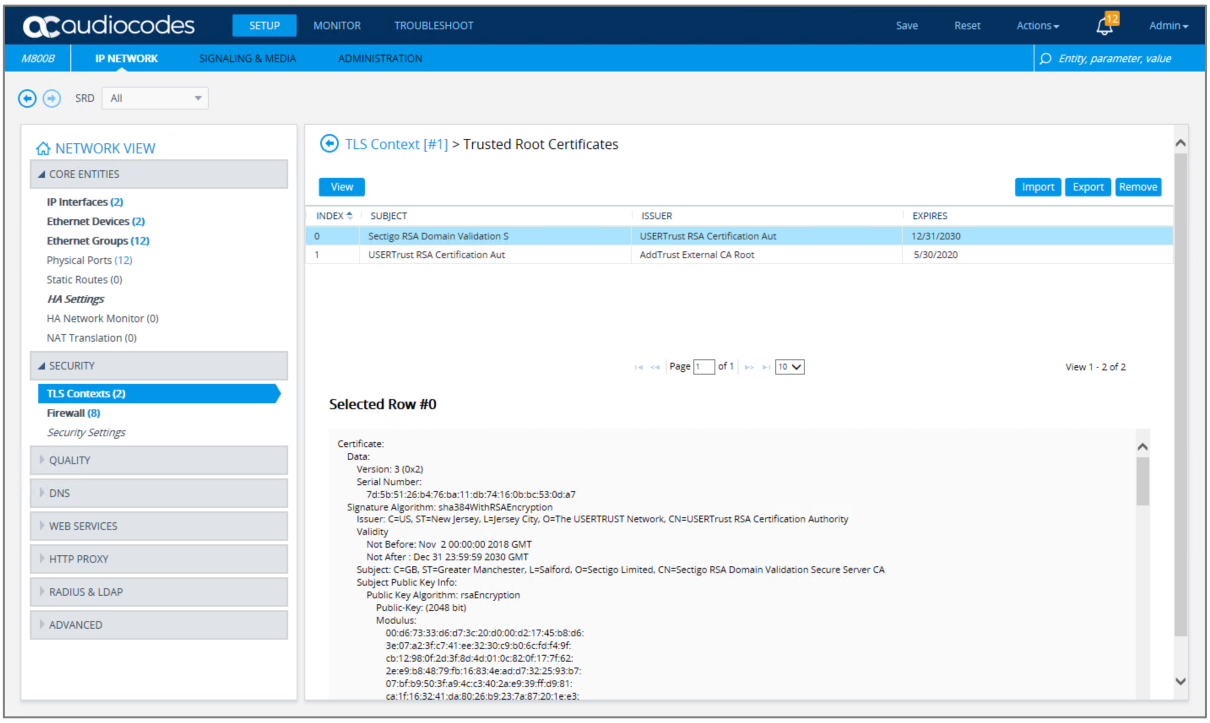
On **TLS Contexts** click the **Change Certificates** link and on the page that appears, scroll down and on the **Upload Certificate Files from Your Computer** section, upload the `privatekey.pem` and `certificate.pem` files, provided by the CA.

A message indicating that the certificate was uploaded successfully is displayed in blue on the lower part of the page.

Note: Before uploading the certificate, check that the **Private Key Size** is configured as 2048 and not 1024 in the **Generate new private key and self-signed certificate** section. If it's set to 1024, then change it to 2048 from the drop-down menu and click **Generate Private-Key.** This process might take couple of seconds to complete. It'll show as *New Private Key Configured* on the same window, upon successful configuration.



Go back to the **TLS Contexts** page and for the **MS Teams TLS Context**, click the **Certificate Information** link to verify the Key size, certificate status and Subject Name.



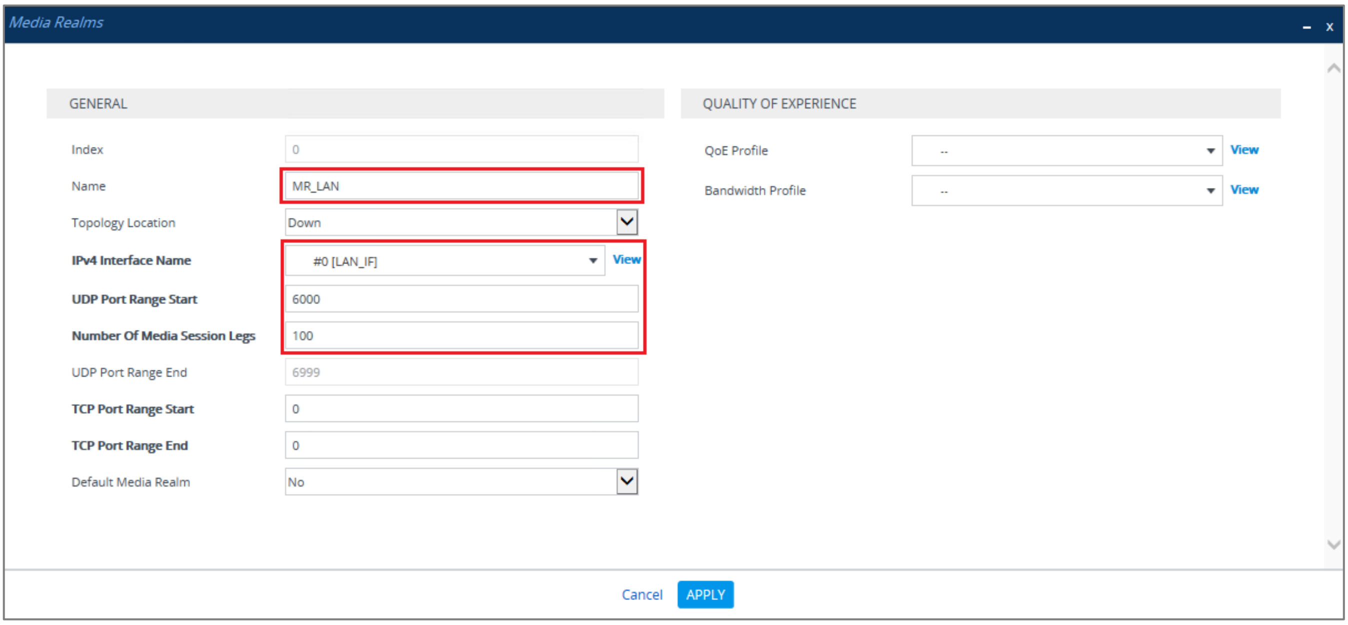
Return to the **TLS Contexts page**, select the required TLS Context index row, and then click the **Trusted Root Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.

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

Click **OK**. The certificate is loaded to the device and listed in the Trusted Certificates store.

4.2.3. Media Realms

Media Realms allow dividing the UDP port ranges for use on different interfaces. For the needs of current certification, two media realms are created; one for the LAN_IF interface and one for the WAN_IF interface.

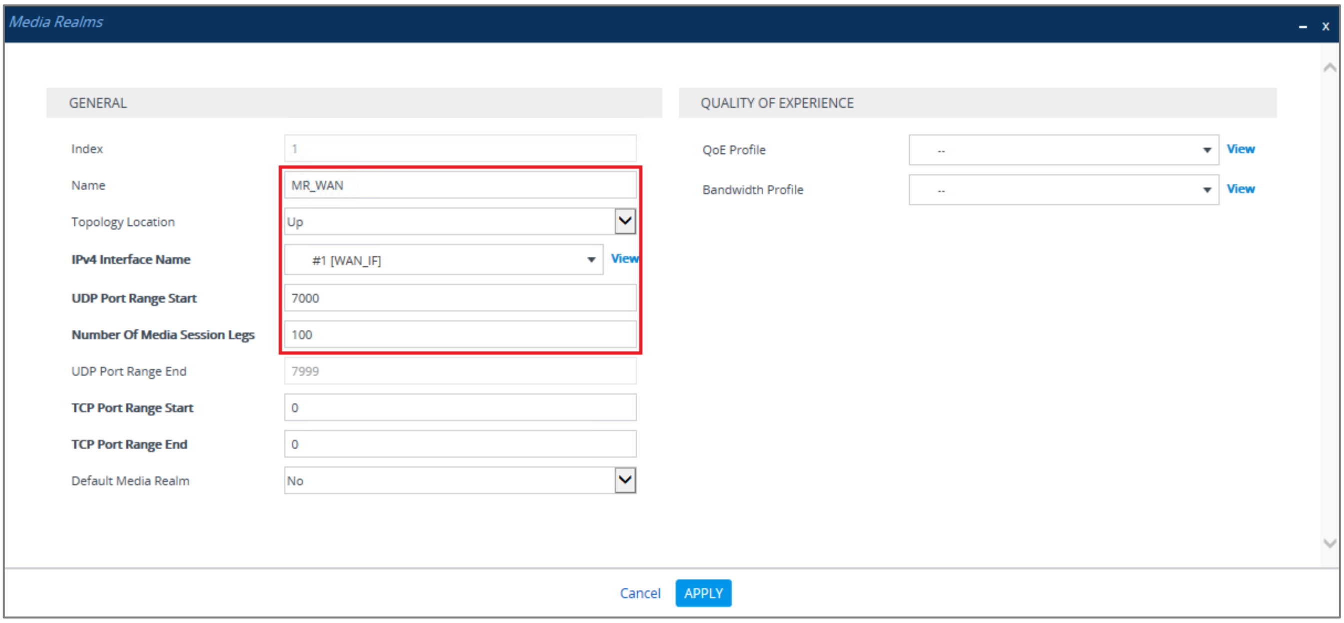


Access the page **SETUP >> SIGNALING & MEDIA >> CORE ENTITIES >> Media Realms** and click **New.**

To configure a media realm for LAN_IF, enter the following:

- **Name**: MR_LAN (LAN media realm friendly name)
- **IPv4 Interface Name**: LAN_IF (see 4.2.1)
- **UDP Port Range Start**: 6000
- **Number Of Media Session Legs**: 100 (need to be calculated based on usage)

Click **Apply**.



Navigate to **SETUP >> SIGNALING & MEDIA >> CORE ENTITIES >> Media Realms** and click **New.** To configure a media realm for WAN_IF, enter the following:

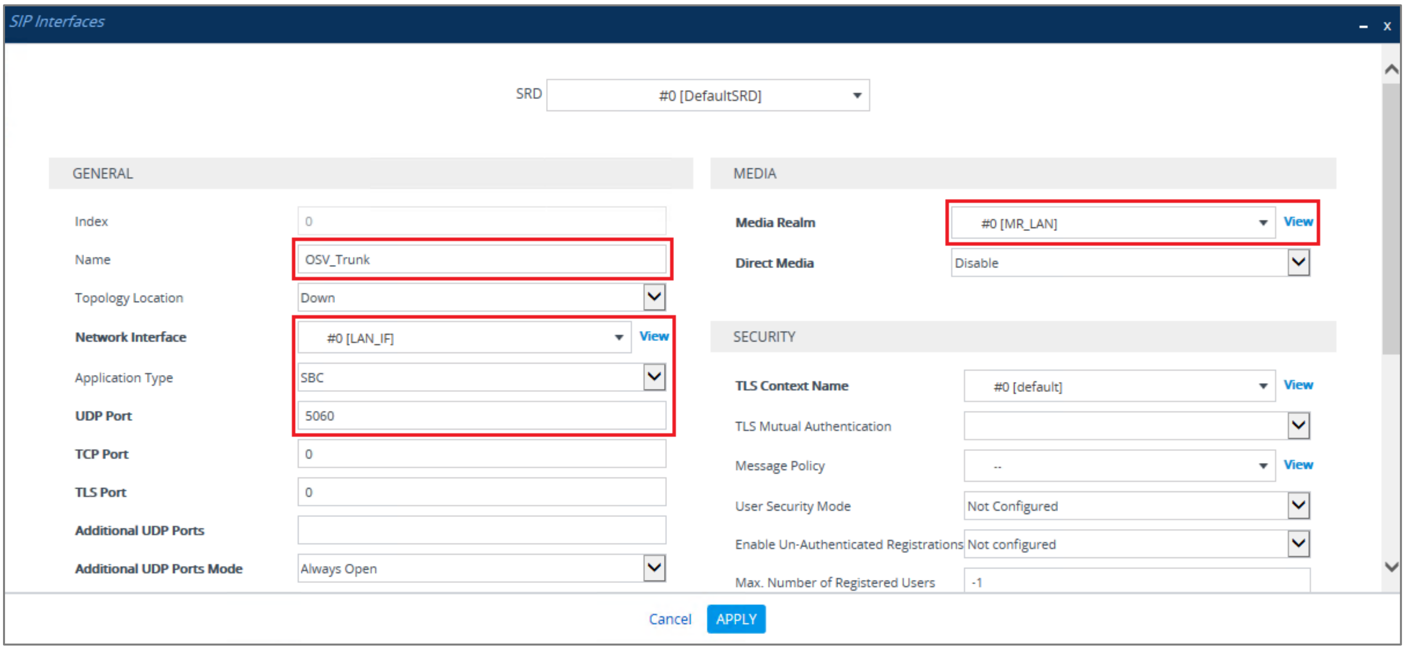
- **Name**: MR_WAN (WAN media realm friendly name)
- **IPv4 Interface Name**: WAN_IF (see 4.2.1)
- **Topology Location** Up
- **UDP Port Range Start**: 7000
- **Number Of Media Session Legs**: 100 (need to be calculated based on usage)

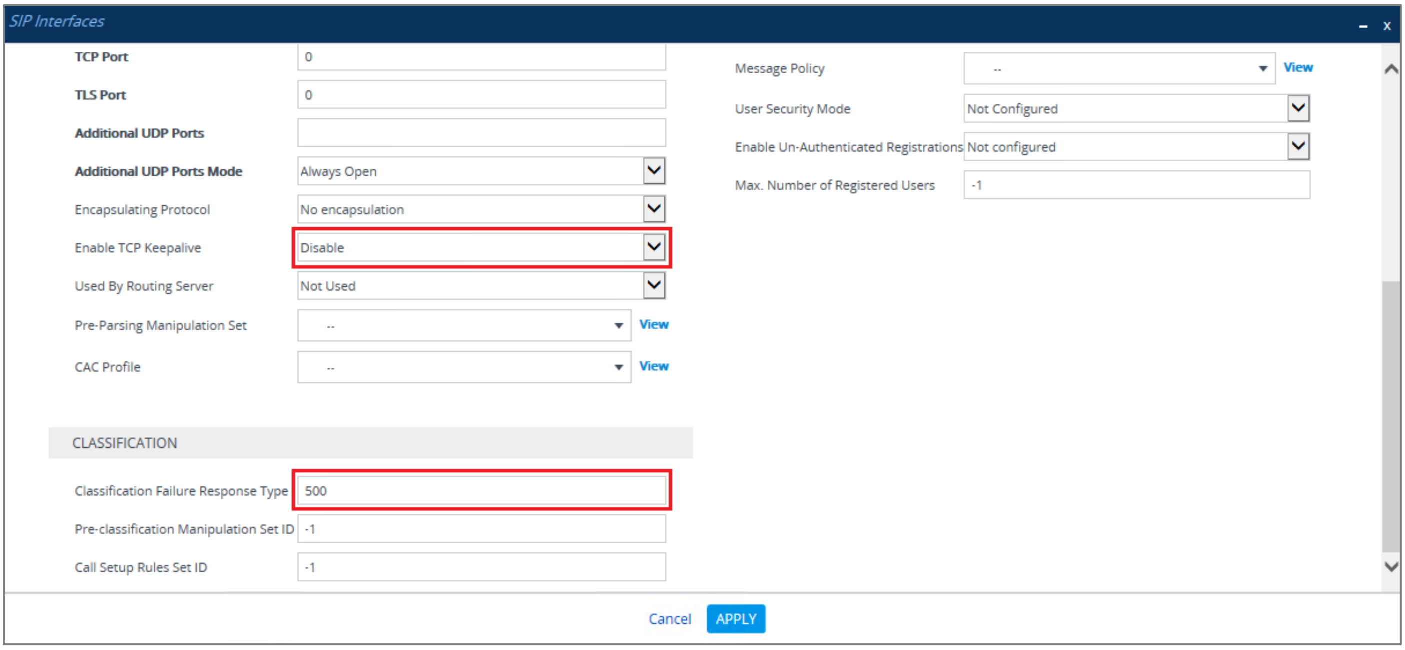
Click **Apply**.

4.2.4. SIP Signaling Interfaces

With the SIP interface configuration, the listening ports and protocols (UDP, TCP, or TLS) are configured for the SIP signaling traffic between the SBC - MS Phone System and the SBC – OS Voice.

For the SBC - MS Phone System link, the communication is always TLS; UDP / TCP isn’t supported due to security reasons.

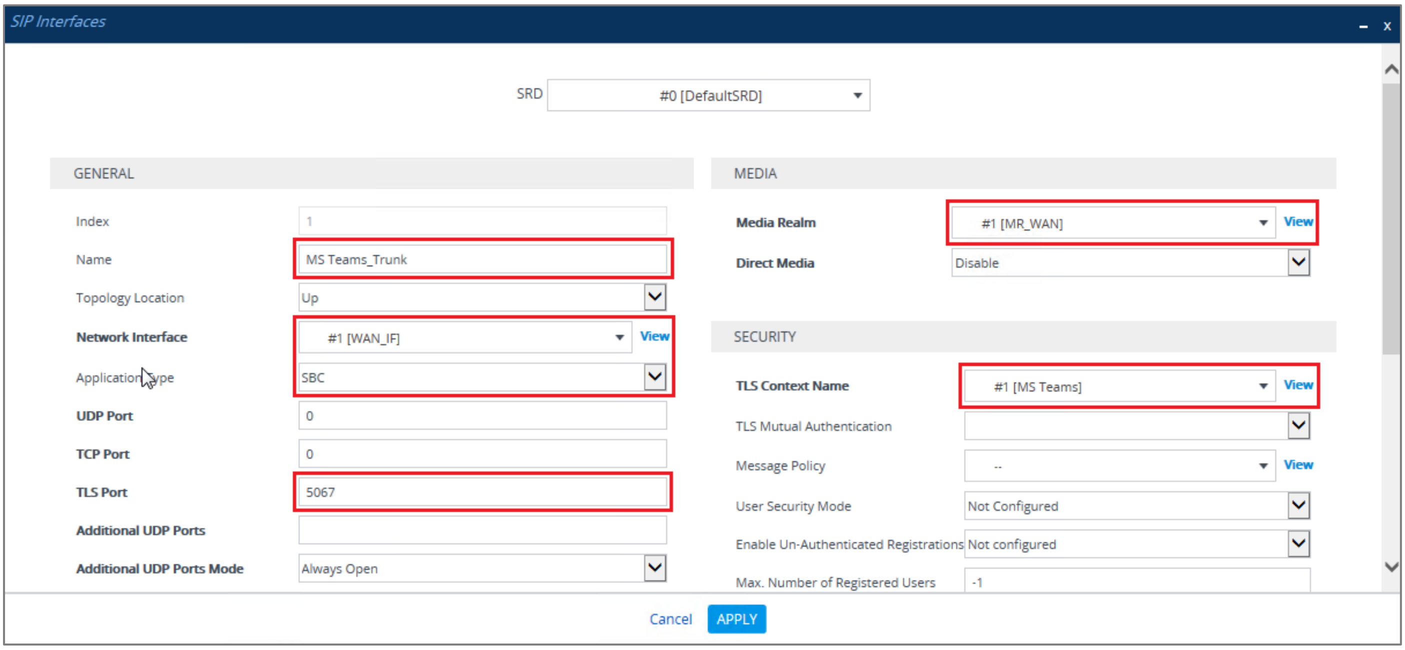


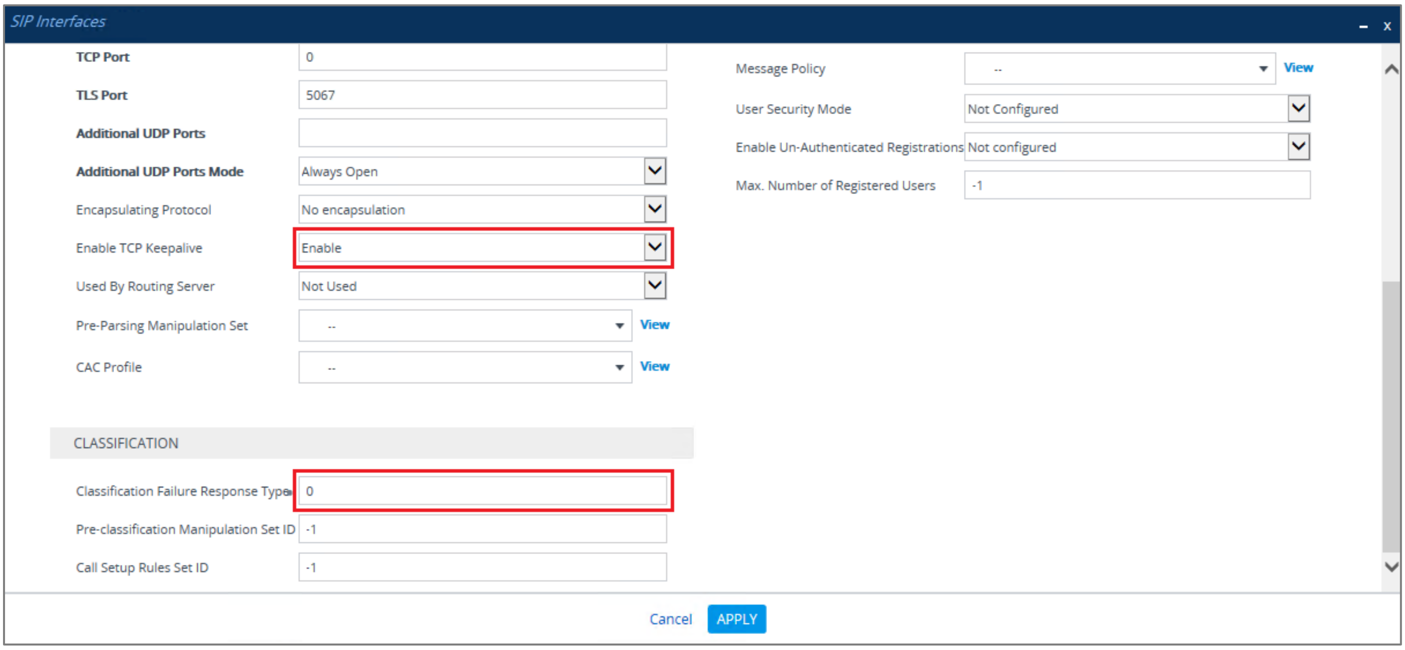


For the SIP trunk with the OS Voice configuration, navigate to **SETUP >> SIGNALING & MEDIA >> CORE ENTITIES >> SIP Interfaces**, click **New** and enter the following:

- **Name**: OSV_Trunk (SIP trunk with OS Voice friendly name)
- **Network Interface**: LAN_IF (see 4.2.1)
- **Application Type**: SBC
- **UDP Port:** 5060, as configured in OS Voice (TCP and TLS ports are set to 0, because the connection with OS Voice is UDP)
- **Enable TCP Keepalive:** Disable (keep default value)
- **Classification Failure response Type:** 500 (leave default setting)
- **Media Realm**: MR_LAN (see 4.2.3)

Click **Apply**.





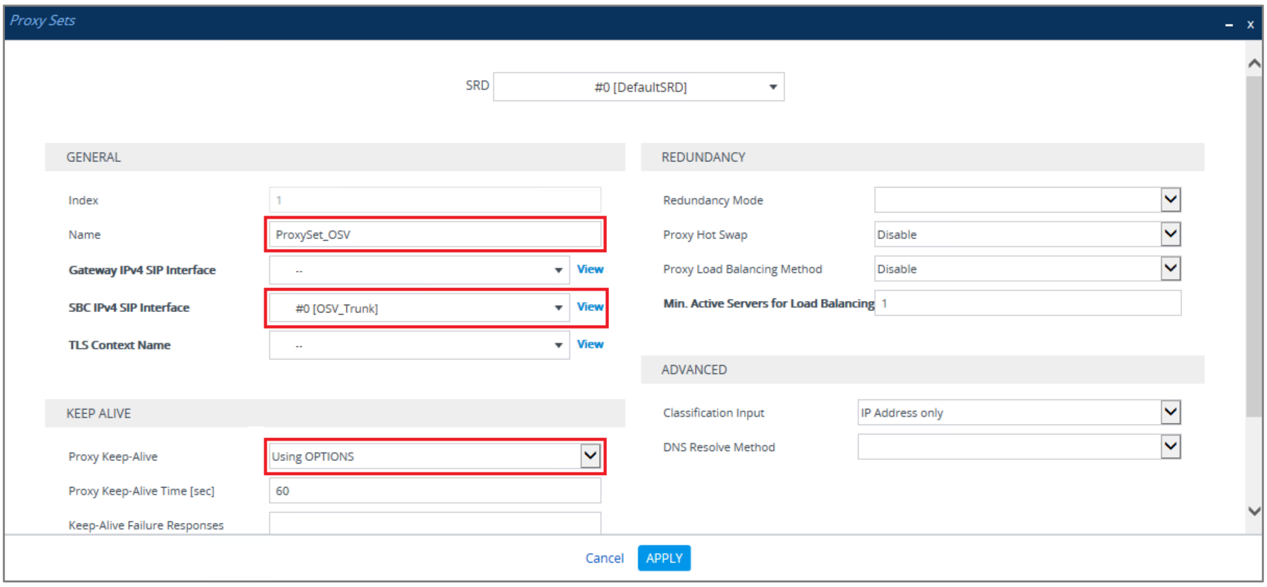
For the SIP trunk configuration, navigate to **SETUP >> SIGNALING & MEDIA >> CORE ENTITIES >> SIP Interfaces**, click **New** and enter the following:

- **Name**: MS Teams_Trunk (SIP trunk with MS Phone System friendly name)
- **Network Interface**: WAN_IF (see 4.2.1)
- **Application Type**: SBC
  UDP Port: 5067, as configured in Teams tenant (UDP and TCP ports are set to 0, because the connection with MS Phone System is TLS only)
- **Enable TCP Keepalive:** Enable
- **Classification Failure response Type:** 0 (recommended to prevent DoS attacks)
- **Media Realm**: MR_LAN (see 4.2.3)
- **TLS Context Name**: MS Teams (see 4.2.2).

Click **Apply**.

4.2.5. Proxy Sets and Proxy Addresses

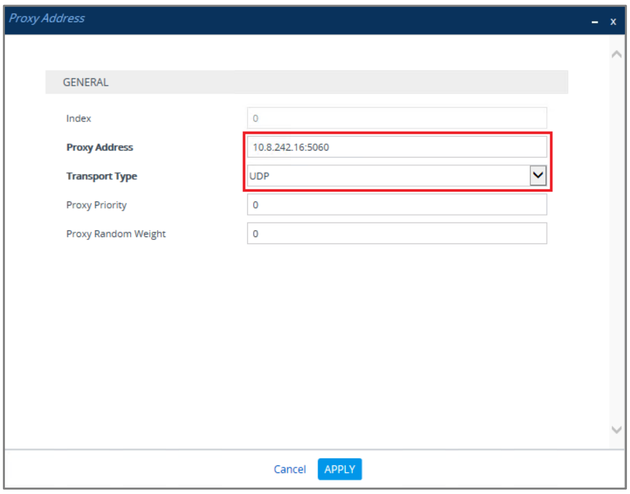
The Proxy Set and Proxy Address defines TLS parameters, IP interfaces, FQDN and the remote entity's port. Proxy Sets can also be used to configure load balancing between multiple servers.



Navigate to **SETUP >> SIGNALING & MEDIA >> CORE ENTITIES >> Proxy Sets** and click **New** to setup the OS Voice **Proxy Set.** Enter the following:

- **Name**: ProxySet_OSV (OS Voice proxy set friendly name).
- **SBC IPv4 SIP Interface**: OSV_Trunk (see 4.2.4).
- **Proxy Keepalive:** Using OPTIONS.
- **TLS Context Name**: MS Teams (see 4.2.2).

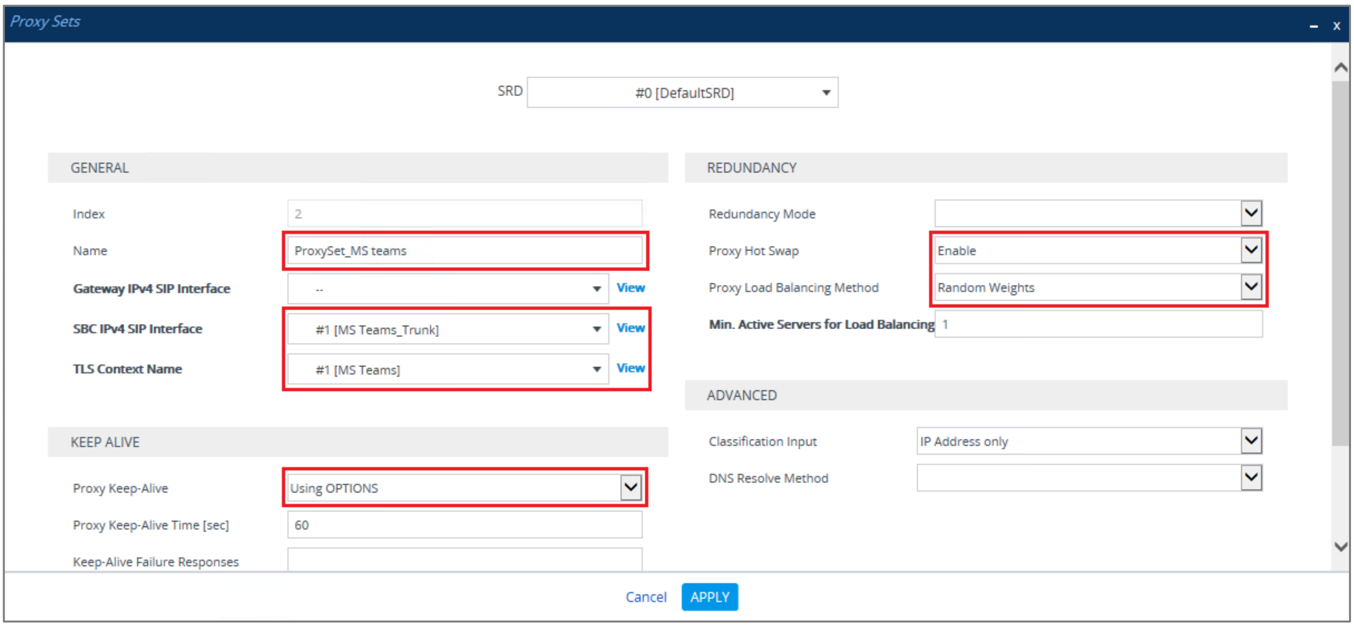
Click **Apply**.



Return to the **Proxy Sets** page, click the **Proxy Address** link and on the page that appears, click **New** to configure the SBC connectivity data with OS Voice:

- **Proxy Address**: 10.8.242.16:5060 (OS Voice IP / FQDN (SIPSM) and port)
- **Transport Type**: UDP

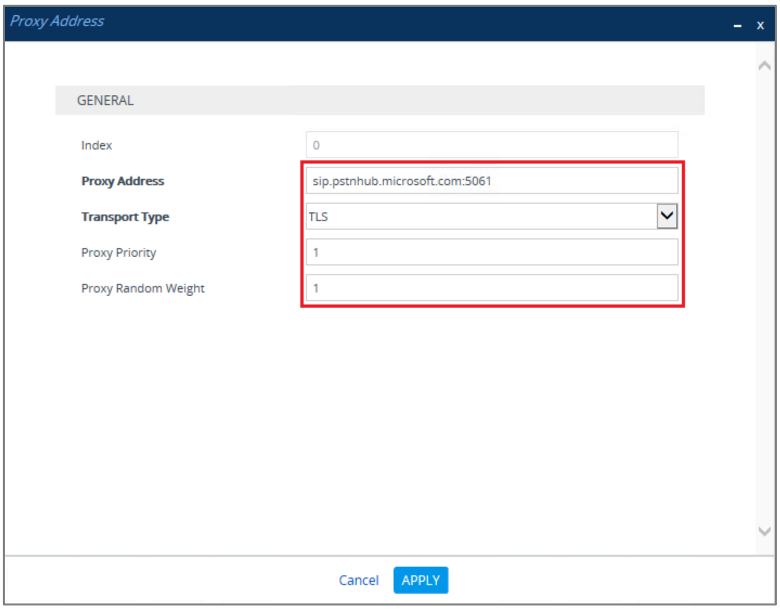
Click **Apply**.

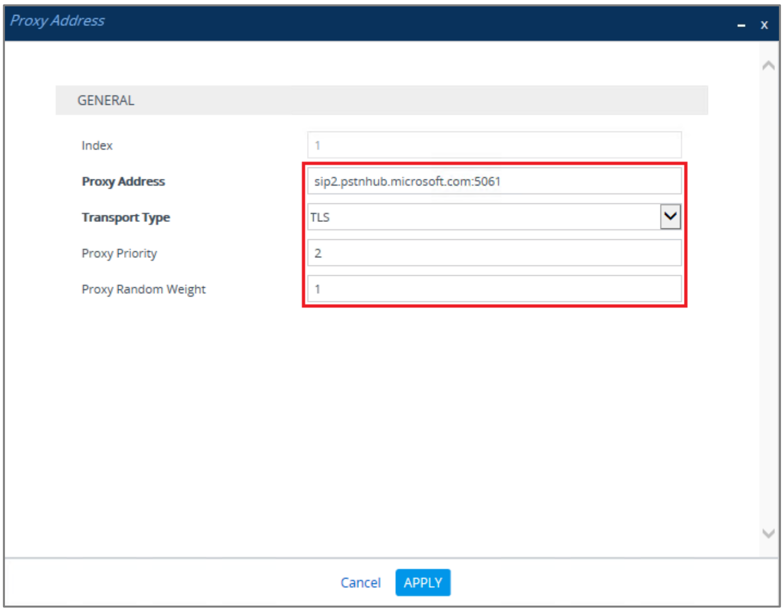


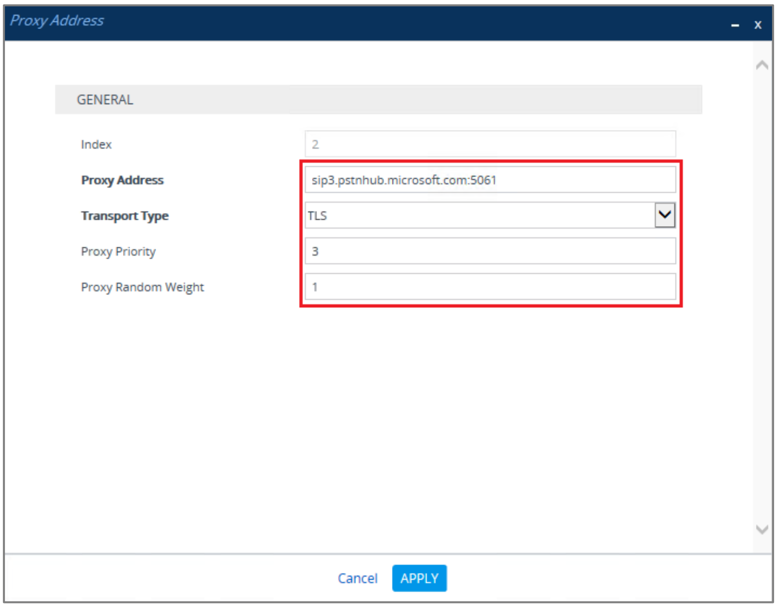
Navigate to **SETUP >> SIGNALING & MEDIA >> CORE ENTITIES >> Proxy Sets** and click **New** to setup the Teams **Proxy Set.** Enter the following:

• **Name**:	ProxySet_MS teams (Teams proxy set friendly name)
• **SBC IPv4 SIP Interface**:	MS Teams_Trunk (see 4.2.4)
• **TLS Context Name**:	MS Teams (see 4.2.2)
• **Proxy Keepalive:**	Using OPTIONS
• **Proxy Hot Swap**:	Enable
• **Proxy Load Balancing Method**:	Random Weights

Click **Apply**.







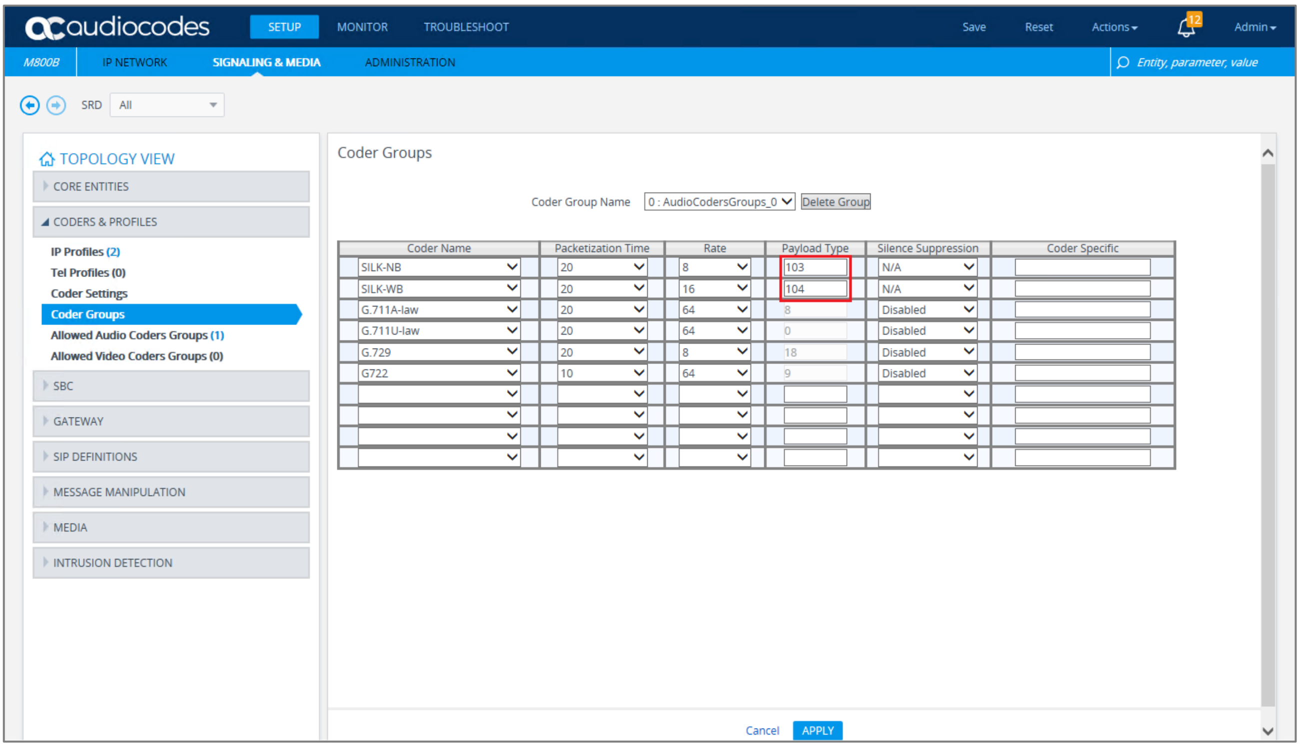
On **Proxy Sets** page, click the **Proxy Address** link and on the page that appears, click **New**. At Teams end, there are 3 SIP Proxies, so the procedure needs to be repeated 3 times. To configure the SBC connectivity data with Teams, enter the following:

• **Proxy Address**:	sip.pstnhub.microsoft.com:5061 (global FQDN and port) sip2.pstnhub.microsoft.com:5061 (failover FQDN and port) sip3.pstnhub.microsoft.com:5061 (failover FQDN and port)
• **Transport Type**:	TLS
• **Proxy Priority**:	1, 2, 3 (for sip, sip2 and sip3 proxy addresses, correspondingly)
• **Proxy Random Weight**:	1

Click **Apply**.

4.2.6. Coder Groups

The various audio codecs used for the communication between an OS Voice subscriber and a Teams user, on SBC side are manipulated from **Coder Group** menu. SILK and OPUS codecs are supported by Teams, but not from OS Voice. A coder group needs to be added with the supported codecs for each connection, i.e. to Teams and to OS Voice. Note that the Coder Group ID for this entity will be assigned to its corresponding IP Profile, described in next section.

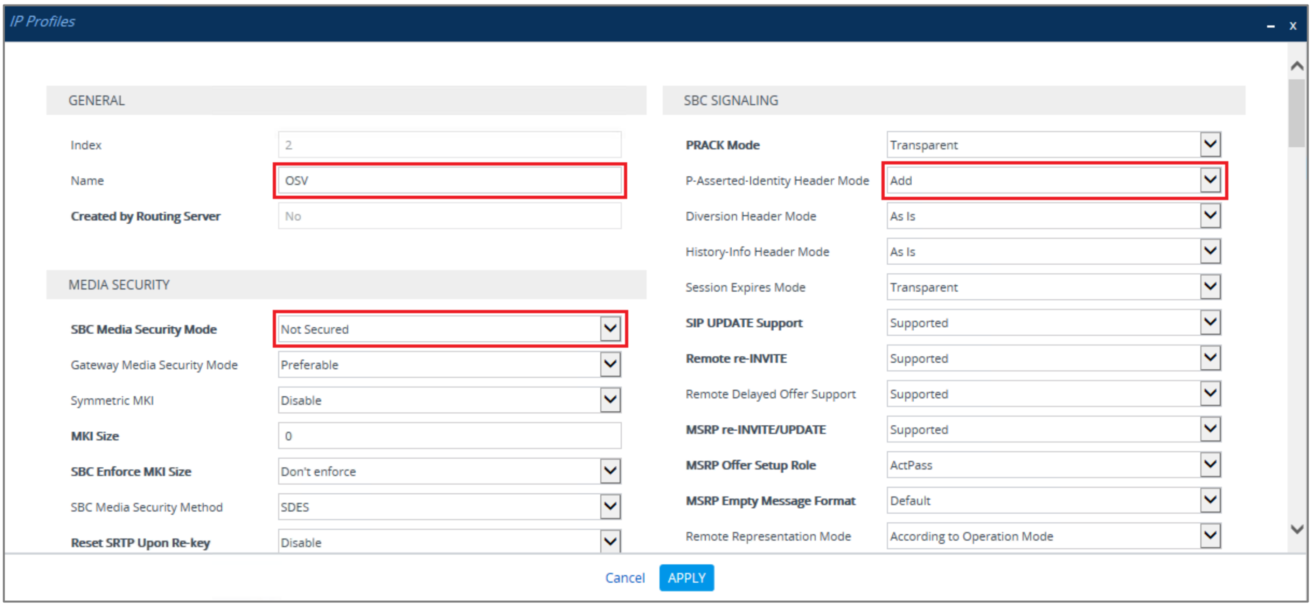


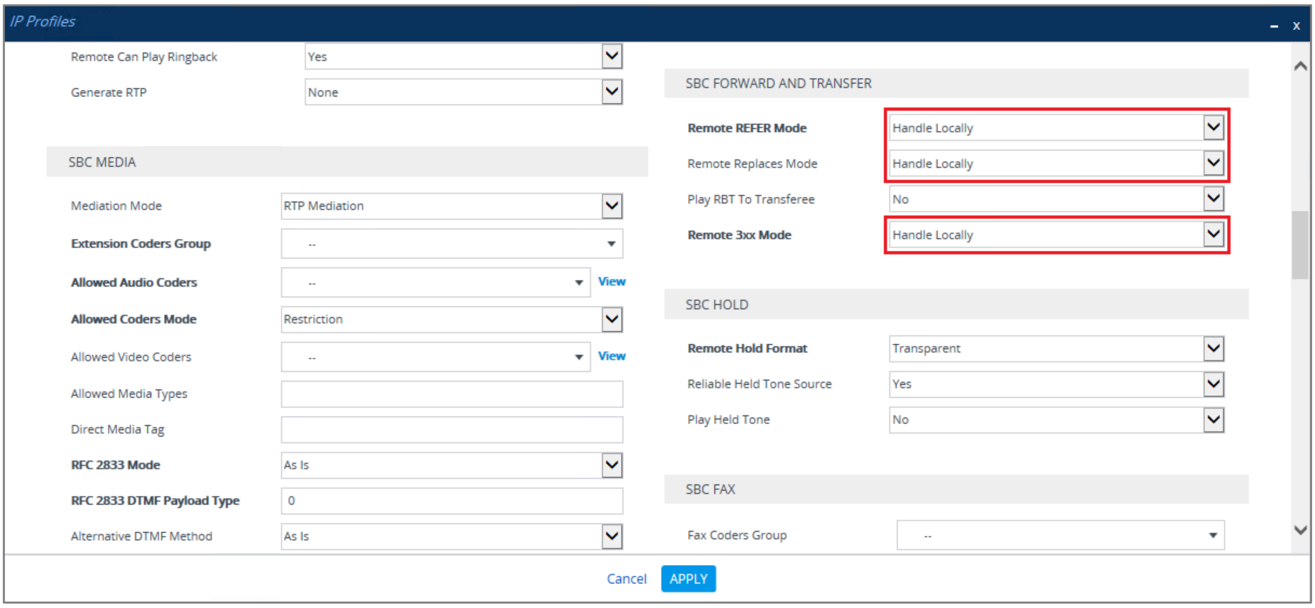
Navigate to: **SETUP >> SIGNALING & MEDIA >> CODERS & PROFILES >> Coder Groups** and from the **Coder Group Name** dropdown list, select *"1:Does Not Exist"* and add the required codecs as shown in the figure above**.**

Note: SILK Codecs are recommended as the preferred codecs to be used for the integration. Missing those, G.711 will still work. But will not be as optimized as using SILK codecs.

4.2.7. IP Profiles

The IP Profile includes parameters with user-defined settings related to signaling (e.g., SIP message terminations such as REFER) and media (e.g., codec). An IP Profile is associated to the specific IP Group.

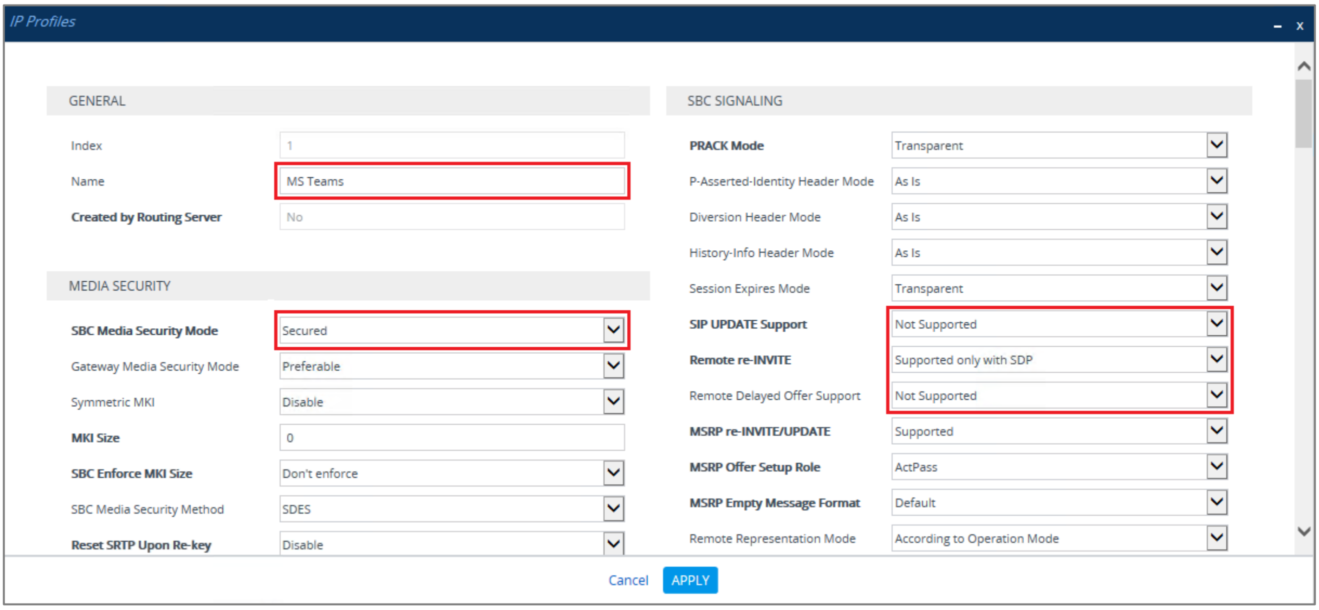


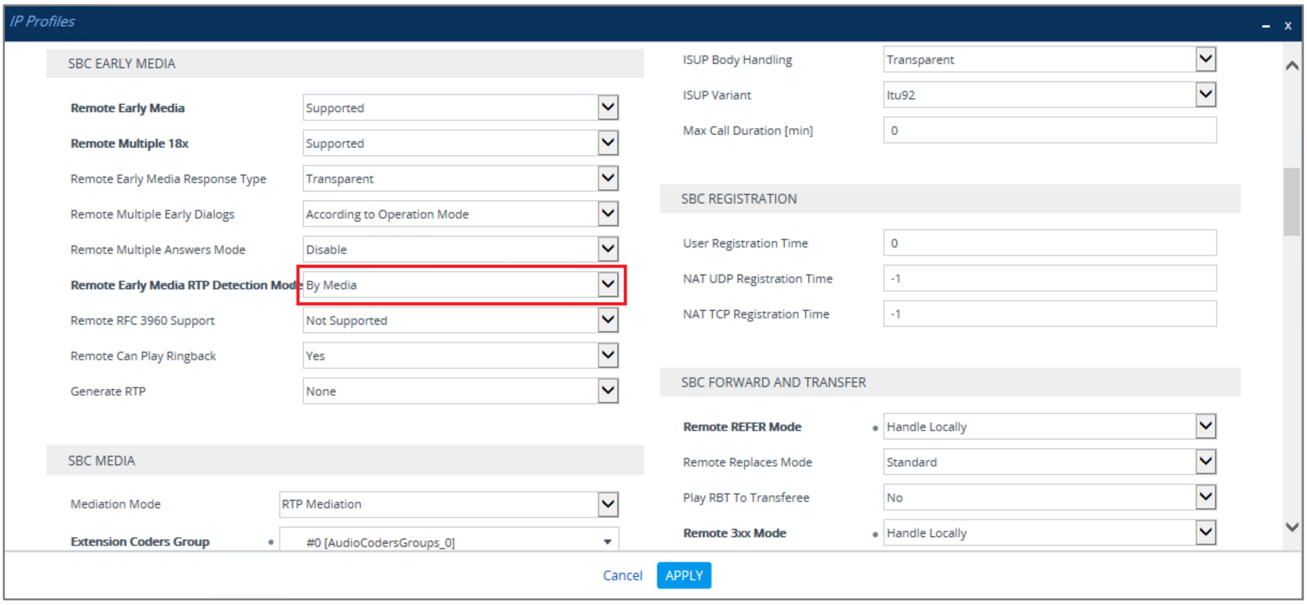


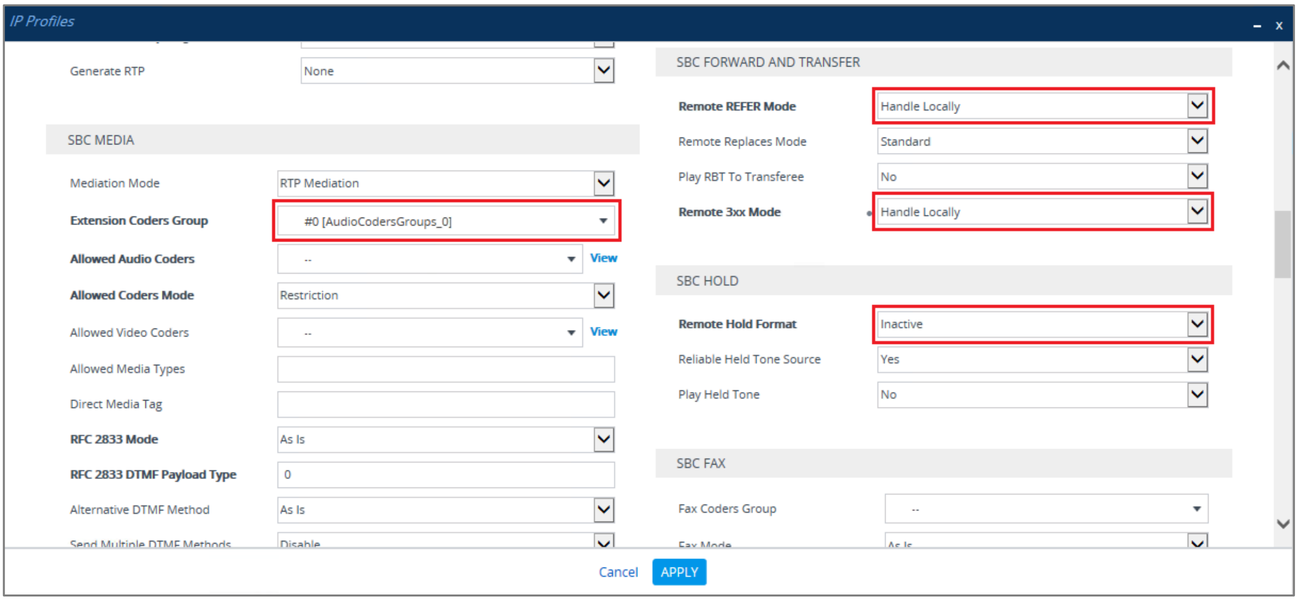
Navigate to **SETUP >> SIGNALING & MEDIA >> CODERS & PROFILES >> IP Profiles** and click **New** to create an IP profile for the OS Voice connection. Enter the following:

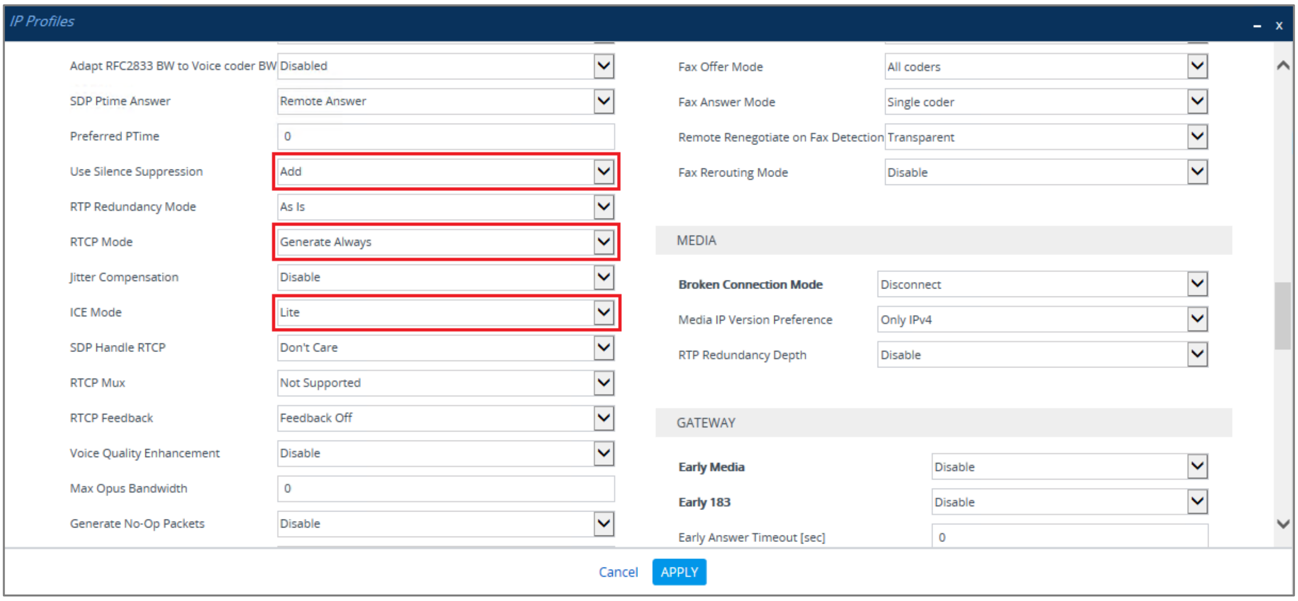
- **Name**: OSV (friendly name for OS Voice)
- **SBC Media Security Mode**: Not Secured (see restrictions in 2.2)
- **P-Asserted-Identity Header Mode**: Add (required for anonymous calls)
- **Remote REFER Mode:** Handle Locally
- **Remote Replaces Mode**: Handle Locally
- **Remote 3xx Mode**: Handle Locally

Click **Apply**.


IP Profiles
GENERAL
Index
1
Name
MS Teams
Created by Routing Server
No
MEDIA SECURITY
SBC Media Security Mode
Secured
Gateway Media Security Mode
Preferable
Symmetric MKI
Disable
MKI Size
0
SBC Enforce MKI Size
Don't enforce
SBC Media Security Method
SDES
Reset SRTP Upon Re-key
Disable
SBC SIGNALING
PRACK Mode
Transparent
P-Asserted-Identity Header Mode
As Is
Diversion Header Mode
As Is
History-Info Header Mode
As Is
Session Expires Mode
Transparent
SIP UPDATE Support
Not Supported
Remote re-INVITE
Supported only with SDP
Remote Delayed Offer Support
Not Supported
MSRP re-INVITE/UPDATE
Supported
MSRP Offer Setup Role
ActPass
MSRP Empty Message Format
Default
Remote Representation Mode
According to Operation Mode
Cancel
APPLY


IP Profiles
SBC EARLY MEDIA
Remote Early Media
Supported
Remote Multiple 18x
Supported
Remote Early Media Response Type
Transparent
Remote Multiple Early Dialogs
According to Operation Mode
Remote Multiple Answers Mode
Disable
Remote Early Media RTP Detection Mode
By Media
Remote RFC 3960 Support
Not Supported
Remote Can Play Ringback
Yes
Generate RTP
None
SBC MEDIA
Mediation Mode
RTP Mediation
Extension Coders Group
#0 [AudioCodersGroups_0]
ISUP Body Handling
Transparent
ISUP Variant
Itu92
Max Call Duration [min]
0
SBC REGISTRATION
User Registration Time
0
NAT UDP Registration Time
-1
NAT TCP Registration Time
-1
SBC FORWARD AND TRANSFER
Remote REFER Mode
Handle Locally
Remote Replaces Mode
Standard
Play RBT To Transferee
No
Remote 3xx Mode
Handle Locally
Cancel
APPLY





Navigate to **SETUP >> SIGNALING & MEDIA >> CODERS & PROFILES >> IP Profiles** and click **New** to create an IP profile for the Teams connection. Enter the following:

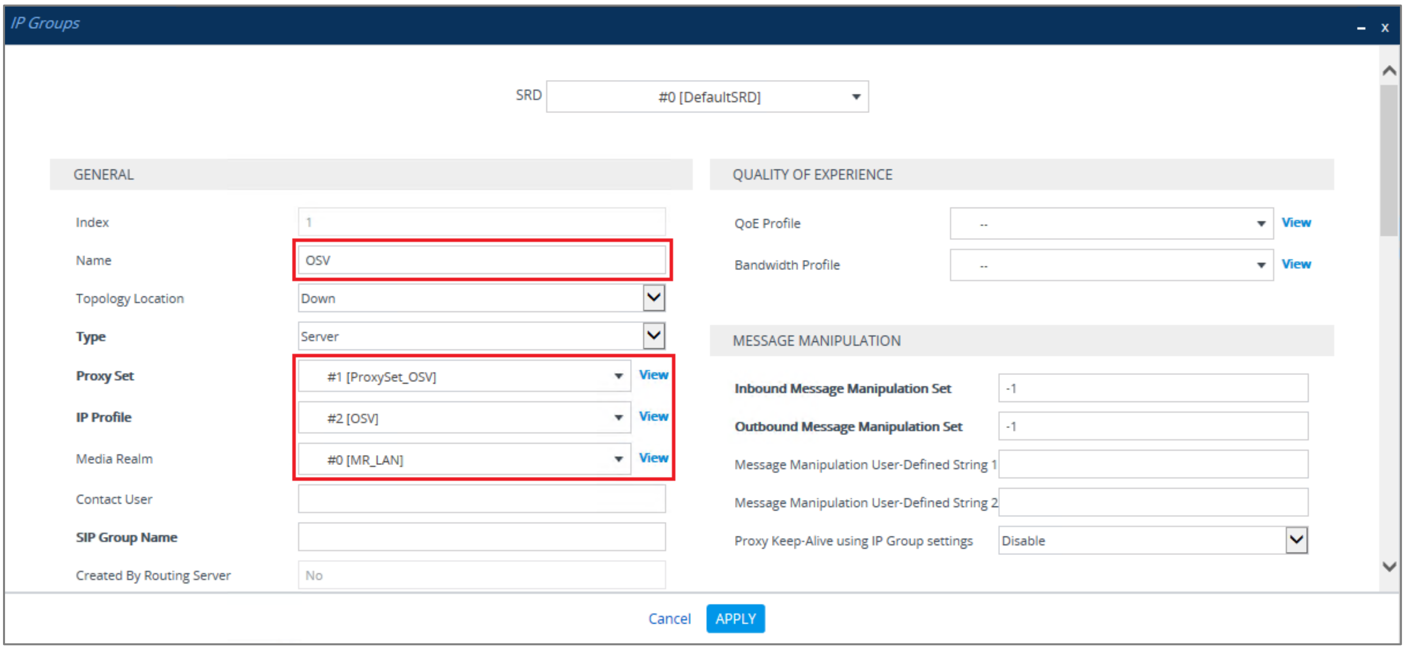
- **Name**: MS Teams (friendly name for Teams)
- **SBC Media Security Mode**: Secured (see restrictions in 2.2)
- **Remote Early Media RTP Detection Mode**: By Media (required, as Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18x response)
- **Extension Coders Group:** AudioCodersGroups_0 (see 4.2.6)
- **Use Silence Suppression:** Add
- **RTCP Mode**: Generate Always (in case RTCP packets aren't generated, but Teams expects them)
- **ICE Mode:** Lite (required only when Media Bypass enabled on Teams).
- **Remote Update Support:** Not Supported
- **Remote re-INVITE Support:** Supported Only With SDP
- **Remote Delayed Offer Support:** Not Supported
- **Remote REFER Mode:** Handle Locally

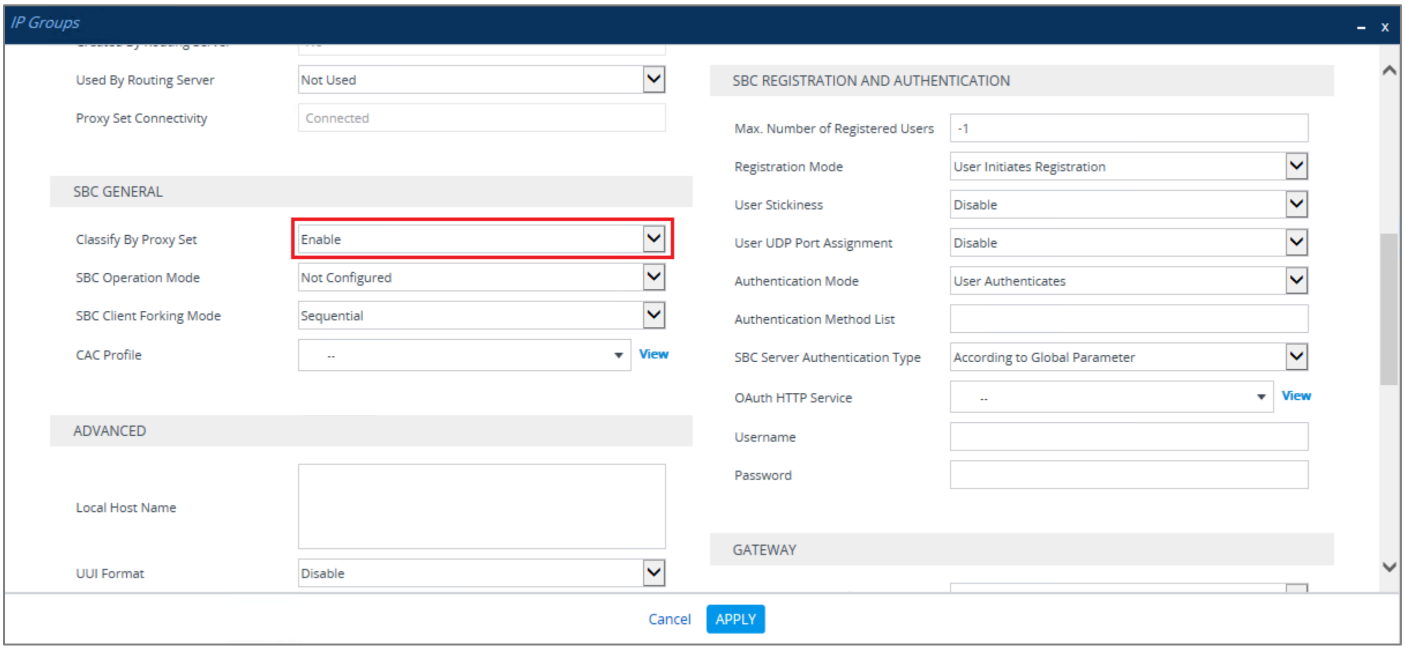
- **Remote 3xx Mode**: Handle Locally
- **Remote Hold Format:** Inactive (some SIP trunks with IP-PBXs may answer with a=inactive and IP=0.0.0.0 in response to the Re-Invite with Hold request from Teams. Microsoft Media Stack doesn't support this format. So, SBC will replace 0.0.0.0 with its IP address)

Click **Apply**.

4.2.8. IP Groups

The **IP Group** is an IP entity such as a server (e.g., IP-PBX or SIP Trunk) or a group of users (e.g., LAN IP phones). For servers (current certification), 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.

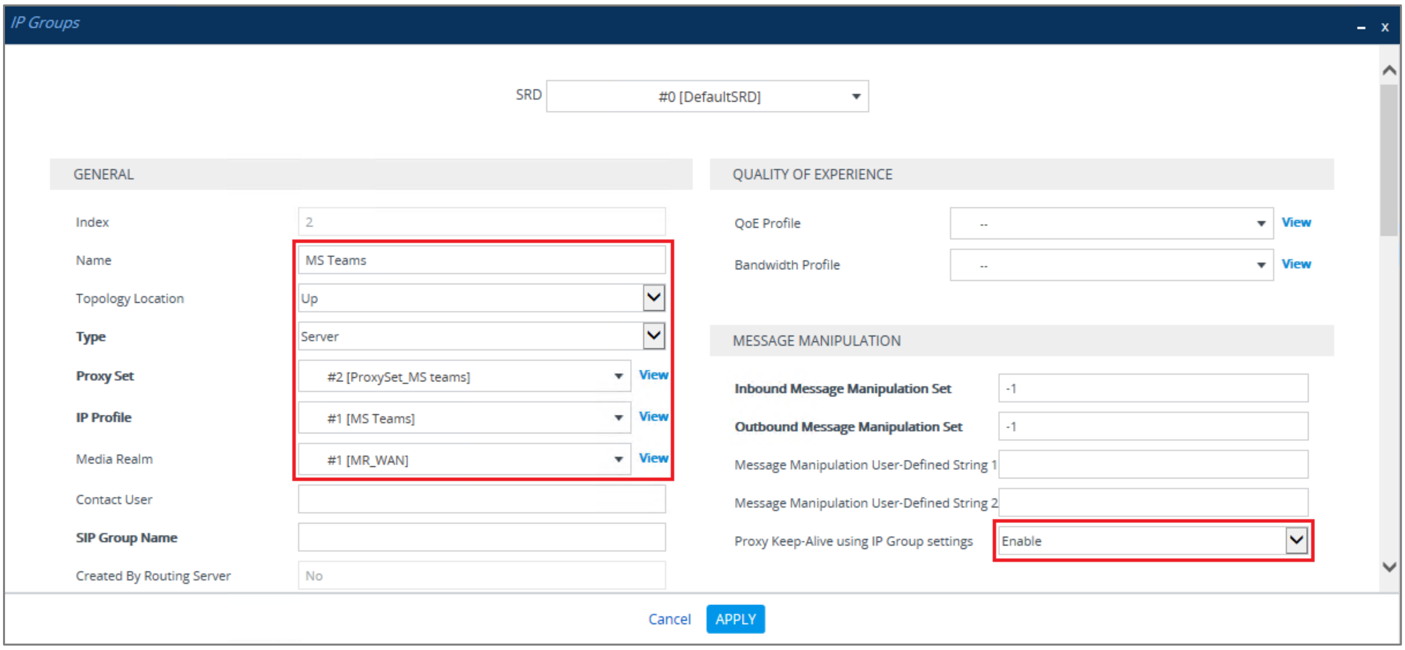


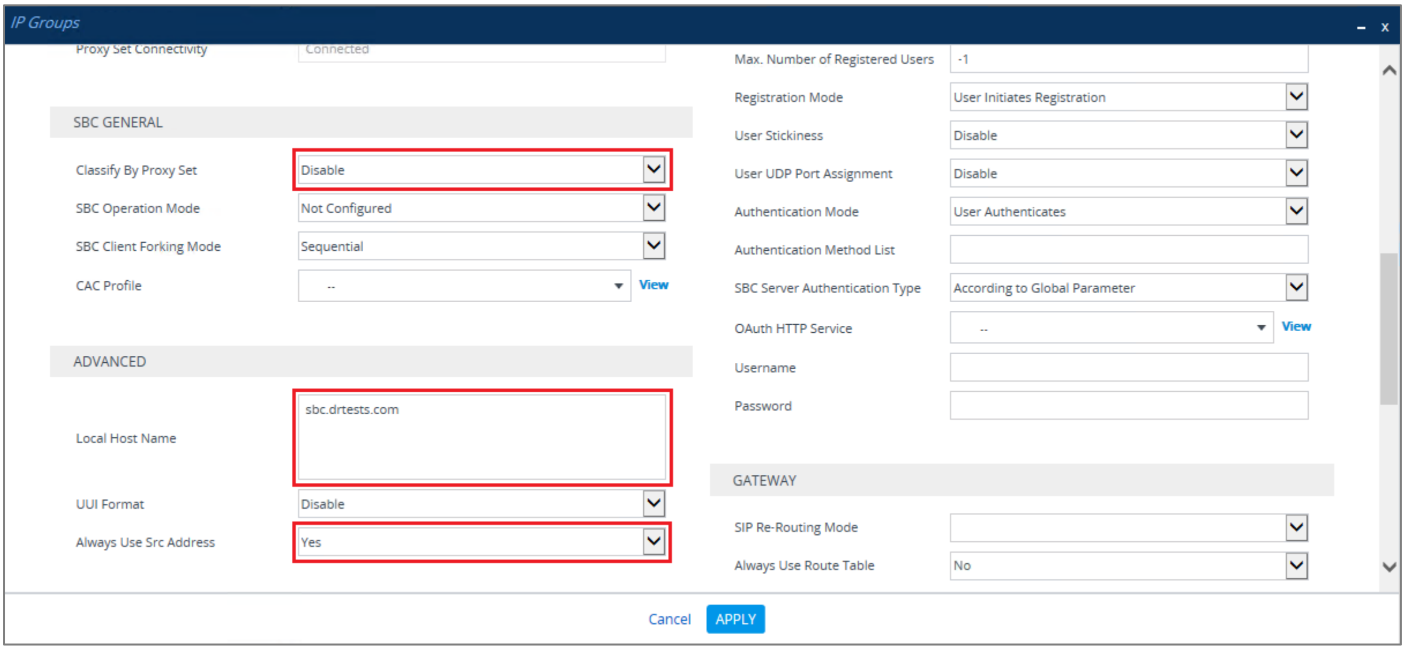


At **SETUP >> SIGNALING & MEDIA >> CORE ENTITIES >> IP Groups** click **New**. Configure an IP Group for OS Voice, by entering the following:

- **Name**: OSV (friendly name for OS Voice)
- **Proxy Set**: ProxySet_OSV (see 4.2.5)
- **IP Profile**: OSV (see 4.2.7)
- **Media Realm:** MR_LAN (see 4.2.3)
- **Classify By Proxy Set**: Enable

Click **Apply**.





At **SETUP >> SIGNALING & MEDIA >> CORE ENTITIES >> IP Groups** click **New**. Configure an IP Group for OS Voice, by entering the following:

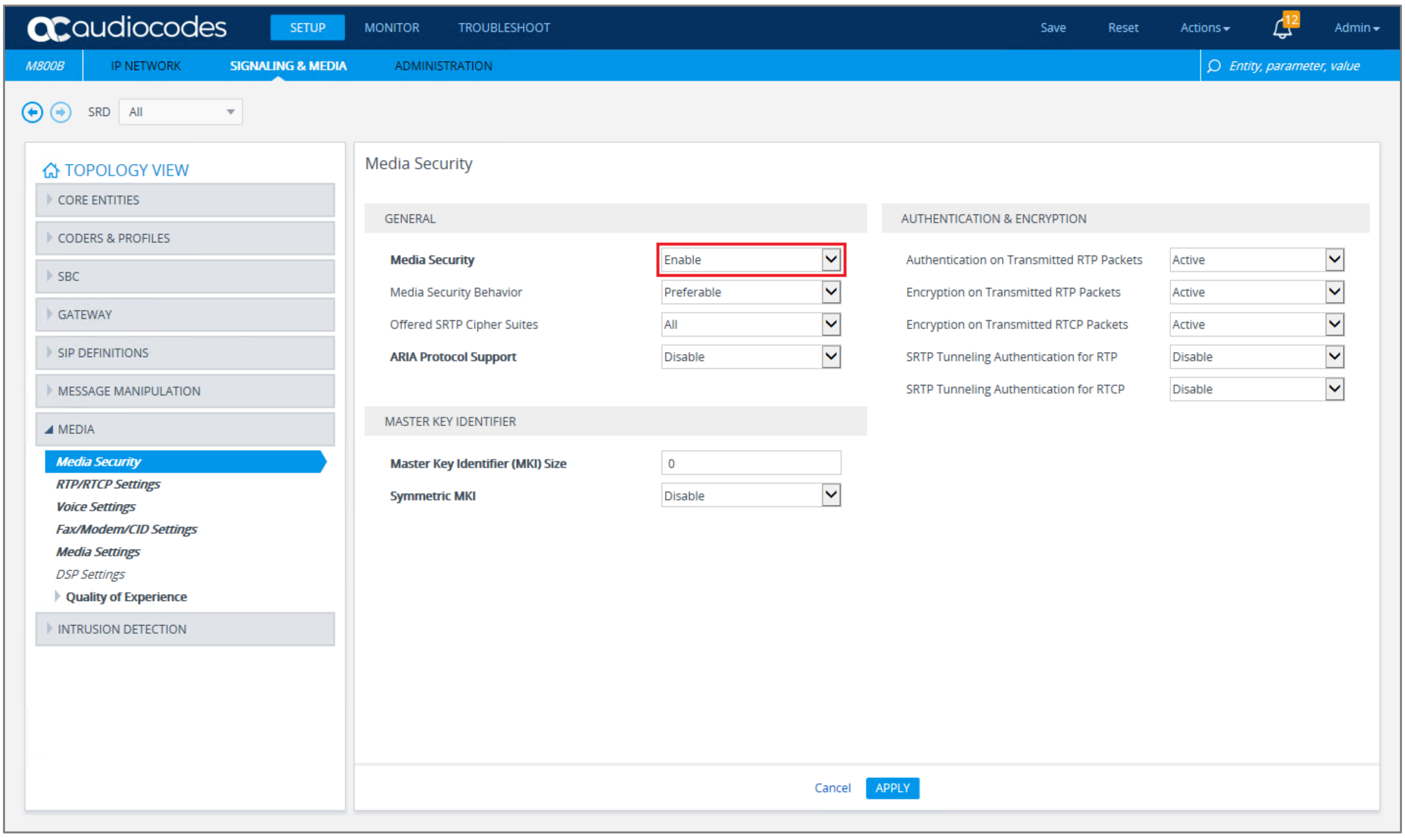
- **Name**: MS Teams (friendly name for Teams)
- **Topology Location:** Up
- **Type:** Server
- **Proxy Set**: ProxySet_MS Teams (see 4.2.5)
- **IP Profile**: MS Teams (see 4.2.7)
- **Media Realm:** MR_WAN (see 4.2.3)
- **Classify By Proxy Set**: Disable
- **Local Host Name**: sbc.drtests.com (public FQDN for SBC in Teams tenant, see 4.1)
- **Always Use Src Address**: Yes
- **Proxy Keep-Alive using IP Group settings:** Enable

Click **Apply**.

Note: The name sbc.drtests.com defines the host name (string) that the device uses in the SIP message's Via and Contact headers. This is typically used to define an FQDN as the host name. The device uses this string for Via and Contact headers in outgoing INVITE messages sent to a specific IP Group, and the Contact header in SIP 18x and 200 OK responses for incoming INVITE messages received from a specific IP Group.

4.2.9. Media Security

The link between Teams and SBC requires to use SRTP only, so the SBC must be configured for this.

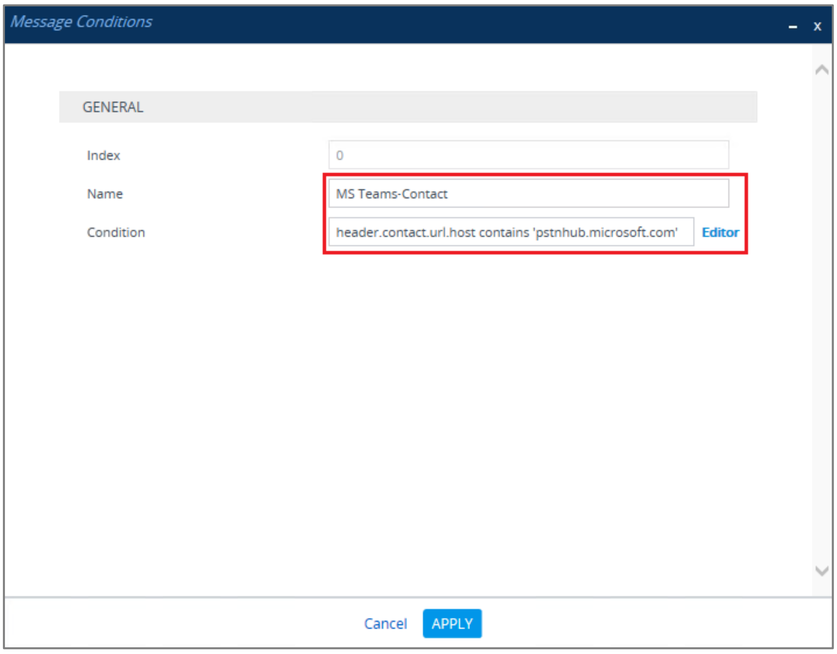


Navigate to **SETUP >> SIGNALING & MEDIA >> MEDIA >> Media Security** and set **Media Security** to Enable to enable SRTP and then click **Apply**.

4.2.10. Message Condition Rules

A Message Condition Rule defines special conditions (requisites) for incoming SIP messages. These rules can be used as additional matching criteria for the IP-to-IP routing rules in the IP-to-IP Routing table.

The following condition verifies that the Contact header contains Teams FQDN.



Navigate to **SETUP >> SIGNALING & MEDIA >> MESSAGE MANIPULATION >> Message Condition,** click **New** and configure:

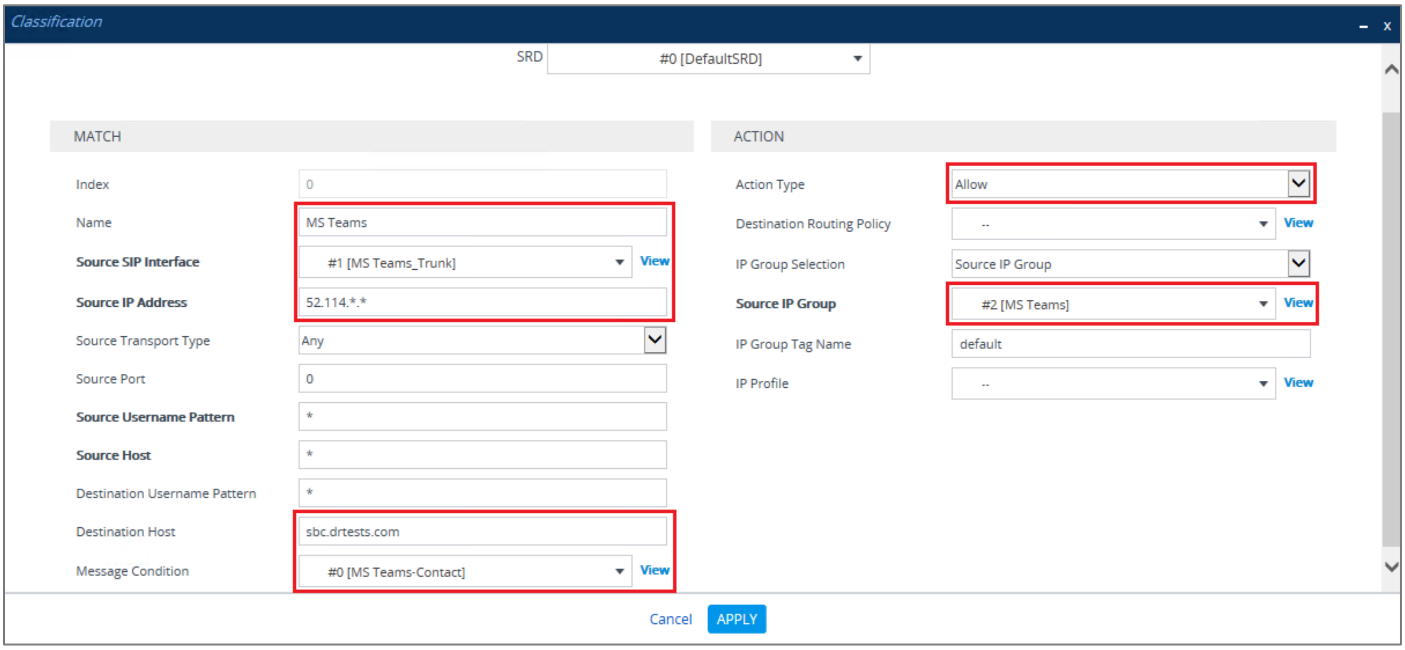
- **Name**: MS Teams-Contact (condition friendly name)
- **Condition:** header.contact.url.host contains 'pstnhub.microsoft.com'

Click **Apply**.

4.2.11. Classification Rules

A **Classification Rule** classifies incoming SIP dialog-initiating requests (e.g., INVITE messages) to a "source" IP Group. The source IP Group is the SIP entity that sends the SIP dialog request. Once classified, the device uses the IP Group to process the call (manipulation and routing).

Classification table may also be used for employing SIP-level access control for successfully classified calls, by configuring classification rules with whitelist and blacklist settings. If a classification rule is configured as a whitelist ("Allow"), the device accepts the SIP dialog and processes the call. On the contrary, if the classification rule is configured as a blacklist ("Deny"), the device rejects the incoming SIP dialog.



Navigate to **SETUP >> SIGNALING & MEDIA >> SBC >> Classification,** click **New** and enter the following:

- **Name**: MS Teams (rule friendly name)
- **Source SIP Interface:** MS Teams_Trunk (see 4.2.4)
- **Source IP Address:** 52.114.*.* (Teams public proxies FQDNs resolve to 52.114.*.* IPs; see 4.2.5 & 4.2.13)
- **Destination Host:** sbc.drtests.com (public FQDN for SBC in Teams tenant, see 4.1)
- **Message Condition:** MS Teams-Contact (see 4.2.10)
- **Action Type:** Allow
- **Source IP Group:** MS Teams (see 4.2.8)

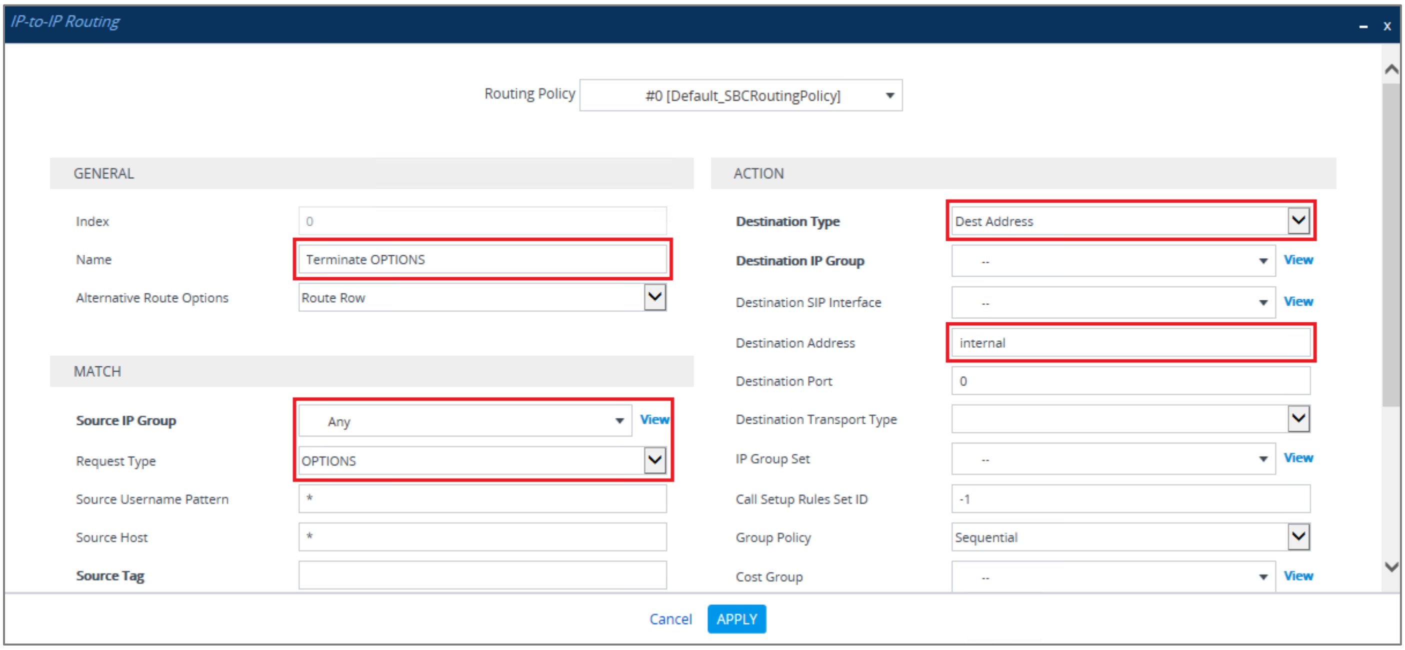
Click **Apply**.

4.2.12. 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 following IP-to-IP Routing Rules will be defined:

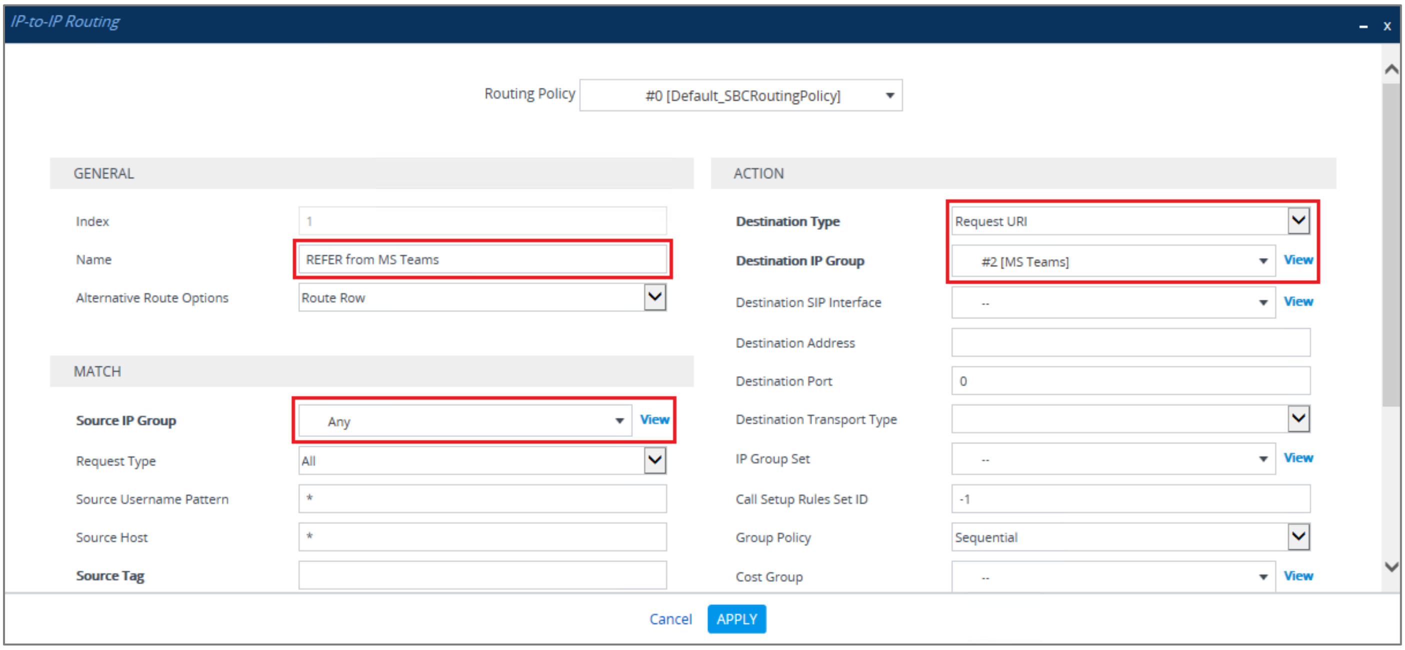
- Terminate SIP OPTIONS messages on the SBC.
- Terminate REFER messages to Teams.
- Calls from Teams to OS Voice.
- Calls from OS Voice to Teams.

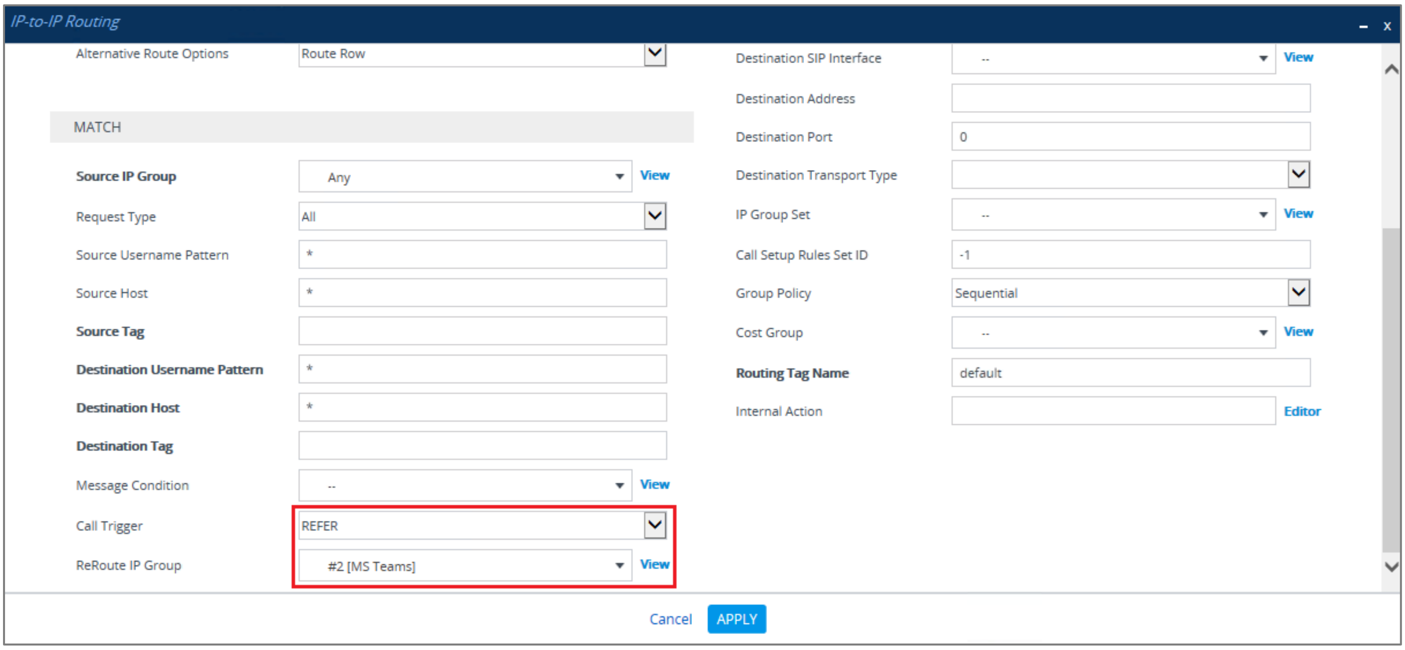


Open IP-to-IP routing table at **SETUP >> SIGNALING & MEDIA >> SBC >> Routing >> IP-to-IP Routing,** click **New** and enter the following:

- **Name**: Terminate OPTIONS (friendly name)
- **Source IP Group:** Any
- **Request Type:** OPTIONS
- **Destination Type:** Dest Address
- **Destination Address:** internal

Click **Apply**.

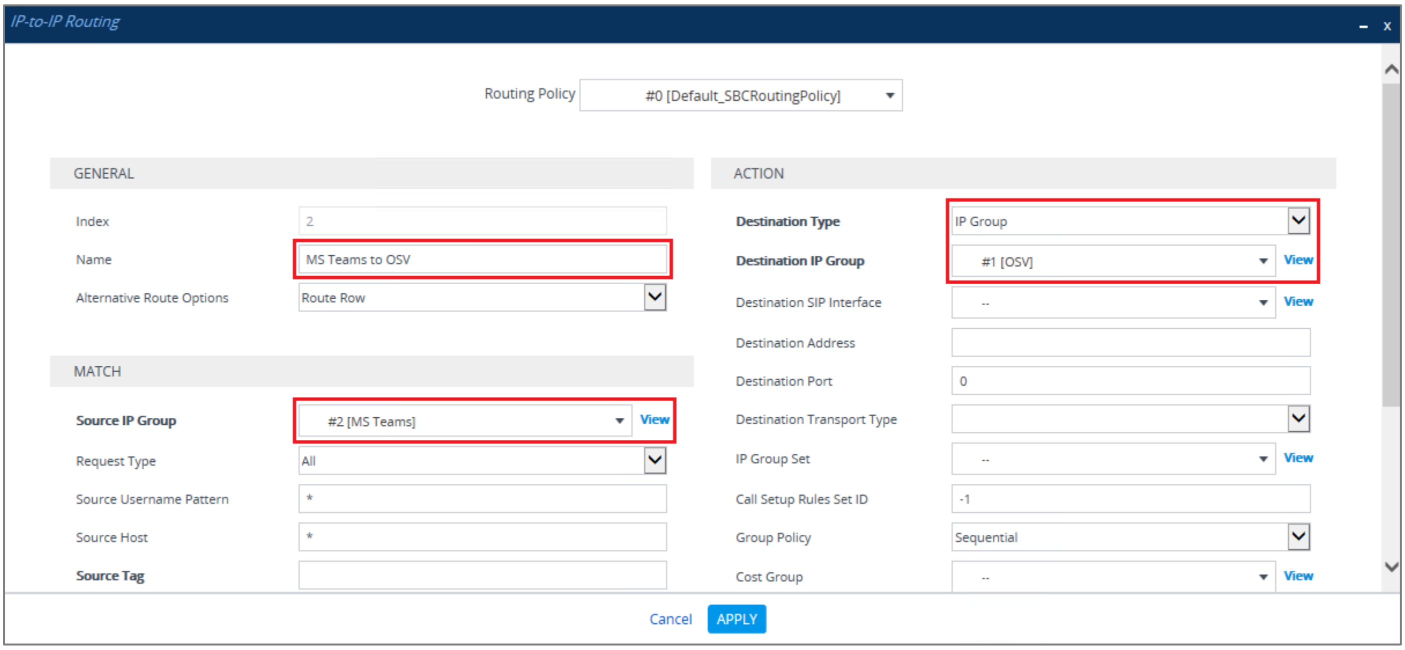




Open the IP-to-IP routing table at **SETUP >> SIGNALING & MEDIA >> SBC >> Routing >> IP-to-IP Routing,** click **New** and enter the following:

- **Name**: REFER from MS Teams (friendly name)
- **Source IP Group:** Any
- **Destination Type:** Request URI
- **Destination IP Group:** MS Teams (see 4.2.8)
- **Call Trigger:** REFER
- **ReRoute IP Group:** MS Teams (see 4.2.8)

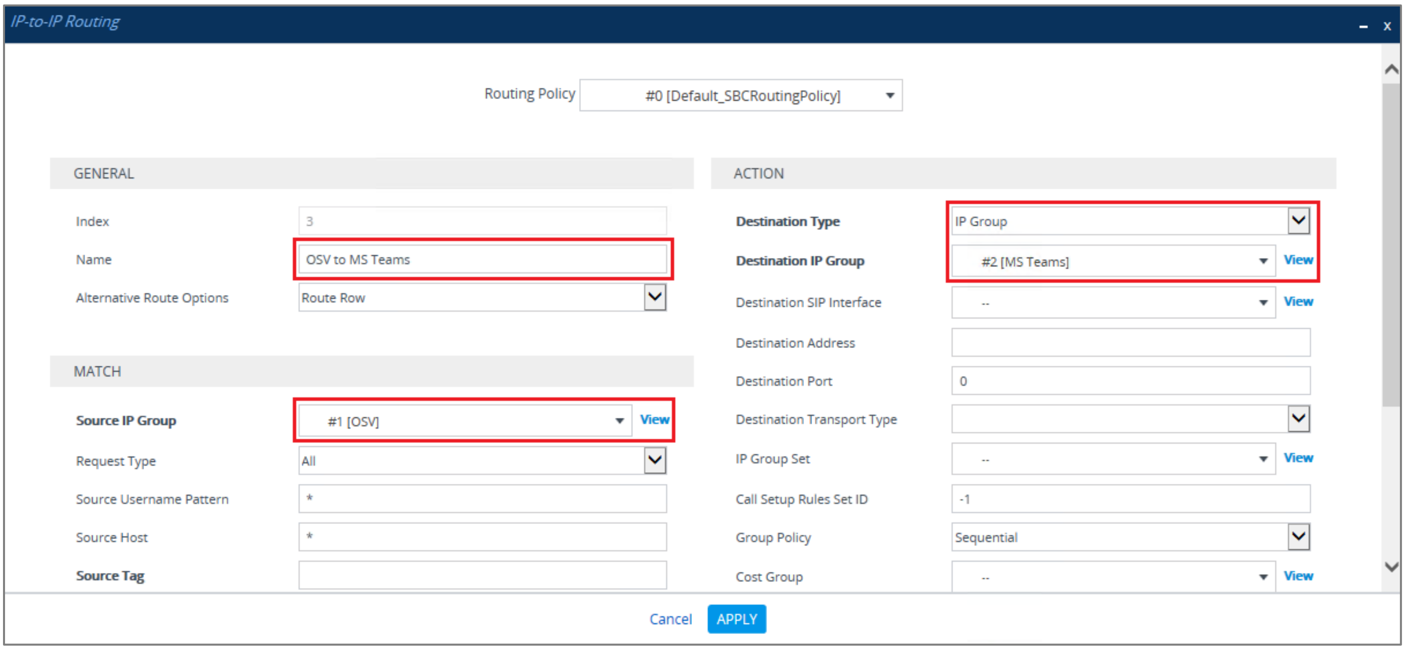
Click **Apply**.



Open the IP-to-IP routing table at **SETUP >> SIGNALING & MEDIA >> SBC >> Routing >> IP-to-IP Routing,** click **New** and enter the following

- **Name**: MS Teams to OSV (friendly name)
- **Source IP Group:** MS Teams (see 4.2.8)
- **Destination Type:** IP Group
- **Destination IP Group:** OSV (see 4.2.8)

Click **Apply**.



Open the IP-to-IP routing table at **SETUP >> SIGNALING & MEDIA >> SBC >> Routing >> IP-to-IP Routing,** click **New** and enter the following:

- **Name**: OSV to MS Teams (friendly name)
- **Source IP Group:** OSV (see 4.2.8)

- **Destination Type:** IP Group
- **Destination IP Group:** MS Teams (see 4.2.8)

Click **Apply**.

4.2.13. Firewall Settings

A set of Firewall rules need to be defined, so that Teams SIP Proxy can communicate with the SBC. As already mentioned in sub-section 4.2.5, Teams uses 3 SIP proxies:

- **sip.pstnhub.microsoft.com** (global FQDN),
- **sip2.pstnhub.microsoft.com** (failover FQDN),
- **sip3.pstnhub.microsoft.com** (failover FQDN).

These DNS records resolve to the IP addresses below:

- **52.114.148.0**
- **52.114.132.46**
- **52.114.75.24**
- **52.114.76.76**
- **52.114.7.24**
- **52.114.14.70**

Refer to: https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sip-signaling-fqdns-and-firewall-ports.

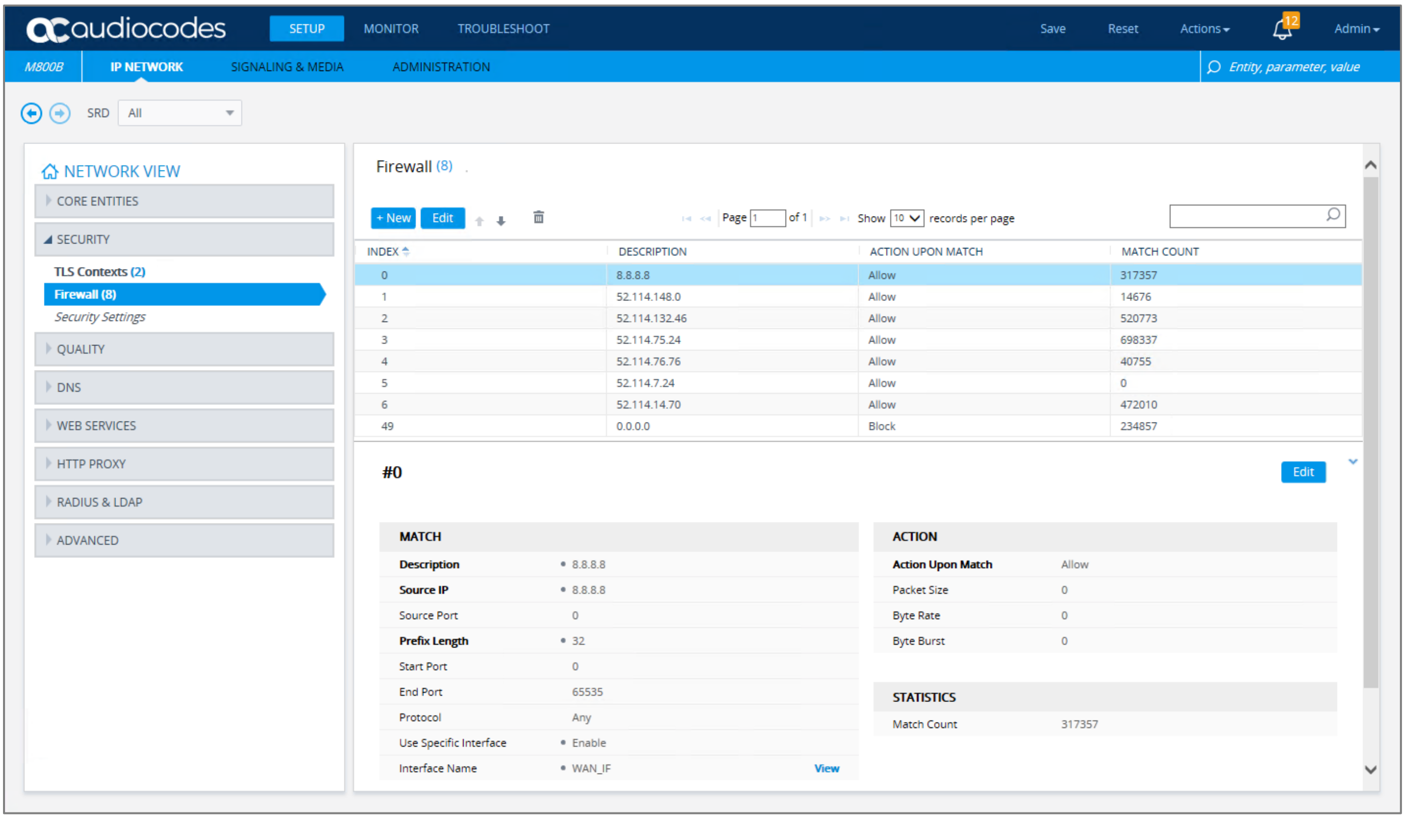
As an extra security to the above note, traffic filtering rules (access list) for incoming traffic are configured on SBC. For each packet received on the configured network interface, the SBC searches the table from top to bottom until the first matching rule is found. The matched rule can permit (allow) or deny (block) the packet. Once a rule in the table is located, subsequent rules further down the table are ignored. If the end of the table is reached without a match, the packet is accepted. Please note that the firewall is stateless. The blocking rules will apply to all incoming packets, including UDP or TCP responses.

Navigate to: **SETUP >> IP NETWORK >> SECURITY >> Firewall,** click **New** and configure the SBC firewall rules according to the table below:

Index	Source IP	Subnet Prefix	Start Port	End Port	Protocol	Use Specific Interface	Interface ID	Allow Type
0	<Public DNS Server IP> (e.g. 8.8.8.8)	32	0	65535	Any	Enable	WAN_IF	Allow
1	52.114.148.0	32	0	65535	TCP	Enable	WAN_IF	Allow
2	52.114.132.46	32	0	65535	TCP	Enable	WAN_IF	Allow
3	52.114.75.24	32	0	65535	TCP	Enable	WAN_IF	Allow
4	52.114.76.76	32	0	65535	TCP	Enable	WAN_IF	Allow
5	52.114.7.24	32	0	65535	TCP	Enable	WAN_IF	Allow

6	52.114.14.70	32	0	65535	TCP	Enable	WAN_IF	Allow
49	0.0.0.0	0	0	65535	Any	Enable	WAN_IF	Block

The firewall rules on SBC look like the figure below:

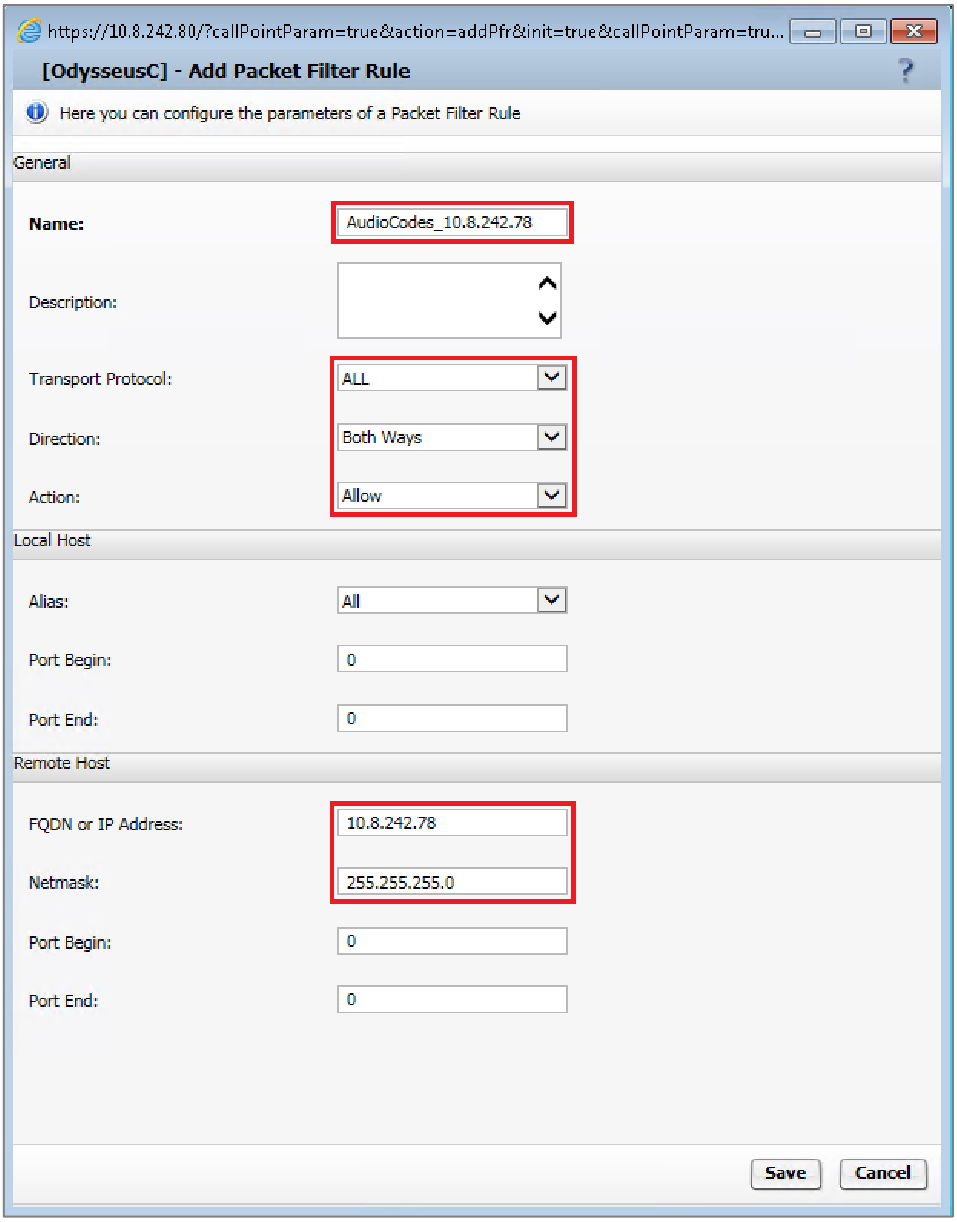


4.3. OpenScape Voice Configuration

This section refers to OS Voice related configuration for the needs of the current certification project. No reference will be made to routine OS Voice (and other Unify components) configuration due to being out of scope.

4.3.1. OS Voice Firewall

For the SBC to communicate with OS Voice via SIP, a firewall rule (packet filter rule) is added to OS Voice.



Navigate to **CMP >> Configuration >> OpenScape Voice >> Administration >> General Settings >> Packet Filter Rules.**

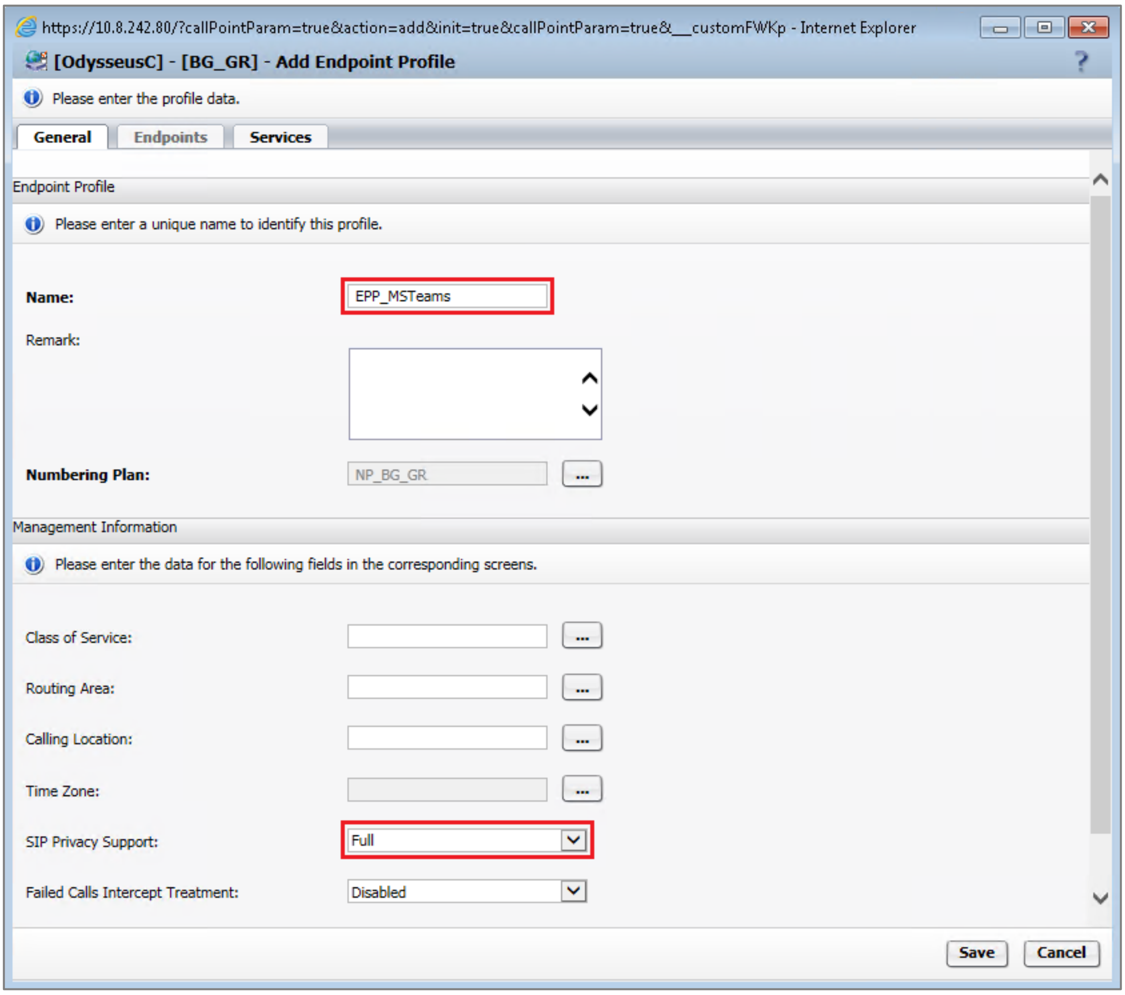
Click **Add** and configure the following to allow incoming/outgoing traffic:

- **Name:** AudioCodes_10.8.242.64 (a common-sense name)
- **Transport Protocol:** ALL (depending on customer requirements, we could configure e.g. UDP only)
- **Direction:** Both Ways
- **Action:** Allow
- **FQDN or IP Address:** 10.8.242.78 (SBC LAN interface)
- **Netmask:** 255.255.255.0

Click on **Save**.

4.3.2. Endpoint

An **Endpoint** is a network component, such as an originating or terminating device and in our case the AudioCodes SBC. An endpoint can be a DN (Directory Number) that does not have a number associated with it yet. An **Endpoint Profile** enables the administrator to set parameters for that endpoint.

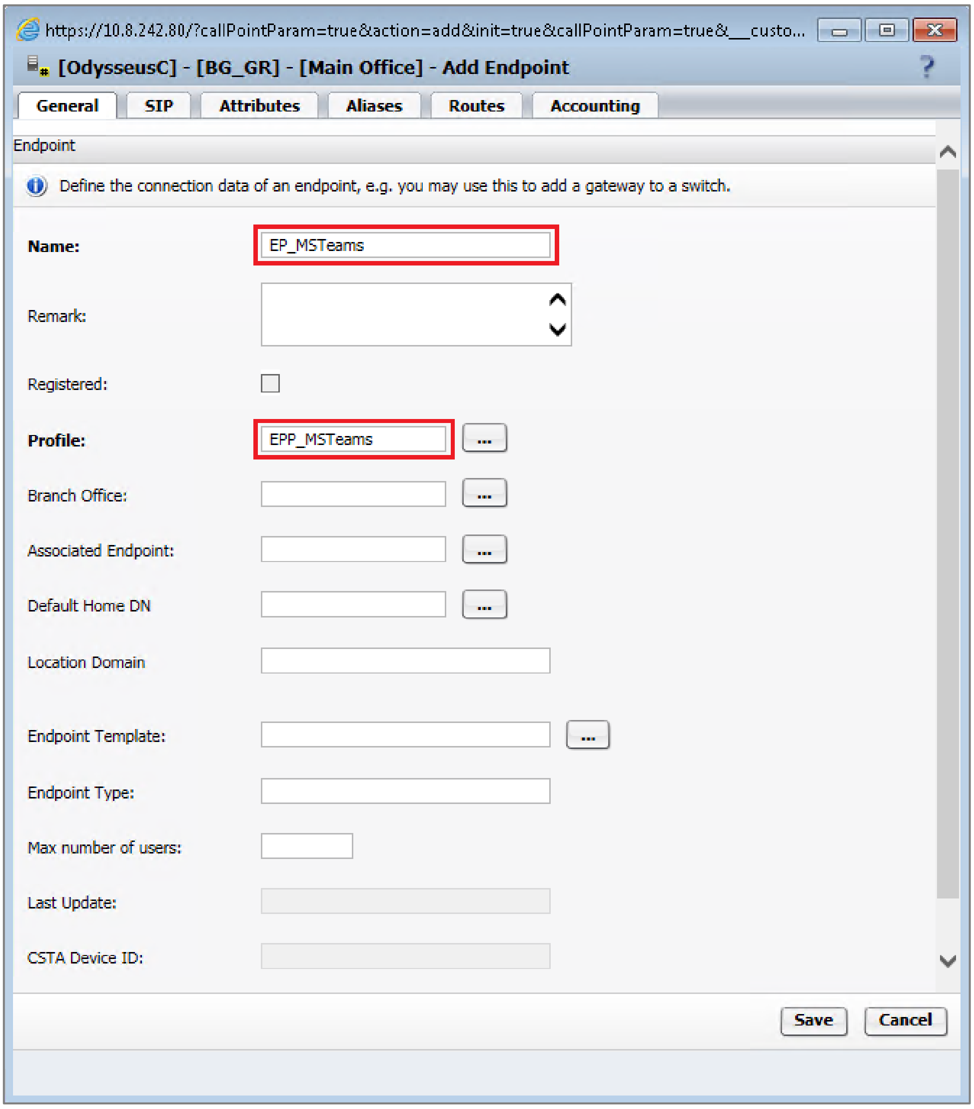


Navigate to **CMP >> Configuration >> OpenScape Voice >> Business Group >> Profiles >> Endpoint** to configure the **Endpoint Profile**.

Click **Add** and on the **General** tab, enter the following:

- **Name**: EPP_MSTeams (a common-sense name)
- **SIP Privacy Support**: Full (to enable RFC 3325 behavior - OS Voice sends a P-Asserted-Identity (or a to P-Preferred-Identity) header field in the messages (requests and responses) to the endpoint; the OS Voice SHALL also accept any received P- Asserted-Identity header fields).

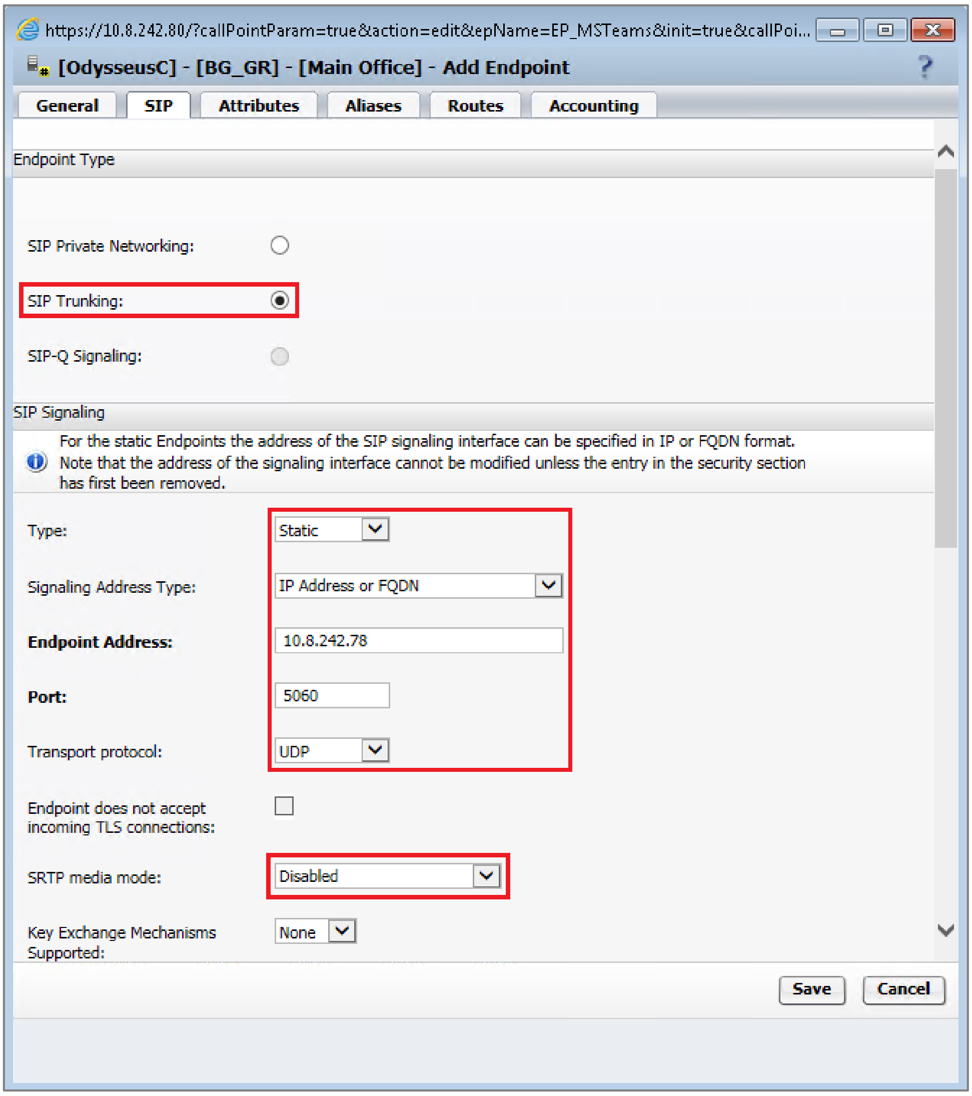
Click **Save**.



Navigate to **CMP >> Configuration >> OpenScape Voice >> Business Group >> Members >> Endpoints** to configure the **Endpoint**.

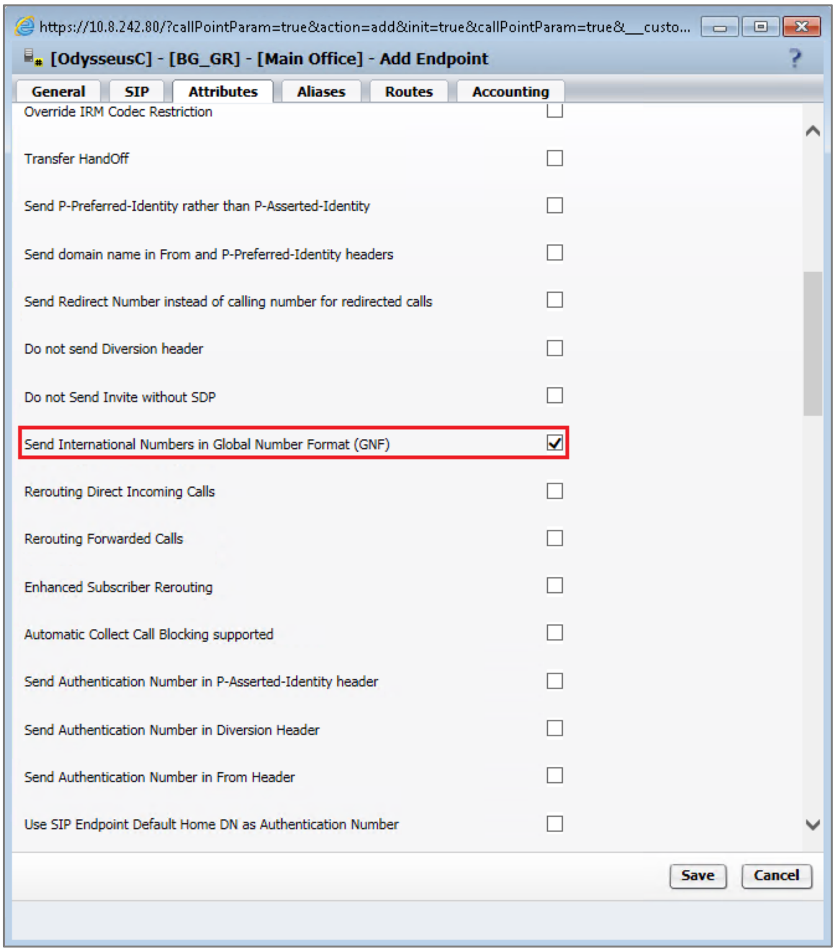
Click **Add** and on the **General** tab, enter the following:

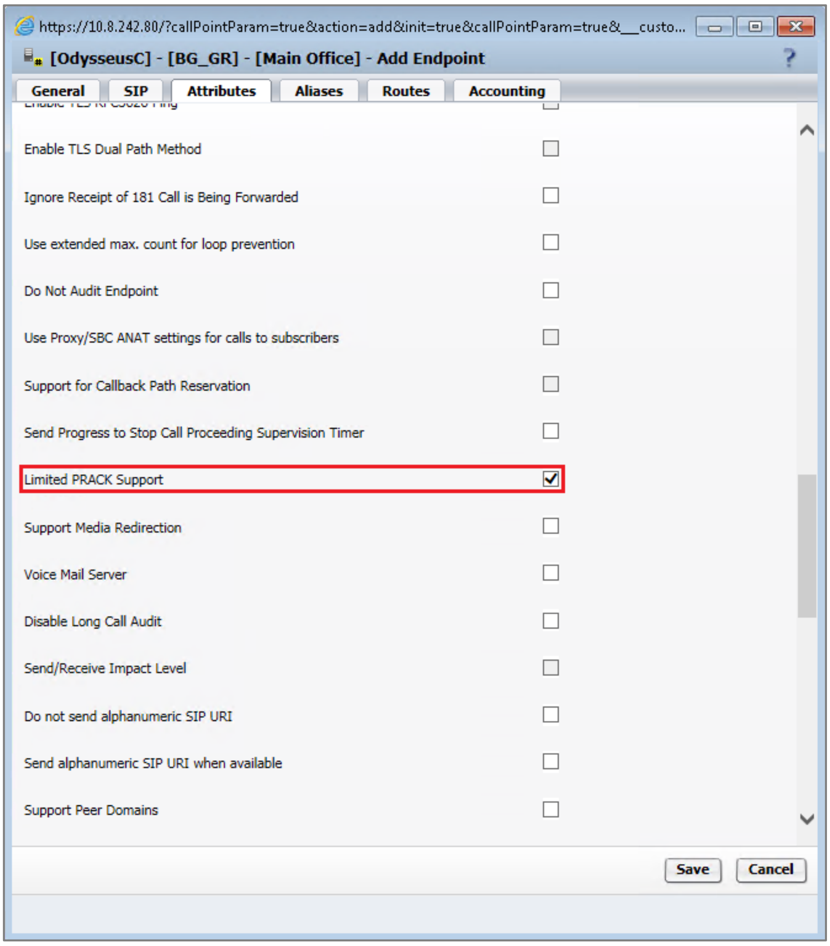
- **Name**: EP_MSTeams (a common-sense name)
- **Profile**: EPP_MSTeams (select previously created endpoint profile)



Click the **SIP** tab and enter the following:

- **SIP Trunking**: Enabled
- **Type**: Static
- **Signaling Address Type:** IP Address or FQDN
- **Endpoint Address:** 10.8.242.78 (SBC LAN interface)
- **Port:** 5060 (default setting, as configured in SBC – see 4.2.4)
- **Transport protocol:** UDP (as configured in SBC – see 4.2.4)
- **SRTP media mode:** Disabled

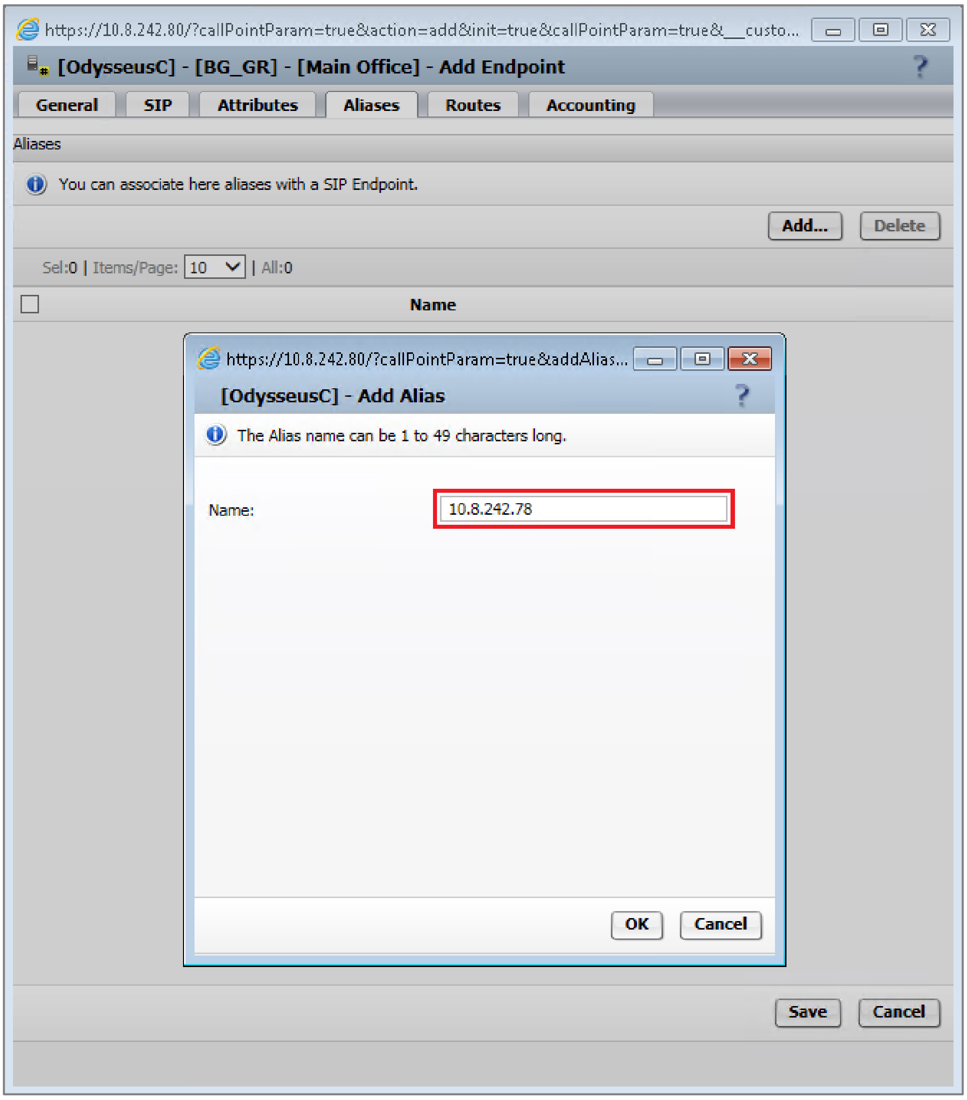

https://10.8.242.80/?callPointParam=true&action=add&init=true&callPointParam=true&__custo...
[OdysseusC] - [BG_GR] - [Main Office] - Add Endpoint
General
SIP
Attributes
Aliases
Routes
Accounting
Override IRM Codec Restriction
Transfer HandOff
Send P-Preferred-Identity rather than P-Asserted-Identity
Send domain name in From and P-Preferred-Identity headers
Send Redirect Number instead of calling number for redirected calls
Do not send Diversion header
Do not Send Invite without SDP
Send International Numbers in Global Number Format (GNF)
Rerouting Direct Incoming Calls
Rerouting Forwarded Calls
Enhanced Subscriber Rerouting
Automatic Collect Call Blocking supported
Send Authentication Number in P-Asserted-Identity header
Send Authentication Number in Diversion Header
Send Authentication Number in From Header
Use SIP Endpoint Default Home DN as Authentication Number
Save
Cancel



Select the **Attributes** tab and configure the following:

- **Send International Numbers in GNF**: Enabled (when selected, the OS Voice adds a '+' in front of all numbers which have NPI = PUBLIC and NOA = INTERNATIONAL. To do this, both Translation and the Display Number Modification tables must be provisioned to s send numbers with NPI = PUBLIC and NOA = INTERNATIONAL to this endpoint).

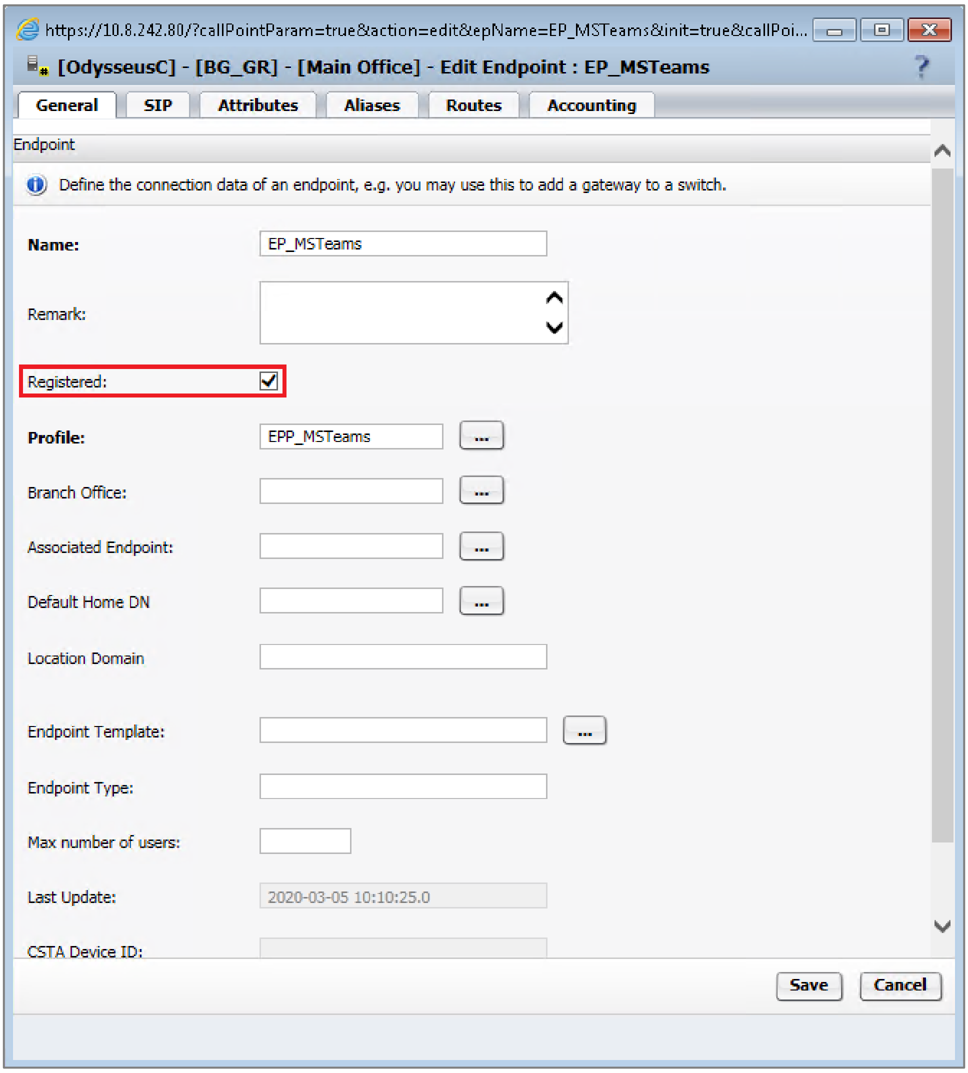
- **Limited PRACK Support**: Static (the PRACK-Lite feature provides a limited form of RFC3262 PRACK within OS Voice, supporting PRACK on a half-call basis and only for SIP network-network interfaces).



Click the **Aliases** tab and click **Add**. Enter the following:

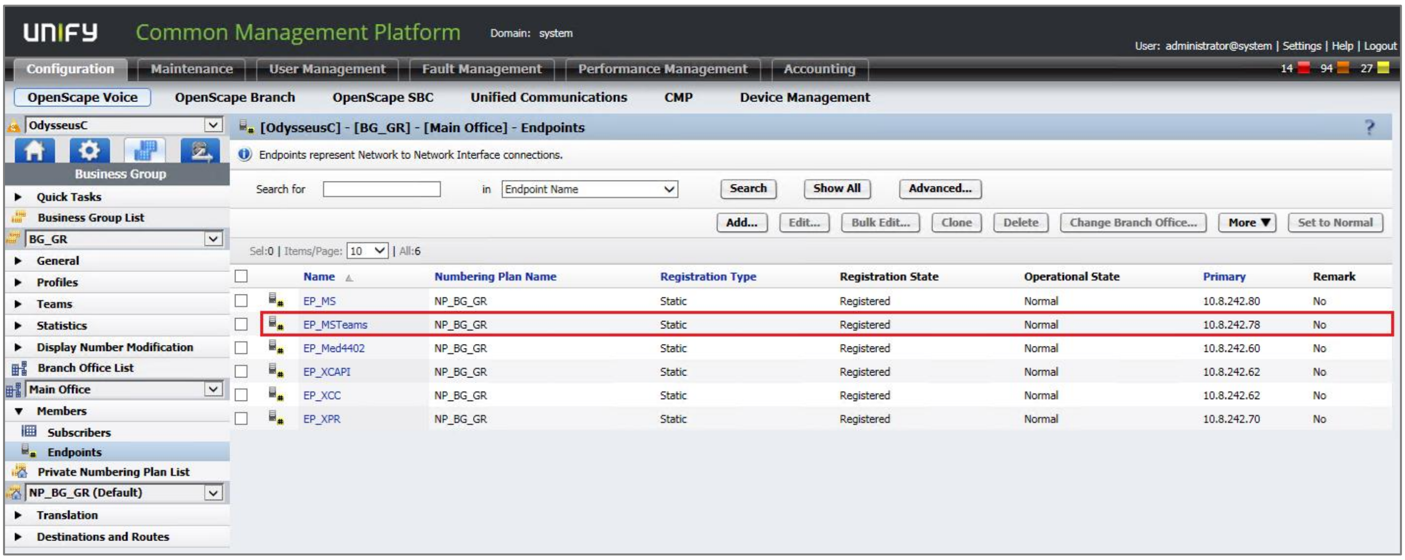
- **Name**: 10.8.242.78 (the SBC LAN interface for incoming SIP traffic; if there is a need to restrict the port 5060, the value 10.8.242.78:5060 should be entered, instead).

Click **OK** and then click **Save**.



Navigate to **CMP >> Configuration >> OpenScape Voice >> Business Group >> Members >> Endpoints**, edit the previously created EP_MSTeams endpoint and select **Registered**.

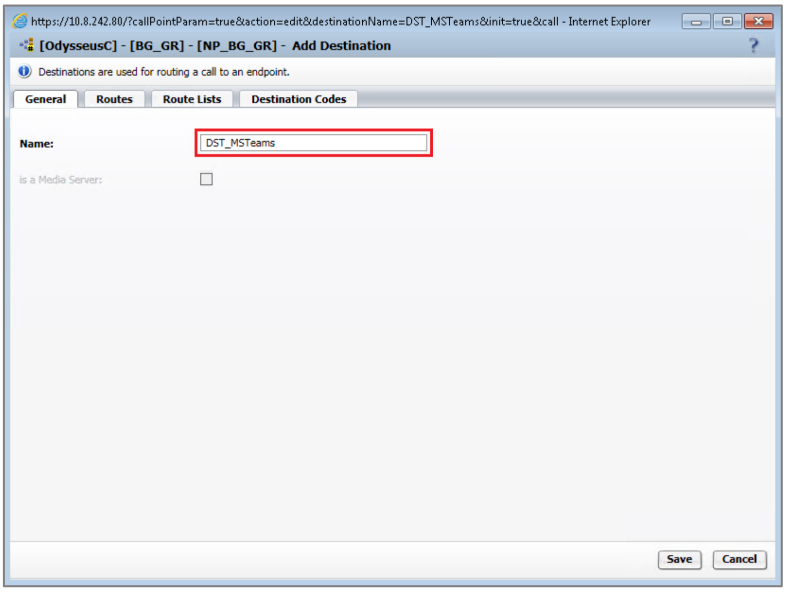
The endpoint status should look like the figure below:



4.3.3. Destinations & Routes

Destinations are logical targets for off-net or on-net routing. When a destination is created, the name of the destination is bound to the numbering plan where the destination is created. Destinations are used to route a call to an endpoint representing a gateway.

Each **Route** is a collection of groups or addresses that provide a path to a destination.

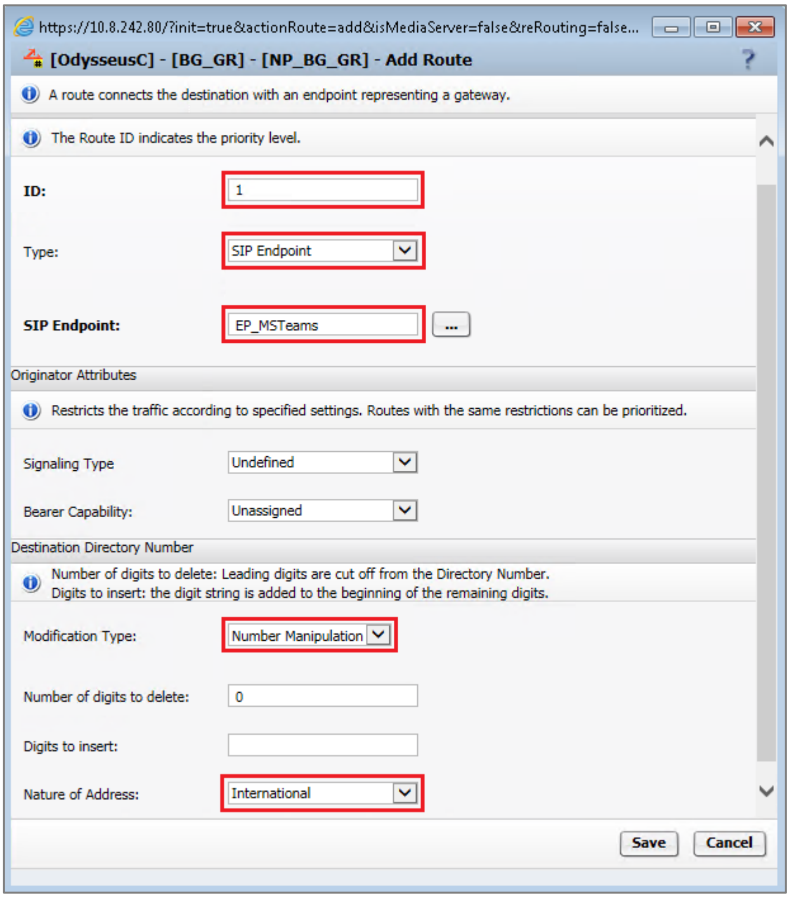


Navigate to **CMP >> Configuration >> OpenScape Voice >> Business Group >> Destinations and Routes >> Destinations**.

Click **Add** and on the **General** tab enter the following:

- **Name**: DST_MSTeams (a common-sense name).

Click **Save.**



Navigate to **CMP >> Configuration >> OpenScape Voice >> Business Group >> Destinations and Routes >> Destinations,** select and **Edit** the DST_MSTeams destination.

Configure the associated Route, by clicking on the **Routes tab** and entering the following:

- **ID**: 1. (the priority of the route; if there are multiple routes to a destination, the route with the lowest numbered route ID has the highest priority and will be selected first; we currently have one route with the SBC).
- **SIP Endpoint**: EP_MSTeams (see 4.3.2).
- **Modification Type:** Number Manipulation.
- **Nature of Address:** International.

Click **Save**.

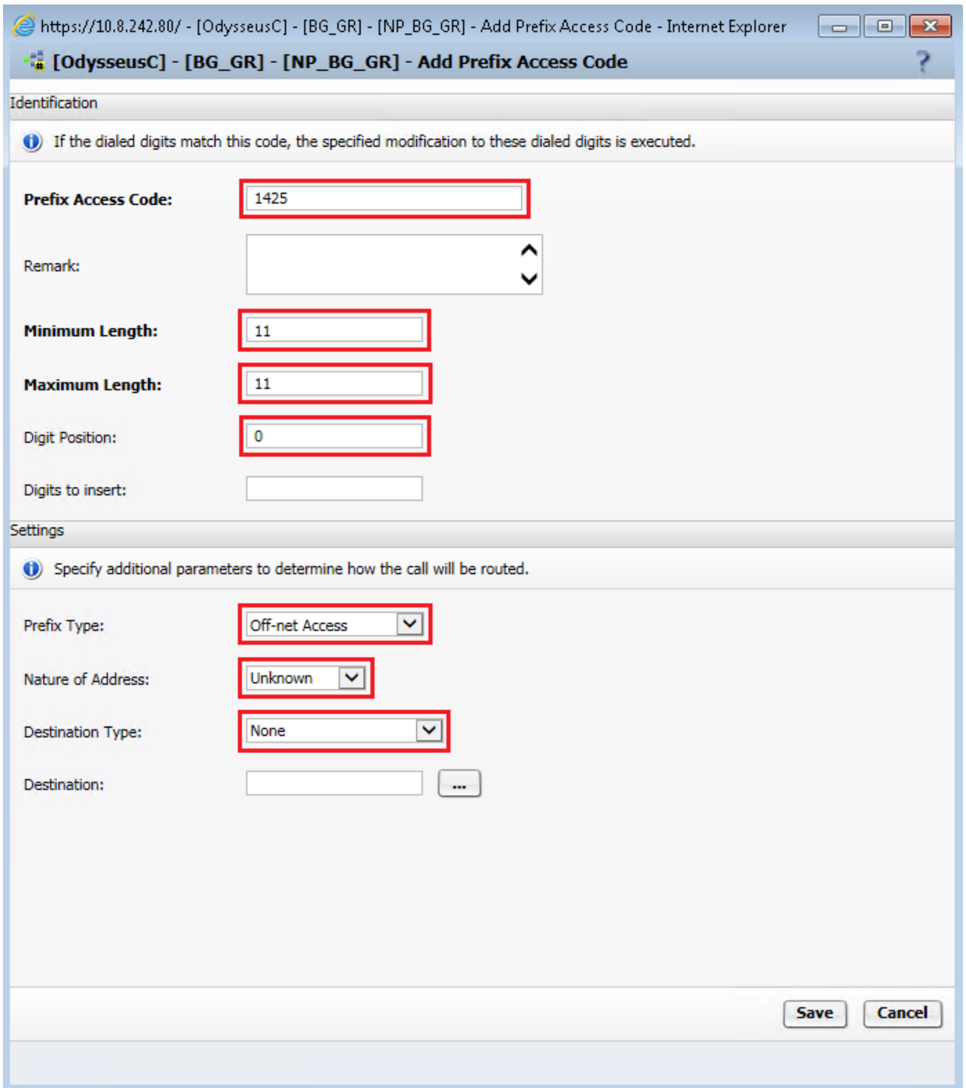
Note: To populate the **SIP Endpoint** box with EP_MSTeams endpoint, click the corresponding button, then select **Main Office** on pop up window, click **Next**, select EP_MSTeams and click **OK**.

4.3.4. Translation

With **Translation,** you can configure where the outgoing calls per dialed digits from OS Voice subscribers are routed to.

A call can only be routed when the dialed digits are matching a **PAC (Prefix Access Code)**.

The **Destination Code** feature provides destination codes for basic telephone service. The destination code will be used for a call when the dialed or modified (in PAC) digits and the nature of the address are matching.

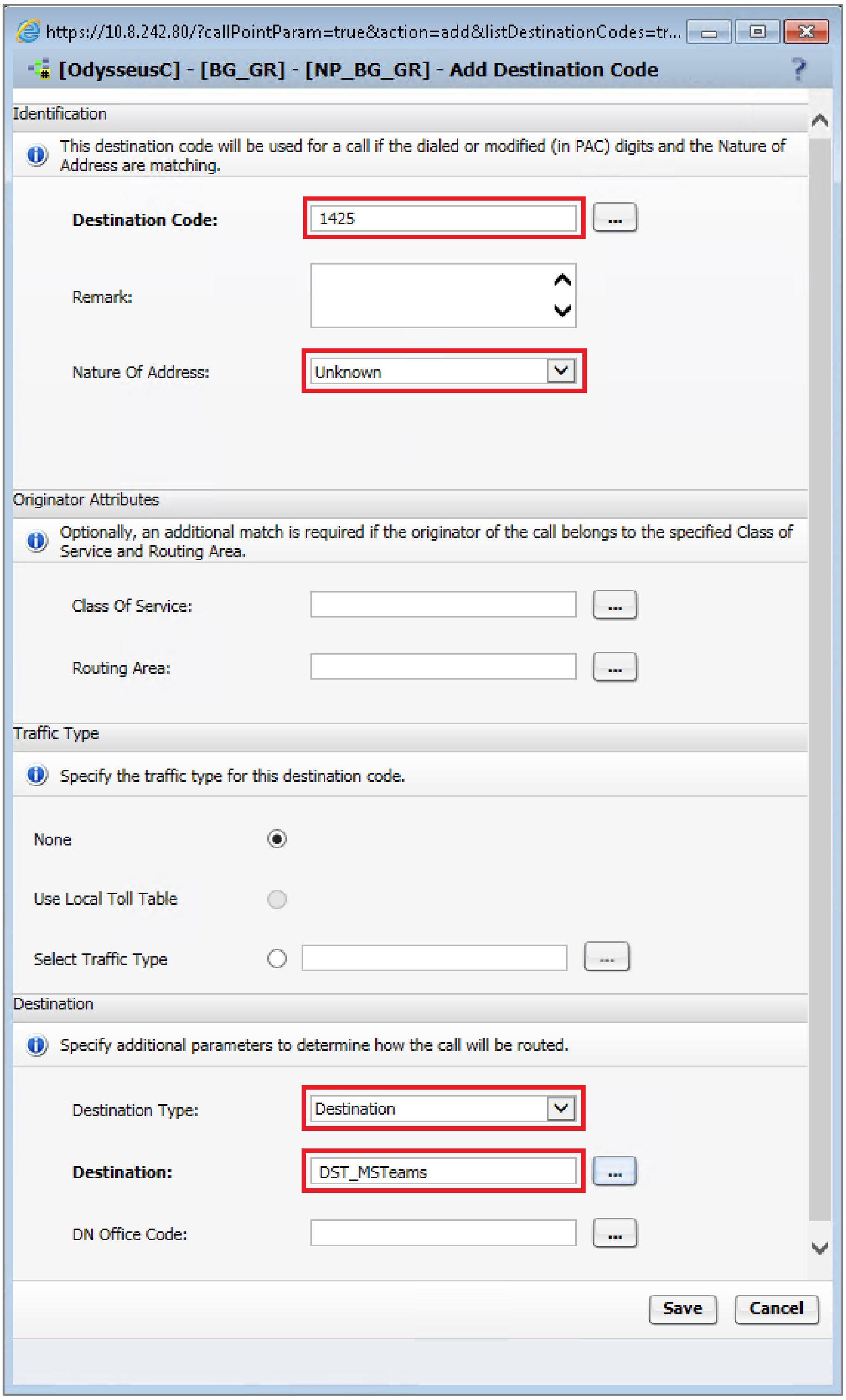


Navigate to **CMP >> Configuration >> OpenScape Voice >> Business Group >> Translation >> Prefix Access Codes.**

Click **Add** and enter the following:

• **Prefix Access Code**:	1425 (the starting digits of Teams subscriber numbers).
• **Minimum Length**:	11 (minimum expected length of Teams numbers)
• **Maximum Length:**	11 (maximum expected length of Teams numbers)
• **Digit Position:**	0 (don't remove any digits from dialed number before sending to destination)
• **Prefix Type:**	Off-net Access (a prefix access code to permit access to remote destinations)
• **Nature of Address:**	Unknown
• **Destination Type:**	None (the resulting digits will be processed in the user's numbering plan's destination codes table)

Click **Save**.



Navigate to **CMP >> Configuration >> OpenScape Voice >> Business Group >> Translation >> Destination Codes.**

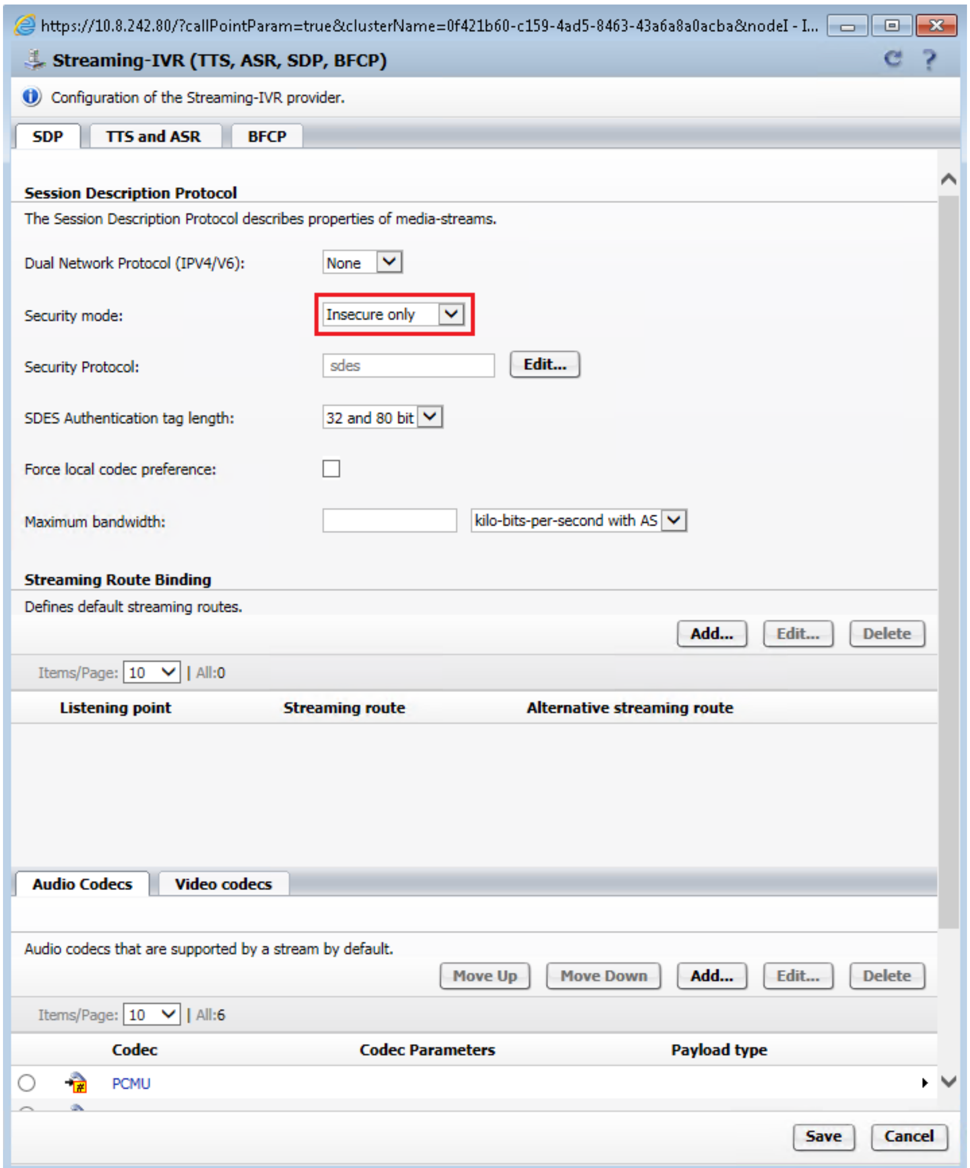
Click **Add** and enter the following:

- **Destination Code**: 1425 (select previously created PAC)
- **Nature of Address:** Unknown
- **Destination Type:** Destination
- **Destination:** DST_MSTeams (see 4.3.3)

Click **Save**.

4.3.5. Media Server Secure Media Setting

For call transfer and large conference scenarios to work, the OpenScape Media Server must not offer SDP with secure m-line.



Navigate to **CMP >> Configuration >> Unified Communications >> Configuration >> Media Server** and click on the configured Media Server, for example **Backend**.

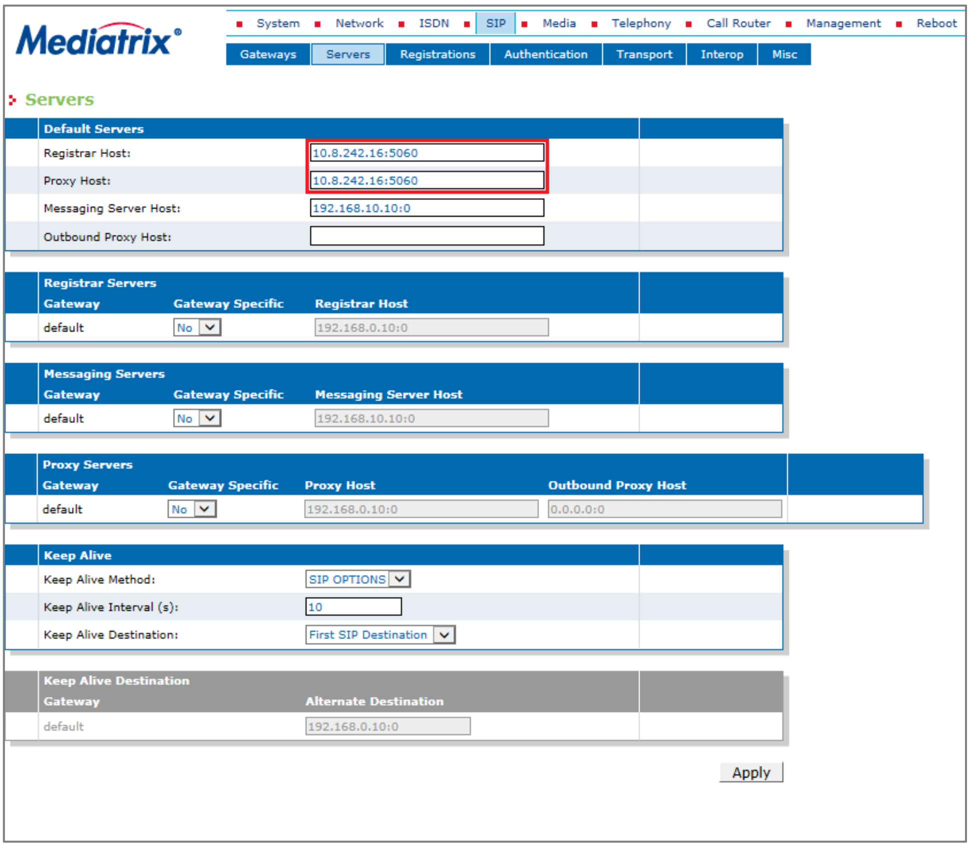
On the pop-up window and **Providers** tab, click **Streaming-IVR (TTS, ASR, SDP, BFCP)** and on the **SDP** tab set “Insecure only” from **Security** mode drop down list.

Click **Save**.

4.4. Mediatrix 4402plus Configuration

The Mediatrix 4402plus is already configured in OS Voice as an endpoint.

The configuration of Mediatrix 4402plus is performed via the device's WBM. Any typical configuration like e.g. call routing to and from OS Voice and for ISDN provider is out of scope and therefore omitted.

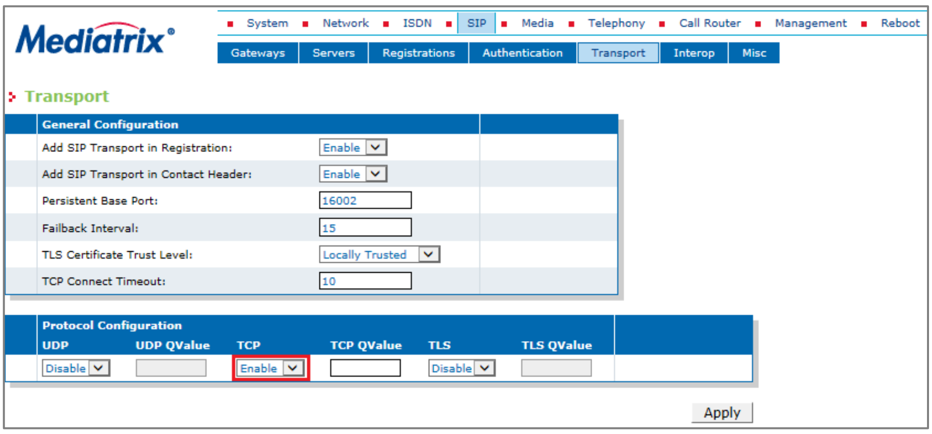


Navigate to **WBM >> SIP >> Servers**.

Configure the value 10.8.242.16:5060 (OS Voice SIPSM & non-secure port) for **Registrar Host** and **Proxy Host**.

The SIP trunk connection between OS Voice and Mediatrix 4402plus has been configured as TCP for the needs of the current project.

Click **Apply**.



Go to **WBM** >> **SIP** >> **Transport**

For TCP connection to OS Voice, **TCP** = Enable.

Click **Apply**.