



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

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. 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

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel”), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2020, Mitel Networks Corporation

All rights reserved

Table of Contents

1. Overview	6
1.1. Executive Summary	6
1.1.1. Description	6
1.1.2. Test Equipment	6
1.2. Test Network	7
2. Limitations and Observations	8
2.1. Remarks	8
2.2. Restrictions	9
2.3. Known Issues	12
3. Configuration Overview	12
3.1. Microsoft Teams & AudioCodes SBC	12
3.2. Unify Component Infrastructure	13
4. Configuration in Detail	15
4.1. Setting up the Domain	15
4.1.1. Pair the SBC to the Direct Routing Service of MS Phone System	18
4.1.2. Enable users for Direct Routing Service	19
4.1.3. Configure Voice Routing	20
4.1.4. Designate the ability to use the calling functionality within Teams	22
4.2. Configuring the AudioCodes SBC	23
4.2.1. LAN and WAN IP Interfaces	24
4.2.2. Teams TLS Context	25
4.2.3. Media Realms	30
4.2.4. SIP Signaling Interfaces	31
4.2.5. Proxy Sets and Proxy Addresses	34
4.2.6. Coder Groups	37
4.2.7. IP Profiles	37
4.2.8. IP Groups	41
4.2.9. Media Security	44
4.2.10. Message Condition Rules	44
4.2.11. Classification Rules	45
4.2.12. IP-to-IP Call Routing Rules	46
4.2.13. Firewall Settings	50
4.3. OpenScape Voice Configuration	51
4.3.1. OS Voice Firewall	51
4.3.2. Endpoint	53
4.3.3. Destinations & Routes	60
4.3.4. Translation	61

4.3.5. Media Server Secure Media Setting	64
4.4. Mediatrix 4402plus Configuration	65

History of Change

Version	Date	Description
1	March 6 th , 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-](https://www.audiocodes.com/library/technical-documents?productFamilyGroup=1637&productGroup=1692&versionGroup=Version+7.2)

[documents?productFamilyGroup=1637&productGroup=1692&versionGroup=Version+7.2](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.

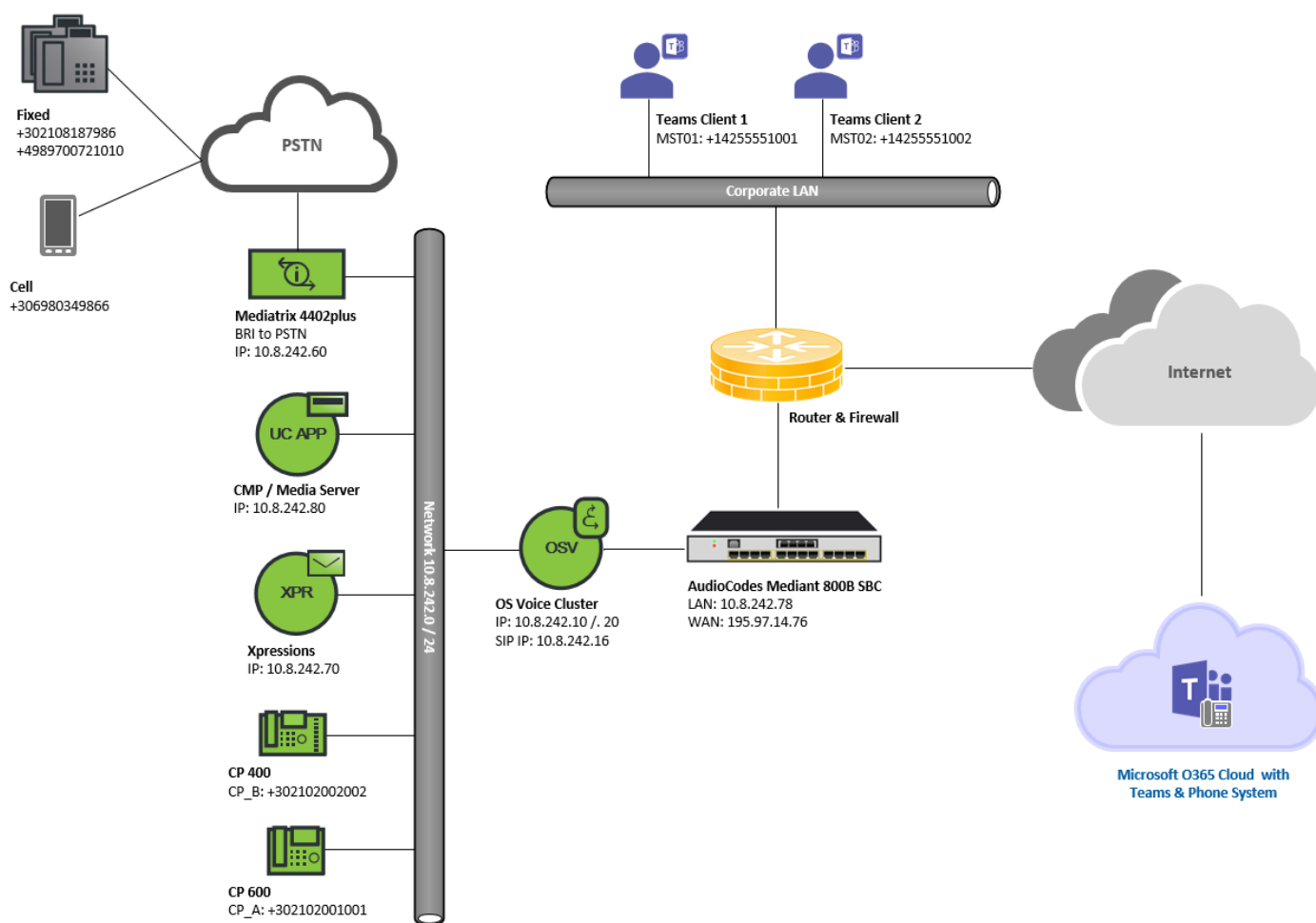


Figure 1 Logical Topology Diagram

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 OpenScope 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.

OpenScope UC applications server supplies OS Voice with media services (Media Server) & UI administration services (CMP).

Voicemail functionality is provided by OS Voice through OpenScope 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

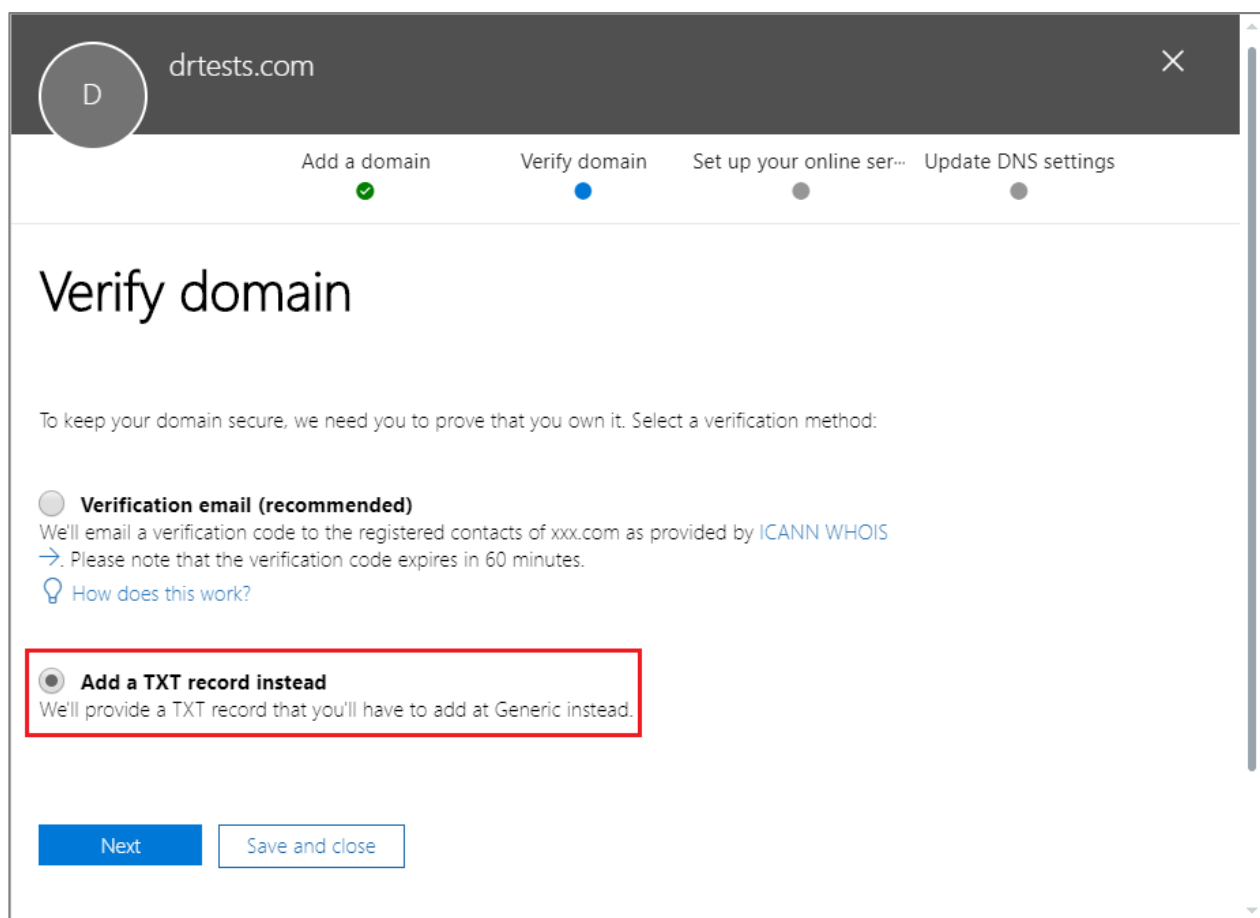
The values of many parameters given in this chapter, such as IP addresses, are given as examples and should be treated as such.

4.1. Setting up the Domain

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



Navigate to O365 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**.

drtests.com

Add a domain Verify domain Set up your online ser... Update DNS settings

Verify domain

To keep your domain secure, we need you to prove that you own it. Adding the record below will prove that you own the domain, but it won't affect your existing email or other services. After the domain is verified as being owned by you and the domain setup is complete, you can safely remove the record from your DNS hosting provider.

Follow these [step-by-step instructions](#) to add the **TXT records with the values below at** your DNS host. [\(Select your DNS Host.\)](#)

Verify by: TXT record MX Record

TXT name: @ or skip if not supported by provider.

TXT value: MS=ms40972383

TTL: 3600 or your provider default.

[Get someone to help you.](#) Let us help you set up your TXT records.

[Verify](#) [Back](#) [Save and close](#)

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**.

drtests.com

Add a domain Verify domain Set up your online services Update DNS settings

Update DNS settings

In this step, you'll activate services for your domain, like email and instant messaging, by adding DNS records for 31857.uctrunk.com at your registrar or DNS hosting provider.
 What's a DNS record? What's a domain registrar?

☐ Add the DNS records for me (recommended)
 Since GoDaddy is your DNS hosting provider, all you have to do is sign in and we'll update your DNS records.

☒ I'll add the DNS records myself
 If you have a complex DNS record structure, choose this option. Next, we'll provide a list of DNS records that you'll need to add for your domain at your DNS host.
 Why would I manage my own DNS records?

Next Back Save and close

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

Microsoft 365 admin center

Contoso

The new admin center

Domains

+ Add domain Buy domain Refresh Search Filter

Domain name	Status	Choose columns
M365x316382.onmicrosoft.com (Default)	Healthy	
drtests.com	Healthy	

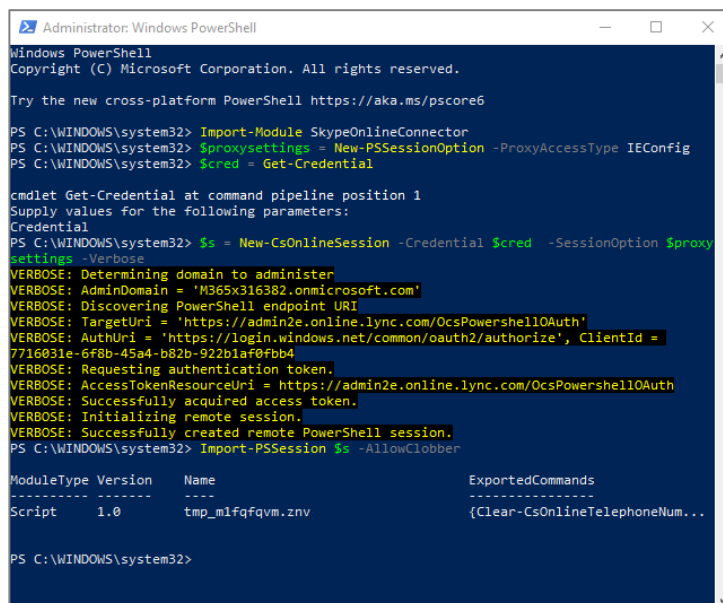
When the SBC's domain setup is completed, the next step is to activate it. For this, a "dummy" user (with a E3 or E5 license) should be added to this specific domain, not the default one. When the setup is completed this "dummy" user could be deleted.

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>.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> Import-Module SkypeOnlineConnector
PS C:\WINDOWS\system32> $proxysettings = New-PSSessionOption -ProxyAccessType IEConfig
PS C:\WINDOWS\system32> $cred = Get-Credential

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
PS C:\WINDOWS\system32> $s = New-CsOnlineSession -Credential $cred -SessionOption $proxy
settings -Verbose
VERBOSE: Determining domain to administer
VERBOSE: AdminDomain = 'M365x316382.onmicrosoft.com'
VERBOSE: Discovering PowerShell endpoint URI
VERBOSE: TargetUri = 'https://admin2e.online.lync.com/OcsPowerShell10Auth'
VERBOSE: AuthUri = 'https://login.windows.net/common/oauth2/authorize', ClientId =
7716031e-6f8b-45a4-b82b-922b1af0fbb4
VERBOSE: Requesting authentication token.
VERBOSE: AccessTokenResourceUri = https://admin2e.online.lync.com/OcsPowerShell10Auth
VERBOSE: Successfully acquired access token.
VERBOSE: Initializing remote session.
VERBOSE: Successfully created remote PowerShell session.
PS C:\WINDOWS\system32> Import-PSSession $s -AllowClobber

ModuleType Version      Name                               ExportedCommands
-----
Script      1.0          tmp_m1fqfqvm.znv                  {Clear-CsOnlineTelephoneNum...
```

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.

```

Administrator: Windows PowerShell

ModuleType Version      Name                               ExportedCommands
-----
Script      1.0             tmp_mlfqfqvm.znv                  {Clear-CsOnlineTelephoneNum...

PS C:\WINDOWS\system32> Get-CsOnlinePSTNGateway -Identity sbc.drtests.com

Identity                : sbc.drtests.com
InboundTeamsNumberTranslationRules : {}
InboundPstnNumberTranslationRules : {}
OutboundTeamsNumberTranslationRules : {}
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
PidfFloSupported        : False
MediaRelayRoutingLocationOverride :
ProxySbc                :
BypassMode              : None

PS C:\WINDOWS\system32>

```

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.

```

Administrator: Windows PowerShell

VERBOSE: AdminDomain = 'M365x316382.onmicrosoft.com'
VERBOSE: Discovering PowerShell endpoint URI
VERBOSE: TargetUri = 'https://admin2e.online.lync.com/OcsPowerShell10Auth'
VERBOSE: AuthUri = 'https://login.windows.net/common/oauth2/authorize', ClientId = 7716031e-6f8b-45a4-b82b-922b1af0fbb4
VERBOSE: Requesting authentication token.
VERBOSE: AccessTokenResourceUri = https://admin2e.online.lync.com/OcsPowerShell10Auth
VERBOSE: Successfully acquired access token.
VERBOSE: Initializing remote session.
VERBOSE: Successfully created remote PowerShell session.
PS C:\WINDOWS\system32> Import-PSSession $s -AllowClobber

ModuleType Version      Name                               ExportedCommands
-----
Script      1.0             tmp_wmdavqlq.n4j                  {Clear-CsOnlineTelephoneNu...

PS C:\WINDOWS\system32> Get-CsOnlineUser -Identity MST01@M365x316382.onmicrosoft.com | fl RegistrarPool

RegistrarPool : sippoolAM42E15.infra.lync.com

PS C:\WINDOWS\system32> Get-CsOnlineUser -Identity MST02@M365x316382.onmicrosoft.com | fl RegistrarPool

RegistrarPool : sippoolAM42E15.infra.lync.com

PS C:\WINDOWS\system32>

```

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 : {}
OutboundTeamsNumberTranslationRules : {}
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"*

```

Administrator: Windows PowerShell

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> Get-CsOnlineVoiceRoutingPolicy "CSL ATH"

Identity      : Tag:CSL ATH
OnlinePstnUsages : {CSL Athens}
Description   :
RouteType     : BYOT

PS C:\WINDOWS\system32>

```

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

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

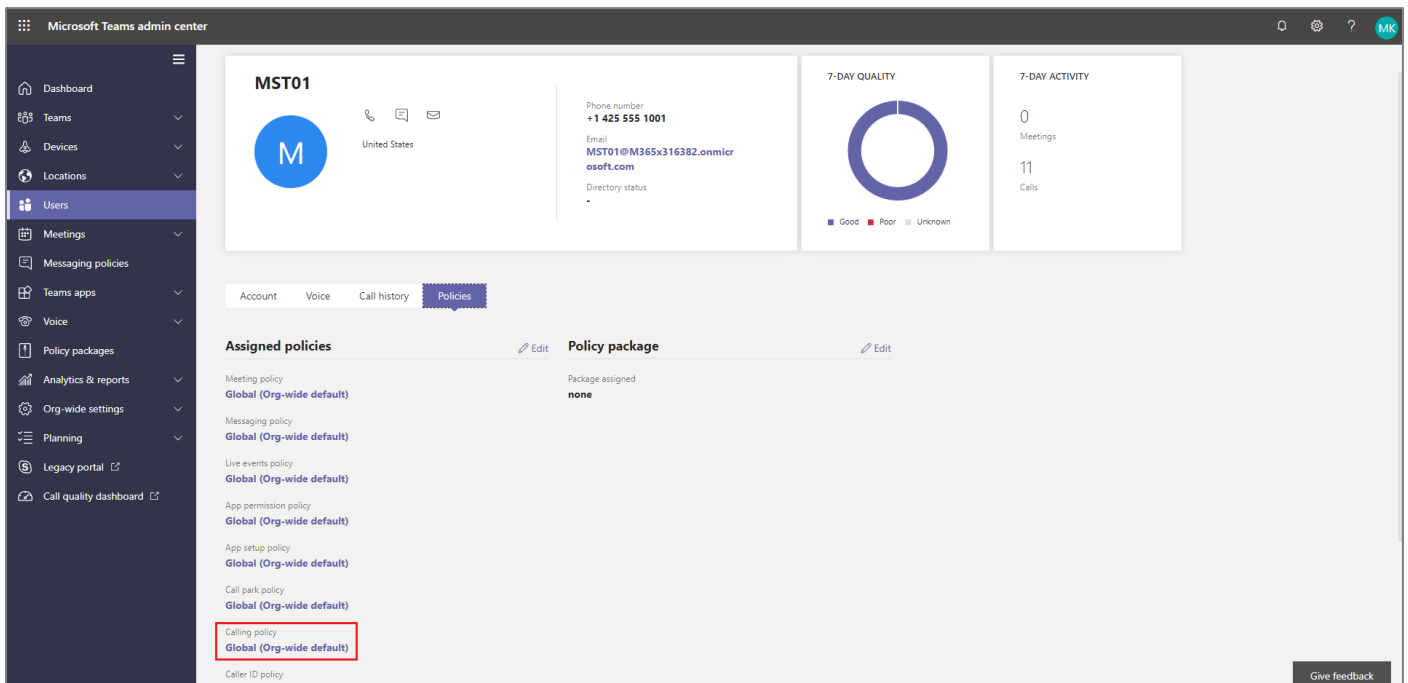
Grant to test users the previously created **Voice Routing Policy** with the commands:

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

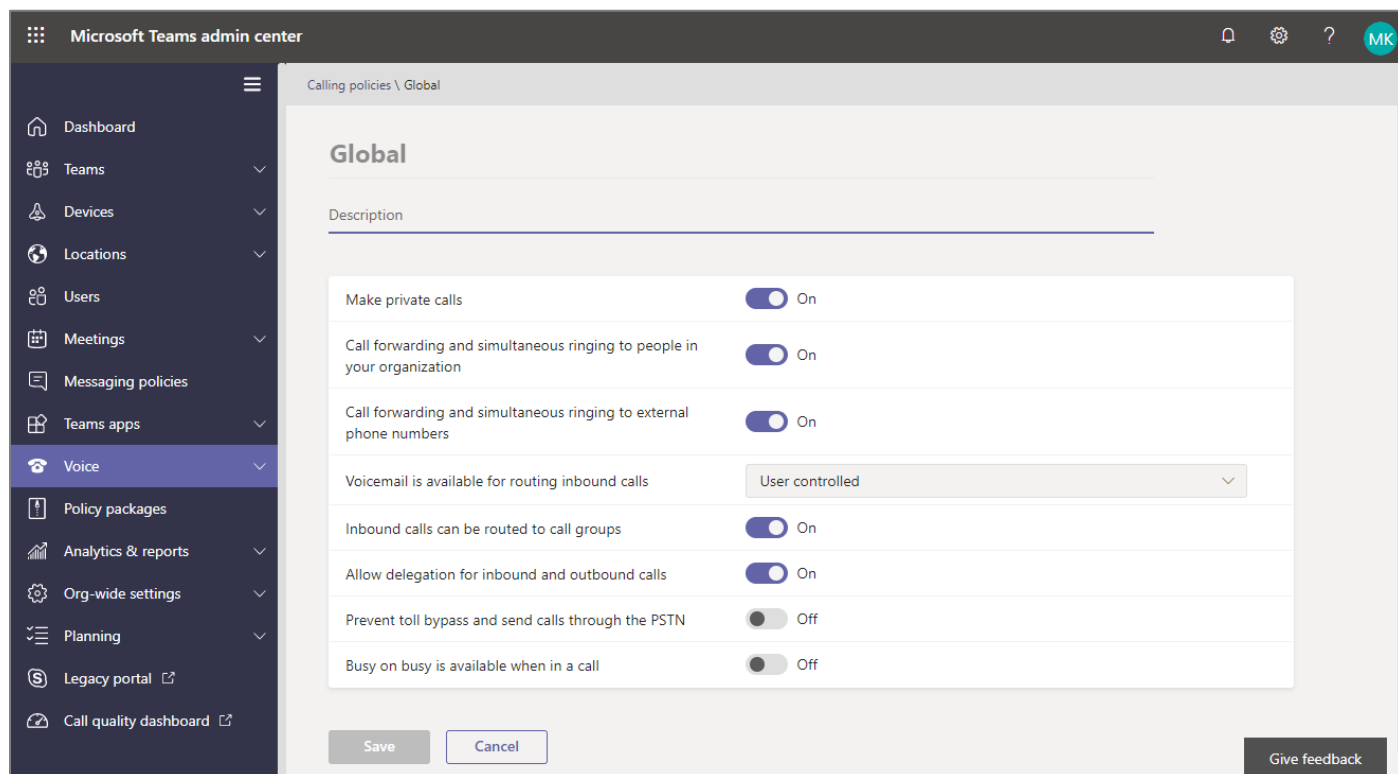
Grant-CsOnlineVoiceRoutingPolicy -Identity MST01@M365x316382.onmicrosoft.com -PolicyName "CSL ATH"

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

The screenshot shows the 'IP Interfaces' configuration window. The 'GENERAL' tab is active, showing fields for Index (0), Name (LAN_IF), Application Type (OAMP + Media + Control), and Ethernet Device (#0 [vlan 1]). The 'IP ADDRESS' tab is also visible, showing Interface Mode (IPv4 Manual), IP Address (10.8.242.78), Prefix Length (24), and Default Gateway (10.8.242.1). Below these is a 'DNS' section with Primary DNS (10.8.251.103) and Secondary DNS (0.0.0.0). At the bottom are 'Cancel' and 'APPLY' buttons. Red boxes highlight the Name, Application Type, Ethernet Device, IP Address, Prefix Length, Default Gateway, and Primary DNS fields.

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**.

The screenshot shows the 'IP Interfaces' configuration window. It is divided into two main sections: 'GENERAL' and 'IP ADDRESS'.
GENERAL Section:
 - Index: 1
 - Name: WAN_IF
 - Application Type: Media + Control (dropdown menu)
 - Ethernet Device: #1 [vlan 2] (dropdown menu with a 'View' link)
DNS Section:
 - Primary DNS: 8.8.8.8
 - Secondary DNS: 0.0.0.0
IP ADDRESS Section:
 - Interface Mode: IPv4 Manual (dropdown menu)
 - IP Address: 195.97.14.76
 - Prefix Length: 27
 - Default Gateway: 195.97.14.65
 At the bottom of the window are 'Cancel' and 'APPLY' buttons.

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.

The screenshot shows the Audiocodes M800B web interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar shows 'TIME & DATE' as the active section. The main content area is divided into 'LOCAL TIME' and 'TIME ZONE' sections. The 'NTP SERVER' section is highlighted with a red box, showing the following configuration:

Field	Value
Enable NTP	Enable
Primary NTP Server Address (IP or FQDN)	10.8.251.104
Secondary NTP Server Address (IP or FQDN)	
NTP Update Interval	Hours: 24 Minutes: 0
NTP Authentication Key Identifier	0
NTP Authentication Secret Key	

The 'TIME ZONE' section shows the following configuration:

Field	Value
UTC Time	28 Feb, 2020 09:41:46
UTC Offset	Hours: 2 Minutes: 0
Daylight Saving Time	Disable
DST Mode	Day of year
Start Time	Jan 01 0 : 0
End Time	Jan 01 0 : 0
Offset [min]	60
Day of Month Start	Jan Sunday First 0 : 0
Day of Month End	Jan Sunday First 0 : 0

At the bottom of the page, there are 'Cancel' and 'APPLY' buttons.

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.

TLS Contexts

GENERAL

Index: 1

Name: MS Teams

TLS Version: TLSv1.2

DTLS Version: Any

Cipher Server: DEFAULT

Cipher Client: DEFAULT

Strict Certificate Extension Validation: Disable

DH key Size: 2048

OCSP

OCSP Server: Disable

Primary OSCP Server: 0.0.0.0

Secondary OSCP Server: 0.0.0.0

OCSP Port: 2560

OCSP Default Response: Reject

Cancel APPLY

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.

The screenshot shows the Audiocodes M800B IP Network configuration interface. The left sidebar contains a 'NETWORK VIEW' menu with options like CORE ENTITIES, SECURITY, and QUALITY. The 'SECURITY' section is expanded, showing 'TLS Contexts (2)'. The main content area displays a table of TLS Contexts with columns for INDEX, NAME, TLS VERSION, DTLS VERSION, and CIPHER SERVER. Below the table, the configuration for context #1 [MS Teams] is shown, including GENERAL and OCSP settings. At the bottom of the configuration section, there are three links: 'Certificate Information >>', 'Change Certificate >>' (highlighted with a red box), and 'Trusted Root Certificates >>'.

INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	default	Any - Including SSLv3	Any	DEFAULT
1	MS Teams	TLSv1.2	Any	DEFAULT

#1[MS Teams]

GENERAL

- Name: MS Teams
- TLS Version: TLSv1.2
- DTLS Version: Any
- Cipher Server: DEFAULT
- Cipher Client: DEFAULT
- Strict Certificate Extension: Disable
- DH key Size: 2048

OCSP

- OCSP Server: Disable
- Primary OCSP Server: 0.0.0.0
- Secondary OCSP Server: 0.0.0.0
- OCSP Port: 2560
- OCSP Default Response: Reject

Links: [Certificate Information >>](#), [Change Certificate >>](#), [Trusted Root Certificates >>](#)

The screenshot shows the Audiocodes M800B IP Network configuration interface, specifically the 'Generate Private Key' and 'Upload Certificate Files from Your Computer' sections. The 'Generate Private Key' section includes fields for Private Key Size (1024) and Private key pass-phrase (optional). Below this, there are instructions and buttons for 'Generate Private-Key' and 'Generate Self-Signed Certificate'. The 'TLS EXPIRY SETTINGS' section includes fields for TLS Expiry Check Start (days) and TLS Expiry Check Period (days), with a 'Submit TLS Expiry Settings' button. The 'UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER' section includes a field for Private key pass-phrase (optional) and a red box highlighting the instructions for uploading the Private Key and Device Certificate files. The red box contains the following text:

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.

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.

PRIVATE KEY

Key size: 2048 bits
Status: OK

CERTIFICATE

Certificate:
Data:
Version: 3 (0x2)
Serial Number: bf:f8:80:9c:11:0f:78:2d:52:97:31:29:e7:e1:c3:cc
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: Jan 27 00:00:00 2020 GMT
Not After: Apr 26 23:59:59 2020 GMT
Subject: CN=opc-directs.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:e5:2c:e0:09:67:49:3a:18:01:b0:2d:4e:0a:33:
d7:a0:88:84:d9:13:90:4e:29:39:e0:26:f5:56:9a:
d1:a5:84:35:c3:7d:e8:c0:c1:cc:02:d2:20:dd:8a:
09:fb:13:e5:77:87:b1:c9:78:7e:ac:44:b4:cc:77:
27:2f:97:01:dac:1:8a:27:f6:25:8d:74:ad:8d:
32:88:9c:31:70:cf:9b:b6:65:44:e3:ce:86:87:58:
2d:70:d9:67:40:2b:37:5a:4a:59:ac:e4:2c:81:98:
ab:00:43:58:00:76:c1:fd:b2:2f:f5:d8:cb:34:40:
4d:1b:51:d0:6b:7b:25:0d:d6:92:30:27:8e:1d:ea:
77:23:25:11:31:10:02:0c:cb:71:5f:eb:16:bd:61:
0e:ed:fb:92:08:61:42:1e:7e:58:36:37:5b:f8:5f:
4c:3a:4a:ca:db:d4:f8:66:b0:01:83:7d:5e:66:cc:
f1:7b:16:32:41:d8:80:26:b9:23:7a:87:20:1e:e3:

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.

View **Import** **Export** **Remove**

INDEX	SUBJECT	ISSUER	EXPIRES
0	Sectigo RSA Domain Validation S	USERTRUST RSA Certification Aut	12/31/2030
1	USERTRUST RSA Certification Aut	AddTrust External CA Root	5/30/2020

Page 1 of 1 | 10 | View 1 - 2 of 2

Selected Row #0

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 7d:5b:51:26:b4:76:ba:11:db:74:16:0b:bc:53:0d:a7
Signature Algorithm: sha384WithRSAEncryption
Issuer: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTRUST RSA Certification Authority
Validity
Not Before: Nov 2 00:00:00 2018 GMT
Not After: Dec 31 23:59:59 2030 GMT
Subject: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:d6:73:33:d6:d7:3c:20:d0:00:d2:17:45:b8:d6:
3e:07:a2:3f:c7:41:ee:32:30:c9:b0:6c:fd:f4:9f:
cb:12:98:0f:2d:3f:8d:4d:01:0c:82:0f:17:7f:62:
2e:e9:b8:48:79:fb:16:83:4e:ad:d7:32:25:93:b7:
07:0f:b9:50:3f:a9:4c:c3:40:2a:e9:39:ff:09:81:
ca:1f:16:32:41:d8:80:26:b9:23:7a:87:20:1e:e3:

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.

The screenshot shows the 'Media Realms' configuration window. The 'GENERAL' tab is active, displaying various configuration fields. The 'Name' field is set to 'MR_LAN', 'IPv4 Interface Name' is set to '#0 [LAN_IF]', and 'Number Of Media Session Legs' is set to '100'. These three fields are highlighted with red rectangular boxes. Other fields include 'Index' (0), 'Topology Location' (Down), 'UDP Port Range Start' (6000), 'UDP Port Range End' (6999), 'TCP Port Range Start' (0), 'TCP Port Range End' (0), and 'Default Media Realm' (No). The 'QUALITY OF EXPERIENCE' tab is also visible, showing 'QoS Profile' and 'Bandwidth Profile' both set to '--' with 'View' links. At the bottom of the window, there are 'Cancel' and 'APPLY' buttons.

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**.

GENERAL		QUALITY OF EXPERIENCE	
Index	1	QoE Profile	-- View
Name	MR_WAN	Bandwidth Profile	-- View
Topology Location	Up		
IPv4 Interface Name	#1 [WAN_IF] View		
UDP Port Range Start	7000		
Number Of Media Session Legs	100		
UDP Port Range End	7999		
TCP Port Range Start	0		
TCP Port Range End	0		
Default Media Realm	No		

Cancel 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.

SIP Interfaces

SRD #0 [DefaultSRD]

GENERAL		MEDIA	
Index	0	Media Realm	#0 [MR_LAN] View
Name	OSV_Trunk	Direct Media	Disable
Topology Location	Down		
Network Interface	#0 [LAN_IF] View		
Application Type	SBC		
UDP Port	5060		
TCP Port	0		
TLS Port	0		
Additional UDP Ports			
Additional UDP Ports Mode	Always Open		

Cancel [APPLY](#)

SIP Interfaces

TCP Port	0	Message Policy	-- View
TLS Port	0	User Security Mode	Not Configured
Additional UDP Ports		Enable Un-Authenticated Registrations	Not configured
Additional UDP Ports Mode	Always Open	Max. Number of Registered Users	-1
Encapsulating Protocol	No encapsulation		
Enable TCP Keepalive	Disable		
Used By Routing Server	Not Used		
Pre-Parsing Manipulation Set	-- View		
CAC Profile	-- View		

Cancel [APPLY](#)

CLASSIFICATION	
Classification Failure Response Type	500
Pre-classification Manipulation Set ID	-1
Call Setup Rules Set ID	-1

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**.

SIP Interfaces

SRD #0 [DefaultSRD]

GENERAL		MEDIA	
Index	1	Media Realm	#1 [MR_WAN] View
Name	MS Teams_Trunk	Direct Media	Disable
Topology Location	Up		
Network Interface	#1 [WAN_IF] View		
Application Type	SBC		
UDP Port	0		
TCP Port	0		
TLS Port	5067		
Additional UDP Ports			
Additional UDP Ports Mode	Always Open		

Cancel [APPLY](#)

SIP Interfaces

TCP Port	0	Message Policy	-- View
TLS Port	5067	User Security Mode	Not Configured
Additional UDP Ports		Enable Un-Authenticated Registrations	Not configured
Additional UDP Ports Mode	Always Open	Max. Number of Registered Users	-1
Encapsulating Protocol	No encapsulation		
Enable TCP Keepalive	Enable		
Used By Routing Server	Not Used		
Pre-Parsing Manipulation Set	-- View		
CAC Profile	-- View		

Cancel [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**.

Proxy Sets

SRD: #0 [DefaultSRD]

GENERAL		REDUNDANCY	
Index	2	Redundancy Mode	
Name	ProxySet_MS teams	Proxy Hot Swap	Enable
Gateway IPv4 SIP Interface	-- View	Proxy Load Balancing Method	Random Weights
SBC IPv4 SIP Interface	#1 [MS Teams_Trunk] View	Min. Active Servers for Load Balancing	1
TLS Context Name	#1 [MS Teams] View		
KEEP ALIVE		ADVANCED	
Proxy Keep-Alive	Using OPTIONS	Classification Input	IP Address only
Proxy Keep-Alive Time [sec]	60	DNS Resolve Method	
Keep-Alive Failure Responses			

Cancel 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**.

Proxy Address

GENERAL	
Index	0
Proxy Address	sip.pstnhub.microsoft.com:5061
Transport Type	TLS
Proxy Priority	1
Proxy Random Weight	1

Cancel APPLY

The image contains two screenshots of the 'Proxy Address' configuration window. Both windows have a title bar with 'Proxy Address' and standard window controls. The main content area is titled 'GENERAL' and contains several fields: 'Index', 'Proxy Address', 'Transport Type', 'Proxy Priority', and 'Proxy Random Weight'. At the bottom, there are 'Cancel' and 'APPLY' buttons.

Top Screenshot (Index 1):

- Index: 1
- Proxy Address: sip2.pstnhub.microsoft.com:5061
- Transport Type: TLS (dropdown menu)
- Proxy Priority: 2
- Proxy Random Weight: 1

Bottom Screenshot (Index 2):

- Index: 2
- Proxy Address: sip3.pstnhub.microsoft.com:5061
- Transport Type: TLS (dropdown menu)
- Proxy Priority: 3
- Proxy Random Weight: 1

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.

The screenshot shows the Audiocodes M800B web interface. The left sidebar has a navigation menu with 'CODERS & PROFILES' selected. The main area is titled 'Coder Groups'. At the top, there is a dropdown for 'Coder Group Name' set to '0: AudioCodersGroups_0' and a 'Delete Group' button. Below this is a table with the following columns: Coder Name, Packetization Time, Rate, Payload Type, Silence Suppression, and Coder Specific. The table contains several rows of codec configurations. The 'Payload Type' column has a red box around the value '103' for the 'SILK-NB' codec.

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
SILK-NB	20	8	103	N/A	
SILK-WB	20	16	104	N/A	
G.711A-law	20	64	8	Disabled	
G.711U-law	20	64	0	Disabled	
G.729	20	8	18	Disabled	
G.722	10	64	9	Disabled	

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.

IP Profiles

GENERAL		SBC SIGNALING	
Index	2	PRACK Mode	Transparent
Name	OSV	P-Asserted-Identity Header Mode	Add
Created by Routing Server	No	Diversion Header Mode	As Is
		History-Info Header Mode	As Is
		Session Expires Mode	Transparent
		SIP UPDATE Support	Supported
		Remote re-INVITE	Supported
		Remote Delayed Offer Support	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

Remote Can Play Ringback	Yes		
Generate RTP	None		
		SBC FORWARD AND TRANSFER	
		Remote REFER Mode	Handle Locally
		Remote Replaces Mode	Handle Locally
		Play RBT To Transferee	No
		Remote 3xx Mode	Handle Locally
		SBC HOLD	
		Remote Hold Format	Transparent
		Reliable Held Tone Source	Yes
		Play Held Tone	No
		SBC FAX	
		Fax Coders Group	--

Cancel APPLY

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

Generate RTP: None

SBC MEDIA

Mediation Mode: RTP Mediation

Extension Coders Group: #0 [AudioCodersGroups_0]

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: 0

Alternative DTMF Method: As Is

Send Multiple DTMF Methods: Disable

SBC FORWARD AND TRANSFER

Remote REFER Mode: Handle Locally

Remote Replaces Mode: Standard

Play RBT To Transferee: No

Remote 3xx Mode: Handle Locally

SBC HOLD

Remote Hold Format: Inactive

Reliable Held Tone Source: Yes

Play Held Tone: No

SBC FAX

Fax Coders Group: --

Fax Mode: As Is

Cancel APPLY

IP Profiles

Adapt RFC2833 BW to Voice coder BW: Disabled

SDP Ptime Answer: Remote Answer

Preferred PTime: 0

Use Silence Suppression: Add

RTP Redundancy Mode: As Is

RTCP Mode: Generate Always

Jitter Compensation: Disable

ICE Mode: Lite

SDP Handle RTCP: Don't Care

RTCP Mux: Not Supported

RTCP Feedback: Feedback Off

Voice Quality Enhancement: Disable

Max Opus Bandwidth: 0

Generate No-Op Packets: Disable

Fax Offer Mode: All coders

Fax Answer Mode: Single coder

Remote Renegotiate on Fax Detection: Transparent

Fax Rerouting Mode: Disable

MEDIA

Broken Connection Mode: Disconnect

Media IP Version Preference: Only IPv4

RTP Redundancy Depth: Disable

GATEWAY

Early Media: Disable

Early 183: Disable

Early Answer Timeout [sec]: 0

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:**
- **Remote Hold Format:**

Handle Locally

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.

SRD #0 [DefaultSRD]

GENERAL

Index 1

Name OSV

Topology Location Down

Type Server

Proxy Set #1 [ProxySet_OSV] View

IP Profile #2 [OSV] View

Media Realm #0 [MR_LAN] View

Contact User

SIP Group Name

Created By Routing Server No

QUALITY OF EXPERIENCE

QoE Profile -- View

Bandwidth Profile -- View

MESSAGE MANIPULATION

Inbound Message Manipulation Set -1

Outbound Message Manipulation Set -1

Message Manipulation User-Defined String 1

Message Manipulation User-Defined String 2

Proxy Keep-Alive using IP Group settings Disable

Cancel APPLY

IP Groups

Used By Routing Server: Not Used
Proxy Set Connectivity: Connected

SBC GENERAL

Classify By Proxy Set: **Enable**
SBC Operation Mode: Not Configured
SBC Client Forking Mode: Sequential
CAC Profile: -- [View](#)

ADVANCED

Local Host Name:
UI Format: Disable

SBC REGISTRATION AND AUTHENTICATION

Max. Number of Registered Users: -1
Registration Mode: User Initiates Registration
User Stickiness: Disable
User UDP Port Assignment: Disable
Authentication Mode: User Authenticates
Authentication Method List:
SBC Server Authentication Type: According to Global Parameter
OAuth HTTP Service: -- [View](#)
Username:
Password:

GATEWAY

Cancel [APPLY](#)

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**.

IP Groups

SRD: #0 [DefaultSRD]

GENERAL

Index: 2
Name: MS Teams
Topology Location: Up
Type: Server
Proxy Set: #2 [ProxySet_MS teams] [View](#)
IP Profile: #1 [MS Teams] [View](#)
Media Realm: #1 [MR_WAN] [View](#)
Contact User:
SIP Group Name:
Created By Routing Server: No

QUALITY OF EXPERIENCE

QoE Profile: -- [View](#)
Bandwidth Profile: -- [View](#)

MESSAGE MANIPULATION

Inbound Message Manipulation Set: -1
Outbound Message Manipulation Set: -1
Message Manipulation User-Defined String 1:
Message Manipulation User-Defined String 2:
Proxy Keep-Alive using IP Group settings: **Enable**

Cancel [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.

The screenshot shows the Audiocodes M800B configuration interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar shows a hierarchy of settings: TOPOLOGY VIEW, CORE ENTITIES, CODERS & PROFILES, SBC, GATEWAY, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, and INTRUSION DETECTION. The 'MEDIA' section is expanded, showing 'Media Security' as the selected option. The main content area displays the 'Media Security' configuration page. It has two tabs: 'GENERAL' and 'AUTHENTICATION & ENCRYPTION'. Under the 'GENERAL' tab, the 'Media Security' dropdown is set to 'Enable' (highlighted with a red box). Other settings include 'Media Security Behavior' (Preferable), 'Offered SRTP Cipher Suites' (All), and 'ARIA Protocol Support' (Disable). Under the 'AUTHENTICATION & ENCRYPTION' tab, settings include 'Authentication on Transmitted RTP Packets' (Active), 'Encryption on Transmitted RTP Packets' (Active), 'Encryption on Transmitted RTCP Packets' (Active), 'SRTP Tunneling Authentication for RTP' (Disable), and 'SRTP Tunneling Authentication for RTCP' (Disable). At the bottom, there are 'Cancel' and 'APPLY' buttons.

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.

The screenshot shows the 'Message Conditions' configuration window. The 'GENERAL' tab is active. The 'Index' field is set to '0'. The 'Name' field is set to 'MS Teams-Contact'. The 'Condition' field is set to 'header.contact.url.host contains 'pstnhub.microsoft.com''. The 'Name' and 'Condition' fields are highlighted with a red rectangle. An 'Editor' button is next to the 'Condition' field. At the bottom are 'Cancel' and 'APPLY' buttons.

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**.

IP-to-IP Routing

Routing Policy #0 [Default_SBCRoutingPolicy]

GENERAL	ACTION
Index: 1	Destination Type: Request URI
Name: REFER from MS Teams	Destination IP Group: #2 [MS Teams]
Alternative Route Options: Route Row	Destination SIP Interface: --
	Destination Address:
	Destination Port: 0
	Destination Transport Type:
	IP Group Set: --
	Call Setup Rules Set ID: -1
	Group Policy: Sequential
	Cost Group: --

Cancel APPLY

IP-to-IP Routing

Alternative Route Options: Route Row

MATCH	
Source IP Group: Any	Destination SIP Interface: --
Request Type: All	Destination Address:
Source Username Pattern: *	Destination Port: 0
Source Host: *	Destination Transport Type:
Source Tag:	IP Group Set: --
Destination Username Pattern: *	Call Setup Rules Set ID: -1
Destination Host: *	Group Policy: Sequential
Destination Tag:	Cost Group: --
Message Condition: --	Routing Tag Name: default
Call Trigger: REFER	Internal Action:
ReRoute IP Group: #2 [MS Teams]	

Cancel 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**.

IP-to-IP Routing

Routing Policy #0 [Default_SBCRoutingPolicy]

GENERAL	ACTION
Index: 2	Destination Type: IP Group
Name: MS Teams to OSV	Destination IP Group: #1 [OSV] View
Alternative Route Options: Route Row	Destination SIP Interface: -- View
	Destination Address:
	Destination Port: 0
	Destination Transport Type:
	IP Group Set: -- View
	Call Setup Rules Set ID: -1
	Group Policy: Sequential
	Cost Group: -- View

Cancel [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**.

IP-to-IP Routing

Routing Policy #0 [Default_SBCRoutingPolicy]

GENERAL	ACTION
Index: 3	Destination Type: IP Group
Name: OSV to MS Teams	Destination IP Group: #2 [MS Teams] View
Alternative Route Options: Route Row	Destination SIP Interface: -- View
	Destination Address:
	Destination Port: 0
	Destination Transport Type:
	IP Group Set: -- View
	Call Setup Rules Set ID: -1
	Group Policy: Sequential
	Cost Group: -- View

Cancel [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:

The screenshot shows the Audiocodes SBC configuration interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar shows 'NETWORK VIEW' and 'SECURITY' sections. The main area displays a table of Firewall rules (8 total) with columns for INDEX, DESCRIPTION, ACTION UPON MATCH, and MATCH COUNT. Rule #0 is highlighted, showing details for a match on 8.8.8.8 with an allow action.

INDEX	DESCRIPTION	ACTION UPON MATCH	MATCH COUNT
0	8.8.8.8	Allow	317357
1	52.114.148.0	Allow	14676
2	52.114.132.46	Allow	520773
3	52.114.75.24	Allow	698337
4	52.114.76.76	Allow	40755
5	52.114.7.24	Allow	0
6	52.114.14.70	Allow	472010
49	0.0.0.0	Block	234857

Below the table, the details for rule #0 are shown:

MATCH		ACTION	
Description	8.8.8.8	Action Upon Match	Allow
Source IP	8.8.8.8	Packet Size	0
Source Port	0	Byte Rate	0
Prefix Length	32	Byte Burst	0
Start Port	0		
End Port	65535		
Protocol	Any		
Use Specific Interface	Enable		
Interface Name	WAN_IF		

The 'STATISTICS' section shows a Match Count of 317357.

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.

https://10.8.242.80/?callPointParam=true&action=addPfr&init=true&callPointParam=tru...

[OdysseyC] - Add Packet Filter Rule

Here you can configure the parameters of a Packet Filter Rule

General

Name: AudioCodes_10.8.242.78

Description:

Transport Protocol: ALL

Direction: Both Ways

Action: Allow

Local Host

Alias: All

Port Begin: 0

Port End: 0

Remote Host

FQDN or IP Address: 10.8.242.78

Netmask: 255.255.255.0

Port Begin: 0

Port End: 0

Save **Cancel**

Navigate to **CMP >> Configuration >> OpenScope 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.

https://10.8.242.80/?callPointParam=true&action=add&init=true&callPointParam=true&__customFWKp - Internet Explorer

[OdysseusC] - [BG_GR] - Add Endpoint Profile

Please enter the profile data.

General Endpoints Services

Endpoint Profile

Please enter a unique name to identify this profile.

Name: EPP_MSTeams

Remark:

Numbering Plan: NP_BG_GR

Management Information

Please enter the data for the following fields in the corresponding screens.

Class of Service:

Routing Area:

Calling Location:

Time Zone:

SIP Privacy Support: Full

Failed Calls Intercept Treatment: Disabled

Save Cancel

Navigate to **CMP >> Configuration >> OpenScope 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**.

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

Endpoint

Define the connection data of an endpoint, e.g. you may use this to add a gateway to a switch.

Name: EP_MSTeams

Remark:

Registered: ☐

Profile: EPP_MSTeams

Branch Office:

Associated Endpoint:

Default Home DN

Location Domain

Endpoint Template:

Endpoint Type:

Max number of users:

Last Update:

CSTA Device ID:

Save Cancel

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)

https://10.8.242.80/?callPointParam=true&action=edit&epName=EP_MSTeams&init=true&callPoi...

[OdysseusC] - [BG_GR] - [Main Office] - Add Endpoint

General SIP Attributes Aliases Routes Accounting

Endpoint Type

SIP Private Networking: ☐

SIP Trunking: ☒

SIP-Q Signaling: ☐

SIP Signaling

For the static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format.
Note that the address of the signaling interface cannot be modified unless the entry in the security section has first been removed.

Type: Static

Signaling Address Type: IP Address or FQDN

Endpoint Address: 10.8.242.78

Port: 5060

Transport protocol: UDP

Endpoint does not accept incoming TLS connections: ☐

SRTP media mode: Disabled

Key Exchange Mechanisms Supported: None

Save Cancel

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 ☐

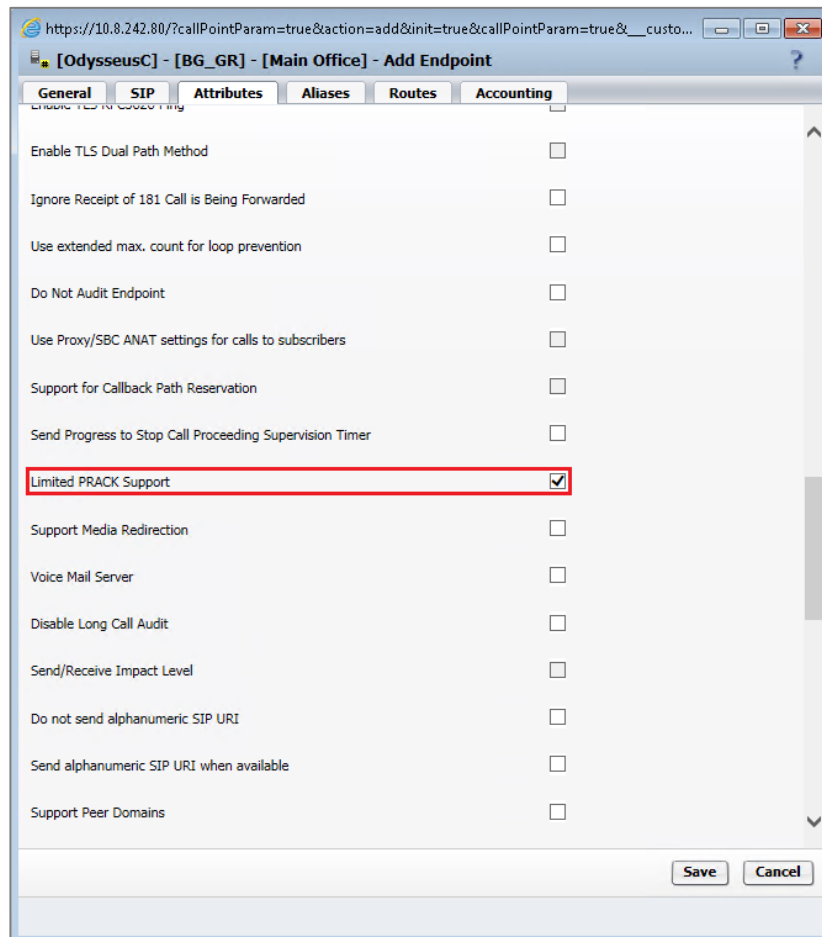
Send Authentication Number in P-Asserted-Identity header ☐

Send Authentication Number in Diversion Header ☐

Send Authentication Number in From Header ☐

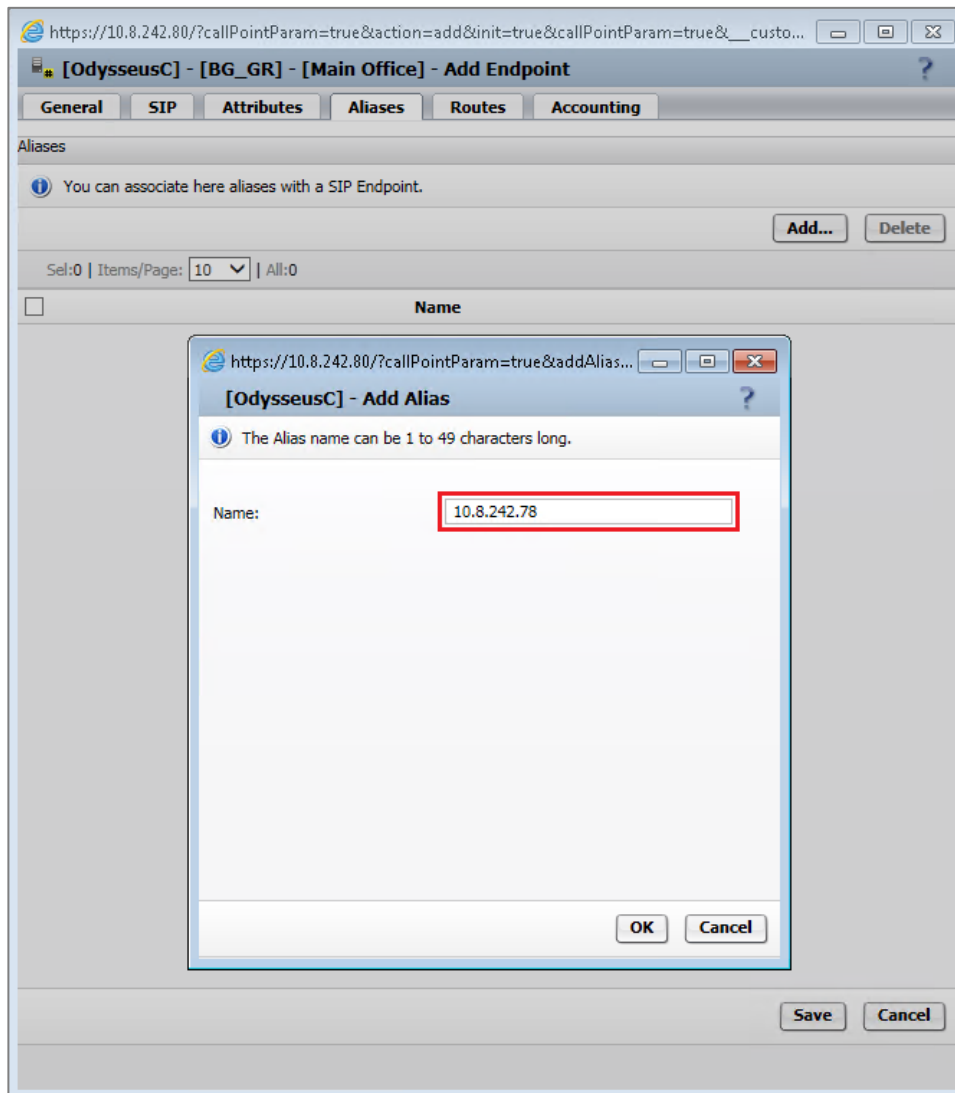
Use SIP Endpoint Default Home DN as Authentication Number ☐

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 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**.

https://10.8.242.80/?callPointParam=true&action=edit&epName=EP_MSTeams&init=true&callPoi...

[OdysseusC] - [BG_GR] - [Main Office] - Edit Endpoint : EP_MSTeams

General SIP Attributes Aliases Routes Accounting

Endpoint

Define the connection data of an endpoint, e.g. you may use this to add a gateway to a switch.

Name: EP_MSTeams

Remark:

Registered: ☒

Profile: EPP_MSTeams

Branch Office:

Associated Endpoint:

Default Home DN

Location Domain

Endpoint Template:

Endpoint Type:

Max number of users:

Last Update: 2020-03-05 10:10:25.0

CSTA Device ID:

Save Cancel

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

The endpoint status should look like the figure below:

UNIFY Common Management Platform Domain: system User: administrator@system | Settings | Help | Logout

Configuration Maintenance User Management Fault Management Performance Management Accounting

OpenScope Voice OpenScope Branch OpenScope SBC Unified Communications CMP Device Management

[OdysseusC] - [BG_GR] - [Main Office] - Endpoints

Endpoints represent Network to Network Interface connections.

Search for in Endpoint Name Search Show All Advanced...

Add... Edit... Bulk Edit... Clone Delete Change Branch Office... More Set to Normal

Sel:0 | Items/Page: 10 | All:6

	Name	Numbering Plan Name	Registration Type	Registration State	Operational State	Primary	Remark
<input type="checkbox"/>	EP_MS	NP_BG_GR	Static	Registered	Normal	10.8.242.80	No
<input checked="" type="checkbox"/>	EP_MSTeams	NP_BG_GR	Static	Registered	Normal	10.8.242.78	No
<input type="checkbox"/>	EP_Med4402	NP_BG_GR	Static	Registered	Normal	10.8.242.60	No
<input type="checkbox"/>	EP_XCAPI	NP_BG_GR	Static	Registered	Normal	10.8.242.62	No
<input type="checkbox"/>	EP_XCC	NP_BG_GR	Static	Registered	Normal	10.8.242.62	No
<input type="checkbox"/>	EP_XPR	NP_BG_GR	Static	Registered	Normal	10.8.242.70	No

Business Group

Quick Tasks

Business Group List

BG_GR

General

Profiles

Teams

Statistics

Display Number Modification

Branch Office List

Main Office

Members

Subscribers

Endpoints

Private Numbering Plan List

NP_BG_GR (Default)

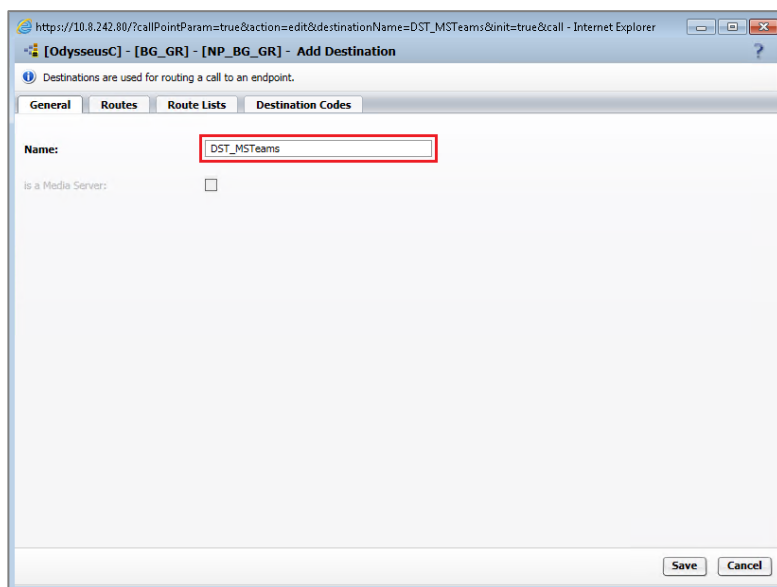
Translation

Destinations and Routes

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 >> OpenScope 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.

https://10.8.242.80/ - [OdysseusC] - [BG_GR] - [NP_BG_GR] - Add Prefix Access Code - Internet Explorer

[OdysseusC] - [BG_GR] - [NP_BG_GR] - Add Prefix Access Code

Identification

If the dialed digits match this code, the specified modification to these dialed digits is executed.

Prefix Access Code: 1425

Remark:

Minimum Length: 11

Maximum Length: 11

Digit Position: 0

Digits to insert:

Settings

Specify additional parameters to determine how the call will be routed.

Prefix Type: Off-net Access

Nature of Address: Unknown

Destination Type: None

Destination:

Save Cancel

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**.

https://10.8.242.80/?callPointParam=true&action=add&listDestinationCodes=tr...

[OdysseyC] - [BG_GR] - [NP_BG_GR] - Add Destination Code

Identification

This destination code will be used for a call if the dialed or modified (in PAC) digits and the Nature of Address are matching.

Destination Code: 1425

Remark:

Nature Of Address: Unknown

Originator Attributes

Optionally, an additional match is required if the originator of the call belongs to the specified Class of Service and Routing Area.

Class Of Service:

Routing Area:

Traffic Type

Specify the traffic type for this destination code.

None ☒

Use Local Toll Table ☐

Select Traffic Type ☐

Destination

Specify additional parameters to determine how the call will be routed.

Destination Type: Destination

Destination: DST_MSTeams

DN Office Code:

Save **Cancel**

Navigate to **CMP >> Configuration >> OpenScope 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.

The screenshot shows the 'Streaming-IVR (TTS, ASR, SDP, BFCP)' configuration window. The 'SDP' tab is selected. Under 'Session Description Protocol', the 'Security mode' dropdown is set to 'Insecure only' and is highlighted with a red box. Other settings include 'Dual Network Protocol (IPv4/V6)' set to 'None', 'Security Protocol' set to 'sdes', 'SDES Authentication tag length' set to '32 and 80 bit', 'Force local codec preference' unchecked, and 'Maximum bandwidth' set to 'kilo-bits-per-second with AS'. Below this is the 'Streaming Route Binding' section with 'Add...', 'Edit...', and 'Delete' buttons. At the bottom, the 'Audio Codecs' tab is selected, showing a table with columns 'Codec', 'Codec Parameters', and 'Payload type'. The table lists 'PCMU' as a supported codec. 'Save' and 'Cancel' buttons are at the bottom right.

Listening point	Streaming route	Alternative streaming route
-----------------	-----------------	-----------------------------

Codec	Codec Parameters	Payload type
PCMU		

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.

The screenshot shows the Mediatrix WBM interface with the 'SIP' tab selected. The 'Servers' sub-tab is active, displaying configuration for Default Servers, Registrar Servers, Messaging Servers, and Proxy Servers. The 'Registrar Host' and 'Proxy Host' fields in the Default Servers section are highlighted with a red box and contain the value '10.8.242.16:5060'. The 'Keep Alive' section shows 'Keep Alive Method' set to 'SIP OPTIONS', 'Keep Alive Interval (s)' set to '10', and 'Keep Alive Destination' set to 'First SIP Destination'. The 'Keep Alive Destination' table shows 'default' with 'Alternate Destination' '192.168.0.10:0'. An 'Apply' button is at the bottom right.

Default Servers			
Registrar Host:	10.8.242.16:5060		
Proxy Host:	10.8.242.16:5060		
Messaging Server Host:	192.168.10.10:0		
Outbound Proxy Host:			

Registrar Servers		
Gateway	Gateway Specific	Registrar Host
default	No	192.168.0.10:0

Messaging Servers		
Gateway	Gateway Specific	Messaging Server Host
default	No	192.168.10.10:0

Proxy Servers			
Gateway	Gateway Specific	Proxy Host	Outbound Proxy Host
default	No	192.168.0.10:0	0.0.0.0:0

Keep Alive	
Keep Alive Method:	SIP OPTIONS
Keep Alive Interval (s):	10
Keep Alive Destination:	First SIP Destination

Keep Alive Destination	
Gateway	Alternate Destination
default	192.168.0.10:0

Apply

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**.

The screenshot shows the Mediatrix WBM interface with the 'SIP' tab selected. The 'Transport' sub-tab is active, displaying configuration for General Configuration and Protocol Configuration. The 'Add SIP Transport in Registration' and 'Add SIP Transport in Contact Header' fields are set to 'Enable'. The 'Persistent Base Port' is '16002', 'Fallback Interval' is '15', 'TLS Certificate Trust Level' is 'Locally Trusted', and 'TCP Connect Timeout' is '10'. The 'Protocol Configuration' table shows 'UDP' set to 'Disable' and 'TCP' set to 'Enable'. An 'Apply' button is at the bottom right.

General Configuration	
Add SIP Transport in Registration:	Enable
Add SIP Transport in Contact Header:	Enable
Persistent Base Port:	16002
Fallback Interval:	15
TLS Certificate Trust Level:	Locally Trusted
TCP Connect Timeout:	10

Protocol Configuration					
UDP	UDP QValue	TCP	TCP QValue	TLS	TLS QValue
Disable		Enable		Disable	

Apply

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

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

Click **Apply**.

