A MITEL
PRODUCT
GUIDE

OpenScape Business V3

Microsoft Teams Interworking

SIP Trunking and Gateway / Trusted external User

- AudioCodes SBC
- anynode SBC

Mitel
Powering connections

Definitions

HowTo

A HowTo describes the configuration of a feature within the administration of the OpenScape Business. It addresses primarily trained administrators.

Tutorial

Within the tutorials procedures for installation, administration and operation of specific devices, applications or 3rd party systems, which are connected to the system, are described. The tutorial addresses primarily trained administrators.

Table of Contents

Table of History

Date	Version	Changes
2020-08-10	1.0	initial version
2021-01-26	1.1	chapt. 2.2: additional options to pair the SBC to the Direct Routing chapt. 4.2: adding trunk lines to SIP interconnection chapt. 6.1: payload issue might require to activate the flag" always use DSP" for the MS Teams Route
2021-06-22	1.2	chapt. 5: add "Busy Signaling" and "Parallel Ringing", update "Call Transfer"
2021-07-20	1.3	add "anynode SBC" rework chapter 2 "Direct Routing"
2021-12-06	1.4	add "Trusted external User" configuration up from OpenScape Business V3R1 FR2
2022-05-24	1.5	add: best practise, WAN restriction
2023-06-14	1.6	add: general security hint
2024-09-16	1.7	editorial changes

***Disclaimer**:*

AudioCodes Branding, Pictures and Icons in this document might be under copyright of AudioCodes.

anynode Branding, Pictures and Icons in this document might be under copyright of anynode.

Microsoft Teams Branding, Pictures and Icons in this document might be under copyright of Microsoft. Please confirm with Microsoft site https://learn.microsoft.com/en-us/microsoftteams/direct-routing-plan#microsoft-365-office-365-and-office-365-gcc-environments the resolution of the Microsoft FQDNs for "Microsoft 365, Office 365, and Office 365 GCC environments" because they are susceptible to change by Microsoft.

The Microsoft Teams, AudioCodes and anynode examples in this document give a rough overview of needed components in a basic setup and need individual verification for customers need.

Settings and configuration might change due to different Software versions.

For detailed information and needed Software and Hardware requirements for Microsoft Teams, licenses resp. license bundles and administration of Microsoft Teams please contact Microsoft or your Microsoft Integration Partner.

Please note:

Unify offers voice interworking capabilities with Microsoft Teams with a technical description of how to configure the OpenScape Business. Microsoft Teams, AudioCodes SBC, anynode SBC and any other Microsoft certified SBC are 3rd party products.

UNIFY doesn´t deliver any administration services for Microsoft Teams. This is up to the responsibility of the Microsoft Integration Partner.

References

[1] Microsoft Teams
https://docs.microsoft.com/en-us/MicrosoftTeams/teams-overview

https://docs.microsoft.com/en-us/MicrosoftTeams/direct-routing-landing-page

[2] AudioCodes Mediant 800B
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

[3] OpenScape Business, Installation Guide

[4] OpenScape Business, Administrator Documentation

[5] OpenScape Business, Tutorial VoIP Interfaces
http://wiki.unify.com/images/8/8c/How_To_Configure_LAN_WAN_Interface_for_VoIP.pdf

[6] Certification Test Report:
Microsoft Teams & AudioCodes SBC with Unify OpenScape Business V3

[7] Certification Test Report:
Microsoft Teams & anynode SBC with Unify OpenScape Business V3

[8] Anynode SBC
https://www.anynode.de/, https://www.youtube.com/user/TESYSTEMS/featured, https://docs.anynodesbc.com/

1. Introduction

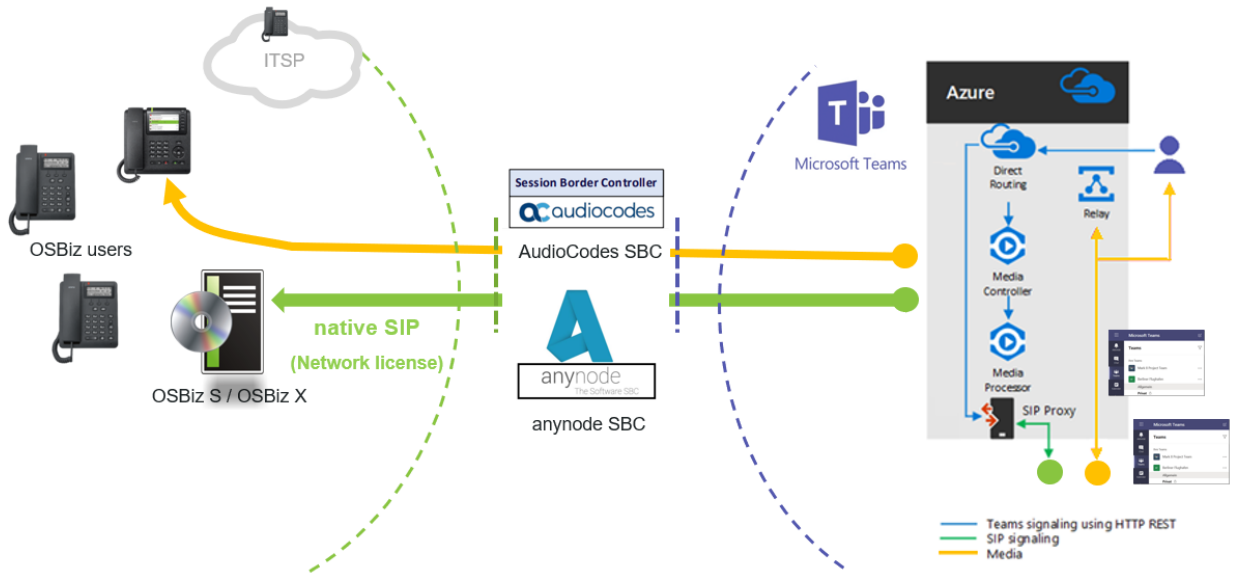
OpenScape Business V3 complements MS Teams with powerful telephony capabilities such as Call Centers, AutoAttendant, DECT, etc.

OpenScape Business (OSBiz) supports "Microsoft Teams Interworking" via native SIP trunking towards a Microsoft certified SBC for Direct Routing and requires a **Networking license and** a valid **Software Support license**.

Direct Routing allows the integration of MS Teams infrastructure into existing on-premise telephony system. MS 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 [1].

Certified SBCs are:

- AudioCodes Mediant 800B [2]
- anynode SBC [8]



Gateway scenario: MS Teams Interworking via Direct Routing with Office 365

Overview of **Office 365 Licenses** which can be obtained to use Direct Routing with a certified SBC and OpenScape Business (status August 2020 – source: Microsoft):

License	Add-on
Microsoft 365 / Office 365 Enterprise E5	
Microsoft 365 / Office 365 Enterprise E3 / E1	Phone System

or

1.1. General Configuration overview

The configuration examples of this document are based on Certification Test Report: Microsoft Teams & AudioCodes SBC with Unify OpenScape Business V3 [6] and may differ if another certified SBC is in use. For further details please refer to this Certification Test Report.

The prerequisites for Direct Routing are:

1. MS Teams users of Direct Routing must have the following licenses assigned in Microsoft 356 / Office 365: *Microsoft 365 / Office 365 Enterprise E3 / E1 (including SfB Online Plan2, Exchange Plan2, and Teams) + Phone System licenses or Microsoft 365 / Office 365 Enterprise E5 (including SfB Online Plan2, Exchange Plan2, Teams, Phone System and Audio Conferencing)*.

2. MS 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.

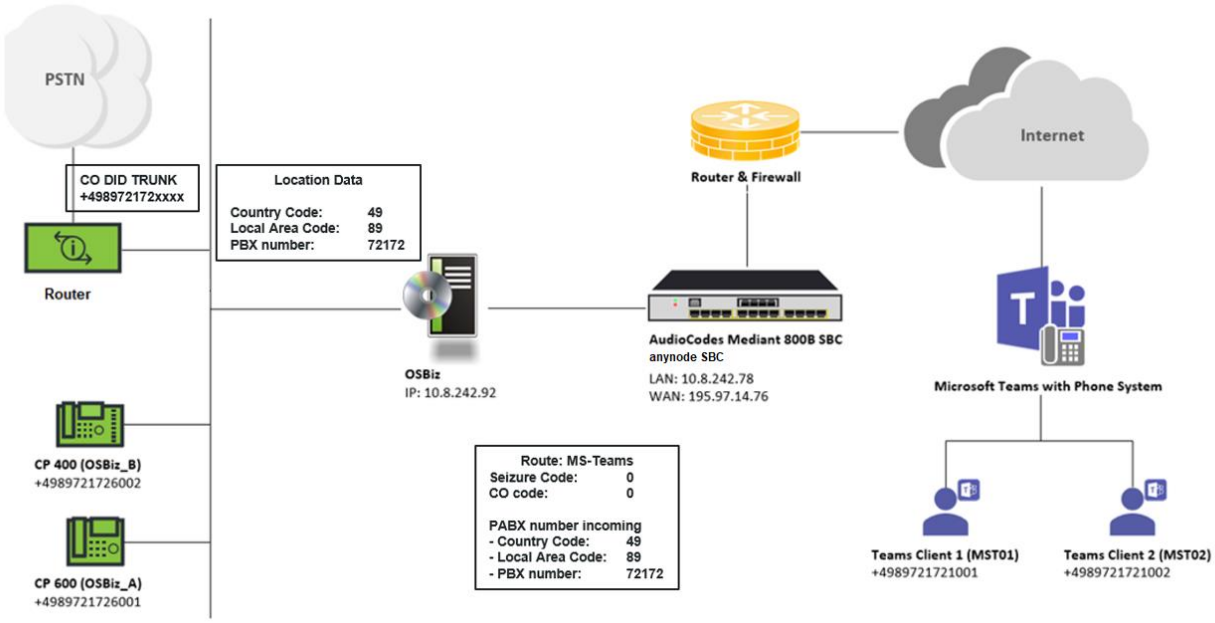
In example environment, Office 365 E5 licenses are available, which are applied to the Teams test users:

- MST01@M365x316382.onmicrosoft.com with phone number +4989721721001
- MST02@M365x316382.onmicrosoft.com with phone number +4989721721002

The AudioCodes M800B, Teams certified SBC, is connected via internet with public IP 195.97.14.76 and public FQDN sbc01.athdrlabs.xyz to Microsoft Phone System in Microsoft Office 365 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 OpenScape Business. Proper firewall rules in SBC are configured for SIP and RTP traffic (see in detail sub-section 3.13).

The MS Teams tenant SIP trunk connectivity to AudioCodes SBC is tested with and without Media Bypass. In a nutshell, with media bypass activated the media is kept directly between the Teams client and the SBC (WAN interface), 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).



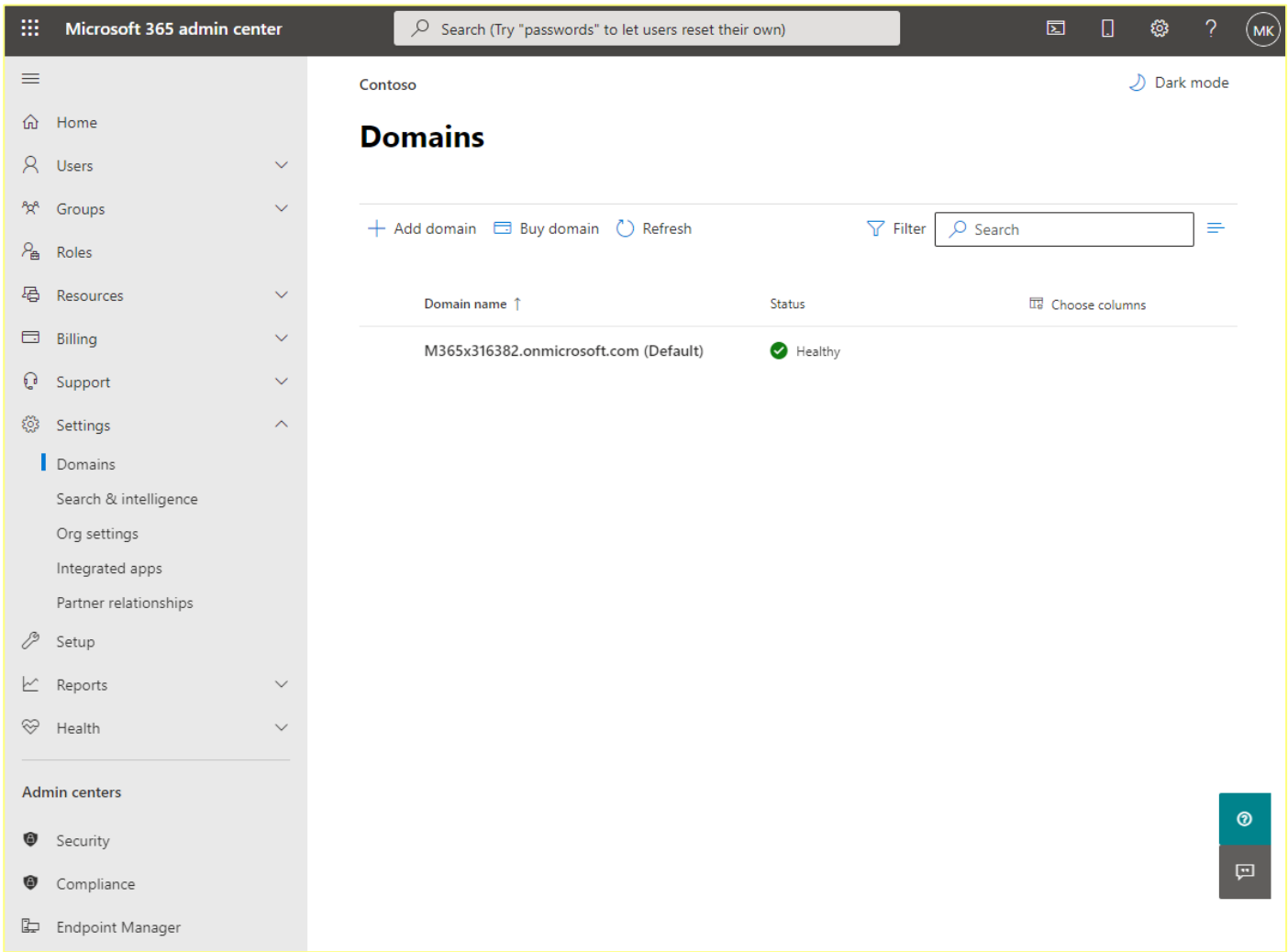
2. Direct Routing

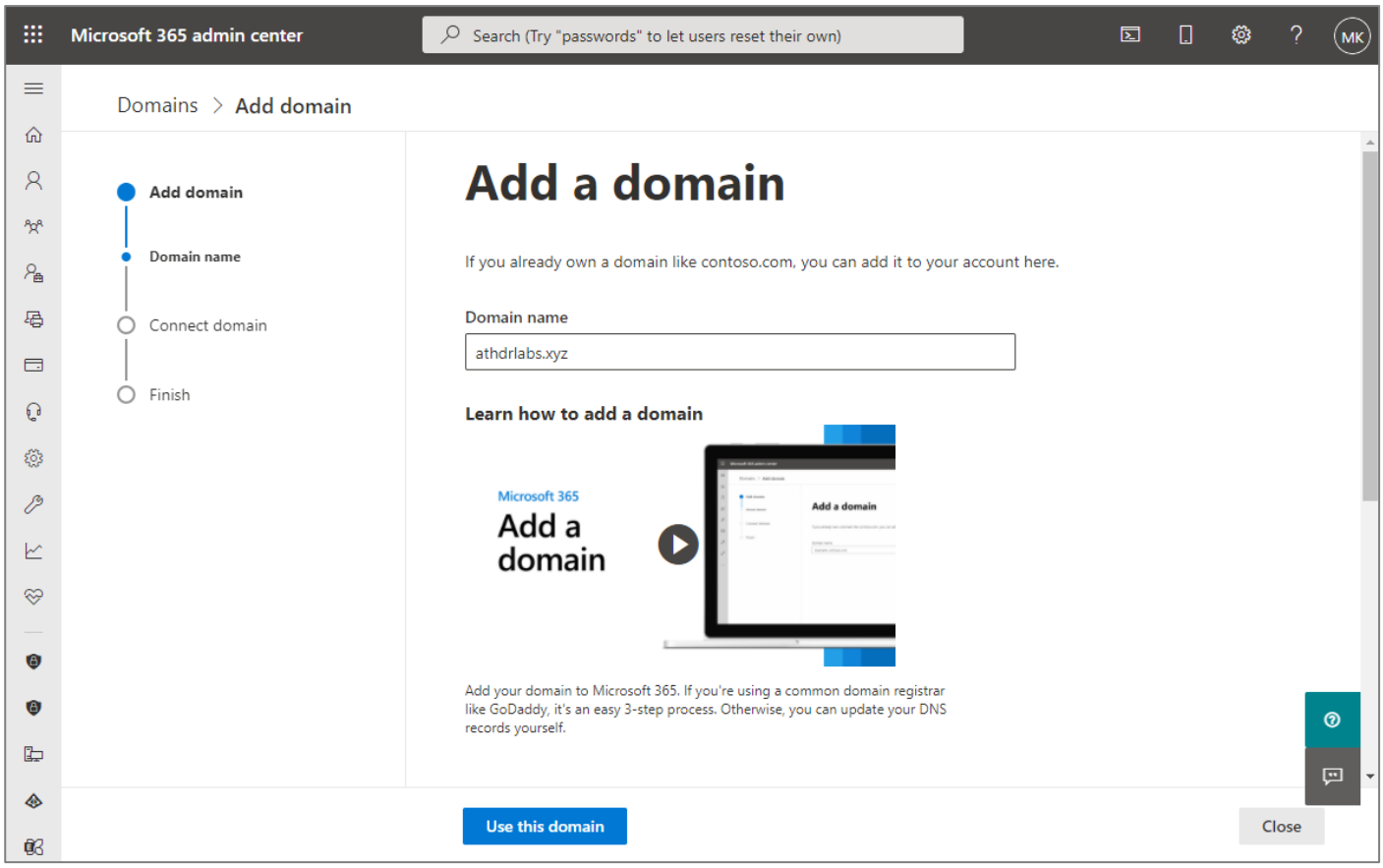
The current section summarizes the example configuration on Microsoft Office 365 tenant for the Direct Routing connection with an AudioCodes or anynode SBC, based on the according certifaction results [6] & [7]. Default or non-project specific Office 365 tenant configuration will not be referenced in subsequent paragraphs.

2.1. Setup the Domain

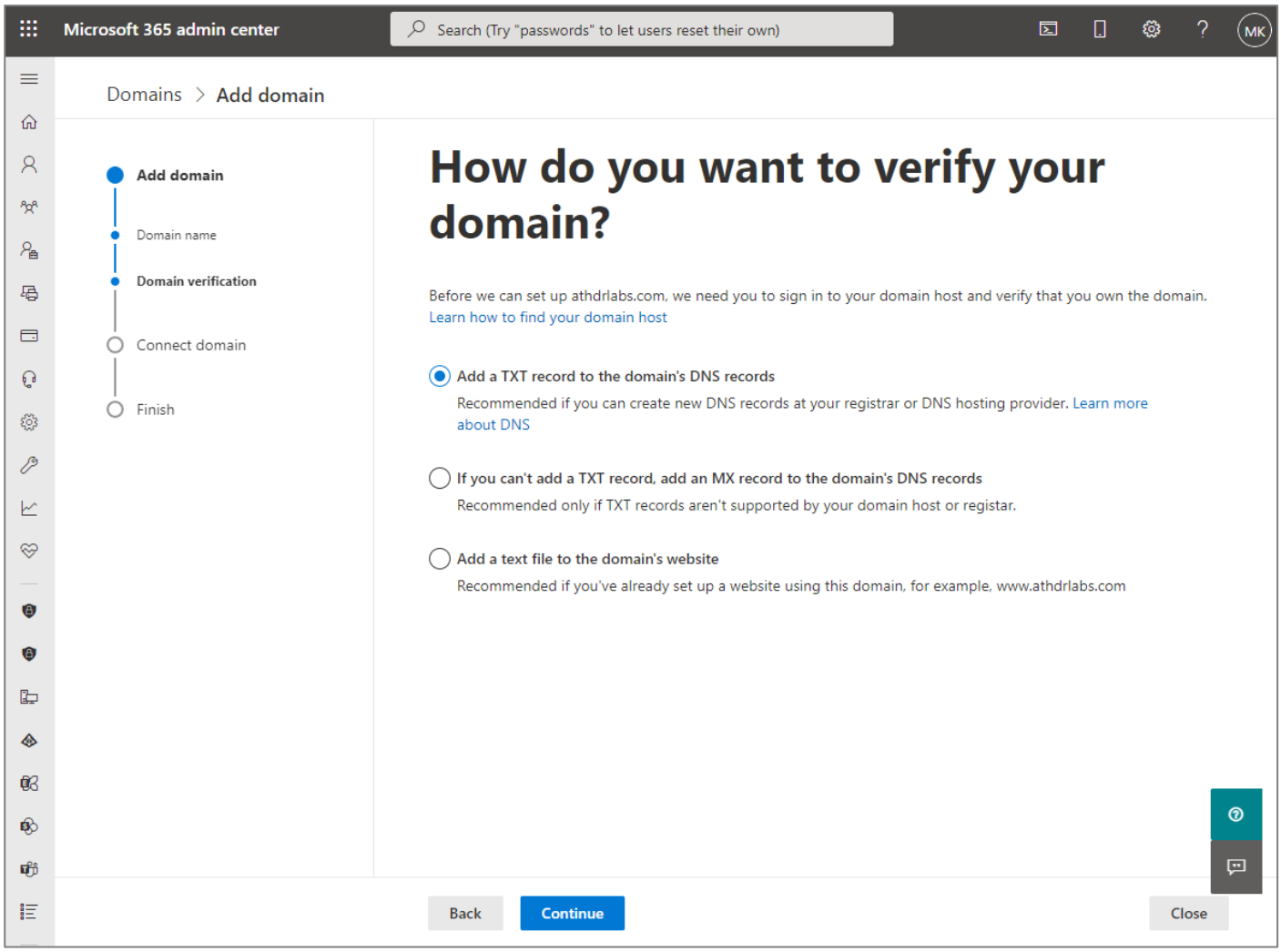
This subsection outlines how to add the SBC domain to the tenant.

Go to O365 portal, select on the left menu Setup >> Domain and click on "Add domain".

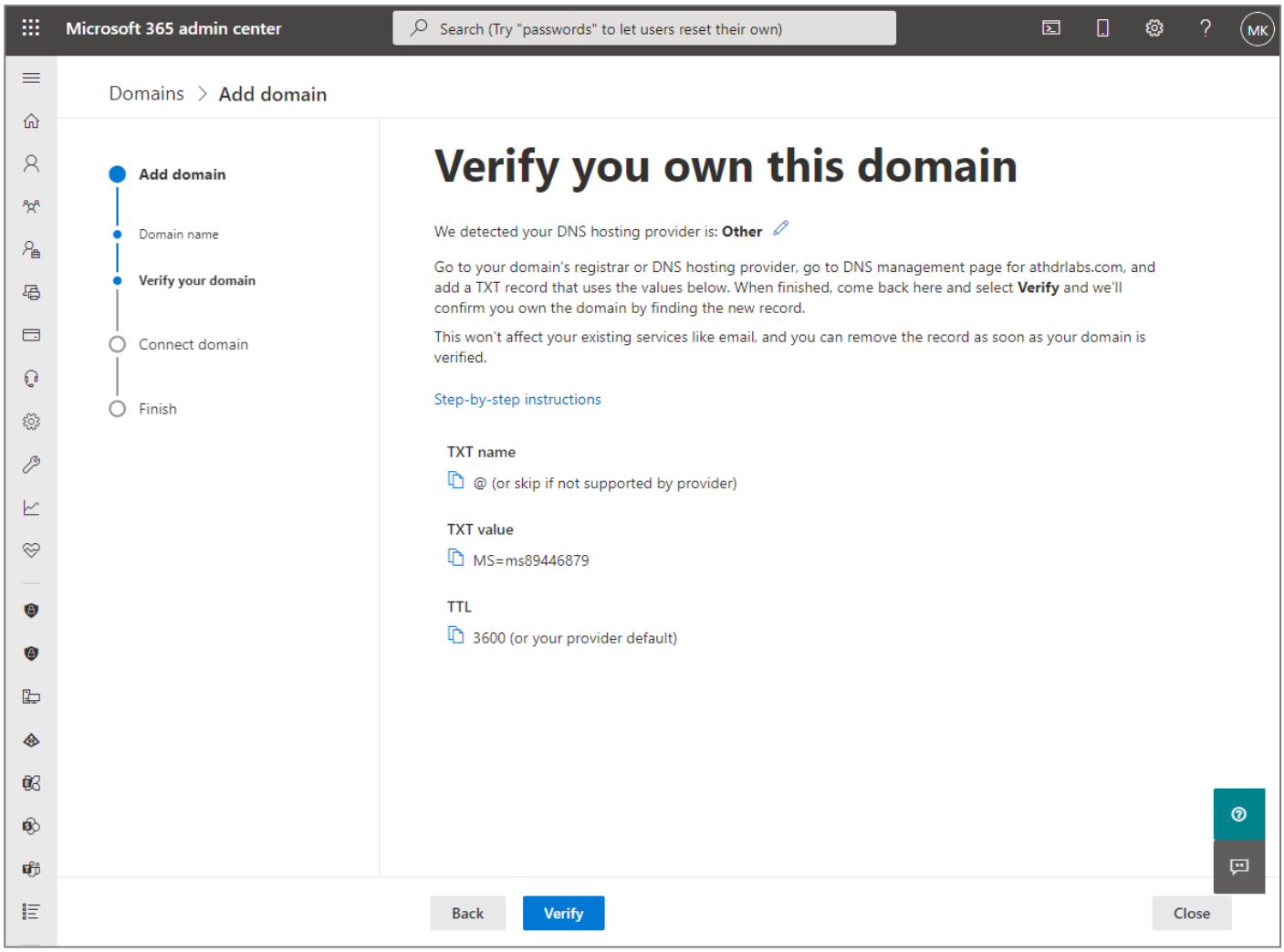




Enter the SBC domain name, e.g. "athdrlabs.xyz" in **"Enter a domain you own"** box.
Click on **[Use this domain]**.

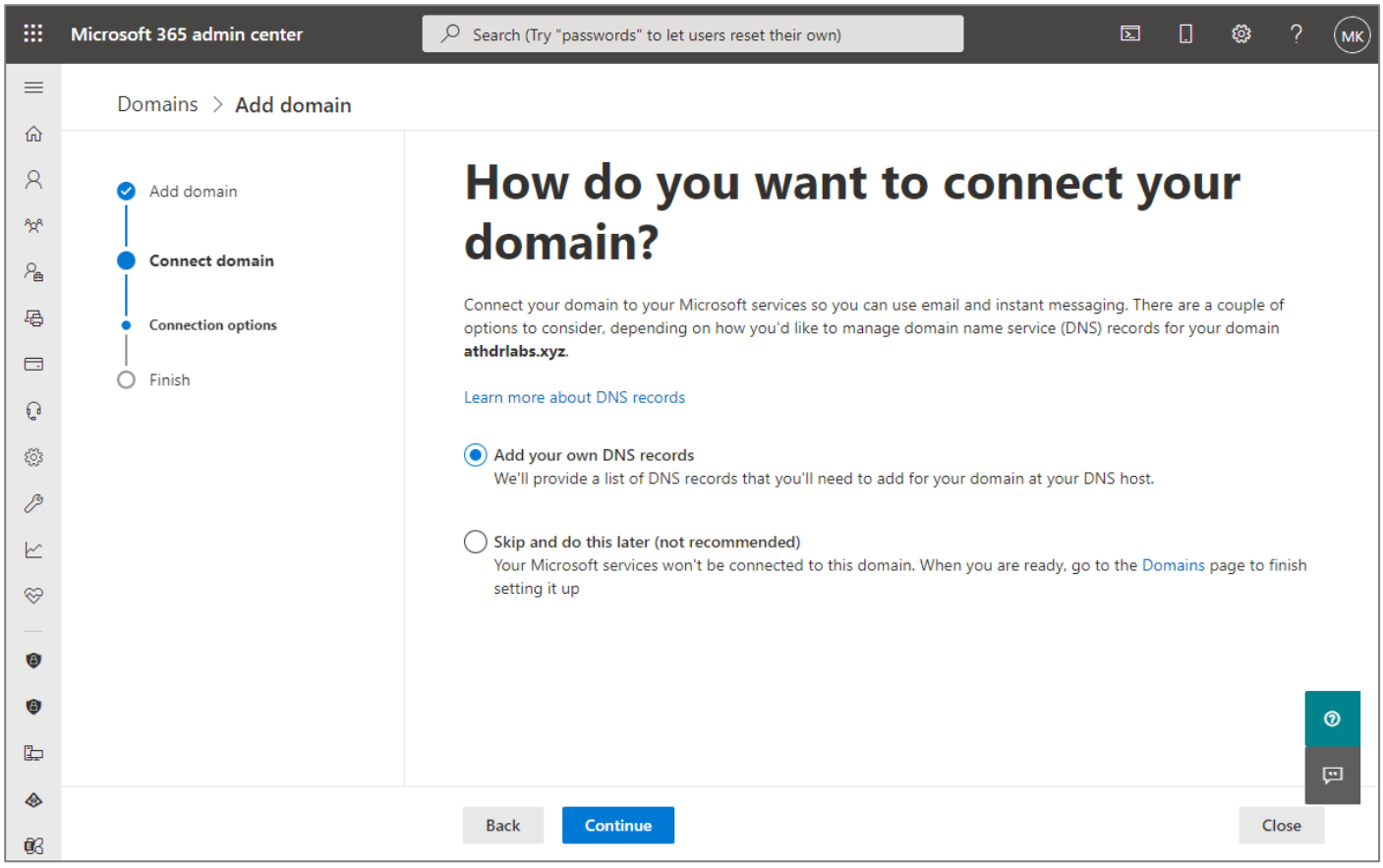


Select "Add a TXT record to the domain's DNS records" and click on **[Continue]**.



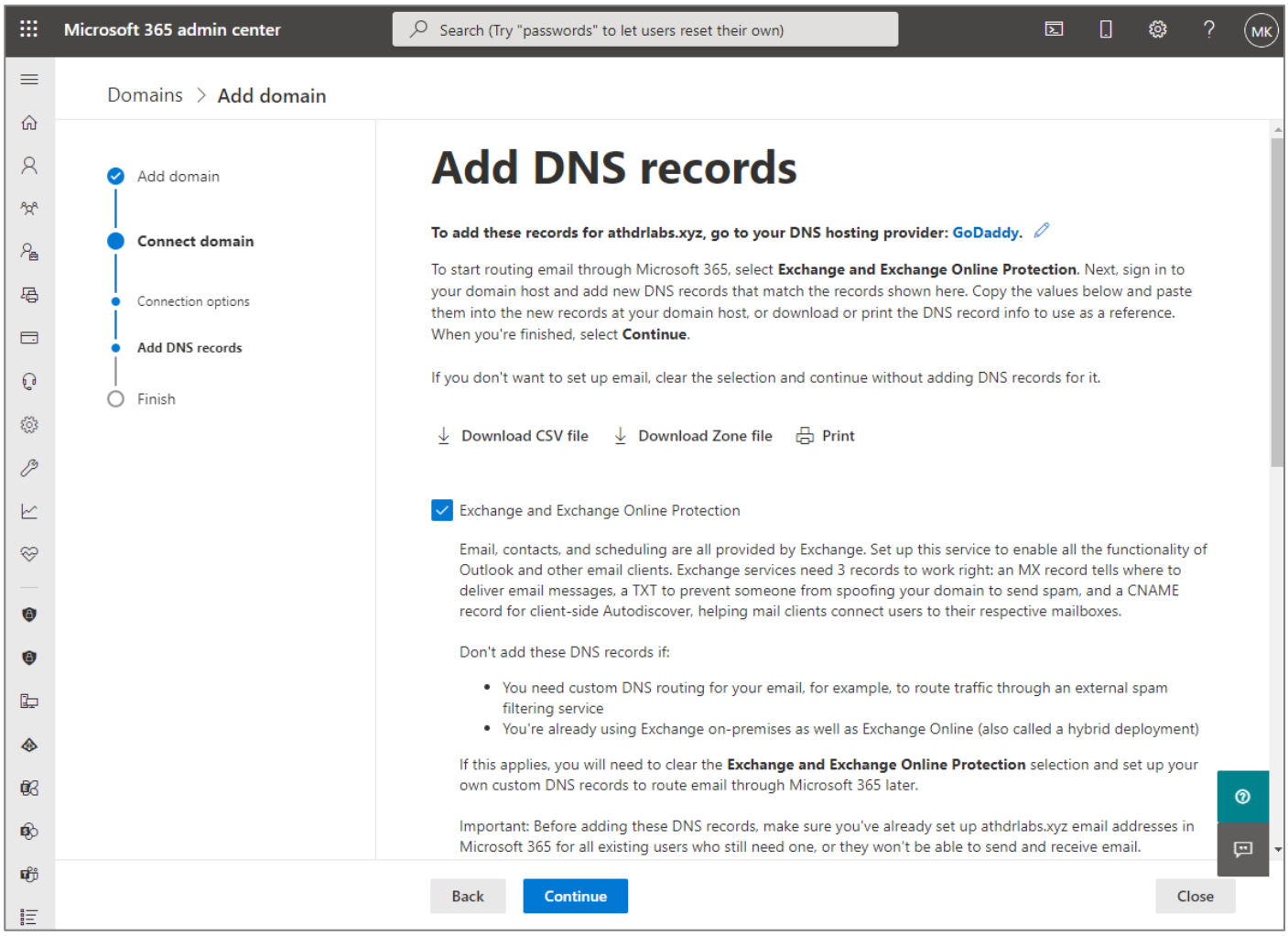
Copy-paste this screen and contact corresponding DNS domain owner to validate domain ownership.

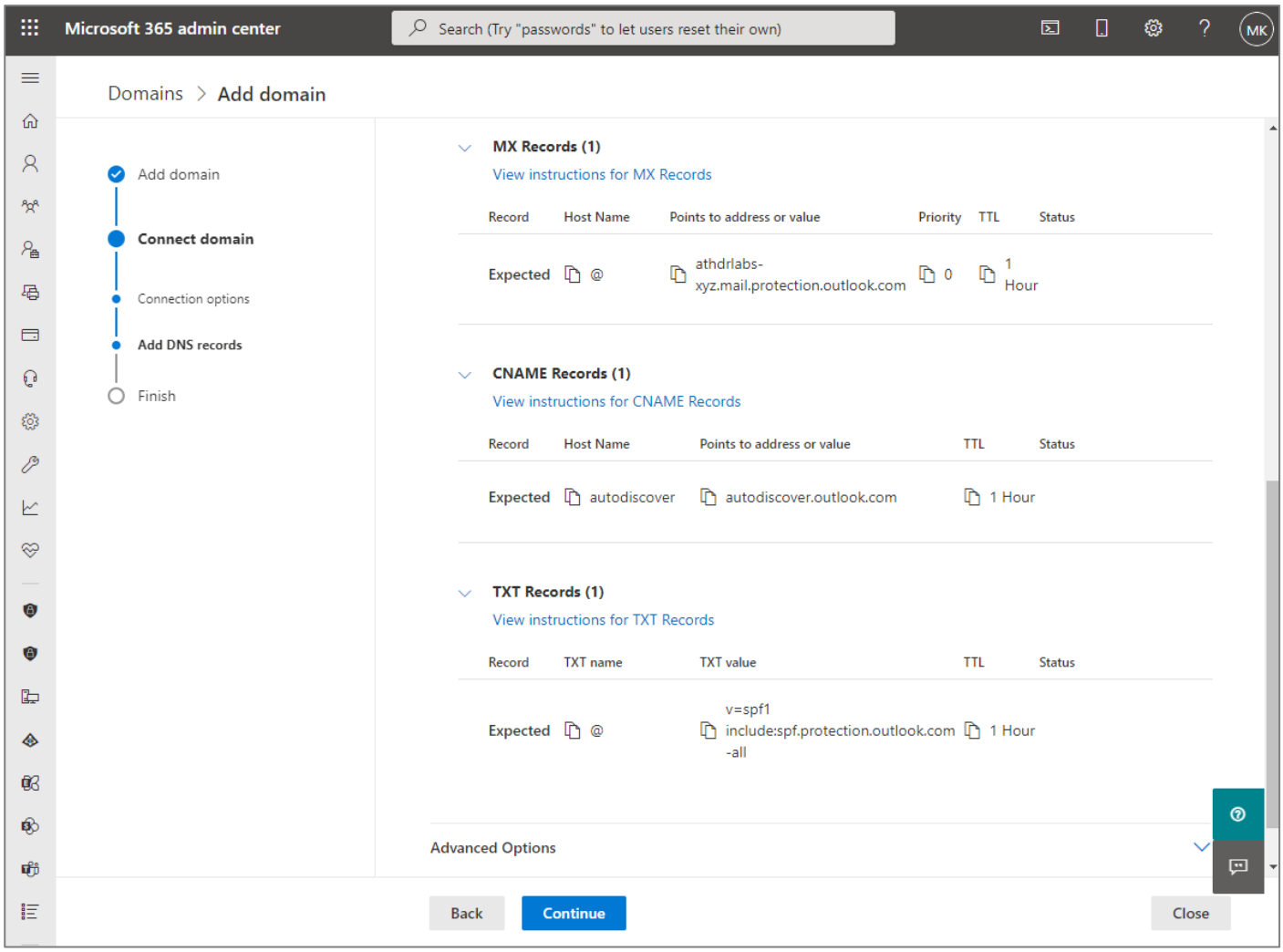
When the confirmation that the TXT value e.g. "MS=ms89446879" verification is ready, go back to this domain set up and start the verification process.



Select "Add your own DNS records".

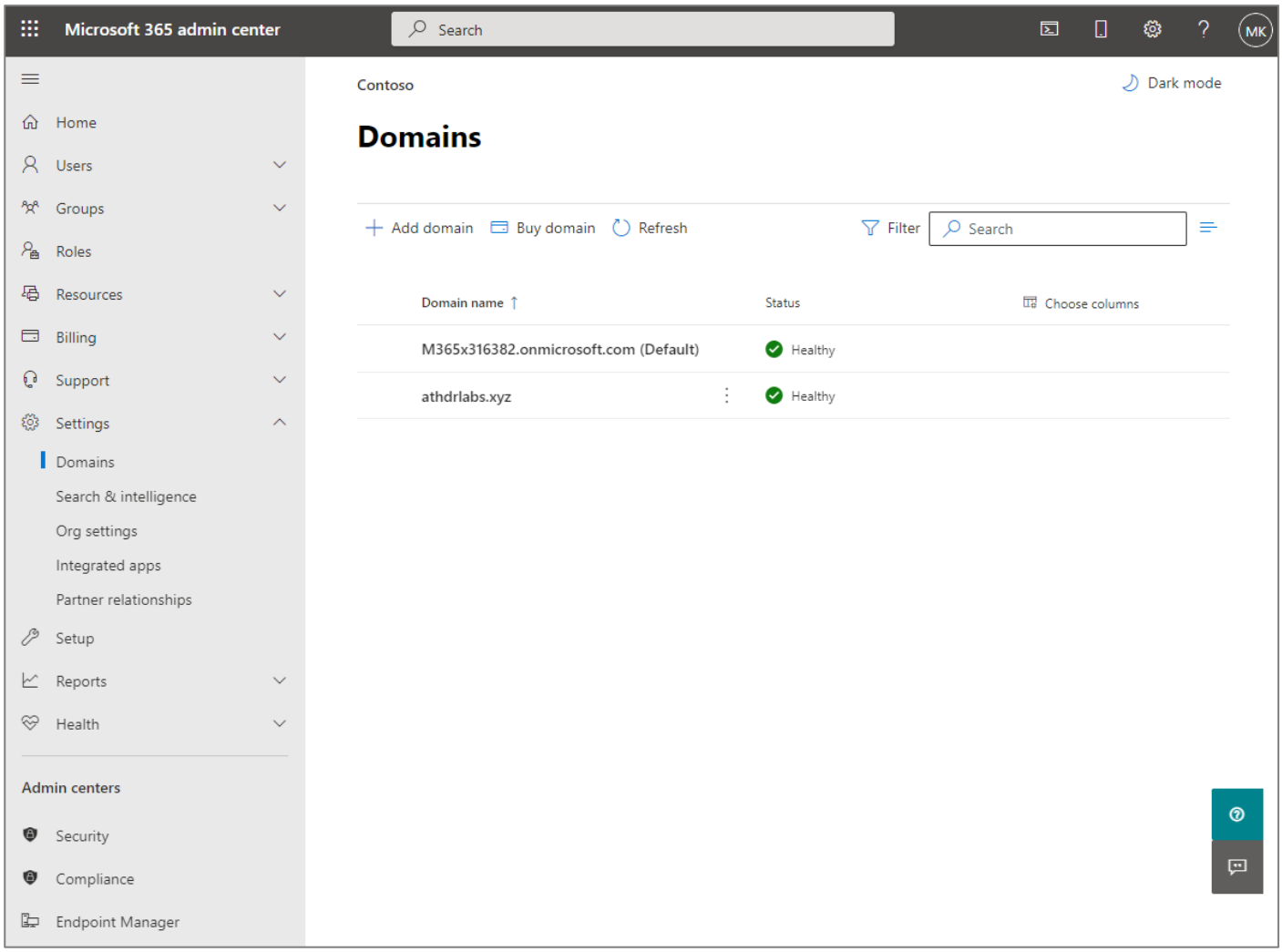
Click on **[Continue]**.


Microsoft 365 admin center
Search (Try "passwords" to let users reset their own)
MK
Domains > Add domain
Add domain
Connect domain
Connection options
Add DNS records
Finish
Add DNS records
To add these records for athdrlabs.xyz, go to your DNS hosting provider: GoDaddy.
To start routing email through Microsoft 365, select Exchange and Exchange Online Protection. Next, sign in to your domain host and add new DNS records that match the records shown here. Copy the values below and paste them into the new records at your domain host, or download or print the DNS record info to use as a reference. When you're finished, select Continue.
If you don't want to set up email, clear the selection and continue without adding DNS records for it.
Download CSV file
Download Zone file
Print
Exchange and Exchange Online Protection
Email, contacts, and scheduling are all provided by Exchange. Set up this service to enable all the functionality of Outlook and other email clients. Exchange services need 3 records to work right: an MX record tells where to deliver email messages, a TXT to prevent someone from spoofing your domain to send spam, and a CNAME record for client-side Autodiscover, helping mail clients connect users to their respective mailboxes.
Don't add these DNS records if:
You need custom DNS routing for your email, for example, to route traffic through an external spam filtering service
You're already using Exchange on-premises as well as Exchange Online (also called a hybrid deployment)
If this applies, you will need to clear the Exchange and Exchange Online Protection selection and set up your own custom DNS records to route email through Microsoft 365 later.
Important: Before adding these DNS records, make sure you've already set up athdrlabs.xyz email addresses in Microsoft 365 for all existing users who still need one, or they won't be able to send and receive email.
Back
Continue
Close



Contact the DNS hosting manager to add the *"Expected"* **"MX Records", "CNAME Records"** and **"TXT Records"**.

Once the procedure is finished return to O365 admin center at **Domains >> Add Domain** page and click on **[Continue]** to finish the configuration.



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 and 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.

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

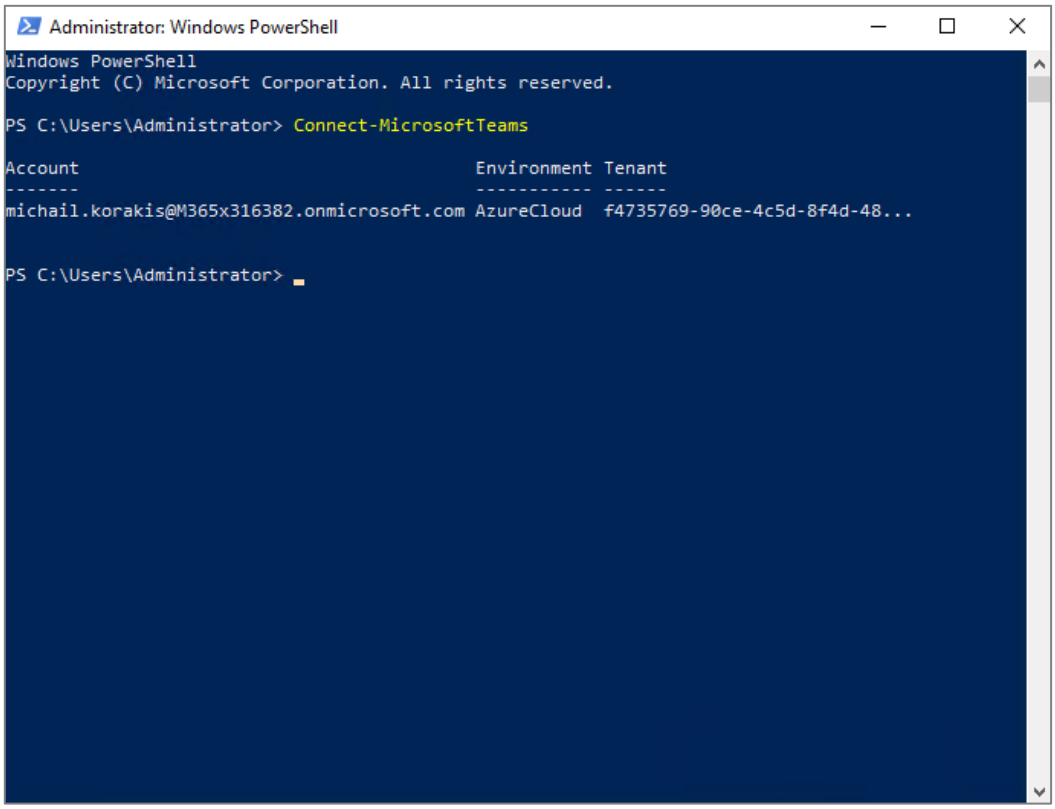
The SBC connection to Microsoft Phone System, routes and routing policies will be configured via PowerShell. Specifically, in the Skype for Business Online PowerShell.

To setup PowerShell in administrator's PC, follow this link: https://docs.microsoft.com/en-us/microsoftteams/teams-powershell-overview.

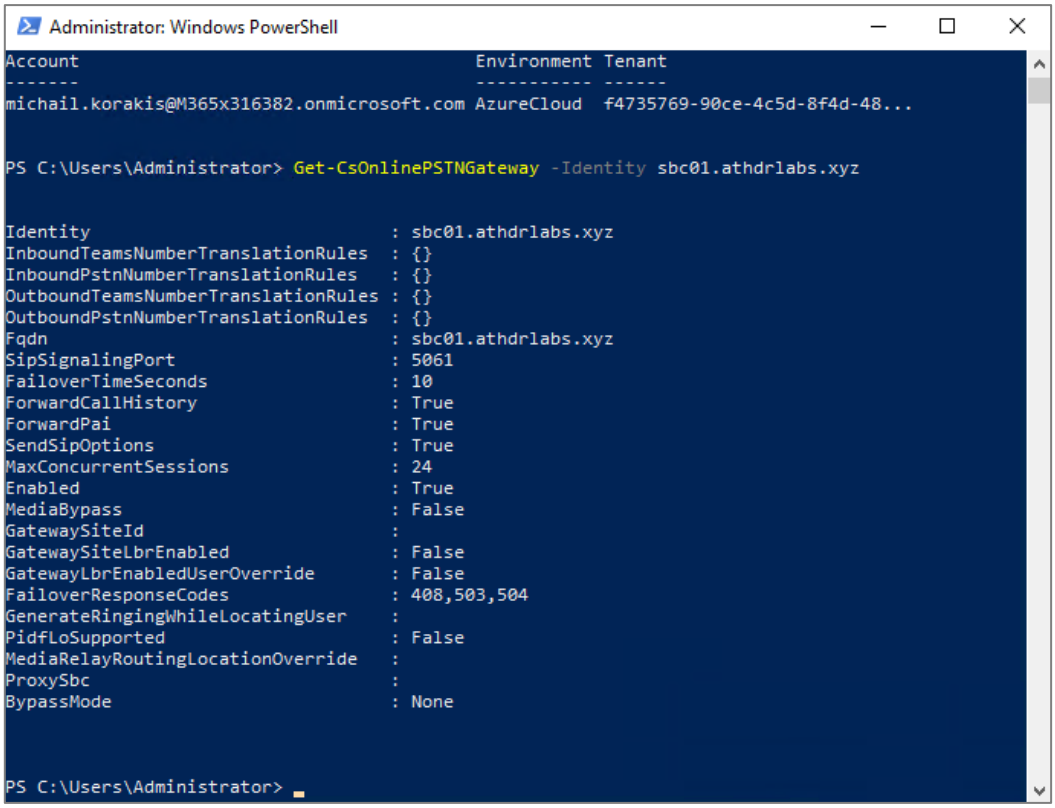
Once PowerShell in administrator's PC is setup, execute below command to connect to Teams:

Connect-MicrosoftTeams

Provide Teams tenant admin credentials to log in.



Create and pair the SBC SIP trunk in Teams tenant.



Run e.g. the command:

New-CsOnlinePSTNGateway -Identity sbc01.athdrlabs.xyz -SipSignalingPort 5061 -ForwardCAllHistory $true -ForwardPAI $true -MediaBypass $false -MaxConcurrentSessions 10 -Enabled $true

Parameters that affect current certification:

- **ForwardCallHistory** True or False. If enabled, MS Phone System sends two SIP headers: History-info and Referred-By (see chapter 6 for call forwarding).
- **ForwardPai** True. It should be handled by the SBC (see chapter 6 for name and number display).
- **MediaBypass** True or False, depending on the customer requirements for media optimization.

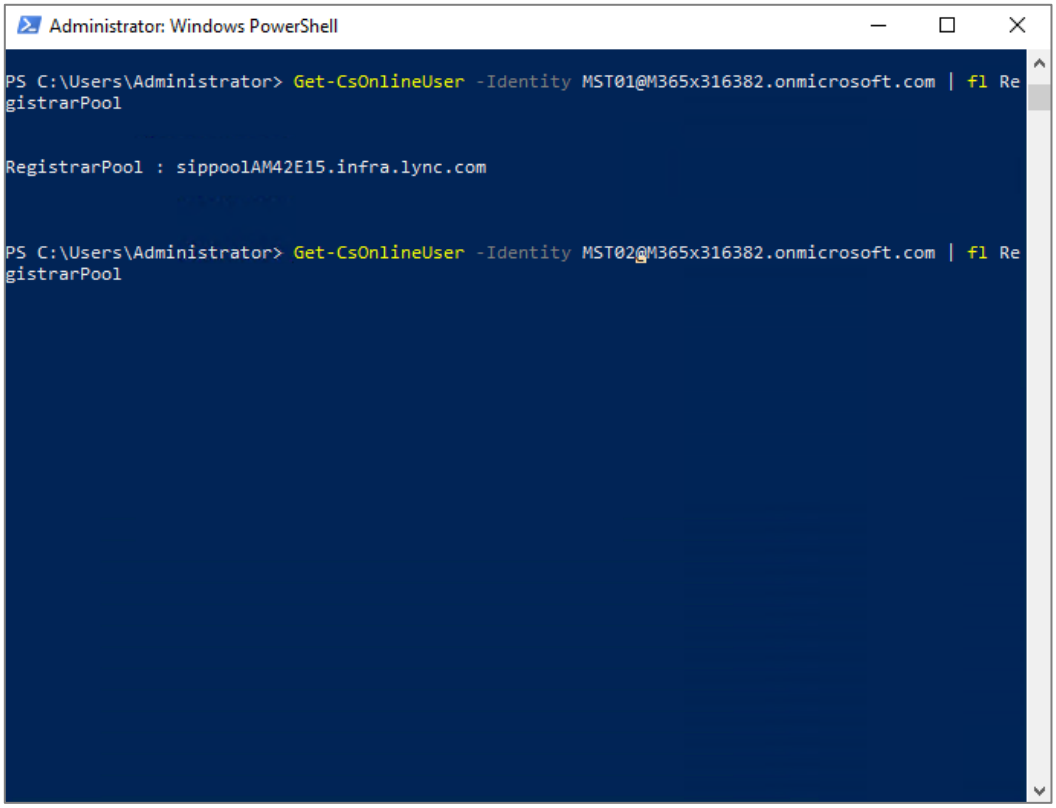
View the newly created *"Online PSTN Gateway"* (SIP trunk) with the command:

Get-CsOnlinePSTNGateway -Identity sbc01.athdrlabs.xyz

Note: This configuration may partially be performed via Teams admin center GUI.

2.3. Enable users for Direct Routing Service

Ensure that the users are homed in Teams Phone System.



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:+ 4989721721001

Set-CsUser -Identity MST02@M365x316382.onmicrosoft.com -EnterpriseVoiceEnabled $true - HostedVoiceMail $true - OnPremLineURI tel:+ 4989721721002

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 MST02@M365x316382.onmicrosoft.com

Note: The users need to be assigned a proper **"Dial Plan"** that translates dialed phone numbers by an individual user into an alternate format (typically E.164) for purposes of call authorization and call routing. Teams dial plan configuration is out of scope of current document and in current certification activities the default Teams Phone System dial plan was utilized.

2.4. 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:

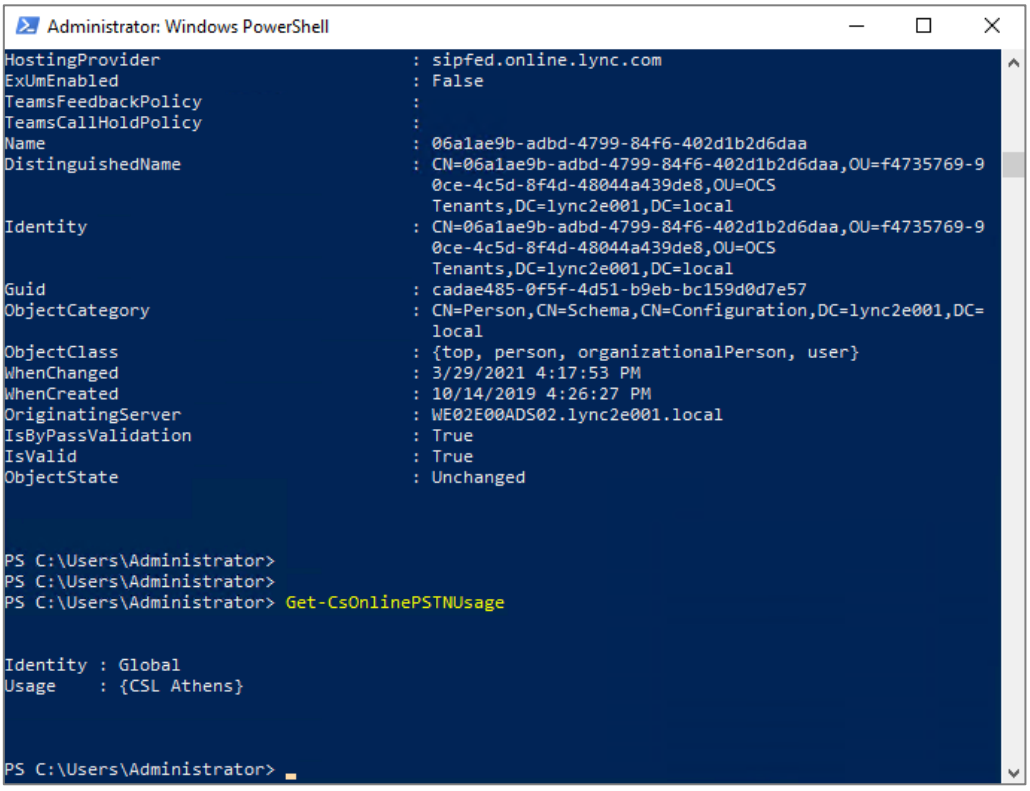
• **Voice Routing Policy** – container for PSTN Usages; can be assigned to a user or to multiple users.

• **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.

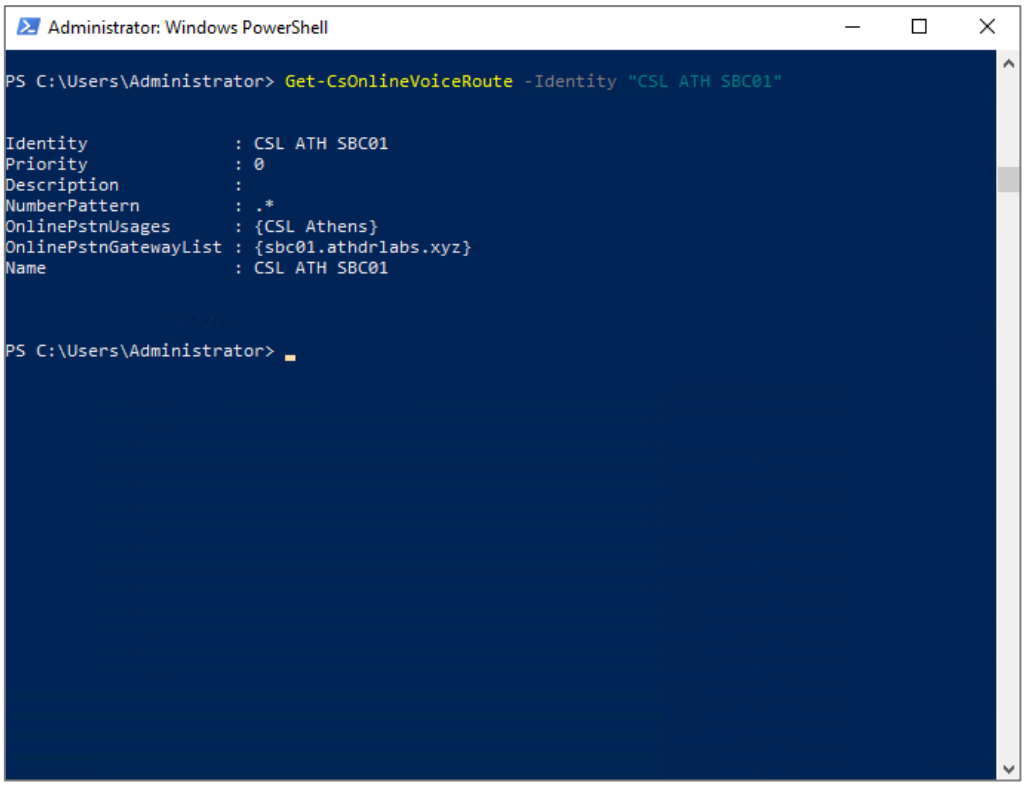
• **Online PSTN Gateway** - pointer to an SBC, also stores the configuration that is applied when call is placed via the SBC, such as forward P-Asserted-Identity (PAI) or Preferred Codecs; can be added to Voice Routes.

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.



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

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



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

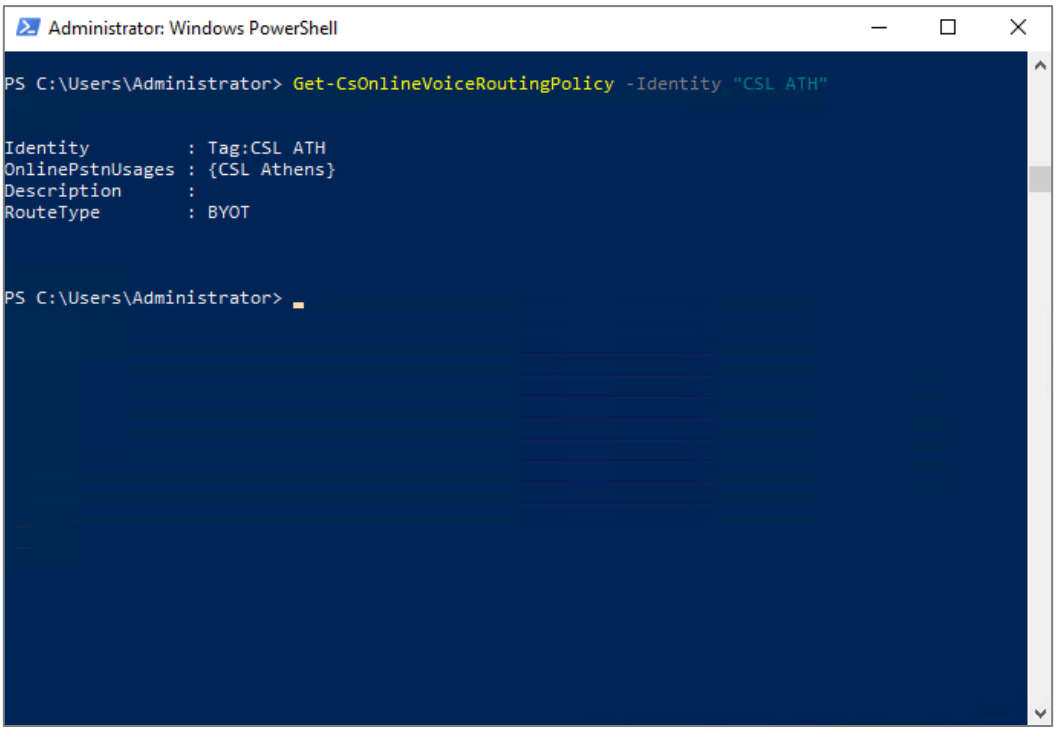
New-CsOnlineVoiceRoute -Identity "CSL ATH SBC01" -NumberPattern "^\+49(\d{8})$" -OnlinePstnGatewayList sbc01.athdrlabs.xyz -Priority 1 -OnlinePstnUsages "CSL Athens"

or

New-CsOnlineVoiceRoute -Identity "CSL ATH OSBiz" -NumberPattern "^\+49(89721726)(\d{3})$" -OnlinePstnGatewayList sbc01.athdrlabs.xyz -Priority 1 -OnlinePstnUsages "CSL Athens"

or

New-CsOnlineVoiceRoute -Identity "CSL ATH OSBiz" -NumberPattern "." -OnlinePstnGatewayList sbc01.athdrlabs.xyz -OnlinePstnUsages "CSL Athens"*



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

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

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

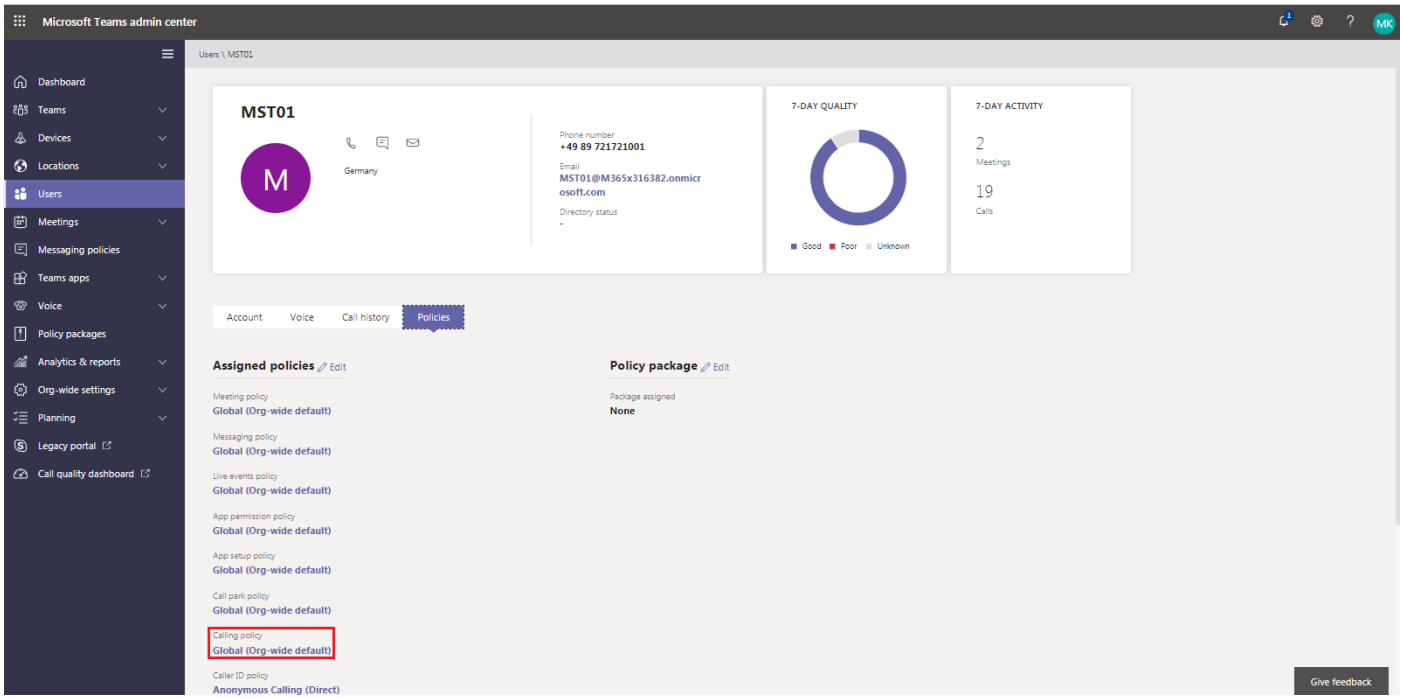
Grant-CsOnlineVoiceRoutingPolicy -Identity MST01@M365x316382.onmicrosoft.com -PolicyName "CSL ATH"

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

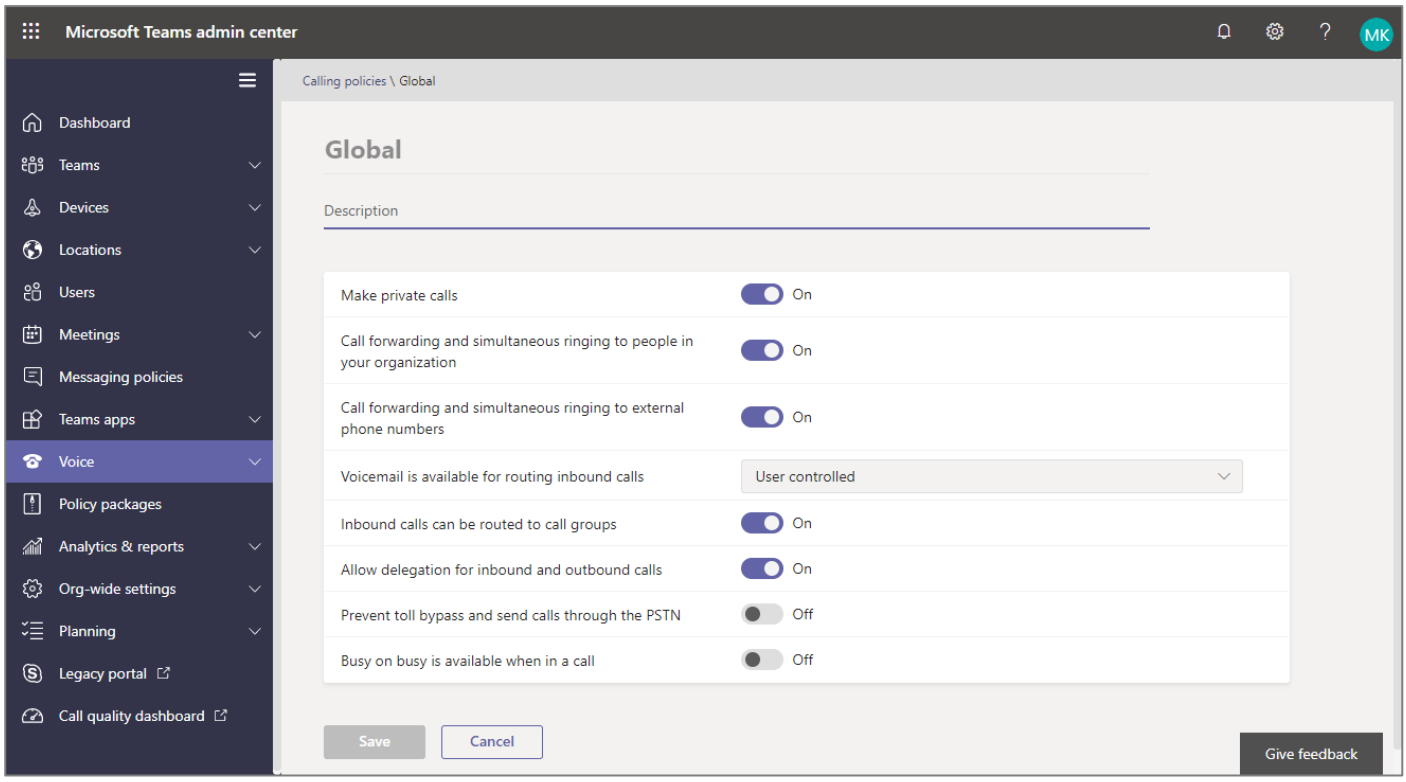
2.5. Designate to a user the ability to use calling functionality within Teams

The users in current testing activities have the Global policy assigned where calling functionality is enabled.

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



Click on **"Global (Org-wide default)"** under **"Calling Policies"** to view various policy options in order to make sure that calls are allowed (along with other features), as shown in the example below:

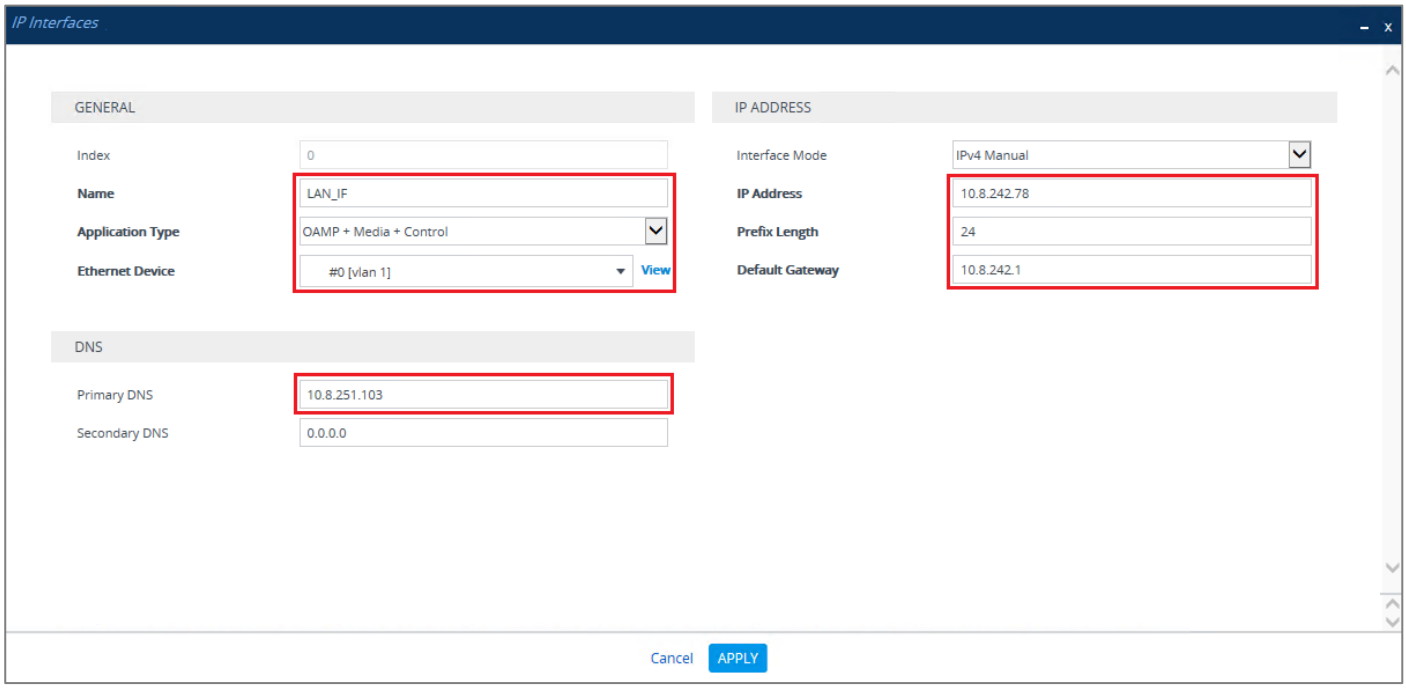


Note: Instead of Teams Admin Center, PowerShell may be used.

3. AudioCodes SBC

In this section the SBC configuration steps for Teams Direct Routing are described. More detailed information on M800B SBC configuration for Teams Direct Routing can be found at: https://www.audiocodes.com/media/13253/connecting-audiocodes-sbc-to-microsoft-teams-direct-routing-enterprise-model-configuration-note.pdf

3.1. LAN and WAN IP Interfaces

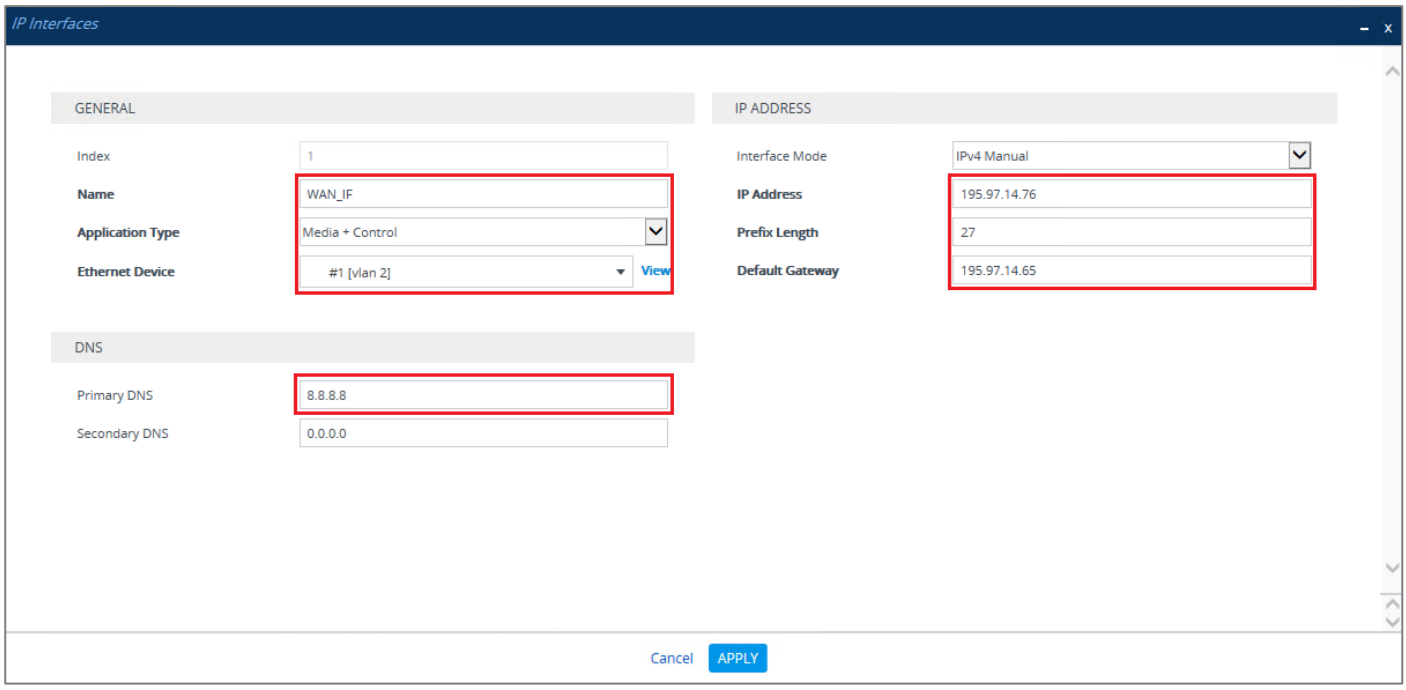


Go to: **SETUP** >> **IP NETWORK** >> **CORE ENTITIES** >> **IP Interfaces** and click on **[New].** To configure the LAN interface (faces to OpenScape Business), enter the following:

In the new window, the following fields need to be configured:

- **Name**: LAN_IF (LAN interface friendly name)
- **Application Type**: OAMP + Media + Control
- **Ethernet Device**: vlan 1 (dedicated VLAN for LAN interface to OSBiz)
- **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 on **[Apply]**



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

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

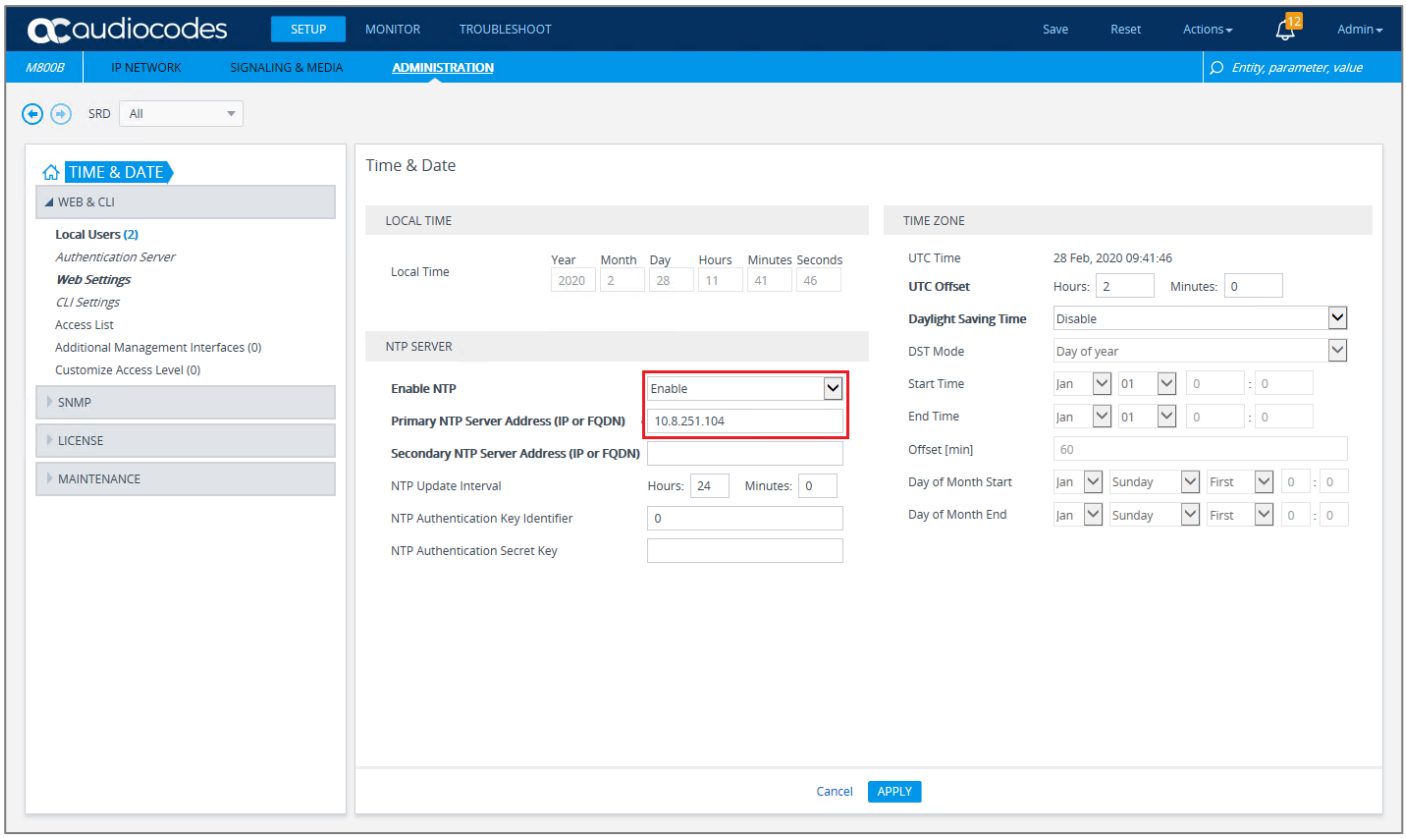
- **Name**: WAN_IF (WAN interface friendly name)
  Application Type: Media + Control (not recommended to activate OAMP i.e. SBC WBM on an interface pointing to internet)
- **Ethernet Device**: vlan 2 (dedicated VLAN for WAN interface to Teams)
- **Primary DNS**: 8.8.8.8 (any known public DNS or according 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 on **[Apply]**.

3.2. 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 Subject Alternative Name (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. It is important, that NTP Server will locate on the Operations, administration and management (OAMP) IP Interface (LAN_IF in our case) or will be accessible through it.

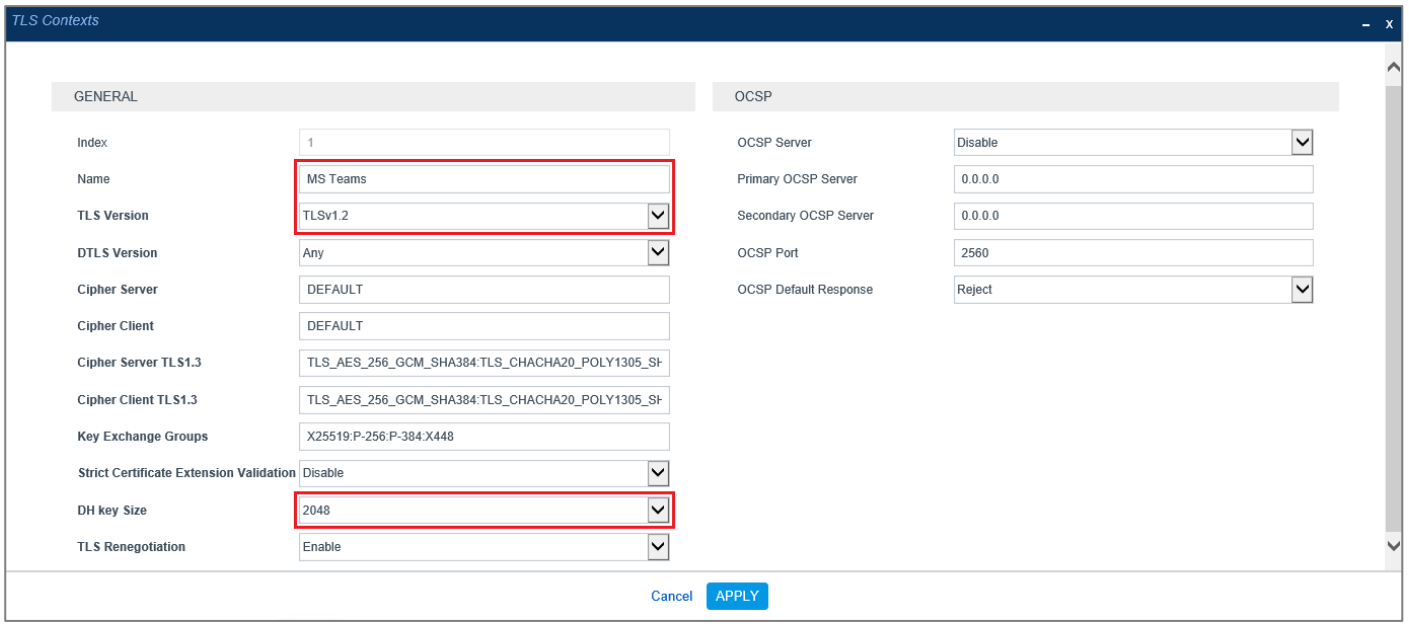


Navigate to: **SETUP >> ADMINISTRATION >> TIME & DATE** and enter the following:

- **Enable NTP:** Enable.
- **Primary NTP Server Address**: 10.8.251.104 (reachable from OAMP IP interface, i.e. LAN_IF interface).

Click on **[Apply]**.

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



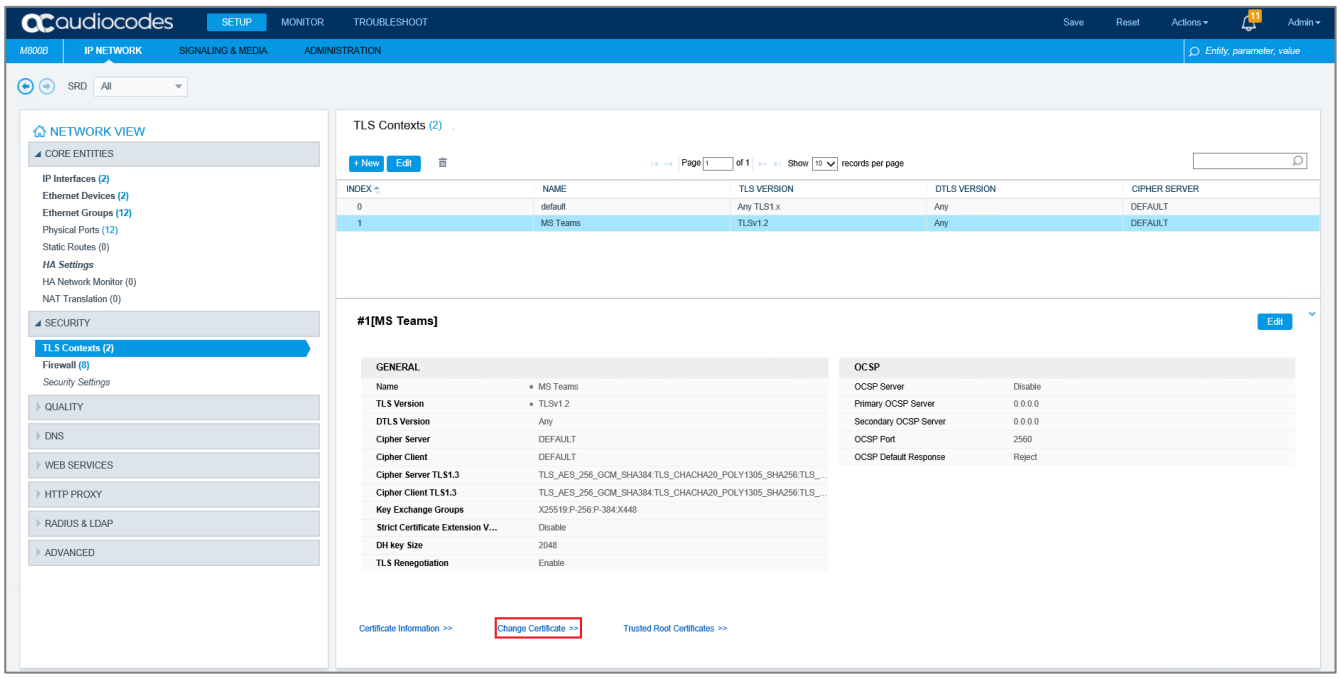
Go to: **SETUP** >> **IP NETWORK** >> **SECURITY** >> **TLS Contexts** and click on **[New]**.

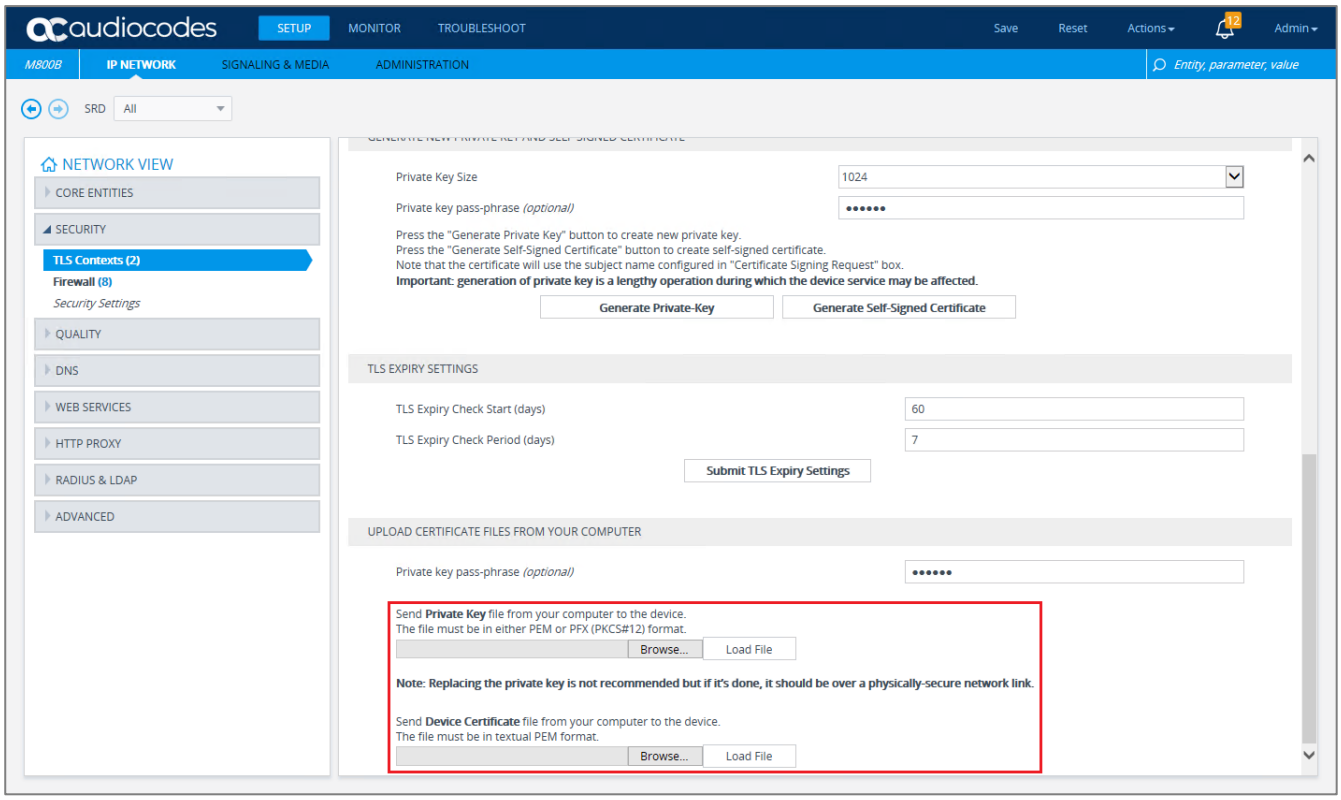
Enter the following:

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

Click on **[Apply]**.

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

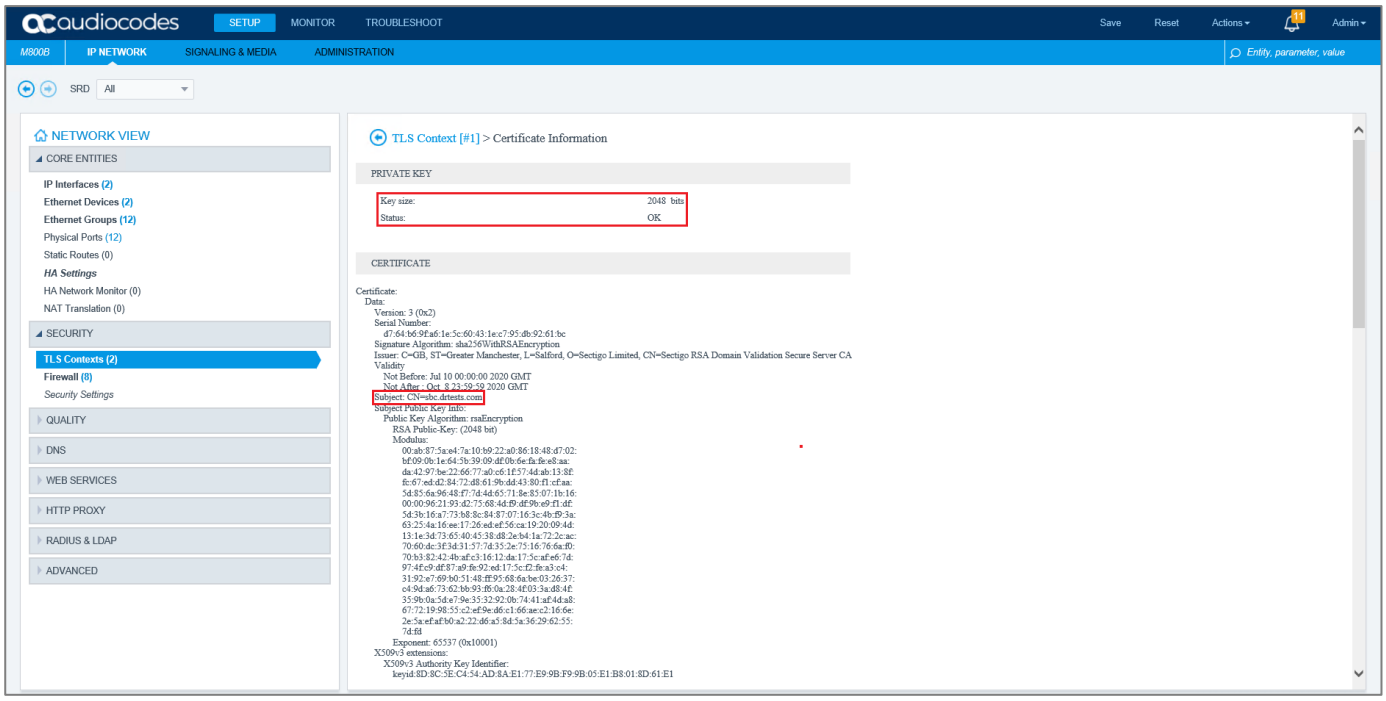




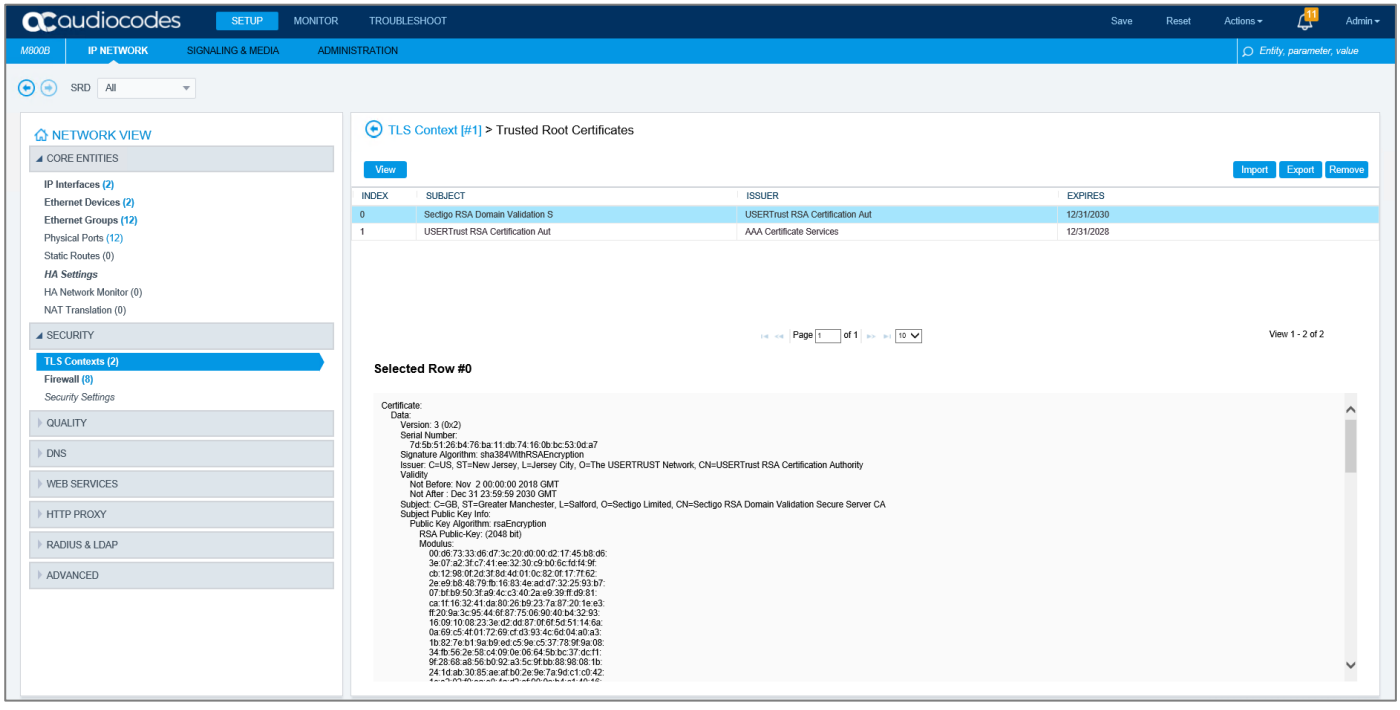
On **TLS Contexts** click on **Change Certificates** link and on the page that appears, scroll down and on **Upload Certificate Files from Your Computer** section, upload the privatekey.pem and certificate.pem files, provided by the CA.

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



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



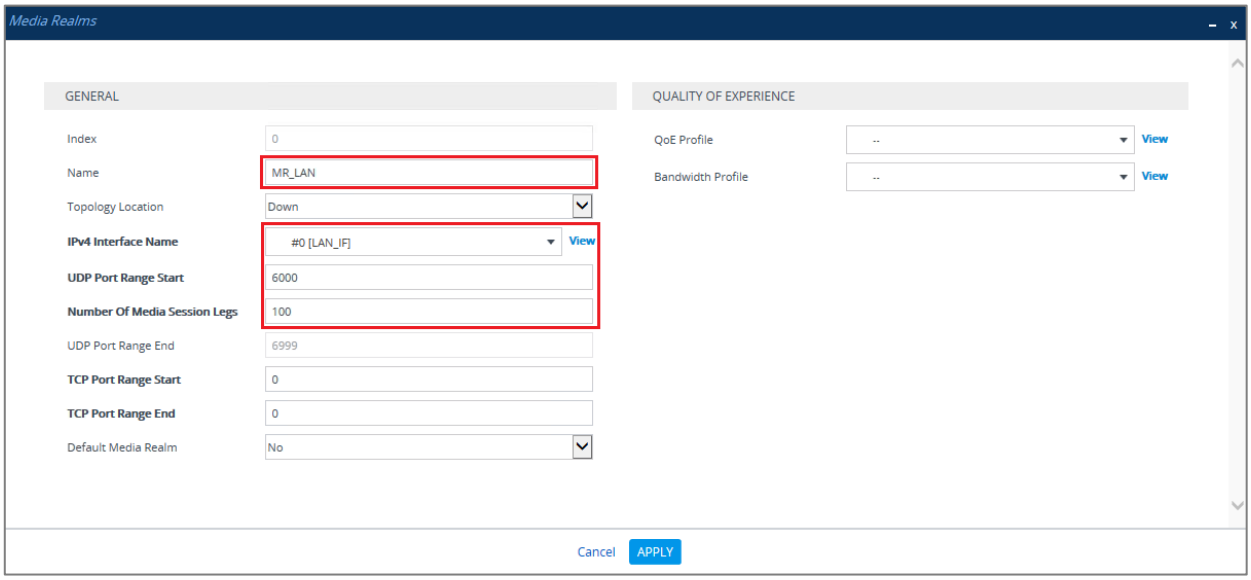
Return to the **TLS Contexts page**, select the required TLS Context index row, and then click the **Trusted Root Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.

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

Click on **[OK]**; the certificate is loaded to the device and listed in the Trusted Certificates store.

3.3. Media Realms

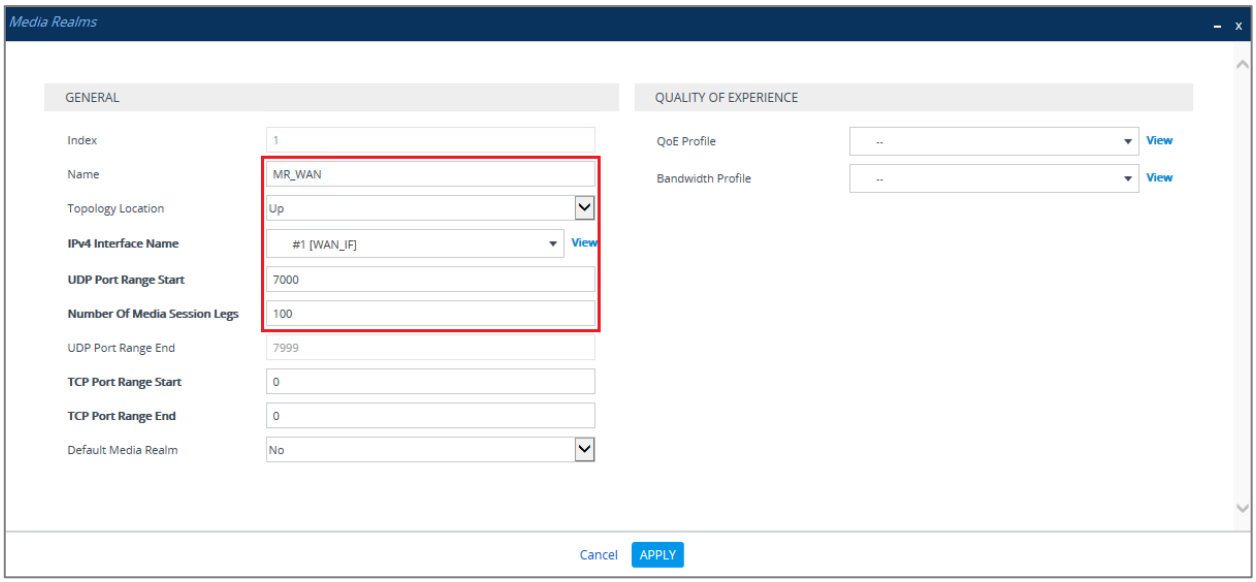
Media Realms allow dividing the UDP port ranges for use on different interfaces. For the needs of current example, two media realms are created; one for the LAN_IF interface and one for the WAN_IF interface.



Access the page **SETUP** >> **SIGNALING & MEDIA** >> **CORE ENTITIES** >> **Media Realms** and click on **[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 sub-section 3.1)
- **UDP Port Range Start**: 6000
- **Number Of Media Session Legs**: 100 (need to be calculated based on usage)

Click on **[Apply]**.



Access the page **SETUP** >> **SIGNALING & MEDIA** >> **CORE ENTITIES** >> **Media Realms** and click on **[New].** To configure a media realm for WAN_IF, enter the following:

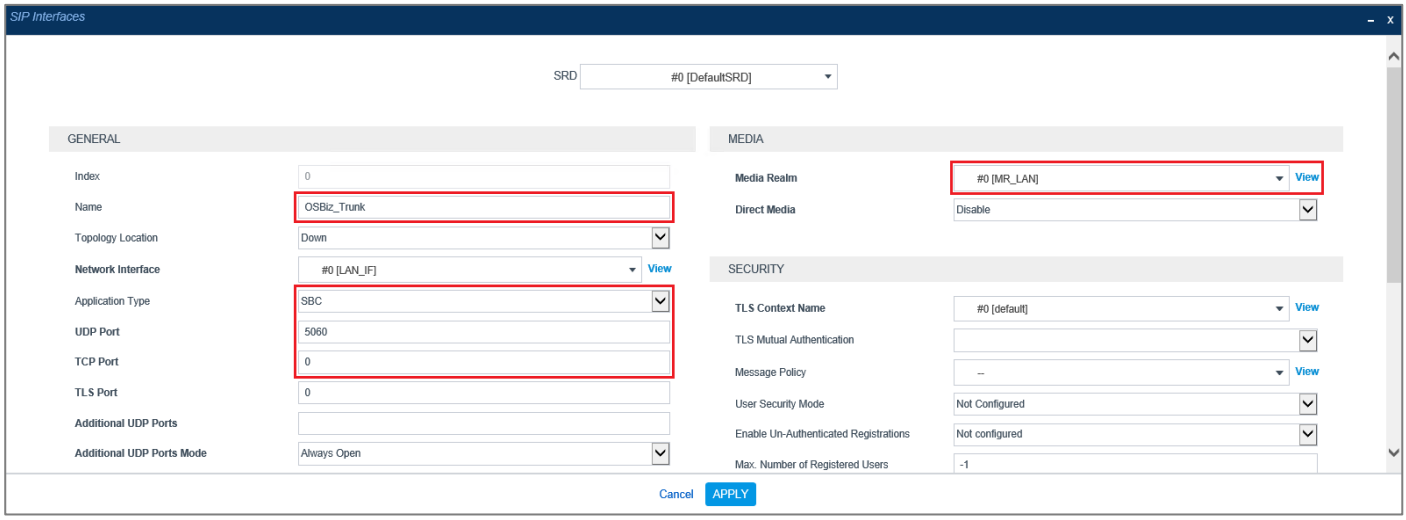
- **Name**: MR_WAN (WAN media realm friendly name)
- **IPv4 Interface Name**: WAN_IF (see sub-section 3.1)
- **Topology Location** Up
- **UDP Port Range Start**: 7000
- **Number Of Media Session Legs**: 100 (need to be calculated based on usage)

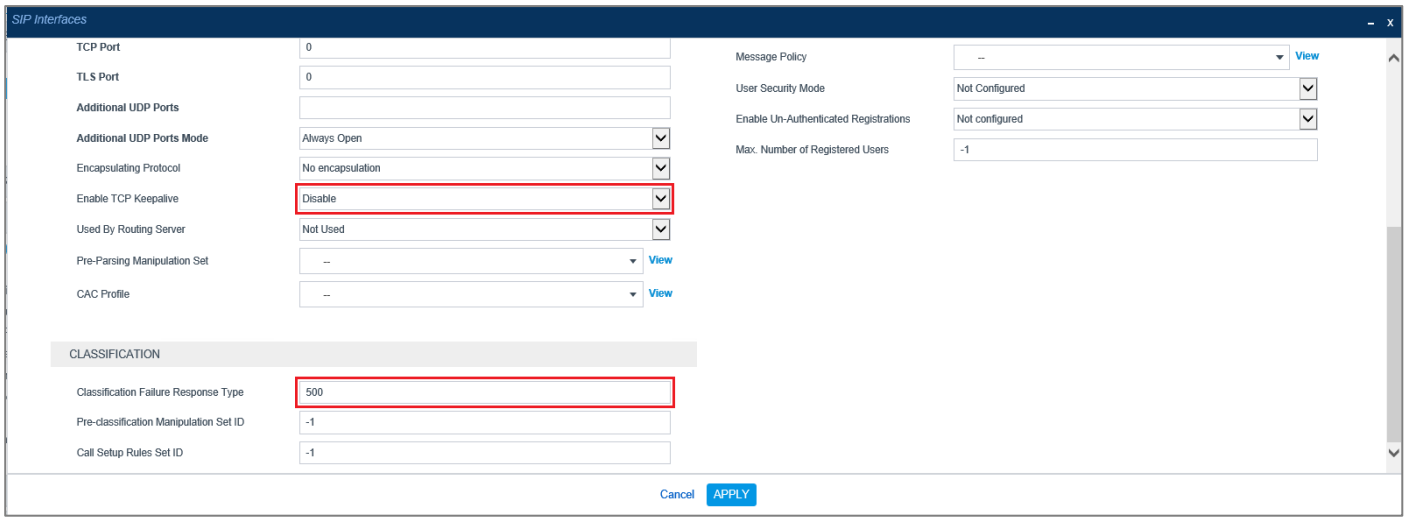
Click on **[Apply]**.

3.4. 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 ⇔ OpenScape Business.

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

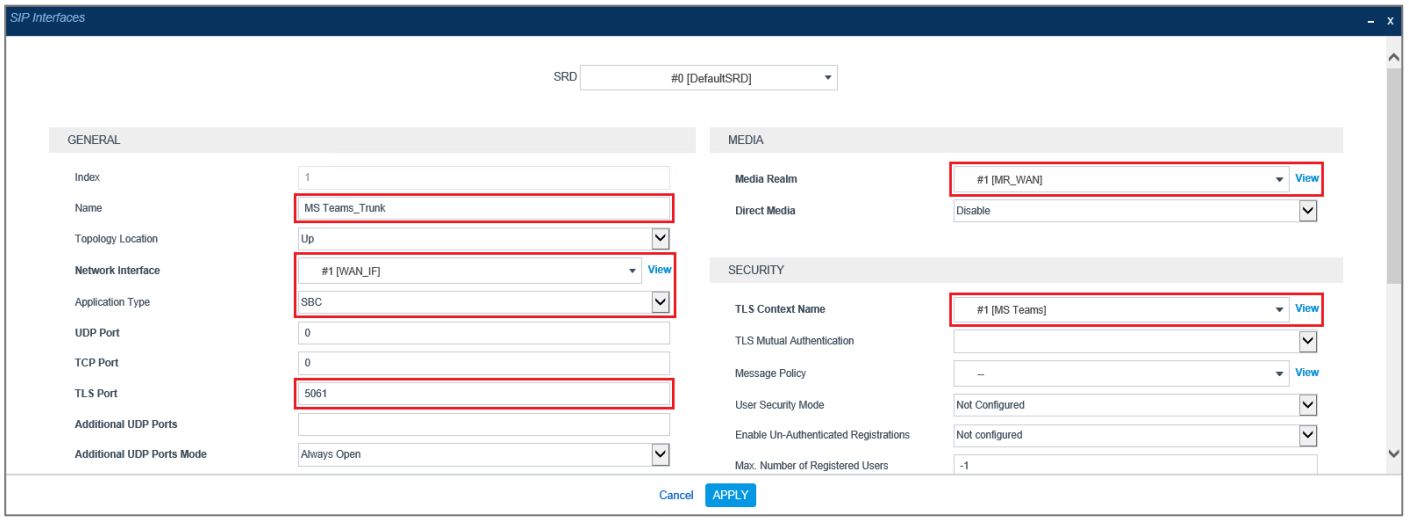


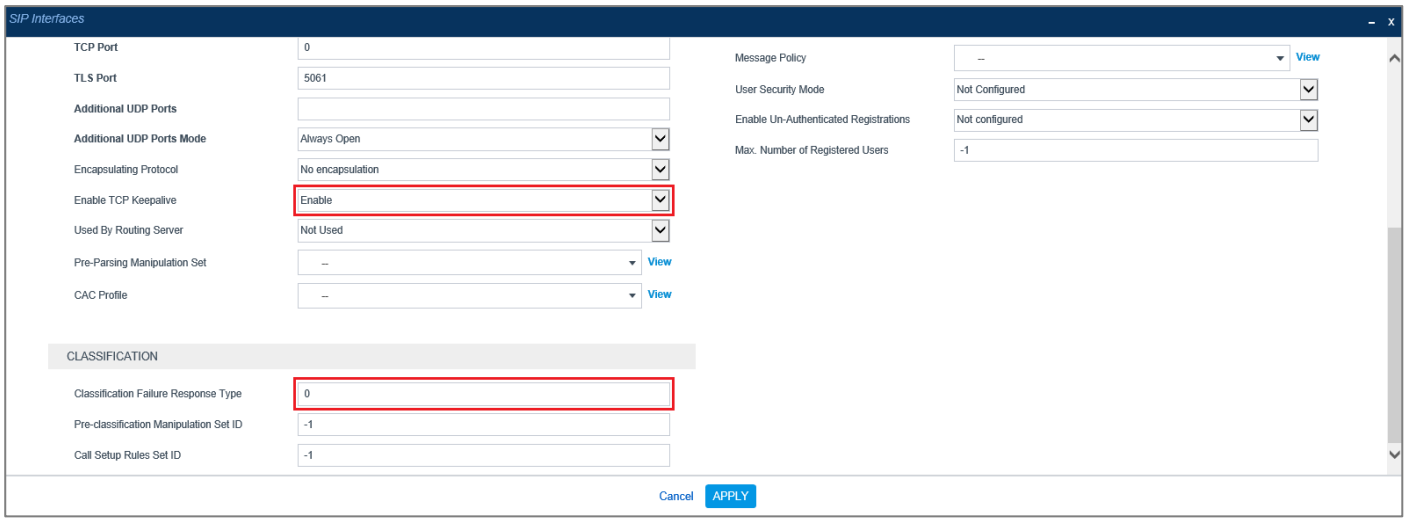


For the SIP trunk with the OS Voice configuration, navigate to **SETUP** >> **SIGNALING & MEDIA** >> **CORE ENTITIES** >> **SIP Interfaces**, click on **[New]** and enter the following:

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

Click on **[Apply]**.





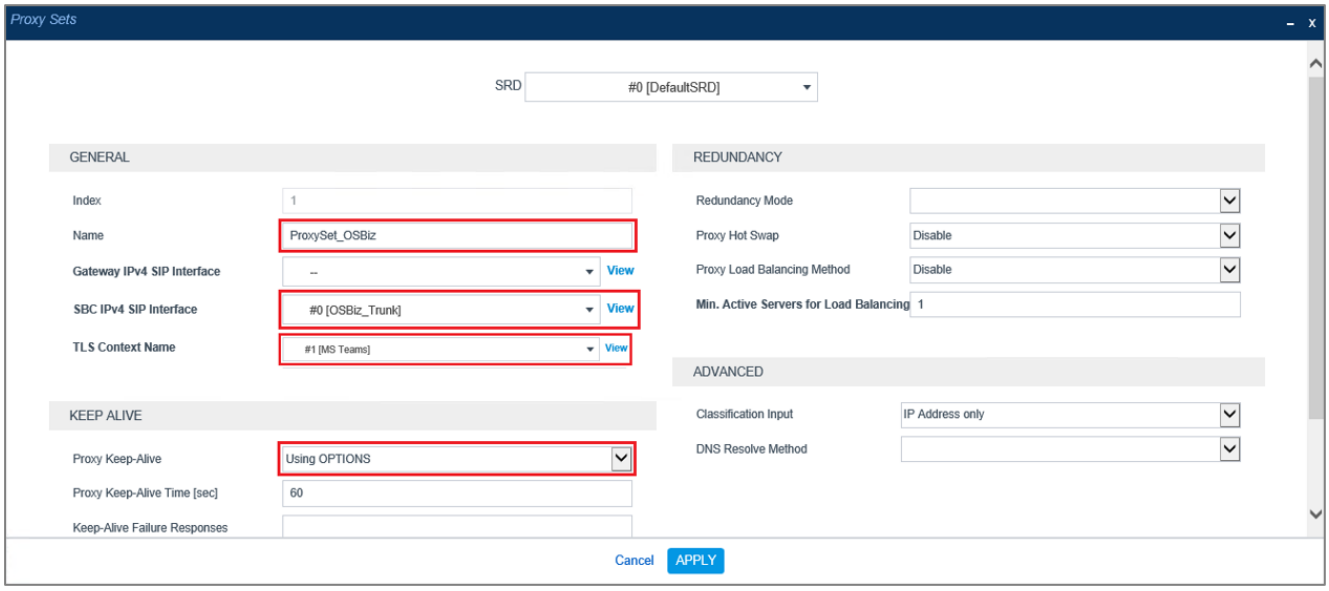
For the SIP trunk configuration, navigate to **SETUP** >> **SIGNALING & MEDIA** >> **CORE ENTITIES** >> **SIP Interfaces**, click on **[New]** and enter the following:

- **Name**: MS Teams_Trunk (SIP trunk with MS Phone System friendly name)
- **Network Interface**: WAN_IF
- **Application Type**: SBC
- **UDP Port:** 5061, 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_WAN
- **TLS Context Name**: MS Teams

Click on **[Apply]**.

3.5. Proxy Sets and Proxy Addresses

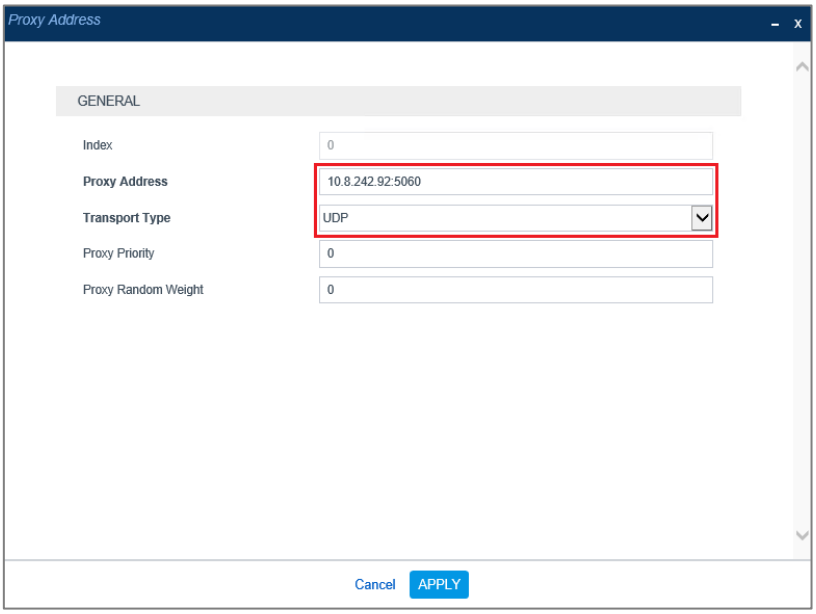
The Proxy Set and Proxy Address defines TLS parameters, IP interfaces, FQDN and the remote entity's port. Proxy Sets can also be used to configure load balancing between multiple servers.



Go to **SETUP** >> **SIGNALING & MEDIA** >> **CORE ENTITIES** >> **Proxy Sets** and click on **[New]** to setup the OpenScape Business **Proxy Set.** Enter the following:

- **Name**: ProxySet_OSBiz (OSBiz proxy set friendly name)
- **SBC IPv4 SIP Interface**: OSBiz_Trunk (see sub-section 3.4)
- **Proxy Keepalive:** Using OPTIONS
- **TLS Context Name**: MS Teams (see sub-section 3.2)

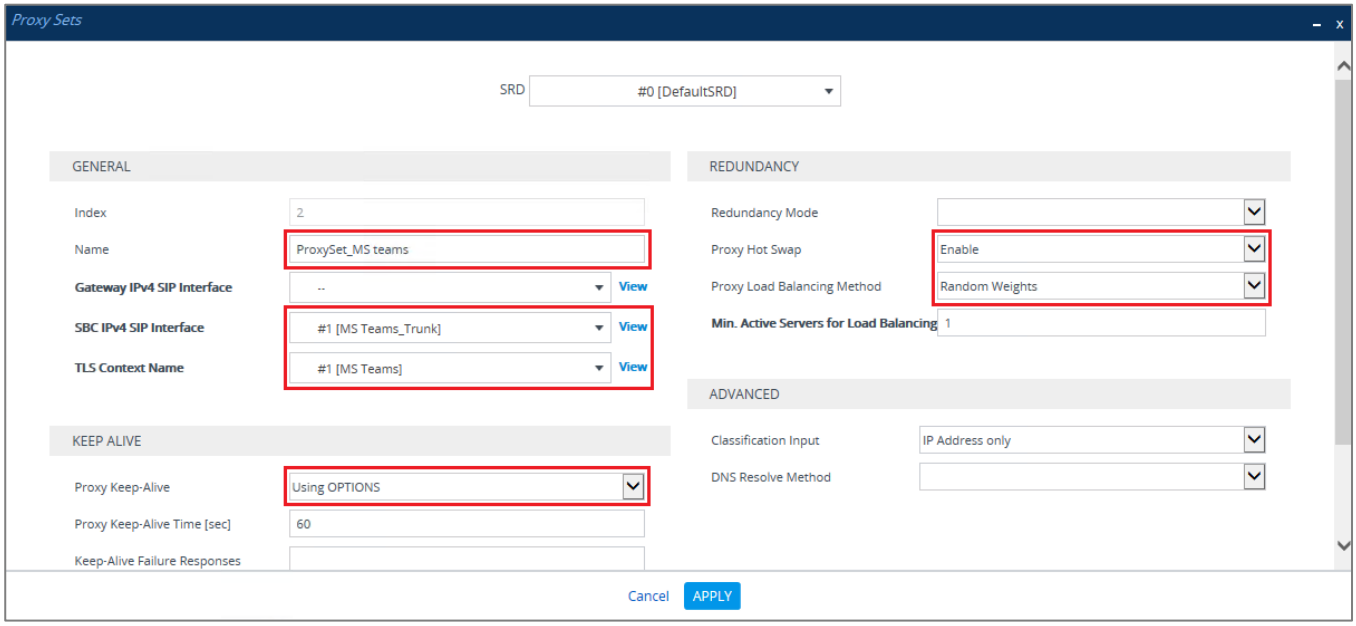
Click on **[Apply]**.



Return to **Proxy Sets** page, click on **Proxy Address** link and on the page that appears, click on **[New]** to configure the SBC connectivity data with OpenScape Business:

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

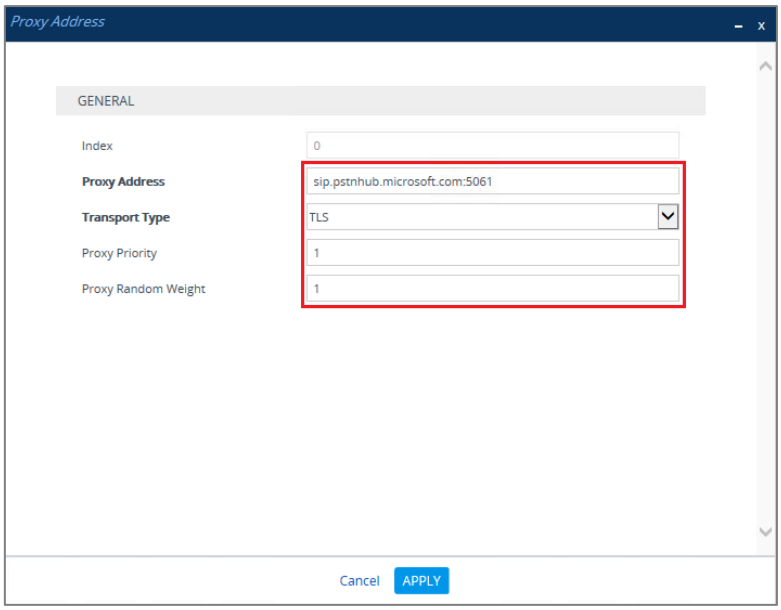
Click on **[Apply]**.

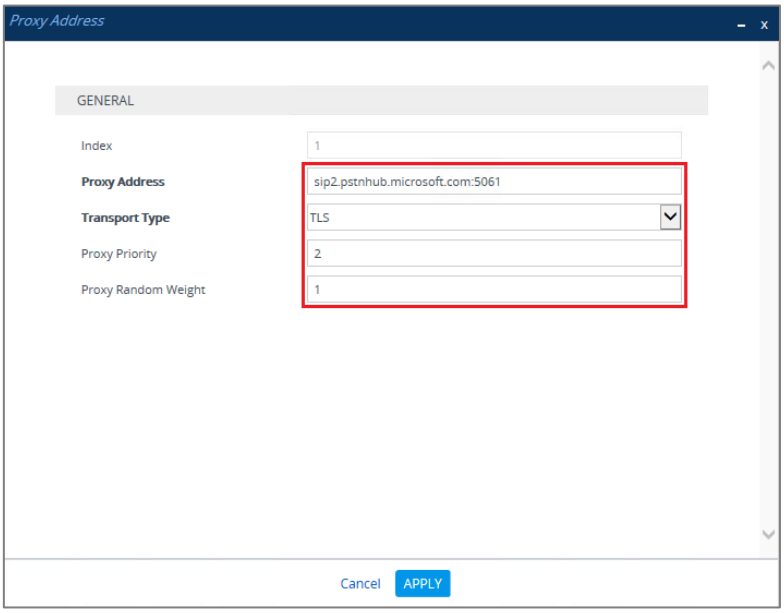


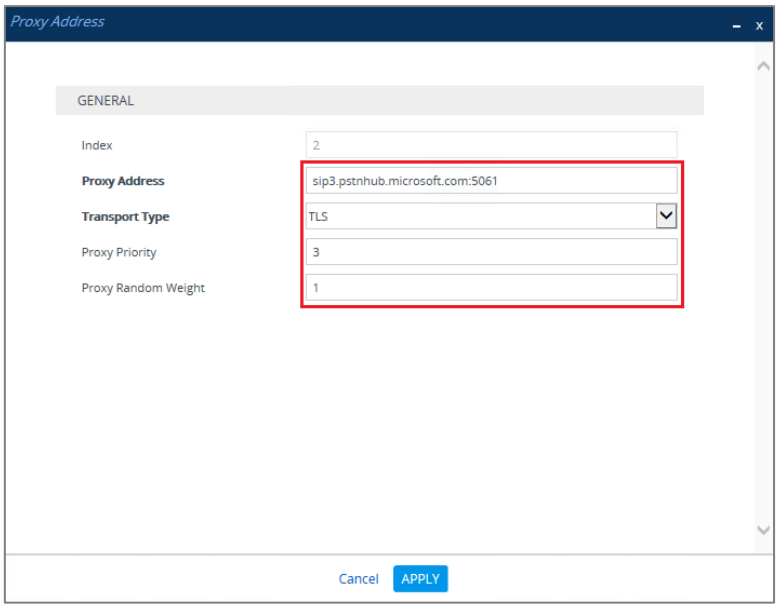
Go to **SETUP** >> **SIGNALING & MEDIA** >> **CORE ENTITIES** >> **Proxy Sets** and click on **[New]** to setup the Teams **Proxy Set.** Enter the following:

- **Name**: ProxySet_MS teams (Teams proxy set friendly name)
- **SBC IPv4 SIP Interface**: MS Teams_Trunk (see sub-section 3.4)
- **TLS Context Name**: MS Teams (see sub-section 3.2)
- **Proxy Keepalive:** Using OPTIONS
- **Proxy Hot Swap**: Enable
- **Proxy Load Balancing Method**: Random Weights

Click on **[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


Proxy Address
GENERAL
Index
1
Proxy Address
sip2.pstnhub.microsoft.com:5061
Transport Type
TLS
Proxy Priority
2
Proxy Random Weight
1
Cancel
APPLY



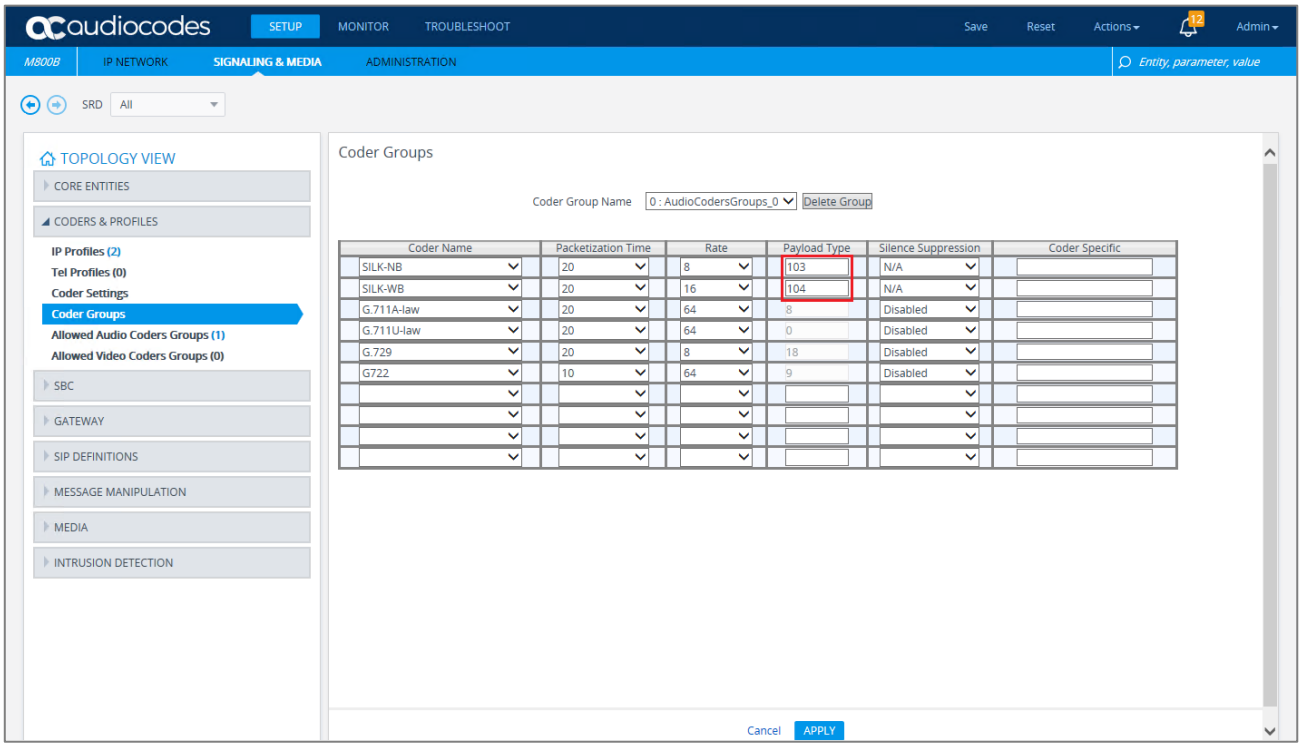
On **Proxy Sets** page, click on **Proxy Address** link and on the page that appears, click on **[New]**. At Teams end, there are 3 SIP Proxies, so the procedure needs to be repeated 3 times. To configure the SBC connectivity data with Teams, enter the following:

- **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 on **[Apply]**.

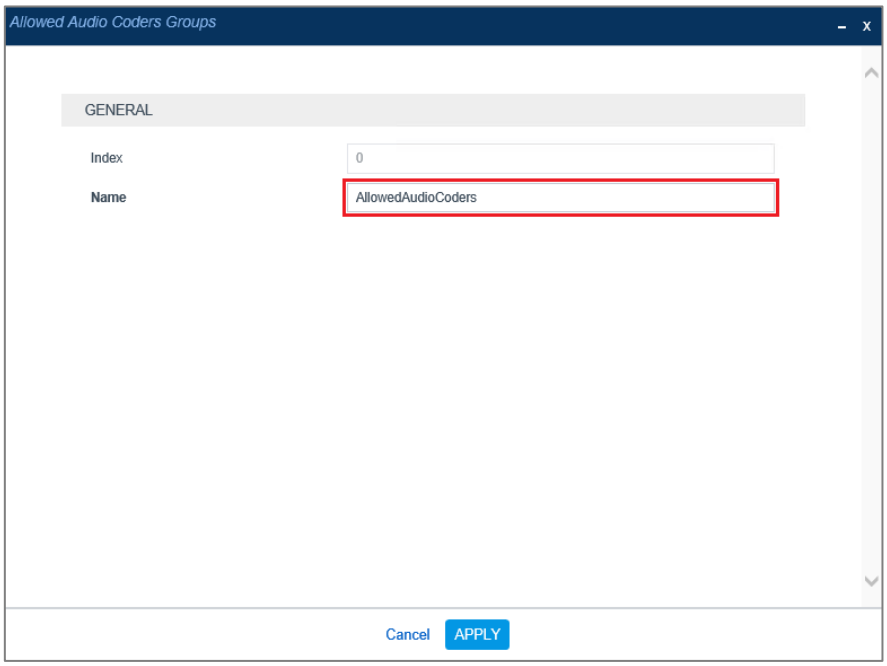
3.6. Coder Groups

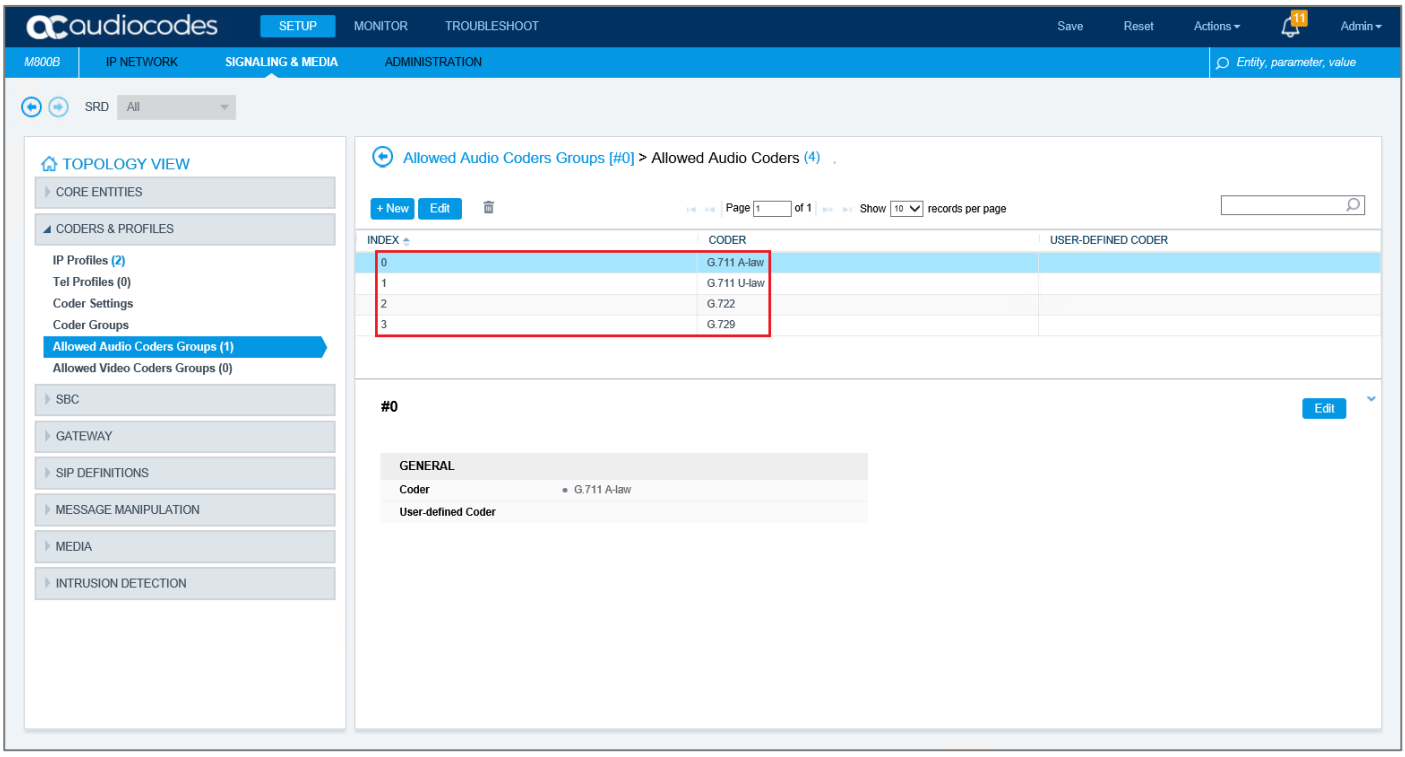
The various audio codecs used for the communication between an OpenScape Business subscriber and a Teams user, on SBC side are manipulated from **Coder Group** menu. SILK and OPUS codecs are supported by Teams, but not from OpenScape Business. A coder group needs to be added with the supported codecs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



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

Configuration in the **Allowed Audio Coders Groups**:





Go to: **SETUP** >> **SIGNALING & MEDIA** >> **CODERS & PROFILES** >> **Allowed Audio Coders Groups.**

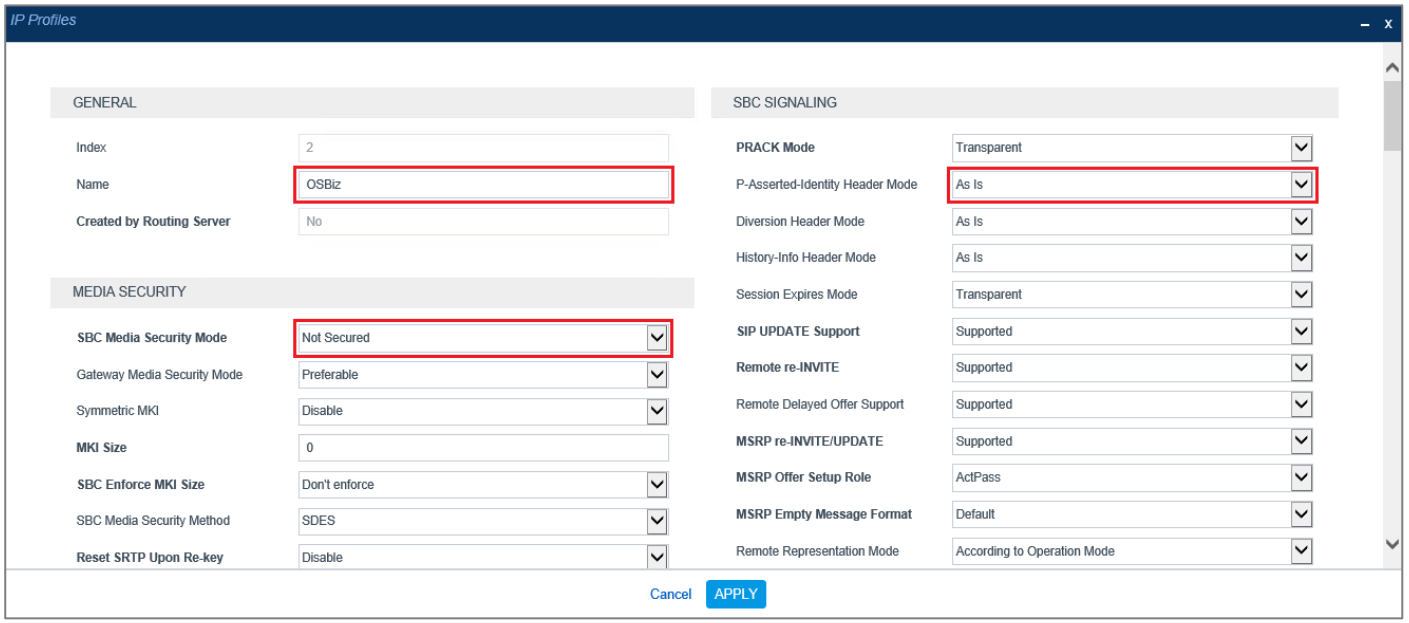
Click on **[New],** enter a friendly name for the new **Allowed Audio Coder Group** (e.g. AllowedAudioCoders) and the click on **[Apply]**.

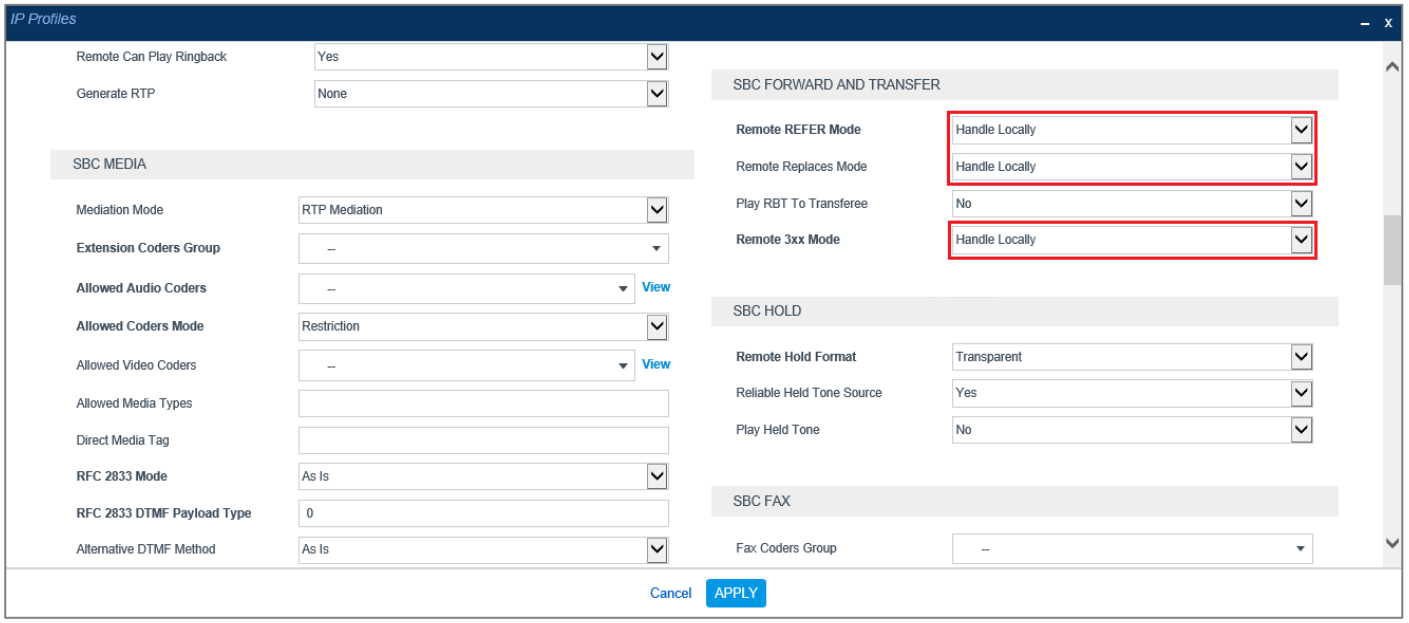
On **Allowed Audio Coders Groups** webpage, edit the AllowedAudioCoders group and setup the coder sequence, as shown in the picture above.

The next step is the coder profile to be assigned to the corresponding IP profile.

3.7. IP Profiles

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



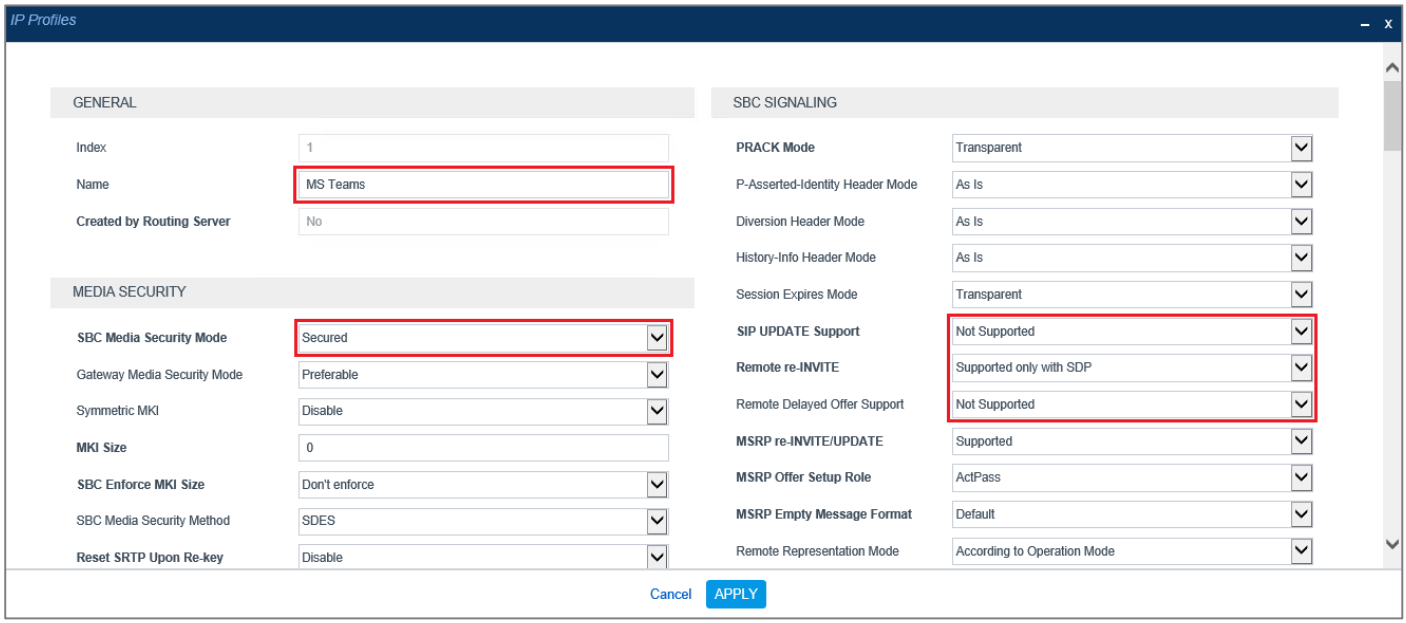


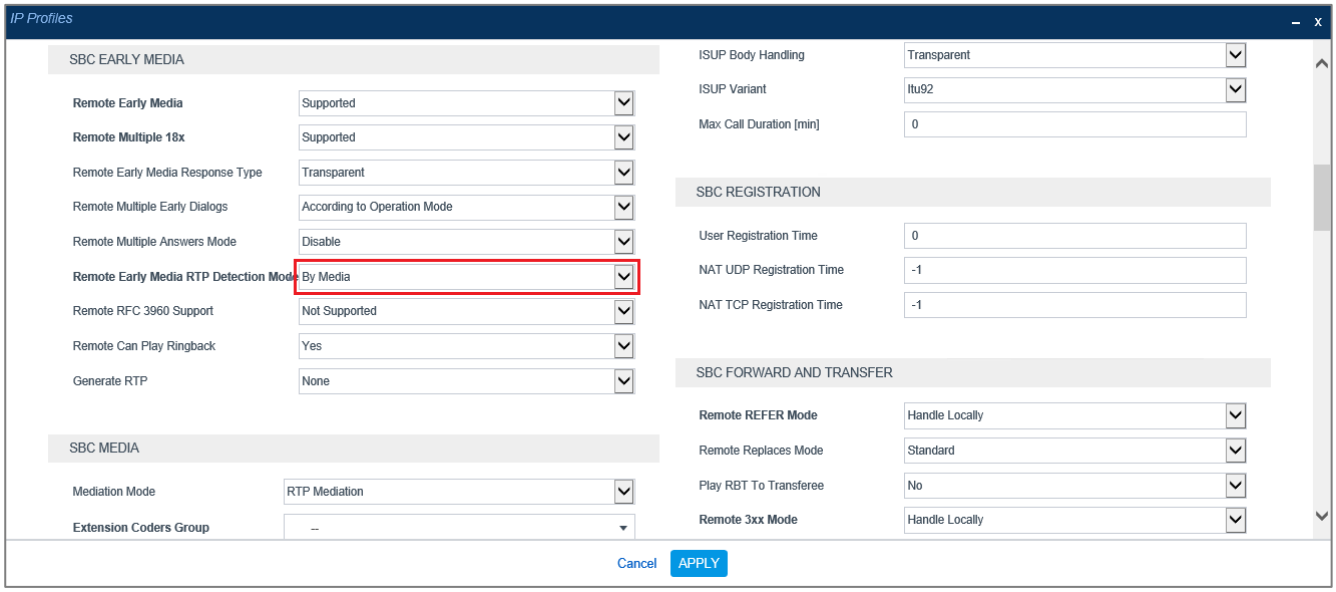
Navigate to **SETUP** >> **SIGNALING & MEDIA** >> **CODERS & PROFILES** >> **IP Profiles** and click on **[New]** to create an IP profile for the OpenScape Business connection. Enter the following:

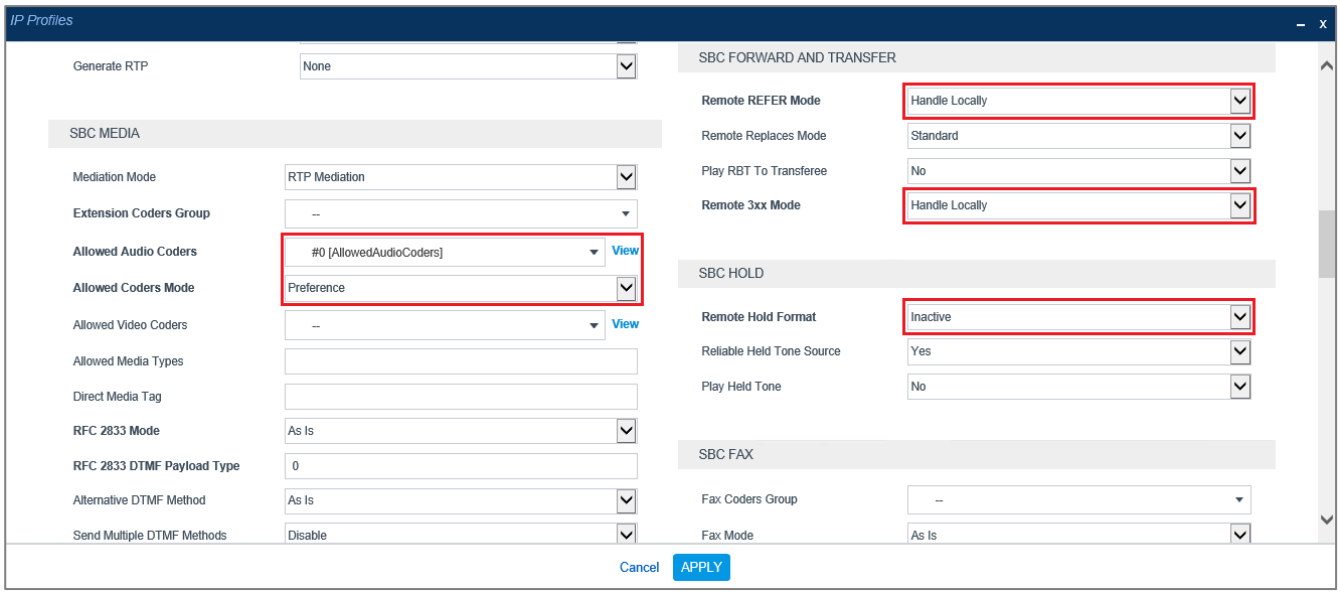
- **Name**: OSBiz (friendly name for OSBiz)
- **SBC Media Security Mode**: Not Secured

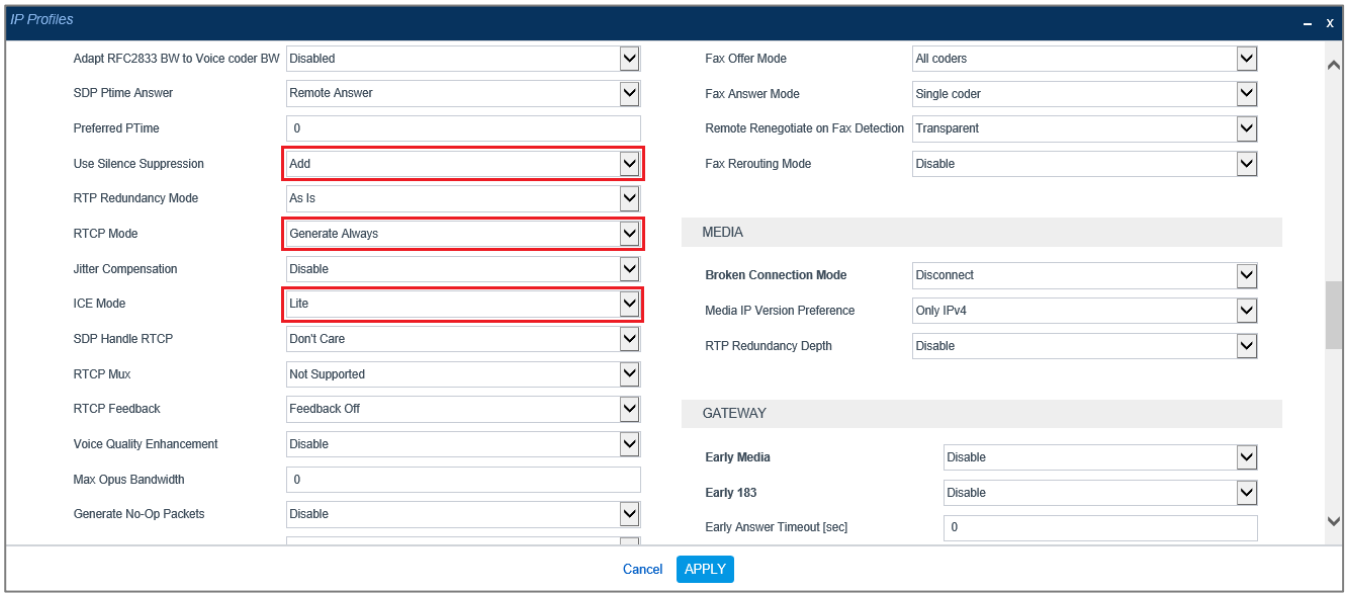
- **P-Asserted-Identity Header Mode**: As Is
- **Remote REFER Mode:** Handle Locally
- **Remote Replaces Mode**: Handle Locally
- **Remote 3xx Mode**: Handle Locally

Click on **[Apply]**.









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

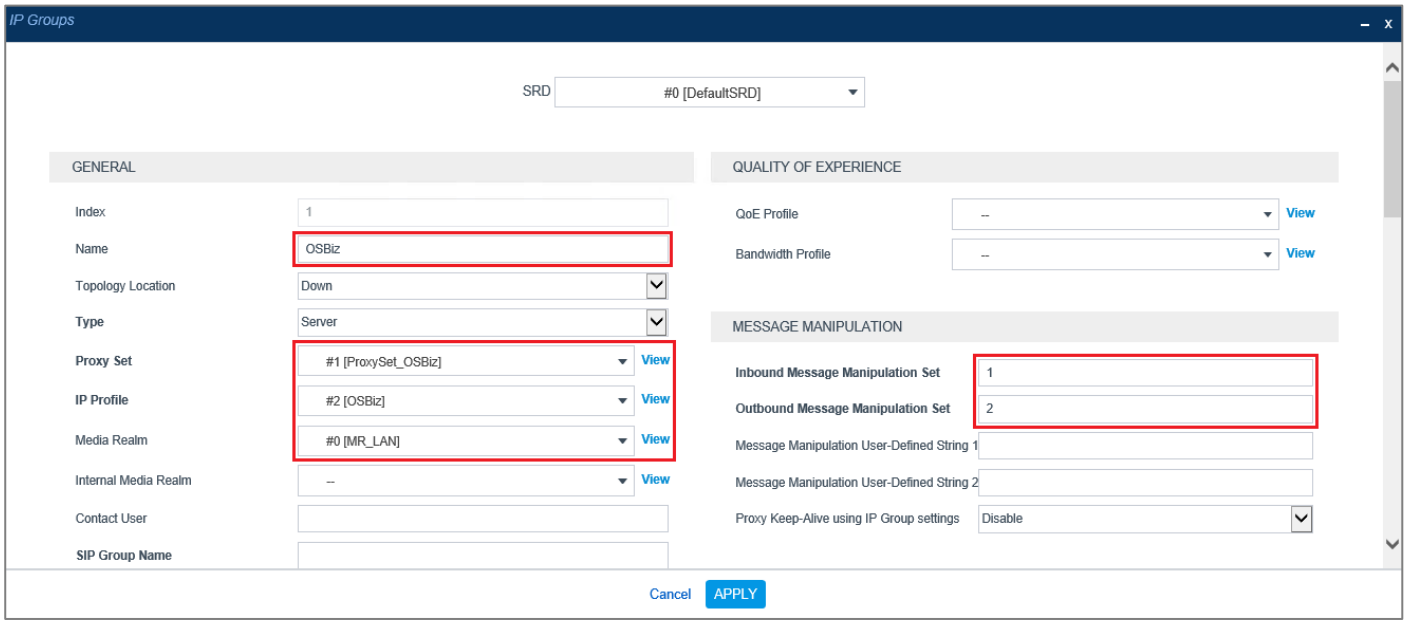
- **Name**: MS Teams (friendly name for Teams)
- **SBC Media Security Mode**: Secured
  Remote Early Media RTP Detection Mode: By Media (required, as Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18x response)
- **Allowed Audio Coders:** AllowedAudioCoders (see sub-section 3.6).
  Allowed Coders Mode: Preference (re-arranges the codecs in SDP for messages coming from Teams side by prioritizing the coders configured in *AllowedAudioCoders* group)
- **Use Silence Suppression:** Add

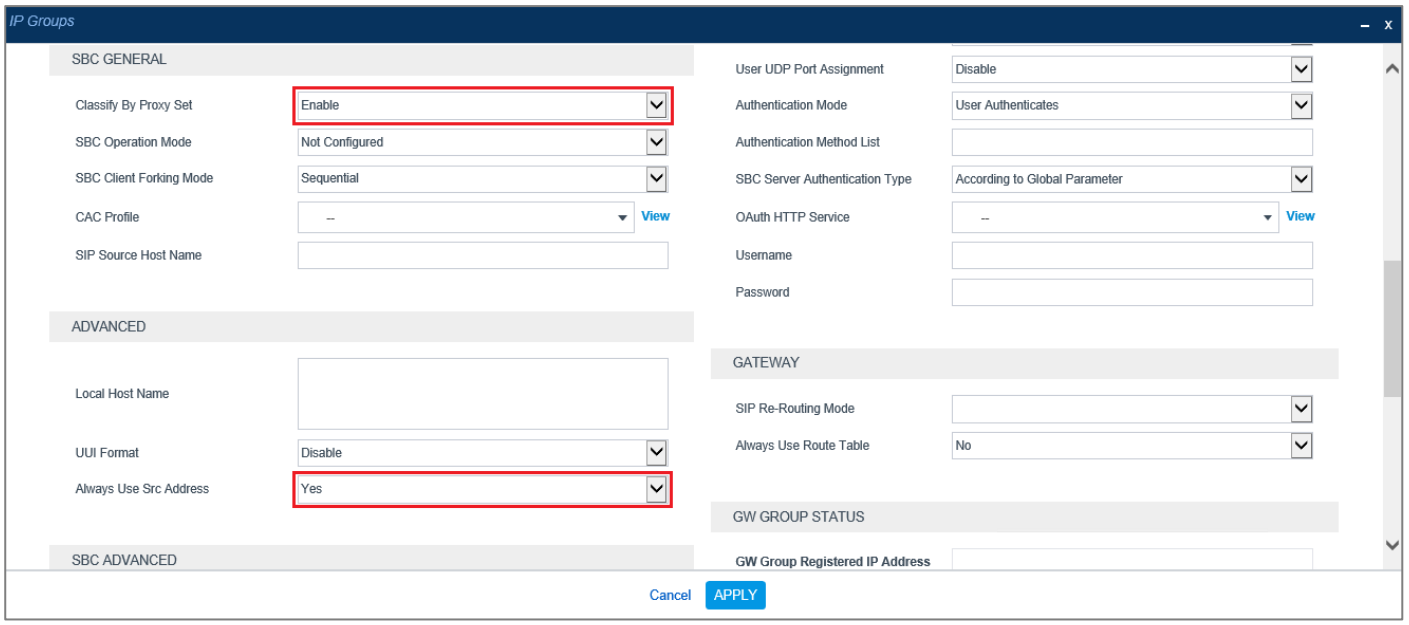
- **RTCP Mode**: Generate Always (in case RTCP packets aren't generated, but Teams expects them)
- **ICE Mode:** Lite (required only if Media Bypass enabled on Teams)
- **Remote Update Support:** Not Supported
- **Remote re-INVITE Support:** Supported Only With SDP
- **Remote Delayed Offer Support:** Not Supported
- **Remote REFER Mode:** Handle Locally
- **Remote 3xx Mode**: Handle Locally
- **Remote Hold Format:** Inactive (some SIP trunks with IP-PBXs may answer with: a=inactive and IP=0.0.0.0 in response to the Re-Invite with Hold request from Teams. Microsoft Media Stack doesn't support this format. So, SBC will replace 0.0.0.0 with its IP address).

Click on **[Apply]**.

3.8. 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 example), the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

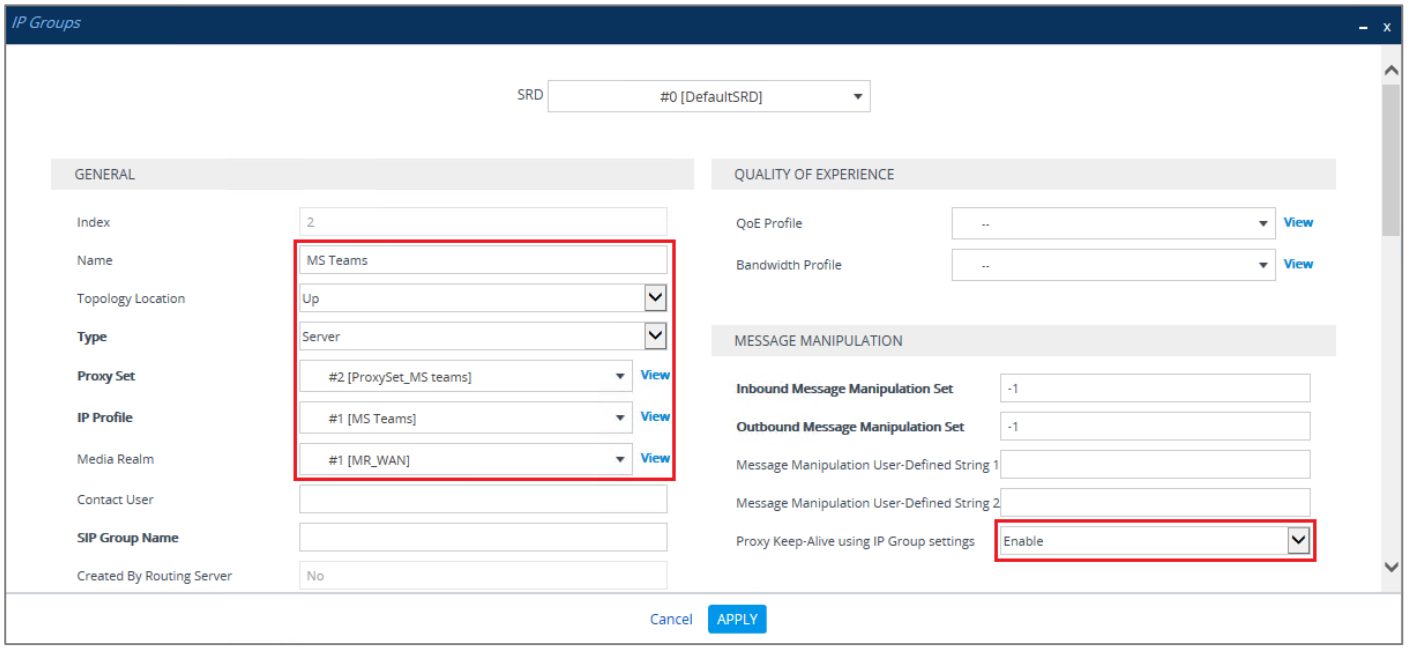


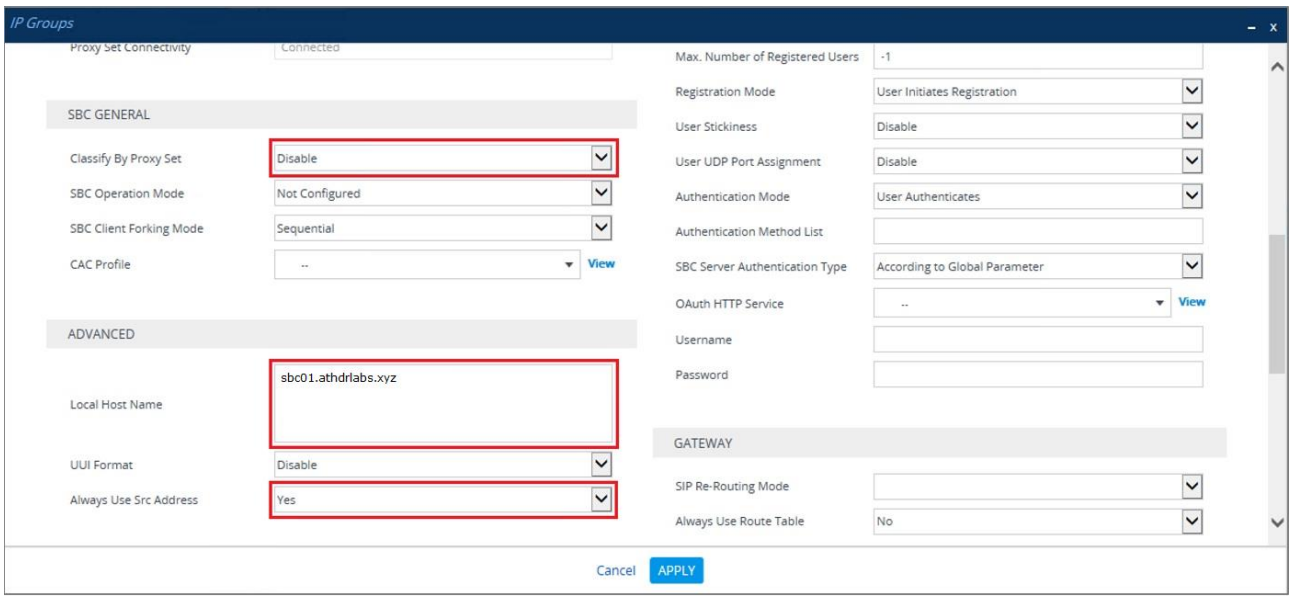


At **SETUP** >> **SIGNALING & MEDIA** >> **CORE ENTITIES** >> **IP Groups** click on **[New]**.
Configure an IP Group for OpenScape Business, by entering the following:

- **Name**: OSBiz (friendly name for OSBiz)
- **Proxy Set**: ProxySet_OSBiz (see sub-section 3.5)
- **IP Profile**: OSBiz (see sub-section 3.7)
- **Media Realm:** MR_LAN (see sub-section 3.3)
- **Inbound Message Manipulation Set:** 1, (see sub-section 3.11)
- **Outbound Message Manipulation Set:** 2, (see sub-section 3.11)
- **Classify By Proxy Set**: Enable
- **Always Use Src Address**: Yes

Click on **[Apply]**.





At **SETUP** >> **SIGNALING & MEDIA** >> **CORE ENTITIES** >> **IP Groups** click on **[New]**. Configure an IP Group for OpenScape Business, by entering the following:

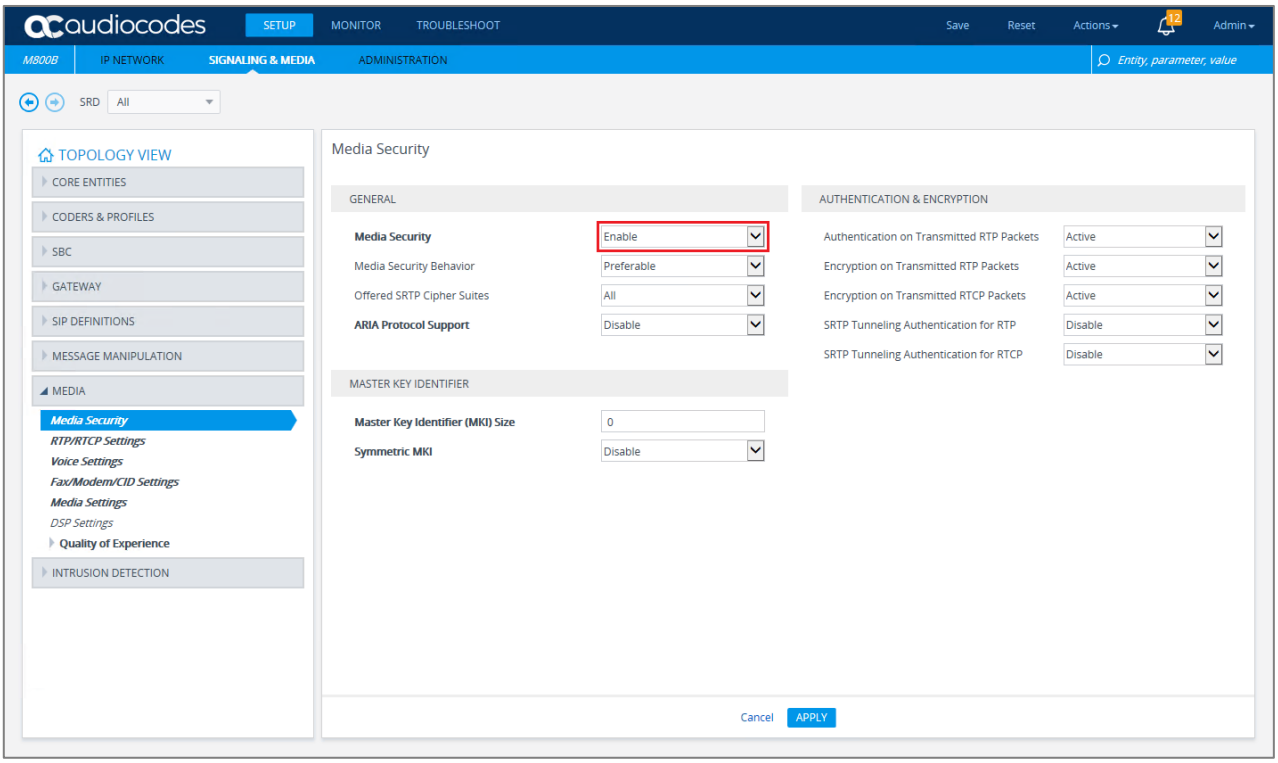
- **Name**: MS Teams (friendly name for Teams)
- **Topology Location:** Up
- **Type:** Server
- **Proxy Set**: ProxySet_MS Teams (see sub-section 3.5)
- **IP Profile**: MS Teams (see sub-section 3.7)
- **Media Realm:** MR_WAN (see sub-section 3.3)
- **Classify By Proxy Set**: Disable
- **Local Host Name**: sbc01.athdrlabs.xyz (public FQDN for SBC in Teams tenant, see sub-section 2.1)
- **Always Use Src Address**: Yes
- **Proxy Keep-Alive using IP Group settings:** Enable

Click on **[Apply]**.

Note: The name sbc01.athdrlabs.xyz 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.

3.9. Media Security

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

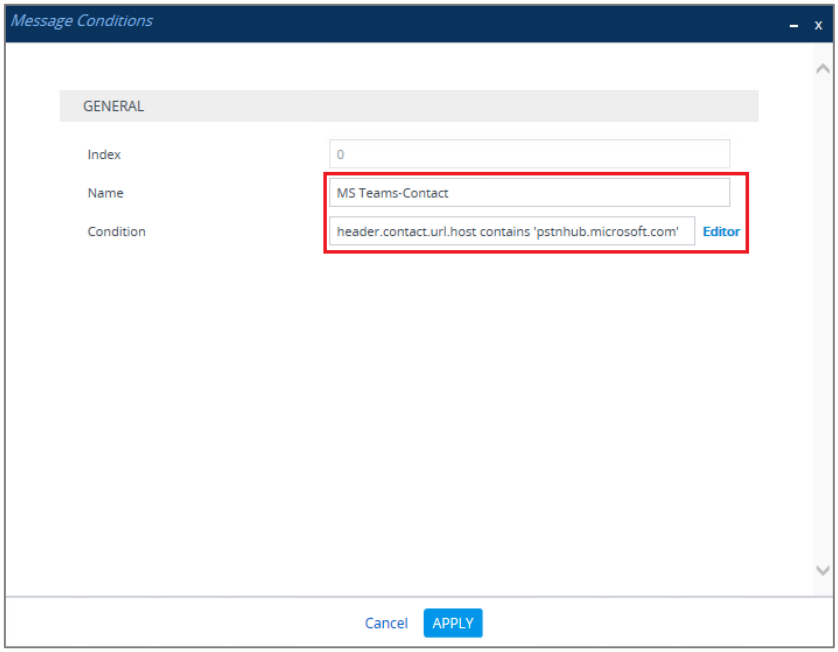


Go to **SETUP** >> **SIGNALING & MEDIA** >> **MEDIA** >> **Media Security** and set **Media Security** to Enable to enable SRTP and then click on **[Apply]**.

3.10. Message Condition and Classification 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.



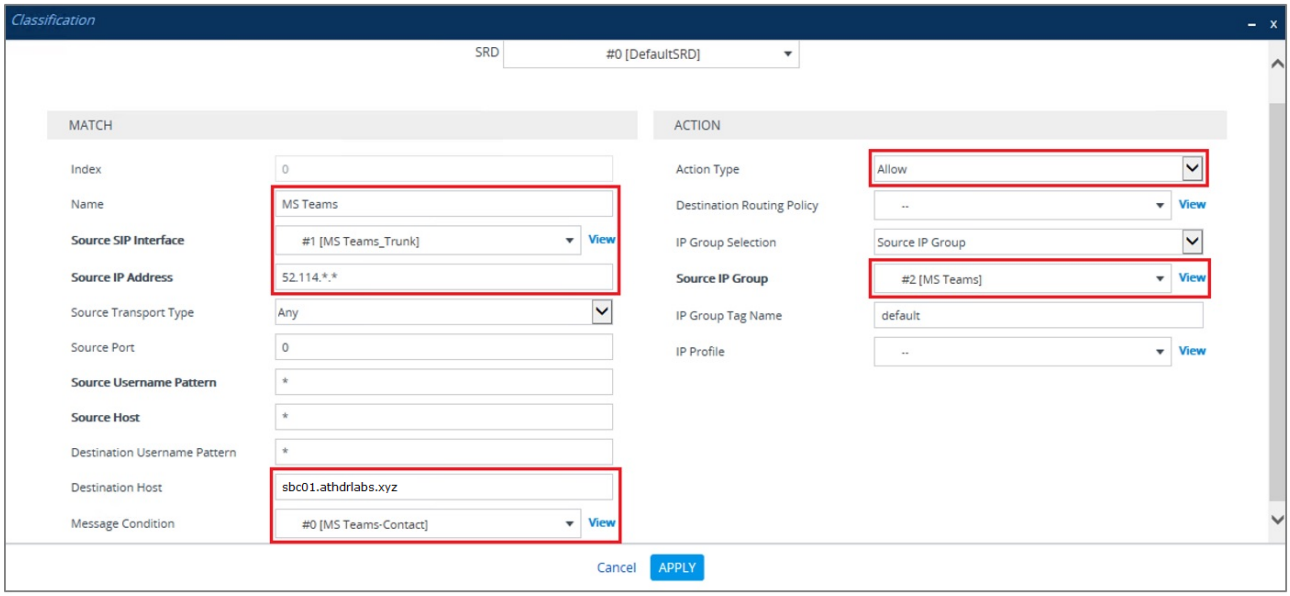
Go to **SETUP** >> **SIGNALING & MEDIA** >> **MESSAGE MANIPULATION** >> **Message Condition,** click on **[New]** and configure:

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

Click on **[Apply]**.

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 on **[New]** and enter the following:

- **Name**: MS Teams (rule friendly name)
- **Source SIP Interface:** MS Teams_Trunk (see sub-section 3.4)
  Source IP Address: 52.114.*.* (Teams public proxies FQDNs resolve to 52.114.*.* IPs; see sub-sections 3.5 and 3.13)
- **Destination Host:** sbc01.athdrlabs.xyz (public FQDN for SBC in Teams tenant, see sub-section 2.1)
- **Message Condition:** MS Teams-Contact
- **Action Type:** Allow
- **Source IP Group:** MS Teams (see sub-section 3.8)

Click on **[Apply].**

3.11. Message Manipulation

With a Message Manipulation rule, the admin can ADD, REMOVE, MODIFY or NORMALIZE a SIP header or SIP message body.

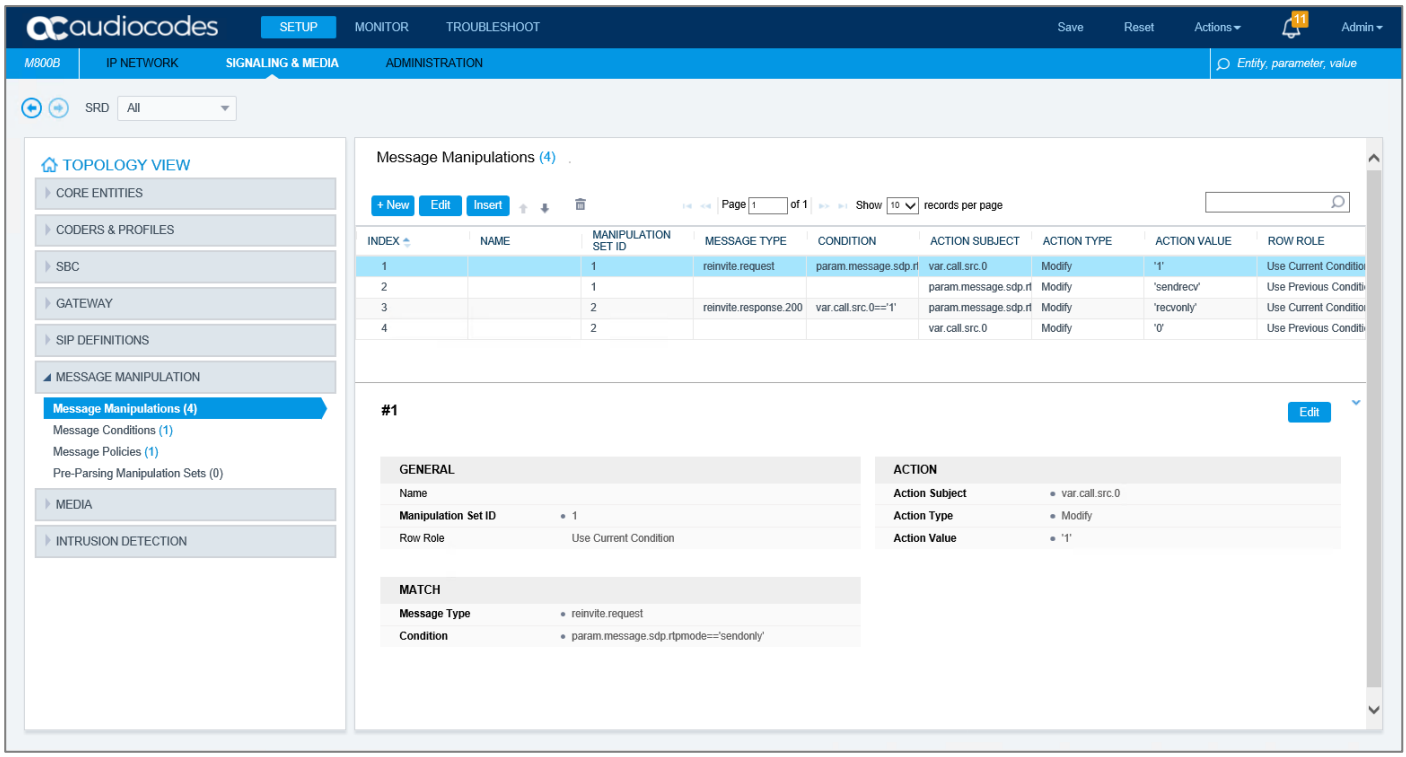
In order to change the default system behavior for call hold scenarios, where it is required to hear MOH on Teams side, when an OSBiz subscriber holds the call with the Teams user, an **Inbound Message Manipulation Set** and an **Outbound Message Manipulation Set** need to be configured at OpenScape Business IP Group (see sub-section 3.8).

The following auxiliary configuration INI file, containing the message manipulation set data, is imported to the SBC:

MM.ini

Content of MM.ini file:

```
[ MessageManipulations ]


FORMAT MessageManipulations_Index = MessageManipulations_ManipulationName,
MessageManipulations_ManSetID, MessageManipulations_MessageType,
MessageManipulations_Condition, MessageManipulations_ActionSubject,
MessageManipulations_ActionType, MessageManipulations_ActionValue,
MessageManipulations_RowRole;

MessageManipulations 1 = "", 1, "reinvite.request",
"param.message.sdp.rtpmode=='sendonly'", "var.call.src.0", 2, "'1'", 0;

MessageManipulations 2 = "", 1, "", "", "param.message.sdp.rtpmode", 2,
"'sendrecv'", 1;

MessageManipulations 3 = "", 2, "reinvite.response.200", "var.call.src.0=='1'",
"param.message.sdp.rtpmode", 2, "'recvonly'", 0;

MessageManipulations 4 = "", 2, "", "", "var.call.src.0", 2, "'0'", 1;


[ \MessageManipulations ]
```



After the auxiliary INI file is imported to the system, the user may view the manipulation sets by accessing the webpage:

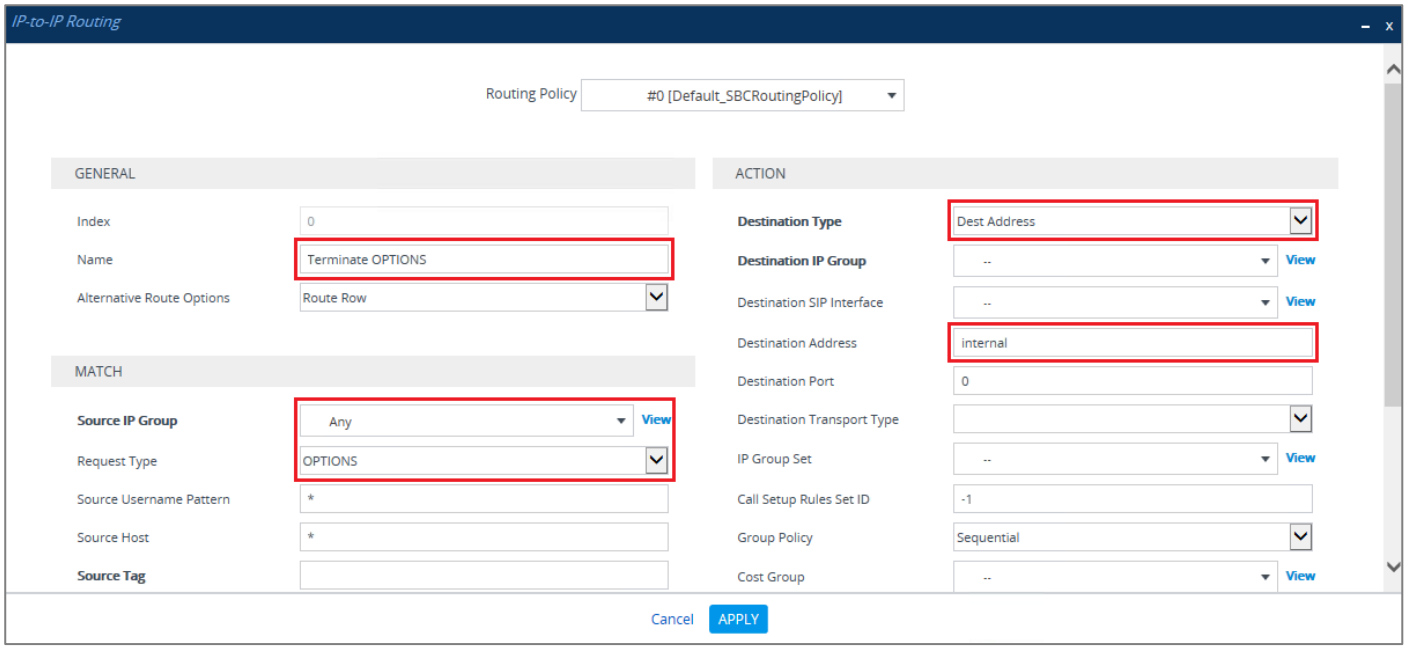
SETUP >> SIGNALING & MEDIA >> MESSAGE MANIPULATION >> Message Manipulations.

3.12. 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:

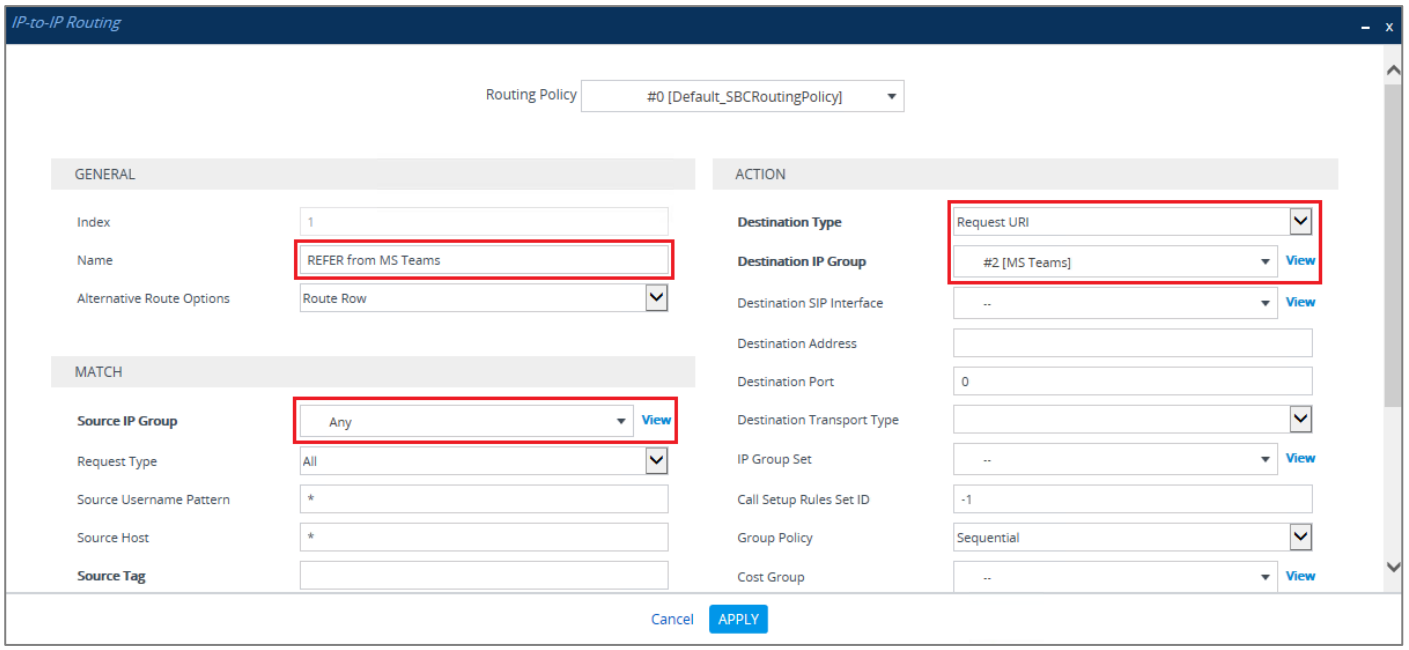
- Terminate SIP OPTIONS messages on the SBC.
- Terminate REFER messages to Teams.
- Calls from Teams to OpenScape Business.
- Calls from OpenScape Business to Teams.

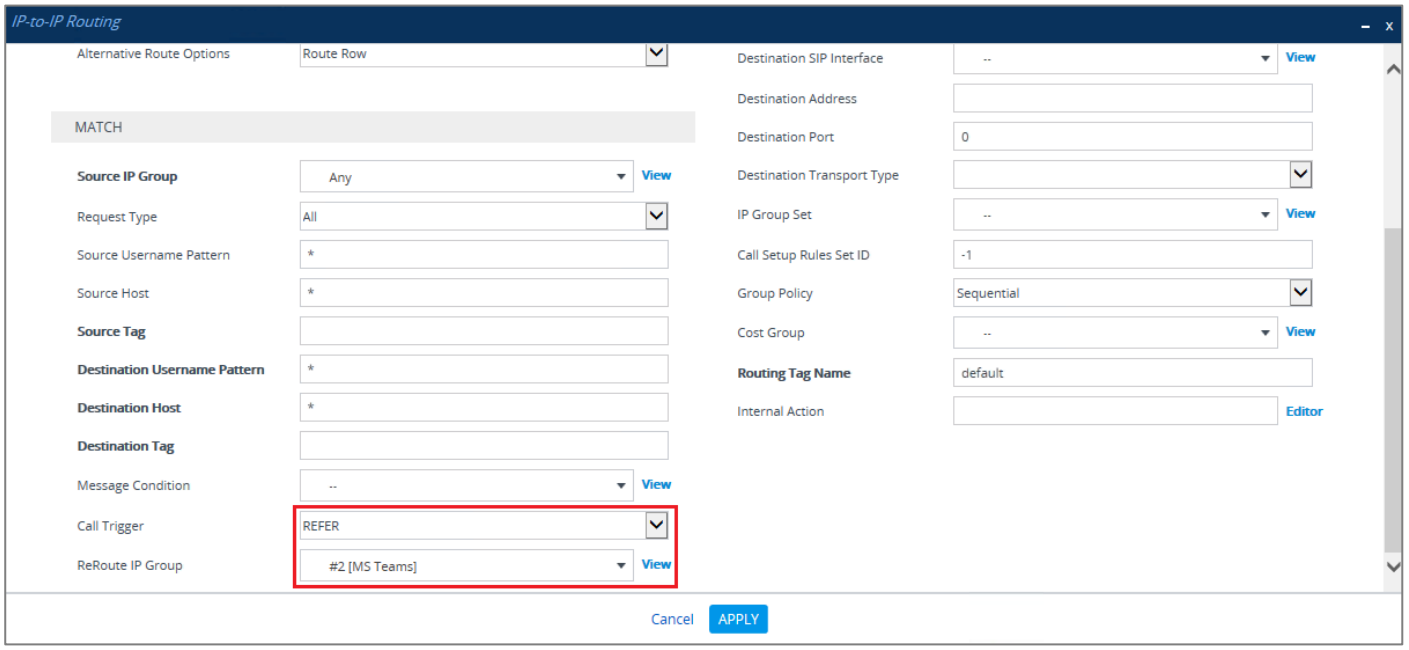


Open IP-to-IP routing table at **SETUP** >> **SIGNALING & MEDIA** >> **SBC** >> **Routing >> IP-to-IP Routing,** click on **[New]** and enter the following:

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

Click on **[Apply]**.

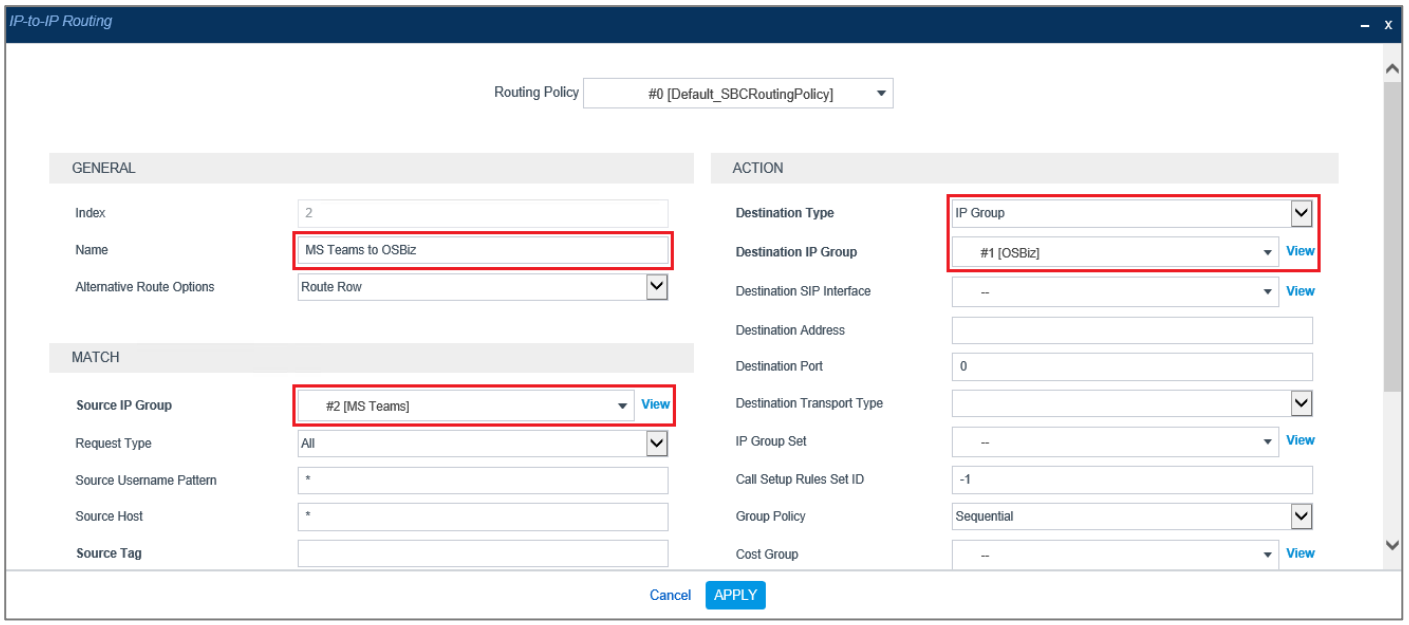




Open IP-to-IP routing table at **SETUP** >> **SIGNALING & MEDIA** >> **SBC** >> **Routing >> IP-to-IP Routing,** click on **[New]** and enter the following:

- **Name**: REFER from MS Teams (friendly name)
- **Source IP Group:** Any
- **Destination Type:** Request URI
- **Destination IP Group:** MS Teams (see sub-section 3.8)
- **Call Trigger:** REFER
- **ReRoute IP Group:** MS Teams (see sub-section 3.8)

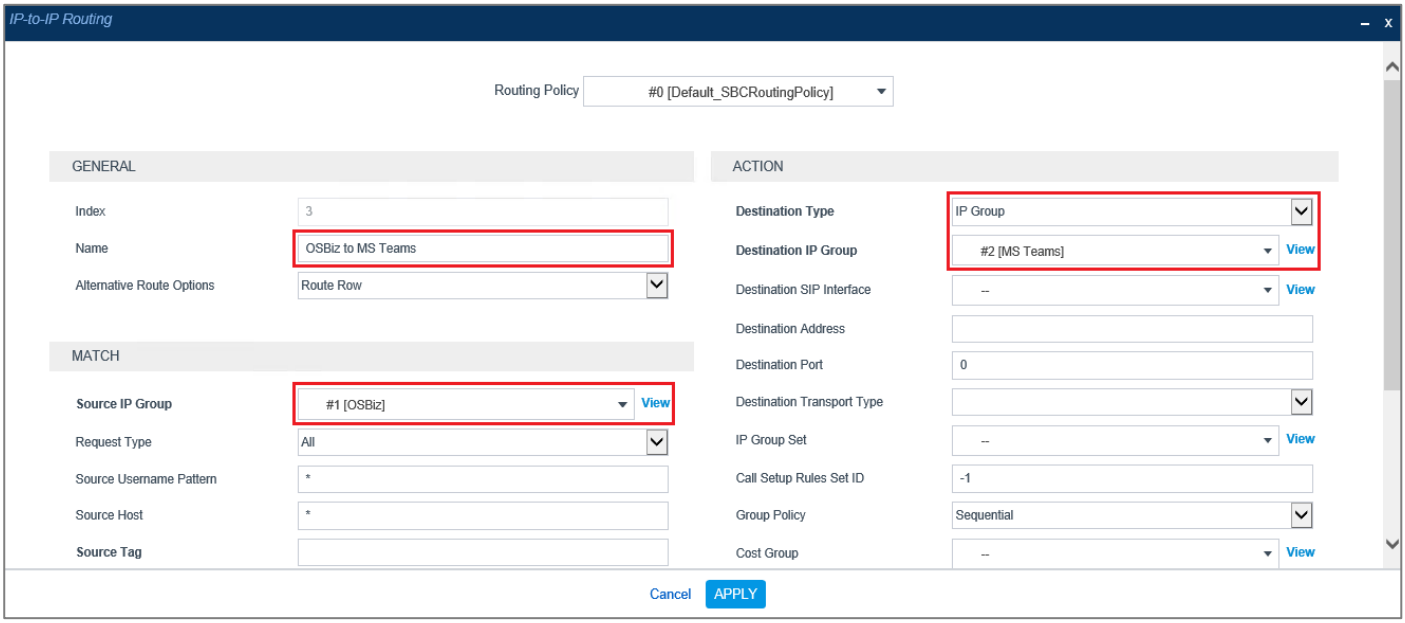
Click on **[Apply]**.



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

- **Name**: MS Teams to OSBiz (friendly name)
- **Source IP Group:** MS Teams (see sub-section 3.8)
- **Destination Type:** IP Group
- **Destination IP Group:** OSBiz (see sub-section 3.8)

Click on **[Apply]**.



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

- **Name**: OSBiz to MS Teams (friendly name)
- **Source IP Group:** OSBiz (see sub-section 3.8)
- **Destination Type:** IP Group
- **Destination IP Group:** MS Teams (see sub-section 3.8).

Click on **[Apply]**.

3.13. 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 3.5, 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 below IP addresses:

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

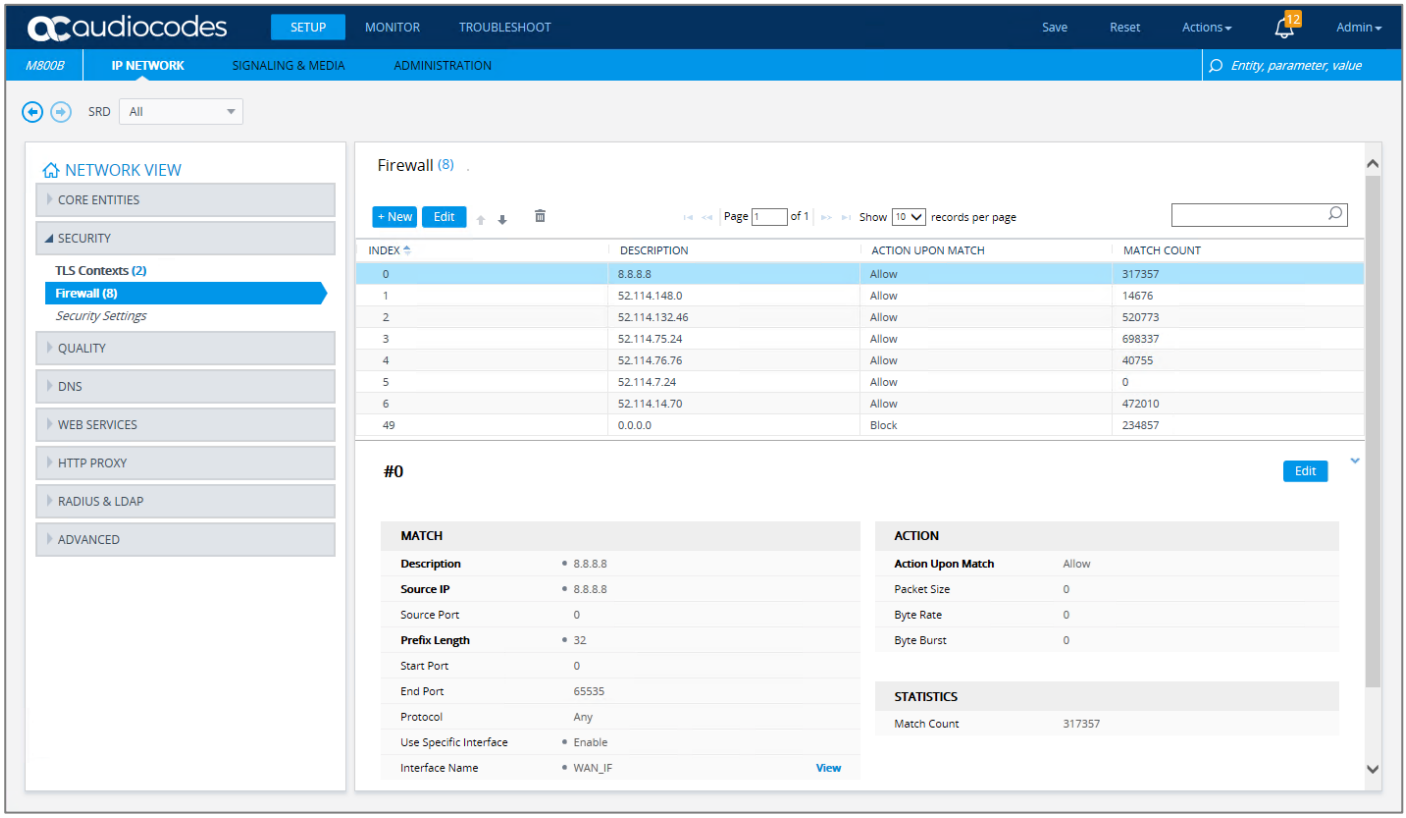
Refer to: https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sip-signaling-fqdns-and-firewall-ports.

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 on **[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	Any	Enable	WAN_IF	Allow
2	52.114.132.46	32	0	65535	Any	Enable	WAN_IF	Allow
3	52.114.75.24	32	0	65535	Any	Enable	WAN_IF	Allow
4	52.114.76.76	32	0	65535	Any	Enable	WAN_IF	Allow
5	52.114.7.24	32	0	65535	Any	Enable	WAN_IF	Allow
6	52.114.14.70	32	0	65535	Any	Enable	WAN_IF	Allow
49	0.0.0.0	0	0	65535	Any	Enable	WAN_IF	Block

The firewall rules on SBC look like the figure below:



4. Anynode SBC

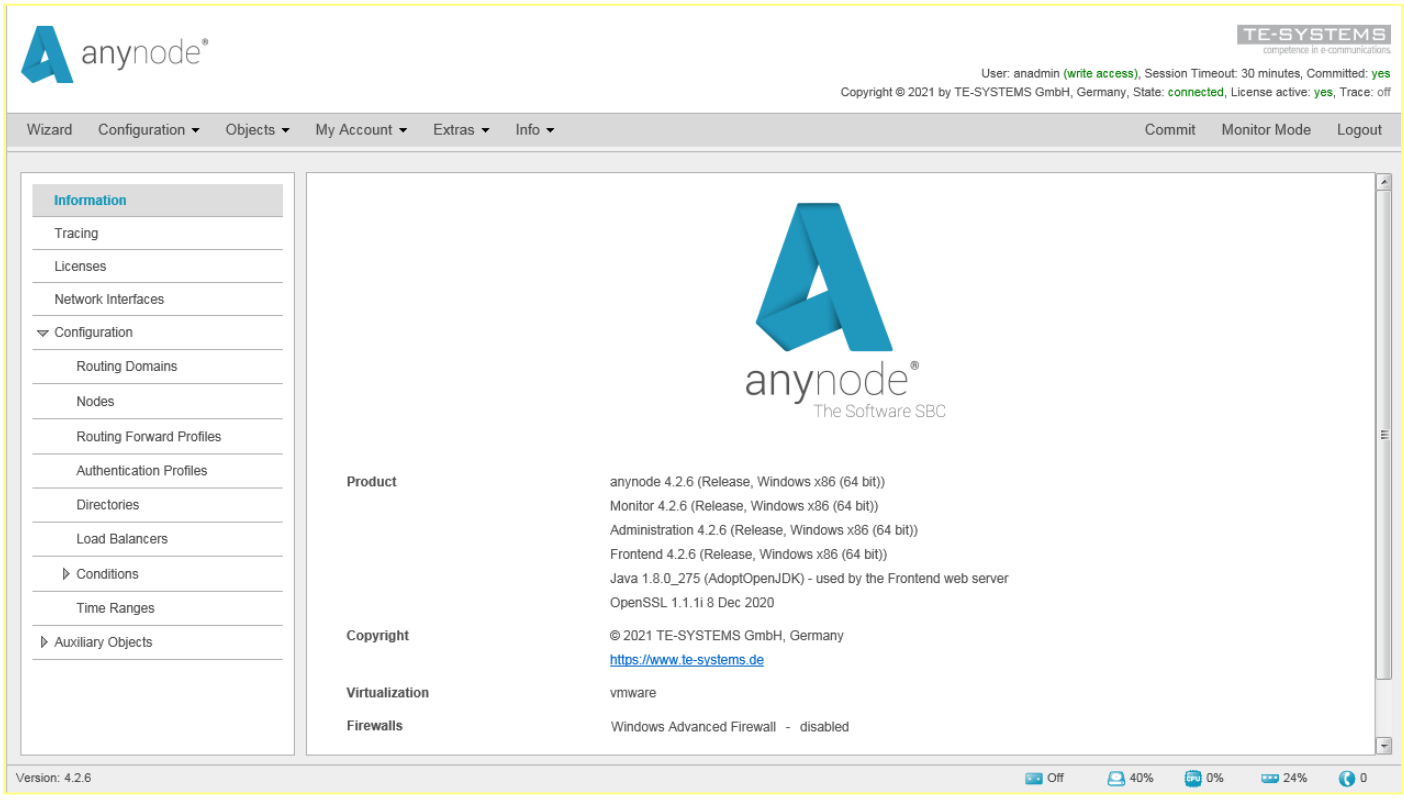
The configuration of anynode SBC for the testing activities needs is performed via **"anynode configuration wizard"**. The following sub-sections demonstrate the example configuration utilized in current certification testing activities; default or non-project specific anynode configuration will not be referenced.

To activate the connections between OSBiz PBX – anynode SBC and Microsoft Phone System – anynode SBC, the OSBiz PBX and the Microsoft Phone System must be configured as **"Nodes"**. Each node can handle several rules for incoming and outgoing numbering manipulations. Routing decisions can be made based on the source or destination prefix, extension ranges, and on the source node. If a call matches such filter rules, it will be routed to the configured destination node.

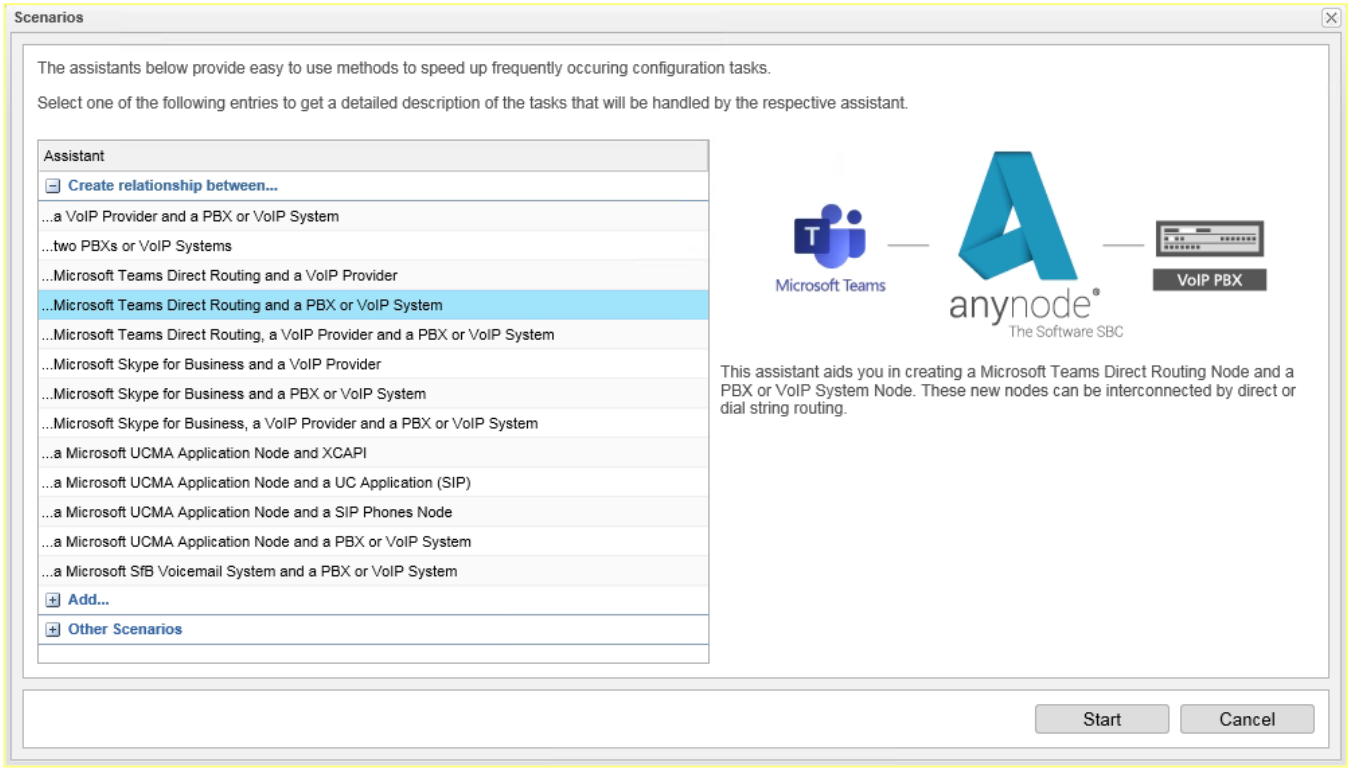
For more information regarding the anynode SBC configuration refer to anynode technote: https://community.te-systems.de/community-download/files?fileId=2587.

4.1. anynode Wizard – Teams / Voice over IP Provider

Access anynode web management portal and select **"Configuration Mode"**.

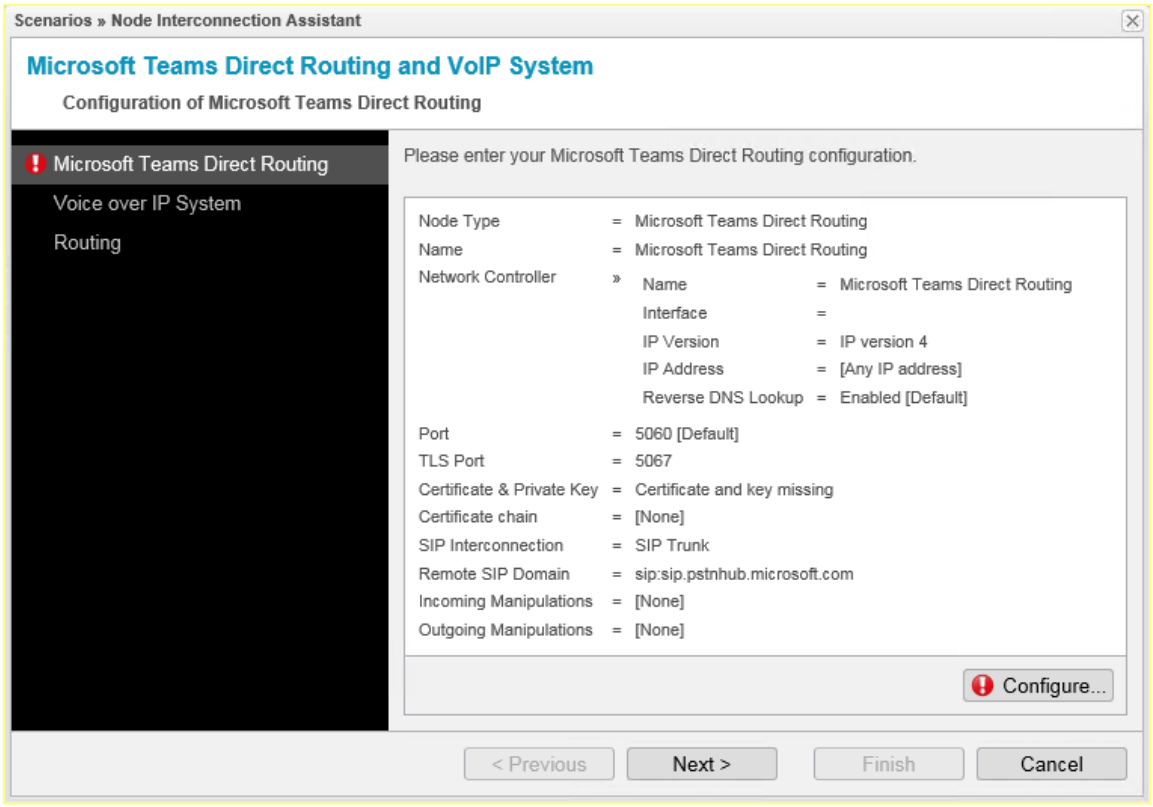


Click on **"Wizard"**.

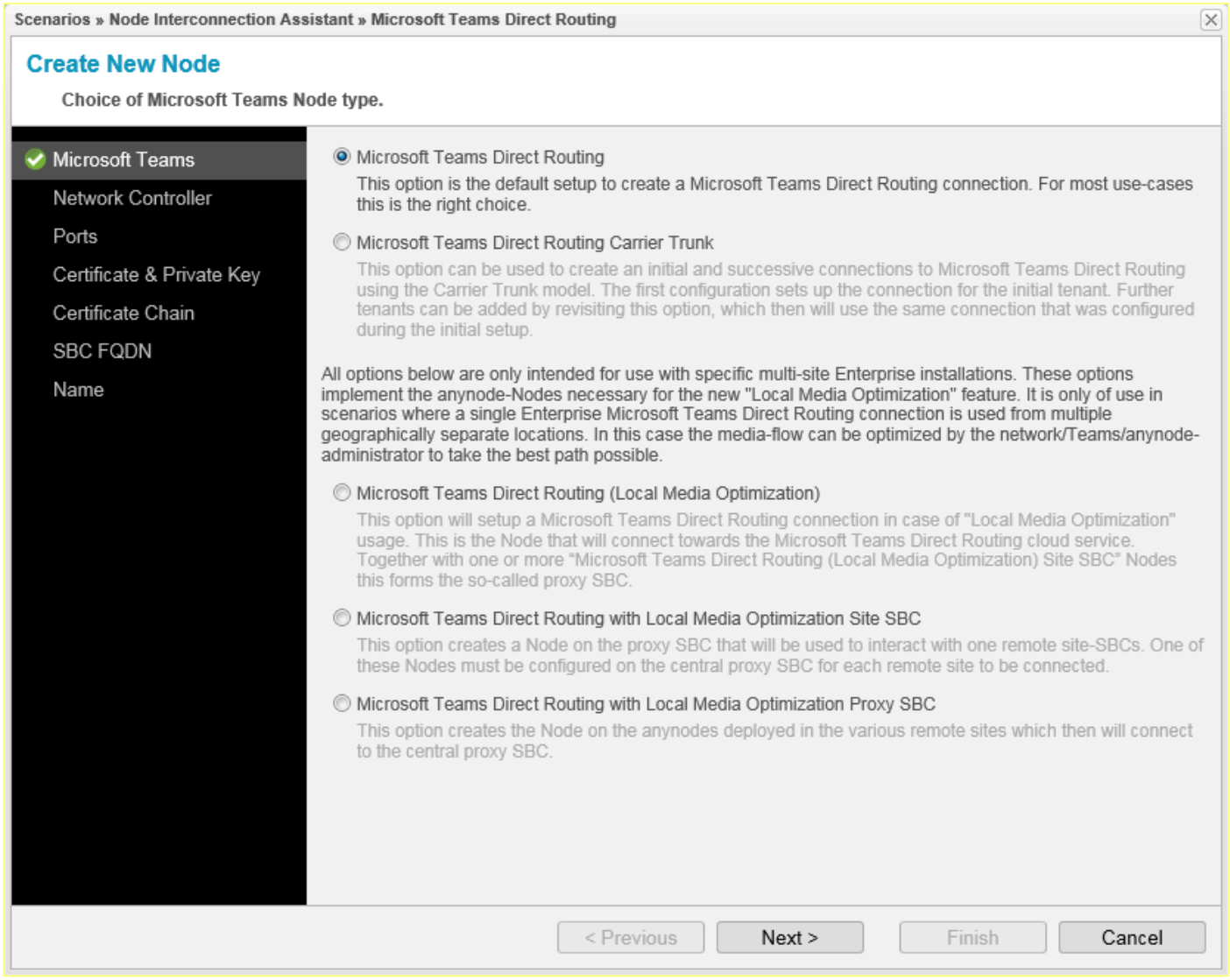


On the windows that appears select "Microsoft Teams Direct Routing and a PBX or VoIP System" under **"Create relationship between..."** and then click on **[Start]**.

The assistant now starts with first Node configuration, the **"Microsoft Teams Direct Routing"** Node.



Click on **[Configure]** after selecting **"Microsoft Teams Direct Routing"** to set up the Node details.

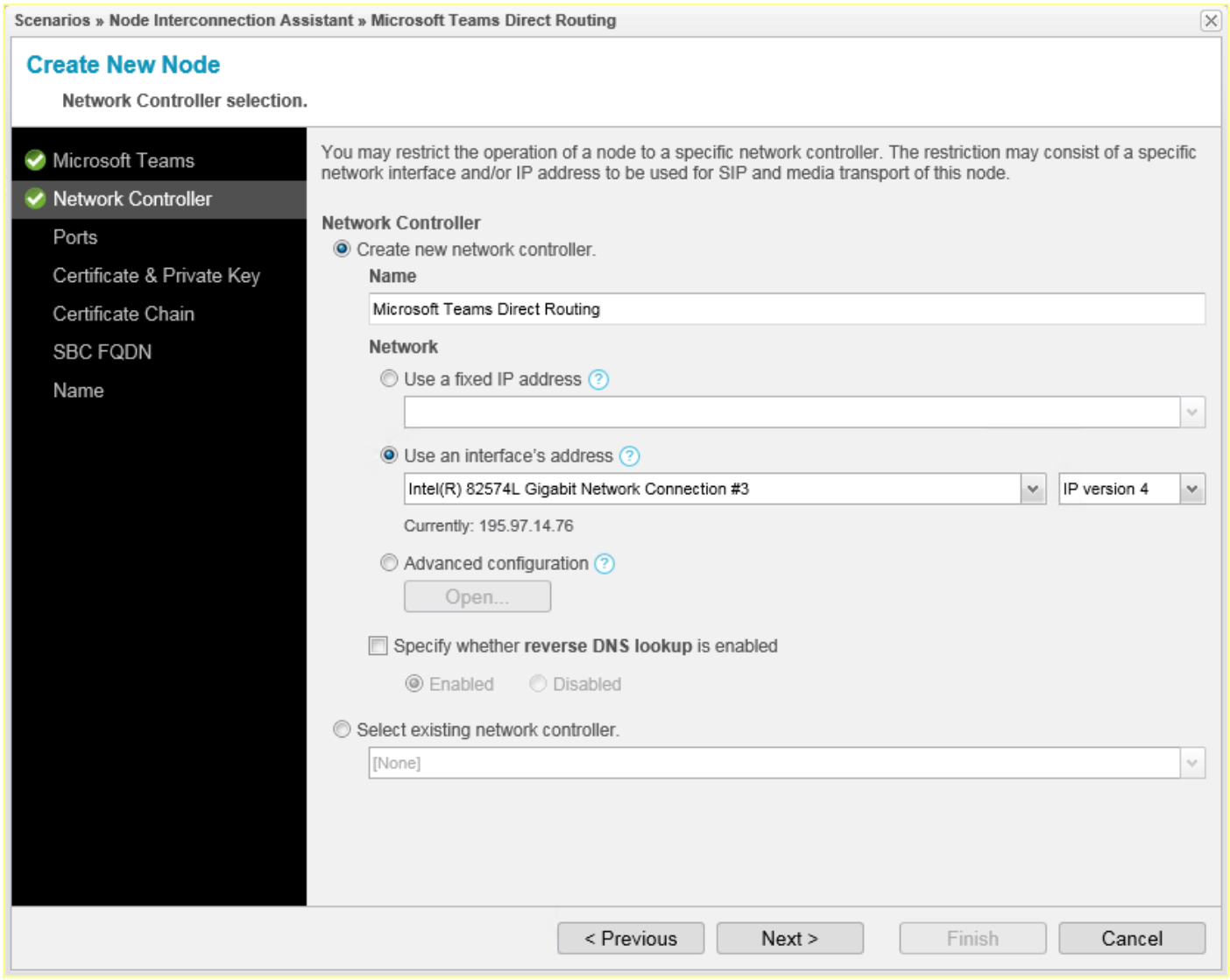


Select the standard trunking model i.e. "Microsoft Teams Direct Routing" in **"Microsoft Teams"** dialog.

Click on **[Next]**.

4.2. anynode Wizard – Teams / Network Controller

In the **"Network Controller"** dialog, create a new network controller.



Enter the following:

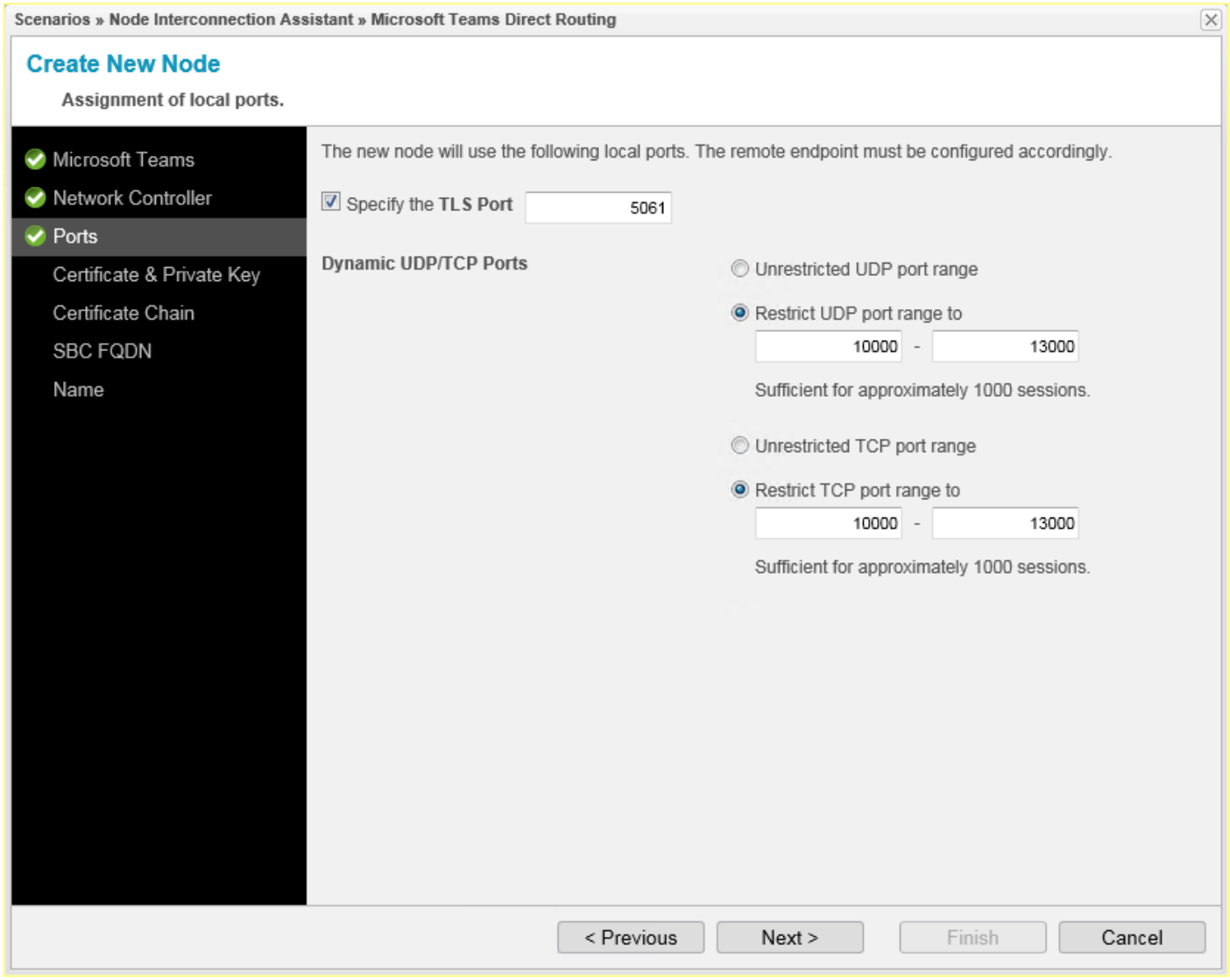
- **Name**: Microsoft Teams Direct Routing (common-sense name).
- **Use an interface's address**: *<Windows WAN machine ethernet adapter>*
  IP version 4 (IP Version)
  195.97.14.76 (Public IP Address).

Click on **[Next]**.

Note: Ensure that **"reverse DNS Lookup"** stays enabled for the public interface as this is a requirement for SIP through TLS connections.

4.3. anynode Wizard – Teams / Ports

For inbound firewall rules, you may define a UDP and SIP TCP port range which restricts the number of ports used by anynode. The number of ports in this range should at least be three times higher than the number of maximum concurrent sessions on this Node. If multiple anynode **"Network Controllers"** share the same physical network interface of the host, make sure to select unique port ranges to avoid any port overlapping.



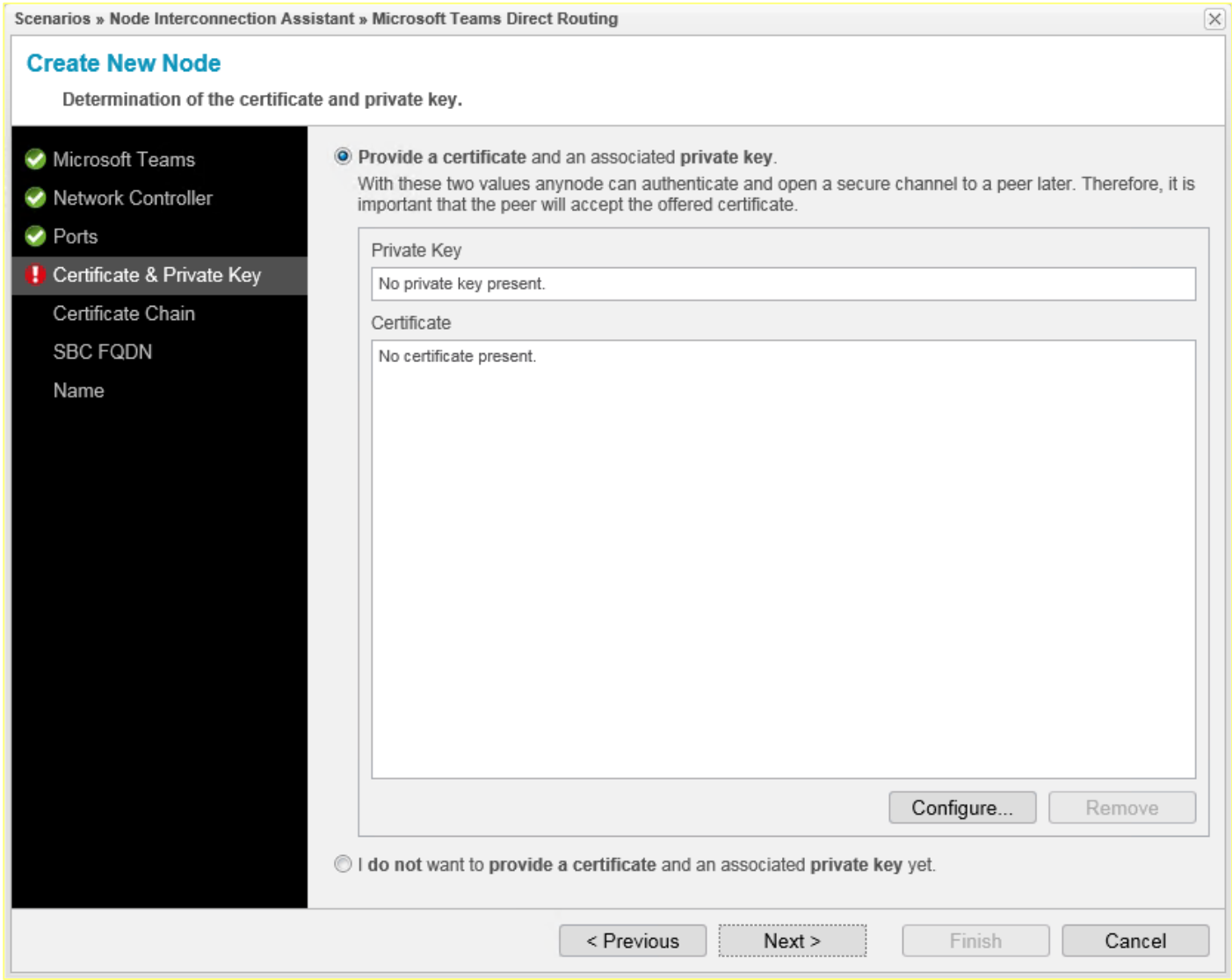
For the Teams Phone System connection set "5061" in **"TLS Port"** box (see sub-section 2.2).

Click on **[Next]**.

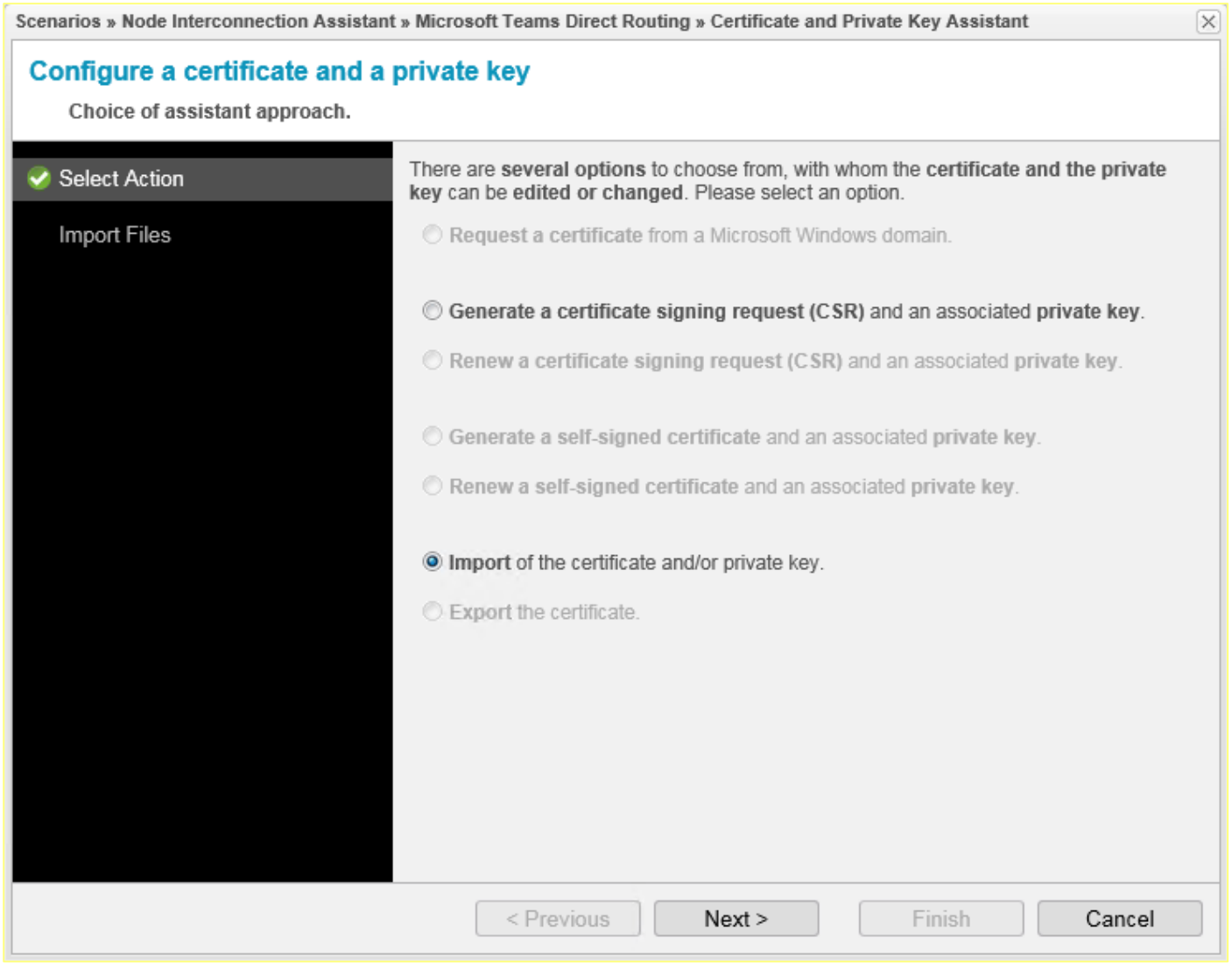
4.4. anynode Wizard – Teams / Certificate & Private Key

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.

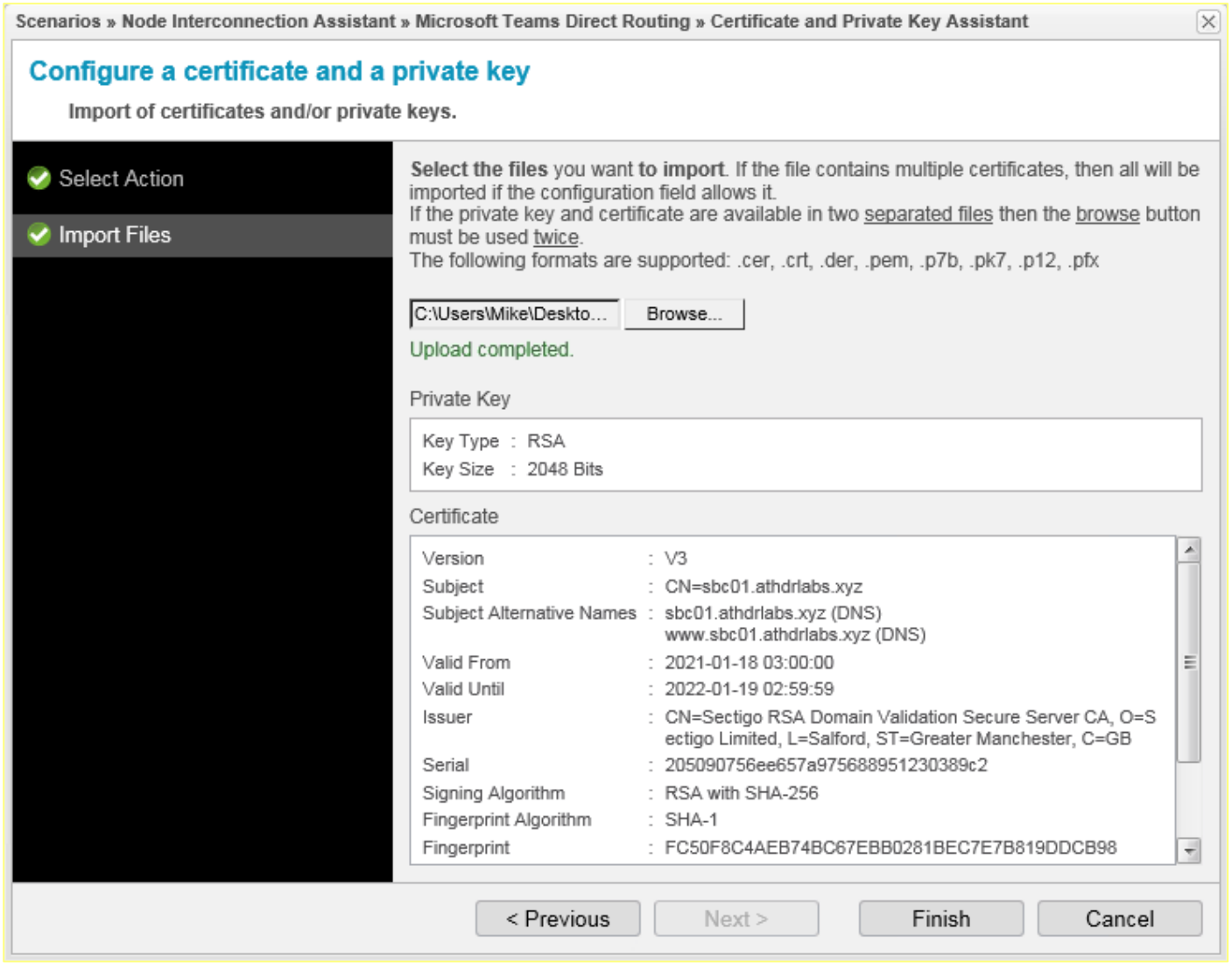
For TLS to work, time synchronization is required. So, NTP configuration is needed on SBC. The NTP used, should be in sync with Microsoft NTP server or any other global server.



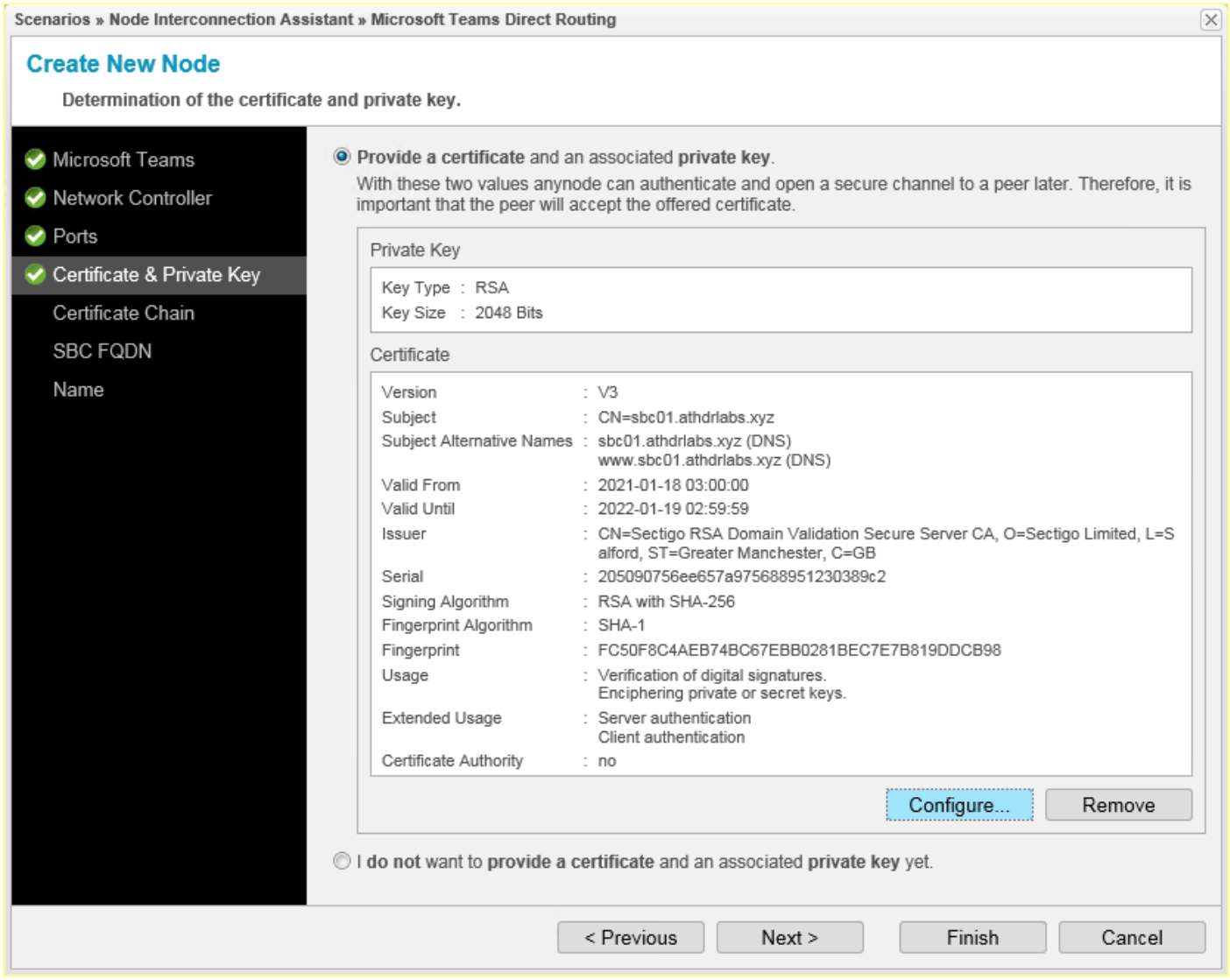
In **"Certificate & Private Key"** dialog, click on **[Configure]**.



On the window that appears in **"Select Action"** dialog, select "Import of the certificate and/or private key" and then click on **[Next]**.



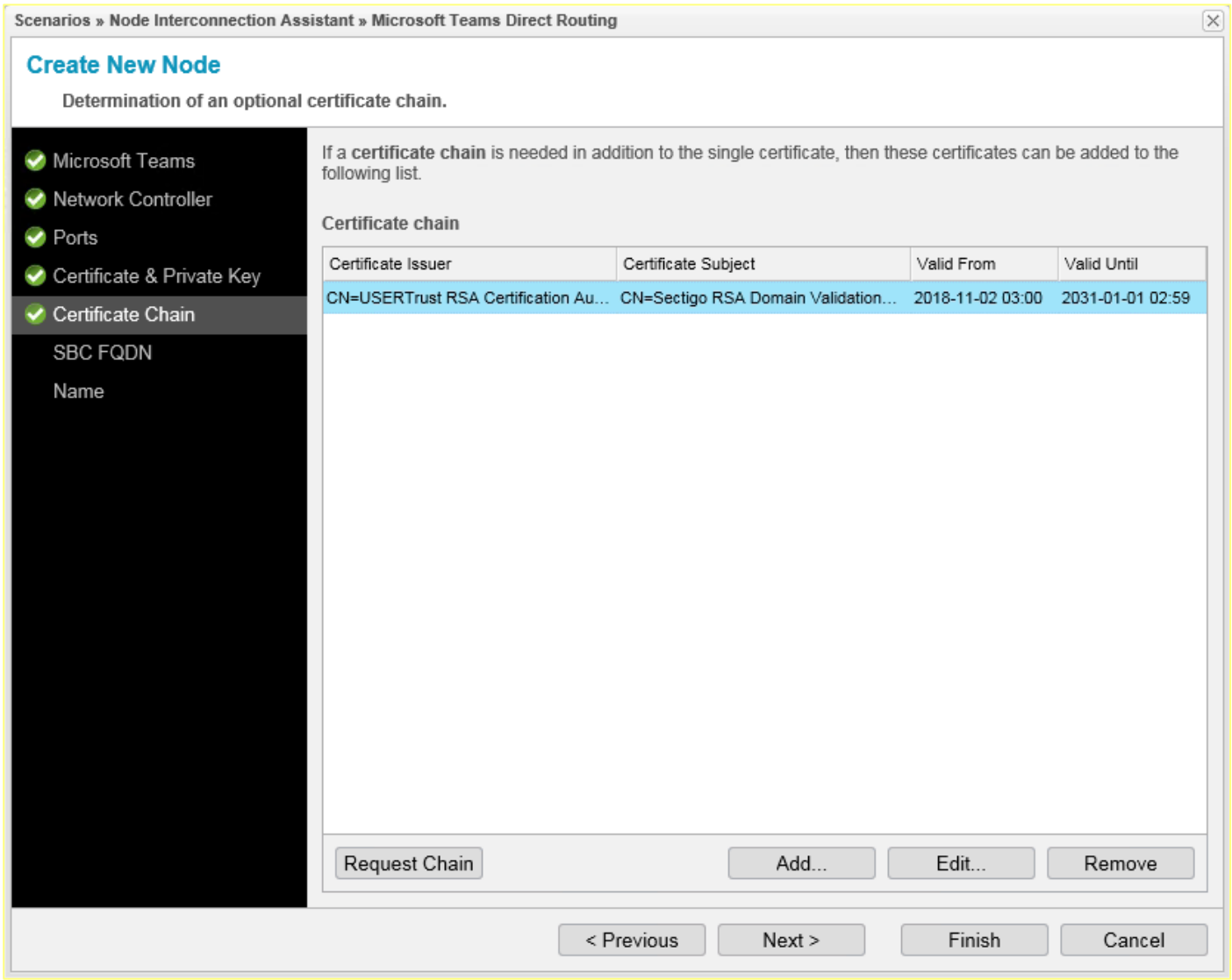
Both certificates provided by the CA must be imported in single files, e.g. "privatekey.pem" and "certificate.pem" files. So, both files must be browsed to, selected, and imported one at a time. If the import and subject validation is fine and nothing is highlighted red, proceed by clicking on **[Finish]**.



If everything is set for the **"Certificate & Private Key"** dialog, proceed by clicking on **[Next]**.

4.5. anynode Wizard – Teams / Certificate Chain

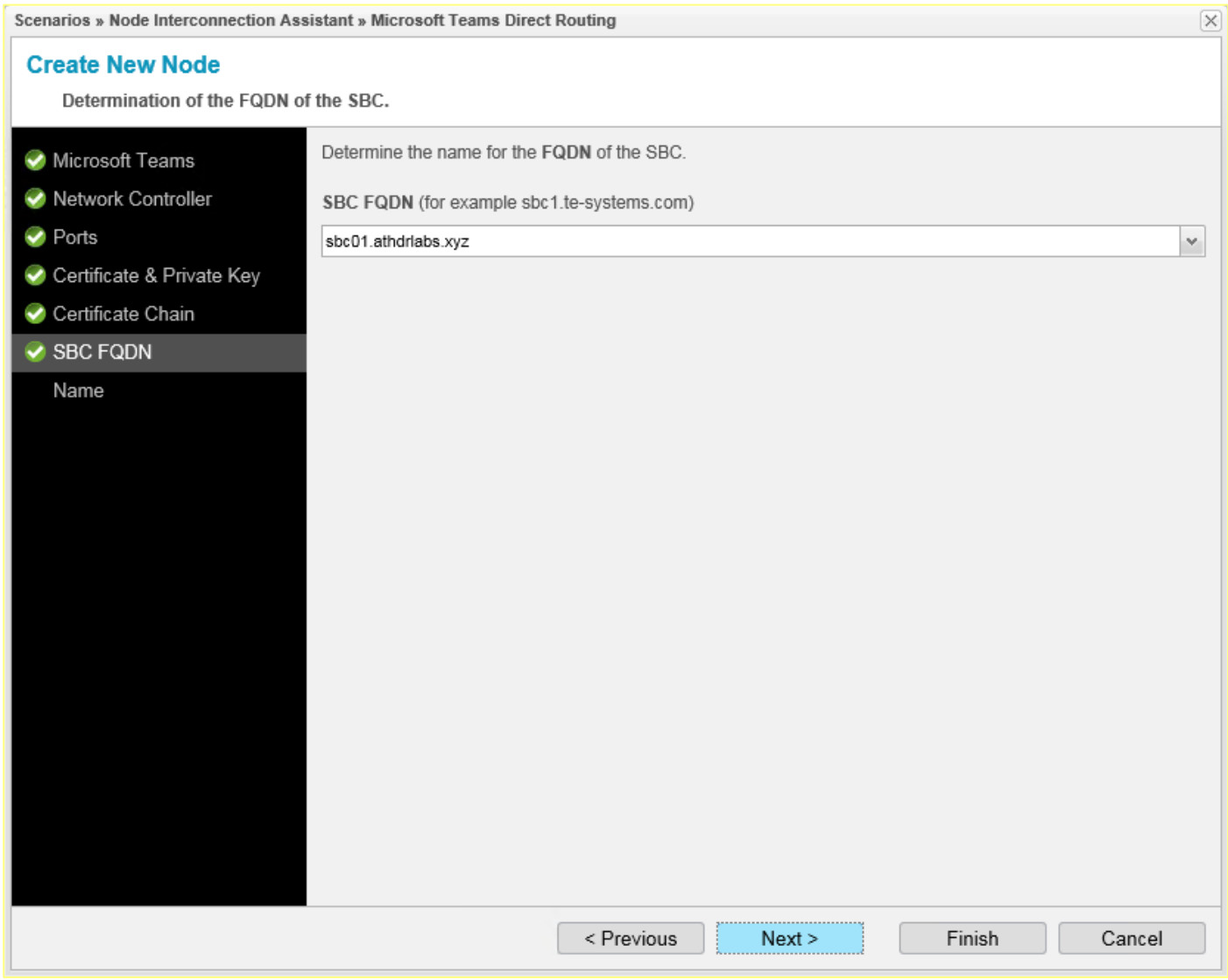
Next, the certificate chain is properly displayed as anynode provides some default validation certificates. If there is no valid chain available, the corresponding certificate (e.g. "ca_chain.pem") must be imported via the **[Add]** button.



Click on **[Next]** to move on to the next configuration dialog.

4.6. anynode Wizard – Teams / SBC FQDN

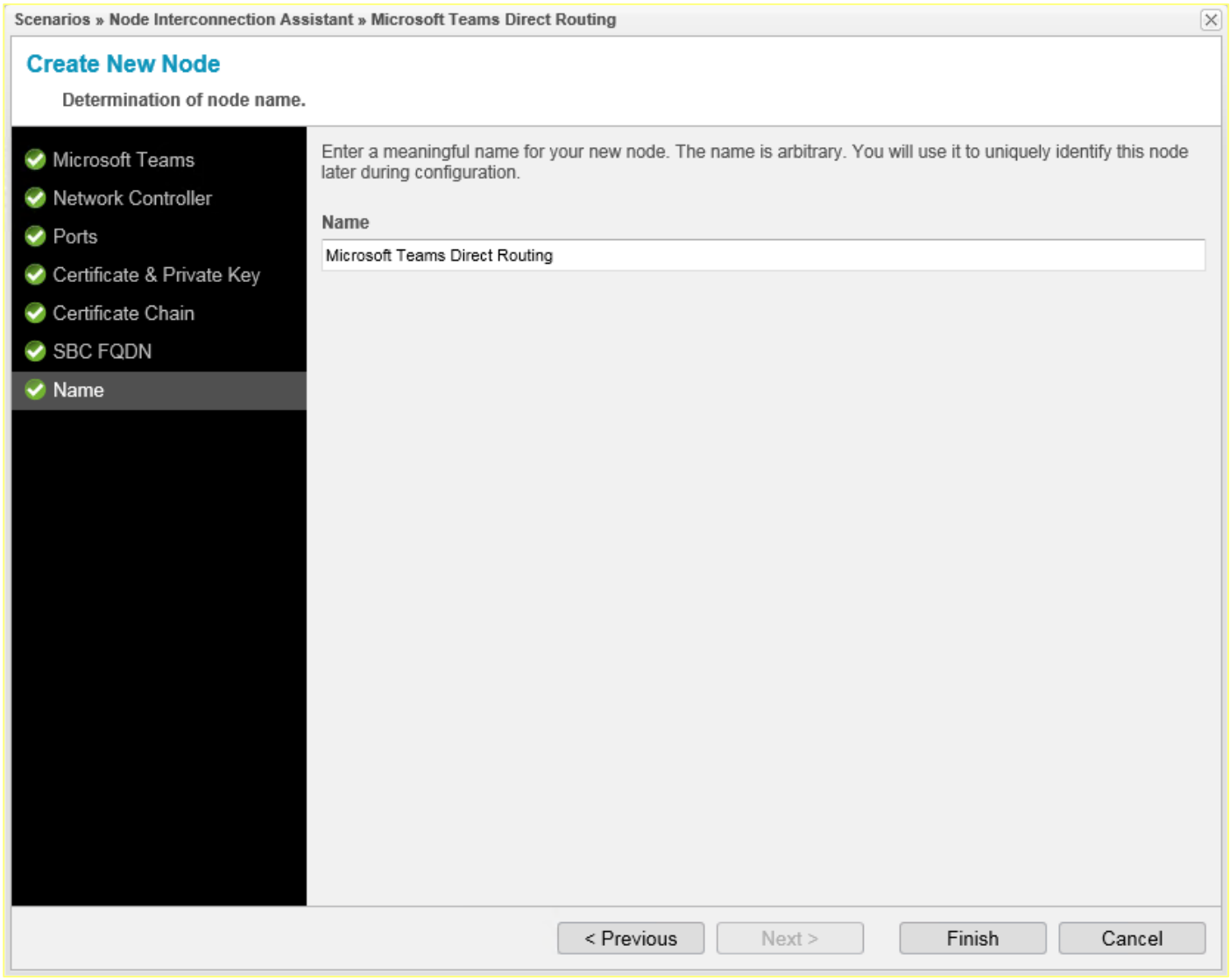
If provided, the FQDN will be automatically determined through the previous given certificates.



Click on **[Next]**.

Note: This FQDN is the one used for the SBC pairing with Office 365 tenant (see sub-section 2.2). This FQDN is statically mapped to the corresponding SIP, from and SIP contact headers, as external host name for the SIP Options packets that will be send by anynode.

4.7. anynode Wizard – Teams / Name

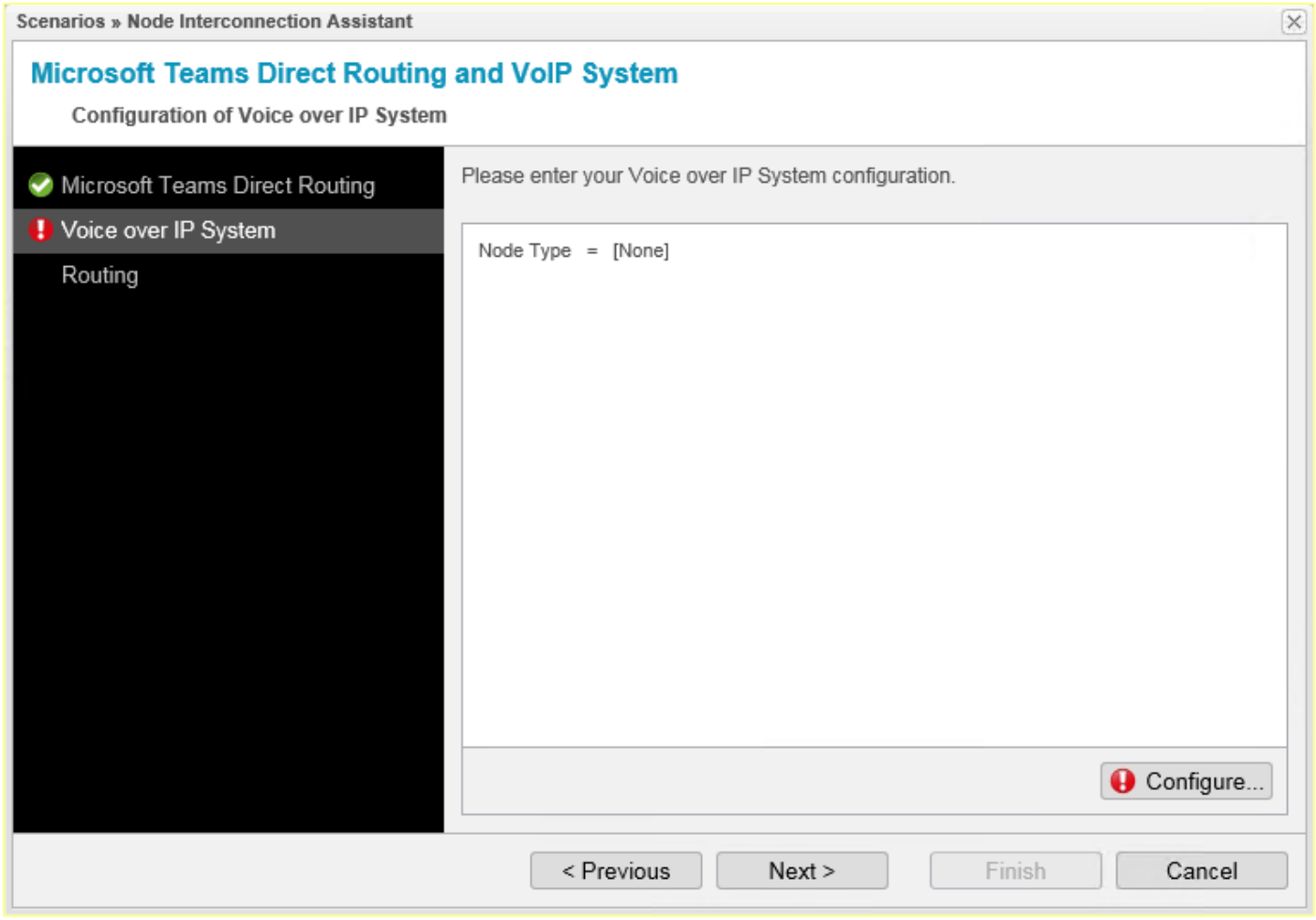


In the final assistant dialog, set friendly name for Teams Phone System, e.g. "Microsoft Teams Direct Routing".

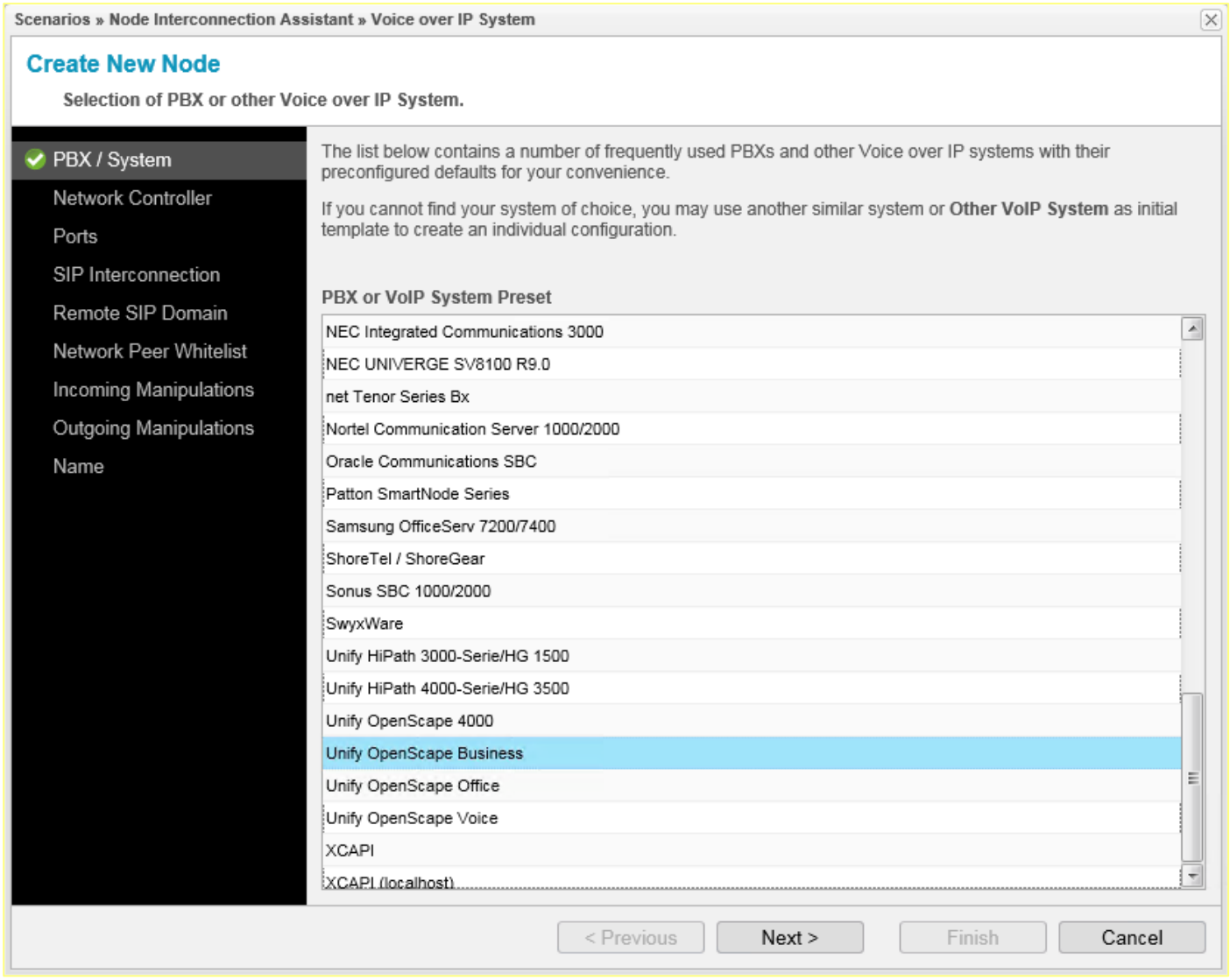
Click on **[Finish]**.

4.8. anynode Wizard – OSBiz / Voice over IP System

After completing the **"Microsoft Teams Direct Routing"** configuration, from the **"Node Interconnection Assistant"** window the connection to OSBiz PBX is going to be setup.

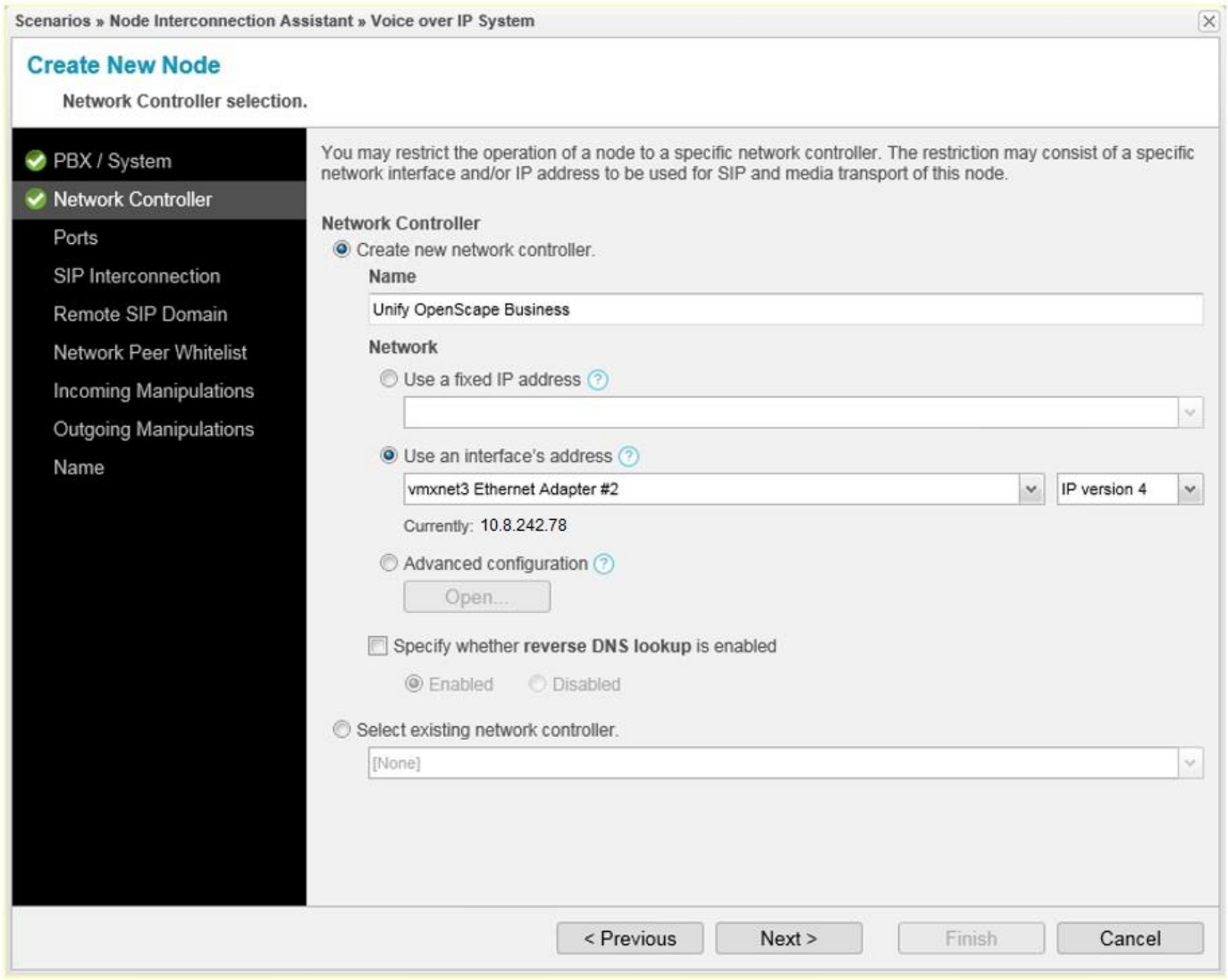


Click on **[Configure]** after selecting **"Voice over IP System"**.



Select "Unify OpenScape Business" under **"PBX / System"** dialog and click on **[Next].**

4.9. anynode Wizard – OSBiz / Network Controller



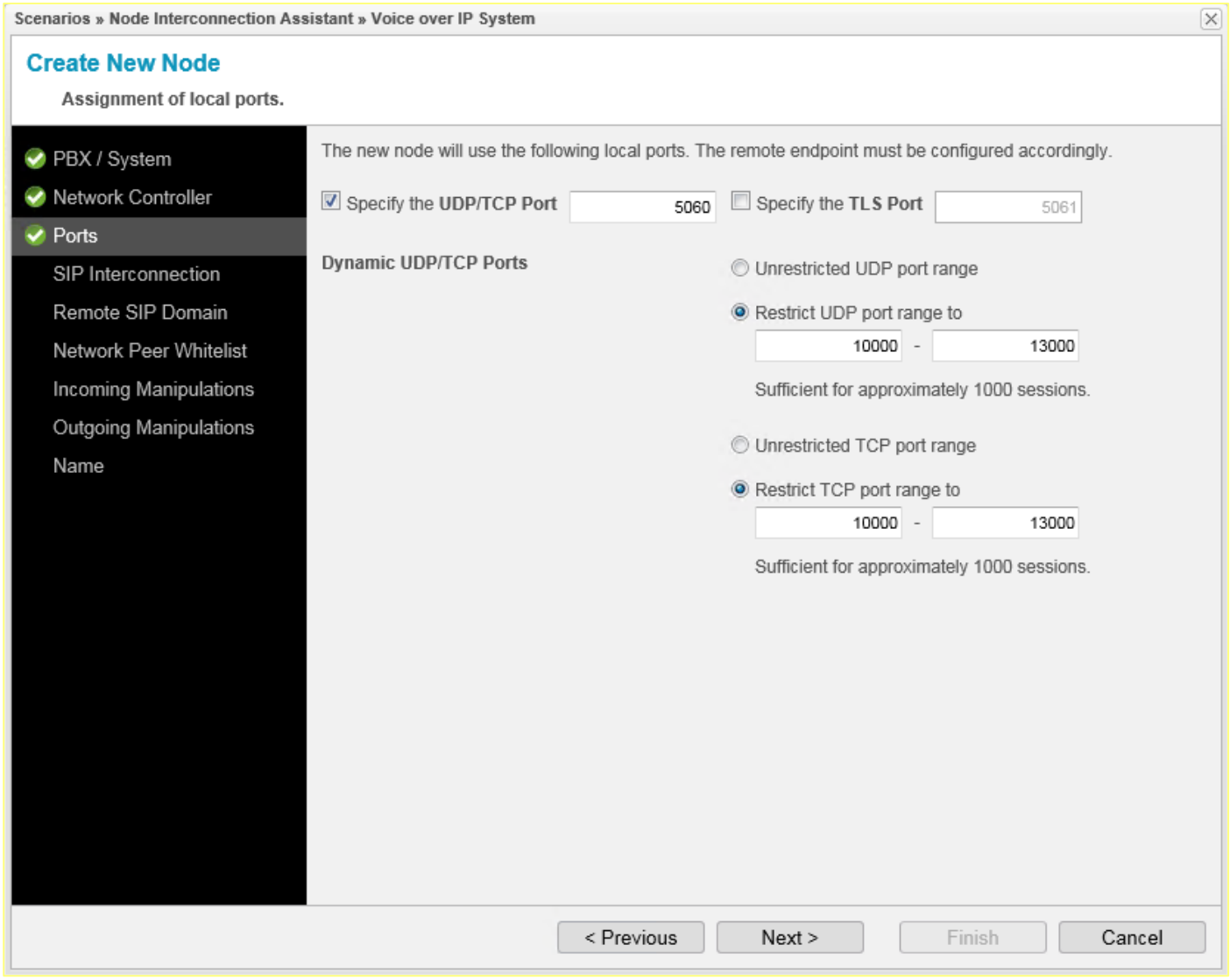
In the **"Network Controller"** dialog, create a new network controller by entering the following:

- **Name**: Unify OpenScape Business (common-sense name).
- **Network**: *<Windows LAN ethernet adapter>* (Interface)
  IP version 4 (IP Version)
  10.8.242.78 (Internal IP Address).

Click on **[Next].**

4.10. anynode Wizard – OSBiz / Ports

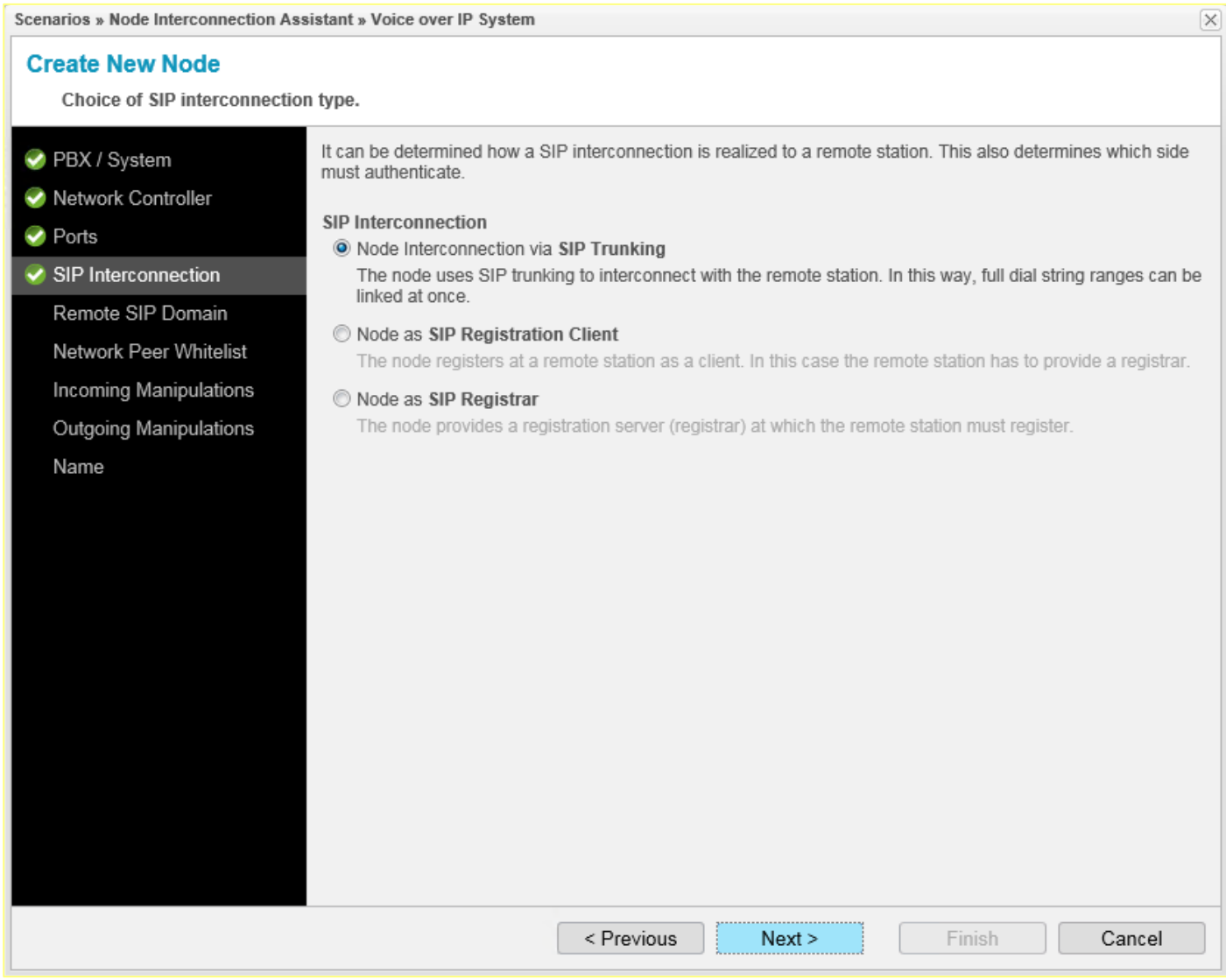
The port values for UDP, TCP and TLS are configured in **"Ports"** dialog. Ensure that those port values are conforming to the network and remote configurations.



For **"UDP/TCP Port"** and for the current test environment set the value "5060" (refer to sub-section 5.2).

Click on **[Next]**.

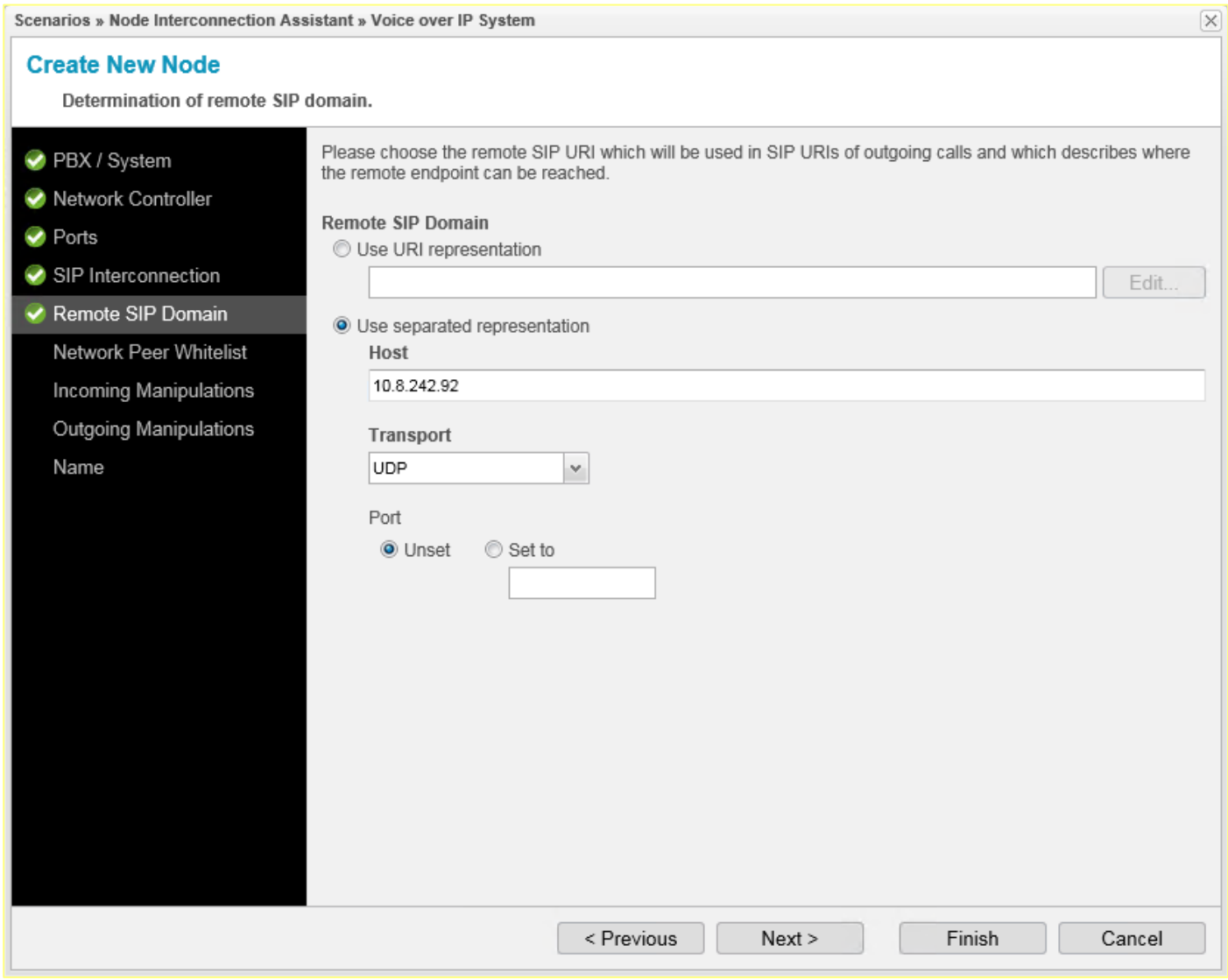
4.11. anynode Wizard – OSBiz / SIP Interconnection



In **"SIP Interconnection"** dialog, enable "Node Interconnection via SIP Trunking" radio button and click on **[Next]**.

4.12. anynode Wizard – OSBiz / Remote SIP Domain

Access the **"Remote SIP Domain"** dialog.



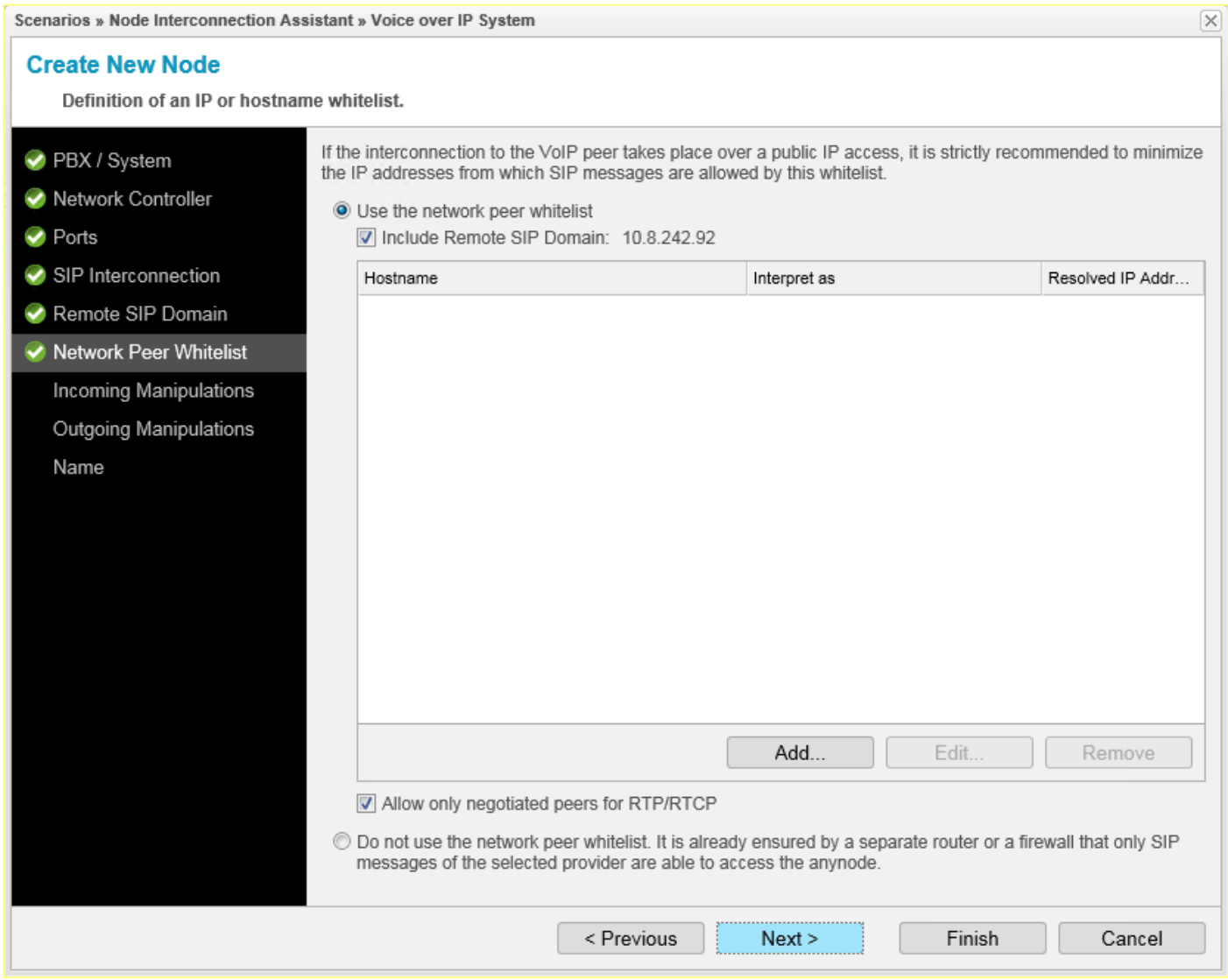
Enter the following:

- **Host**: 10.8.242.92 (OpenScape Business IP).
- **Transport**: UDP (transport protocol for connecting to the OpenScape Business, see also sub-section 5.2).

Click on **[Next]**.

4.13. anynode Wizard – OSBiz / Network Peer Whitelist

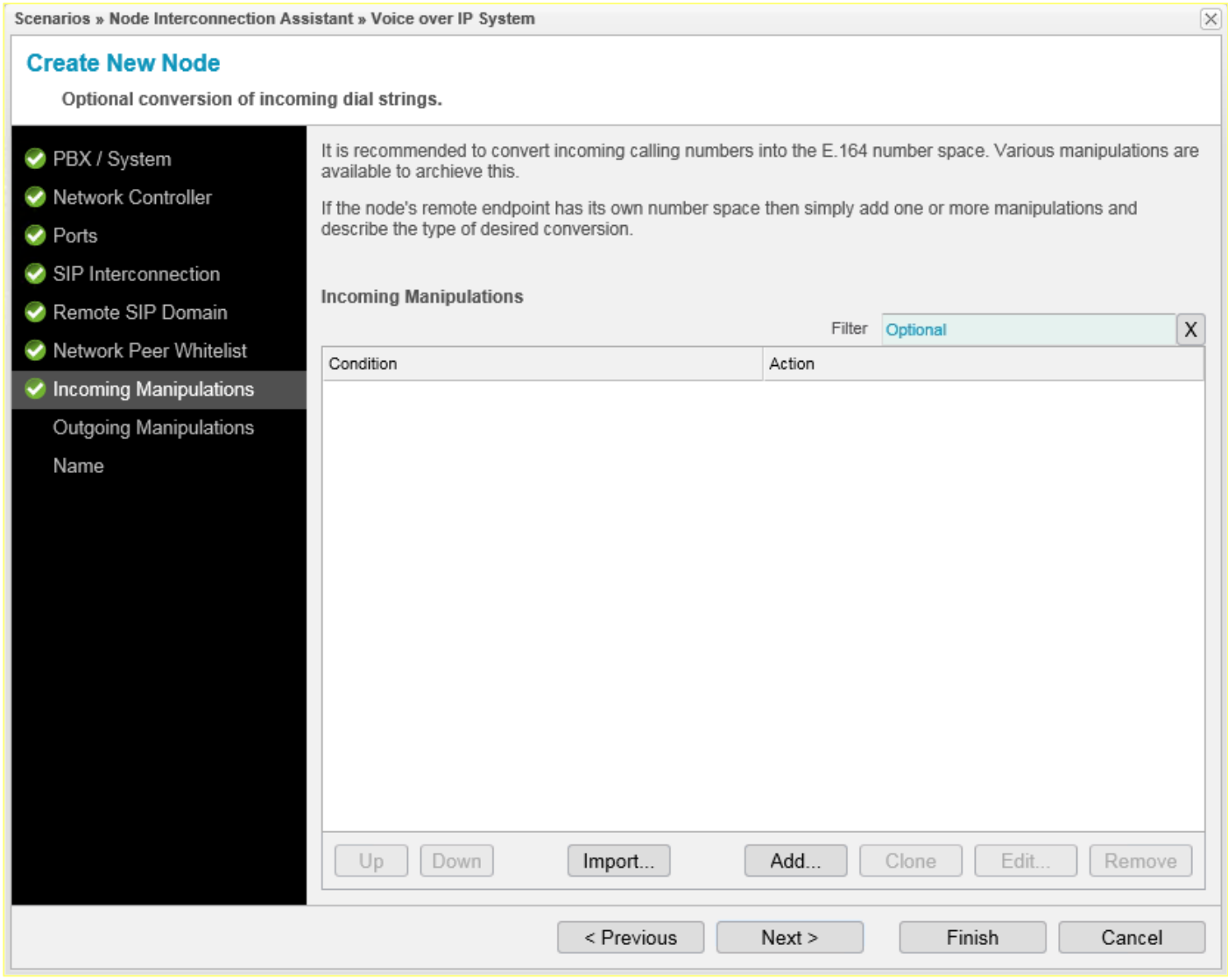
In **"Network Peer Whitelist"** dialog, the default settings are kept.

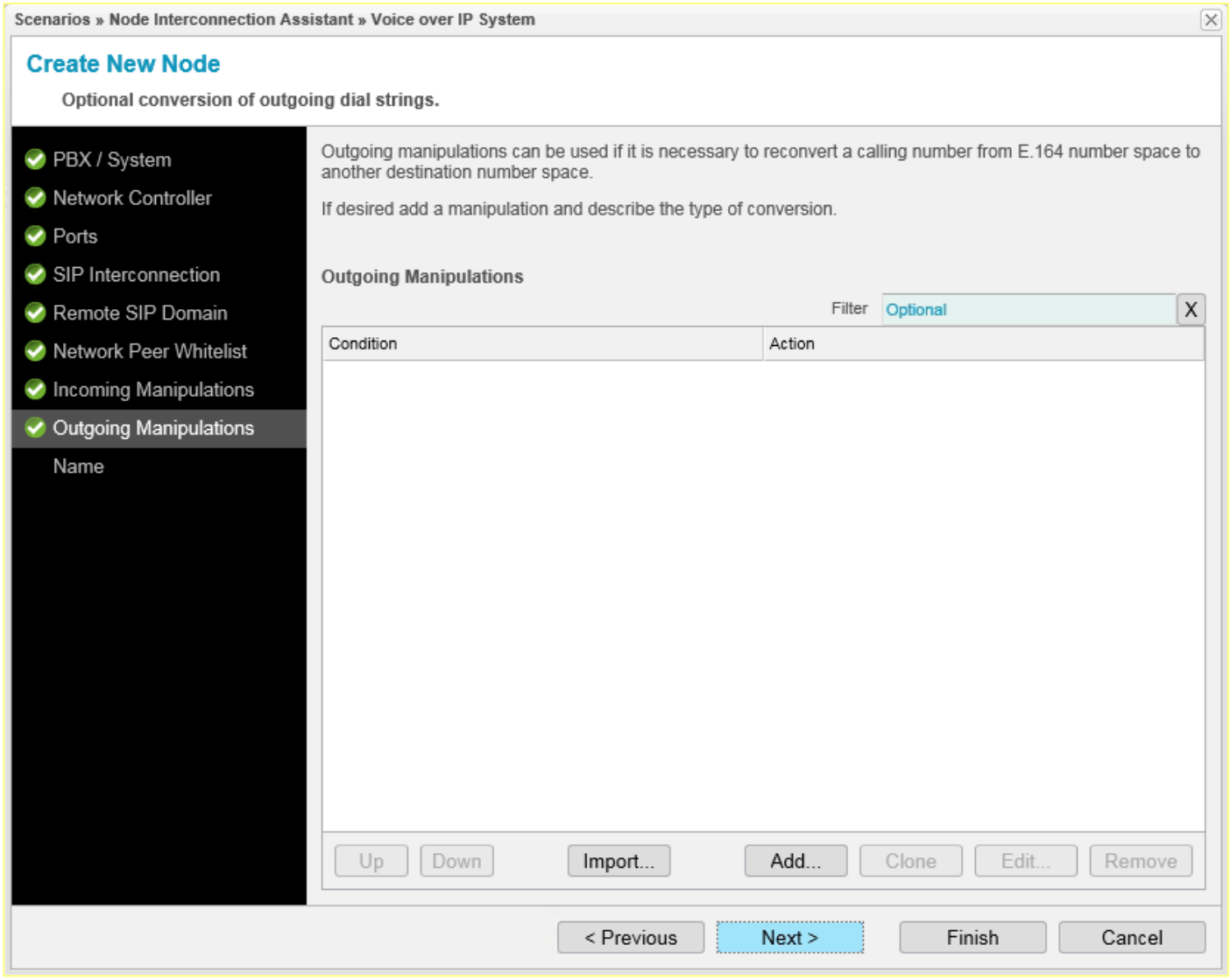


Click on **[Next]**.

4.14. anynode Wizard – OSBiz / Manipulations

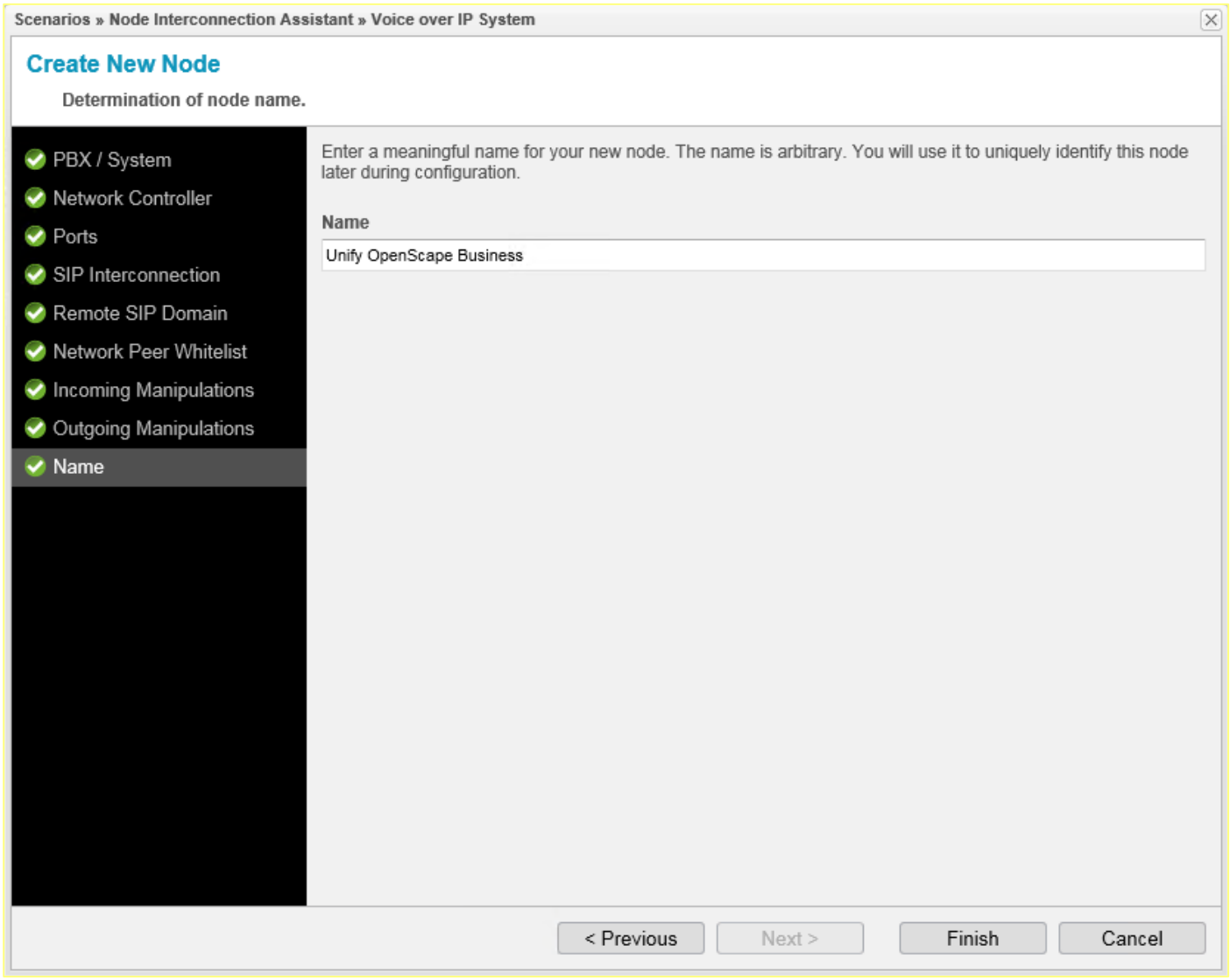
For the needs of current testing activities **"Incoming Manipulations"** and **"Outgoing Manipulations"** dialogs are skipped. There is no need for dialed digit manipulations.





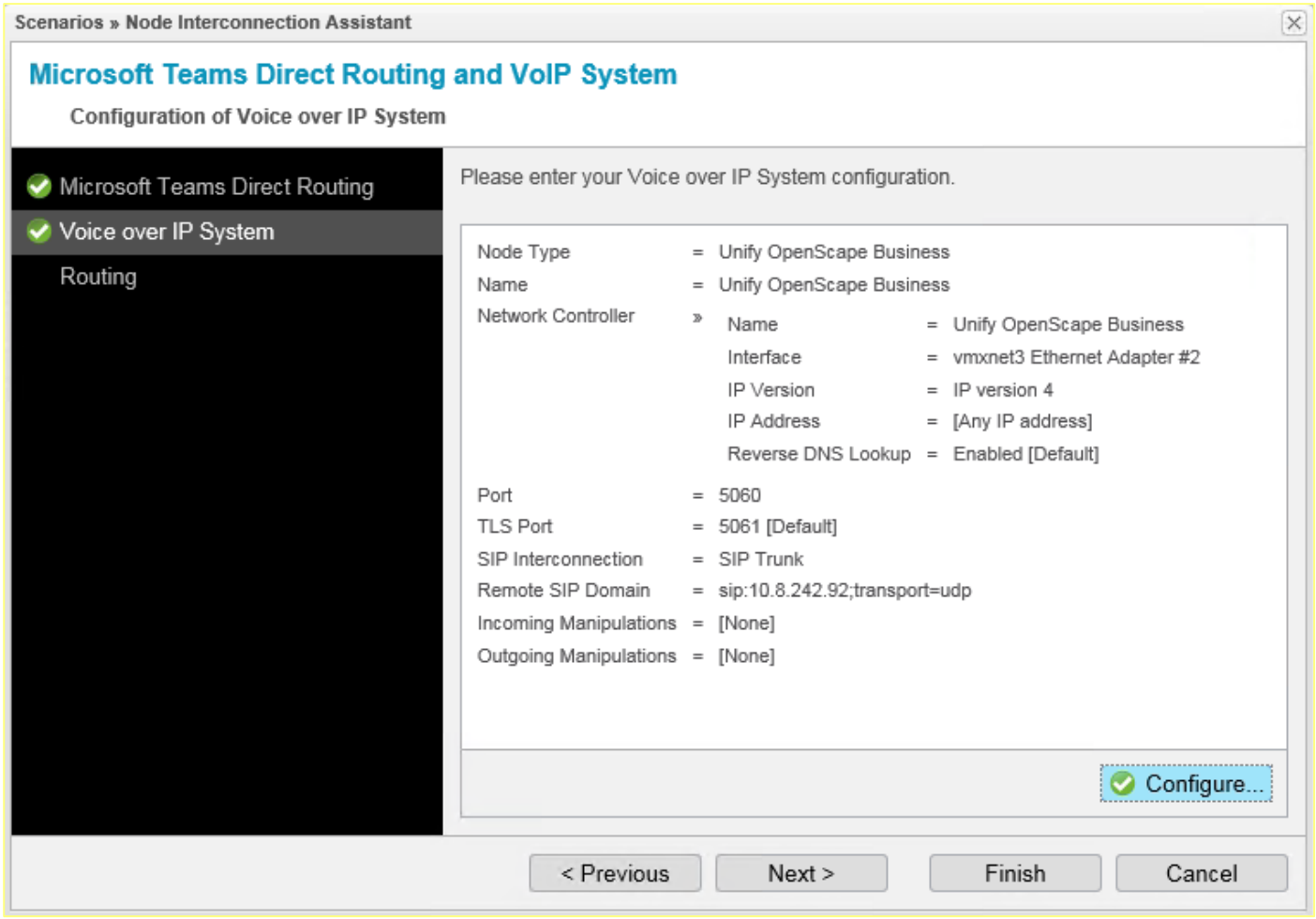
Click on **[Next]**.

4.15. anynode Wizard – OSBiz / Name



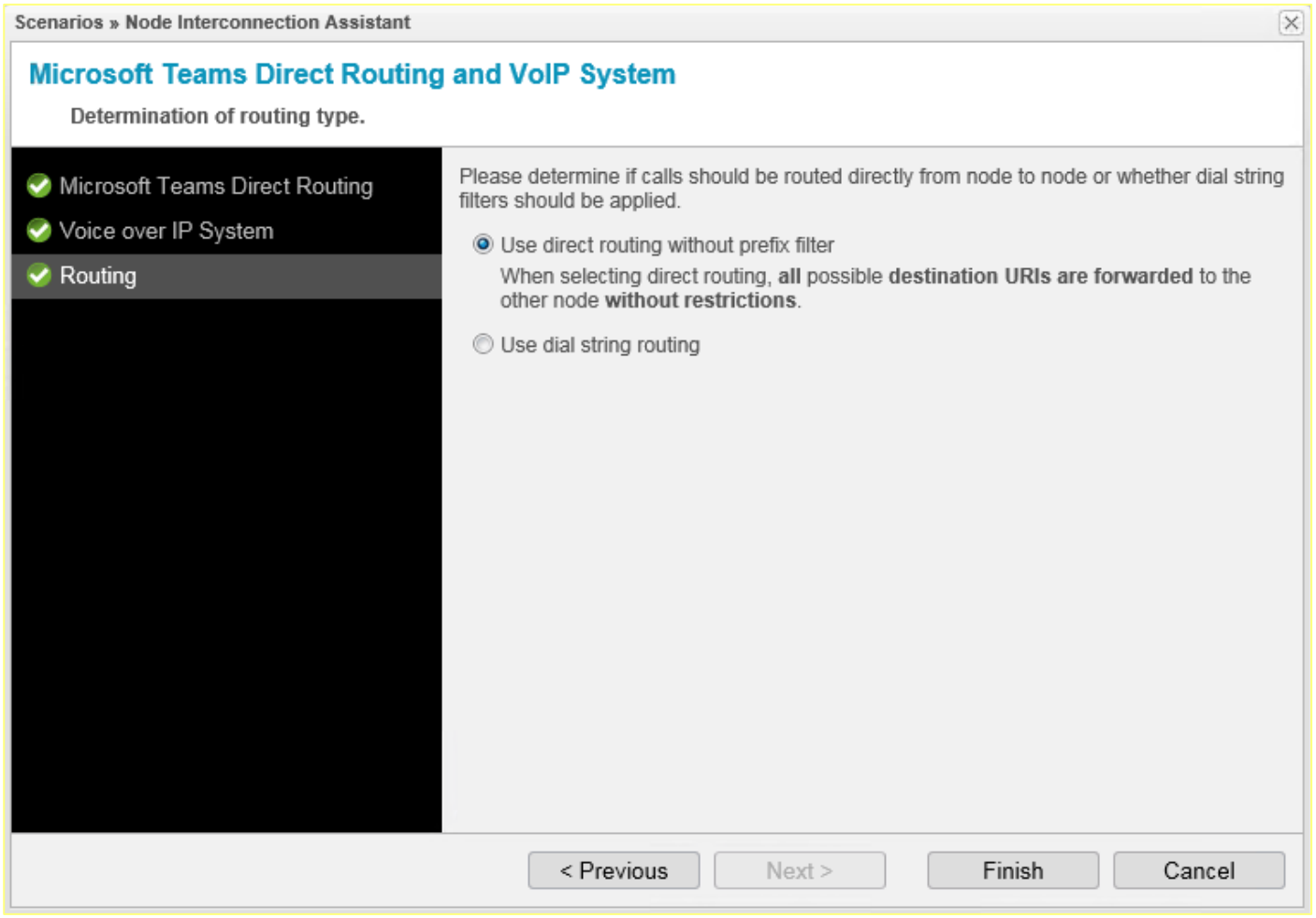
In the final assistant dialog, a default node display common sense name is set, e.g. "Unify OpenScape Business".

Click on **[Finish]**.



Continue with **[Next]** to configure the **"Routing"** and finalize the wizard.

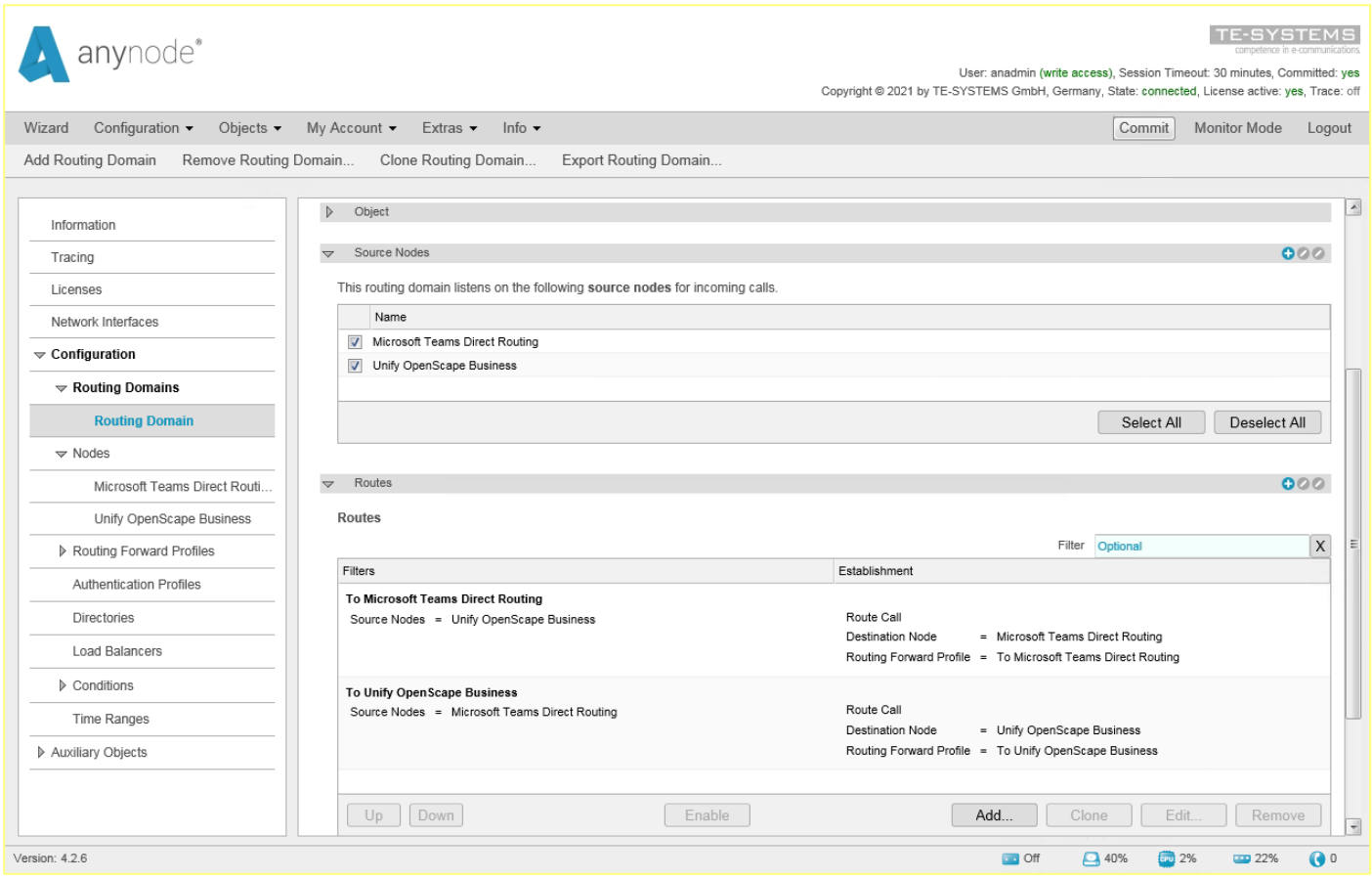
4.16. anynode Wizard – Routing



For **"Routing"** dialog, select "Use direct routing without prefix filter".

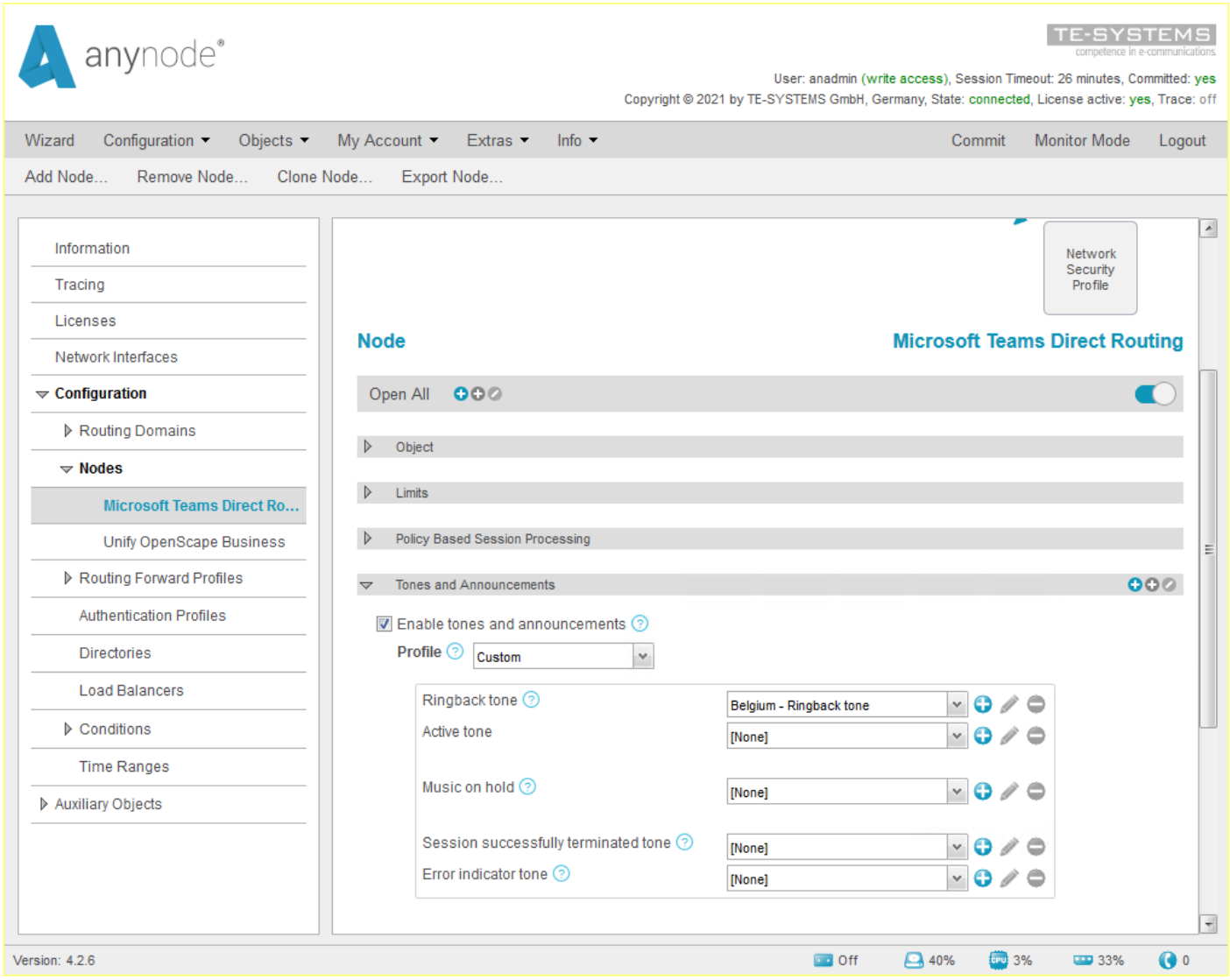
Click on **[Finish]**.

The latter action automatically creates the corresponding entries for anynode's **"Routing Domain"** as shown below:



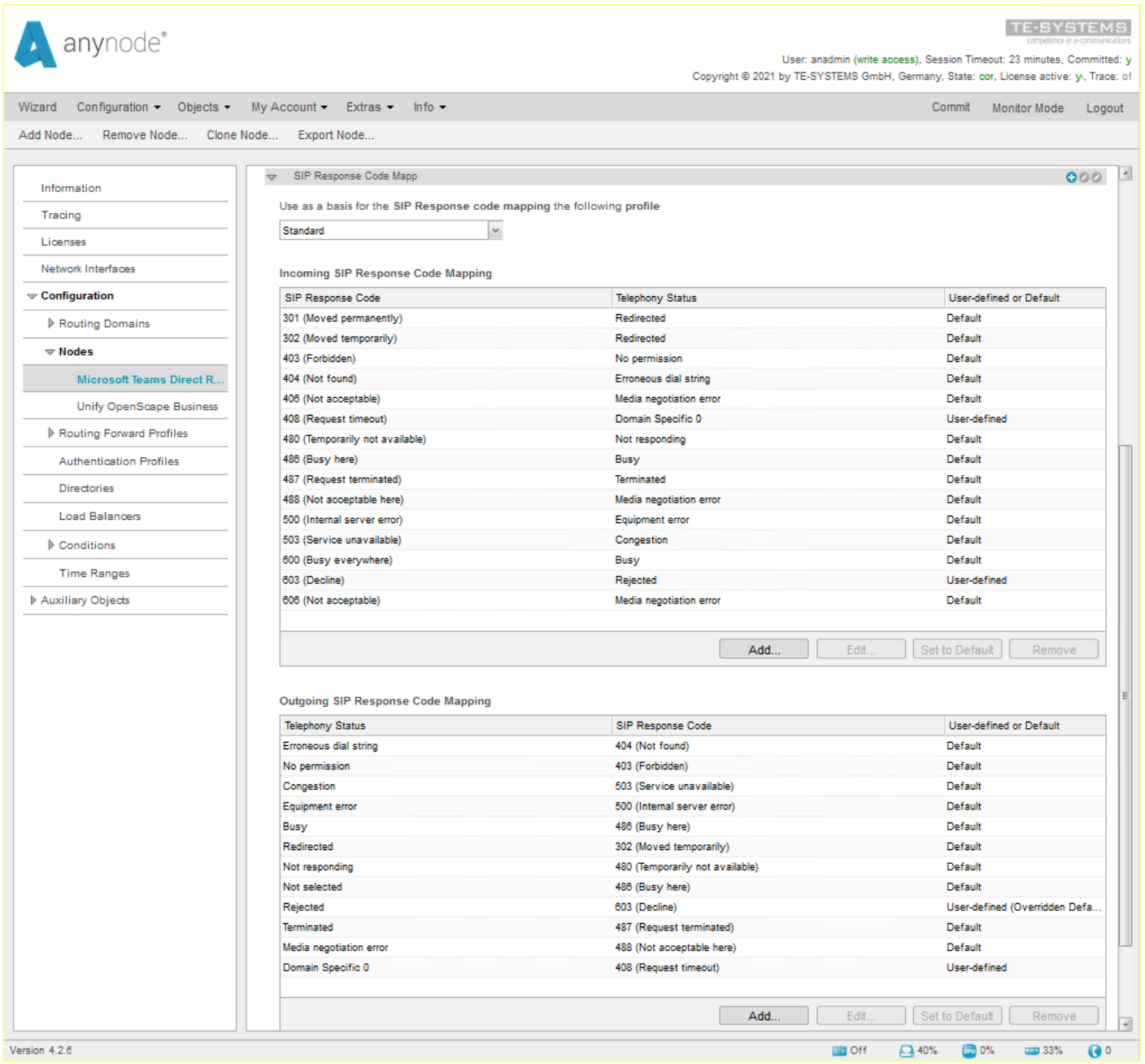
4.17. anynode SBC – Additional Configuration

Navigate to **WBM >> Configuration >> Nodes >> <MS Teams DR node> >> Tones and Announcements** as shown in picture below:



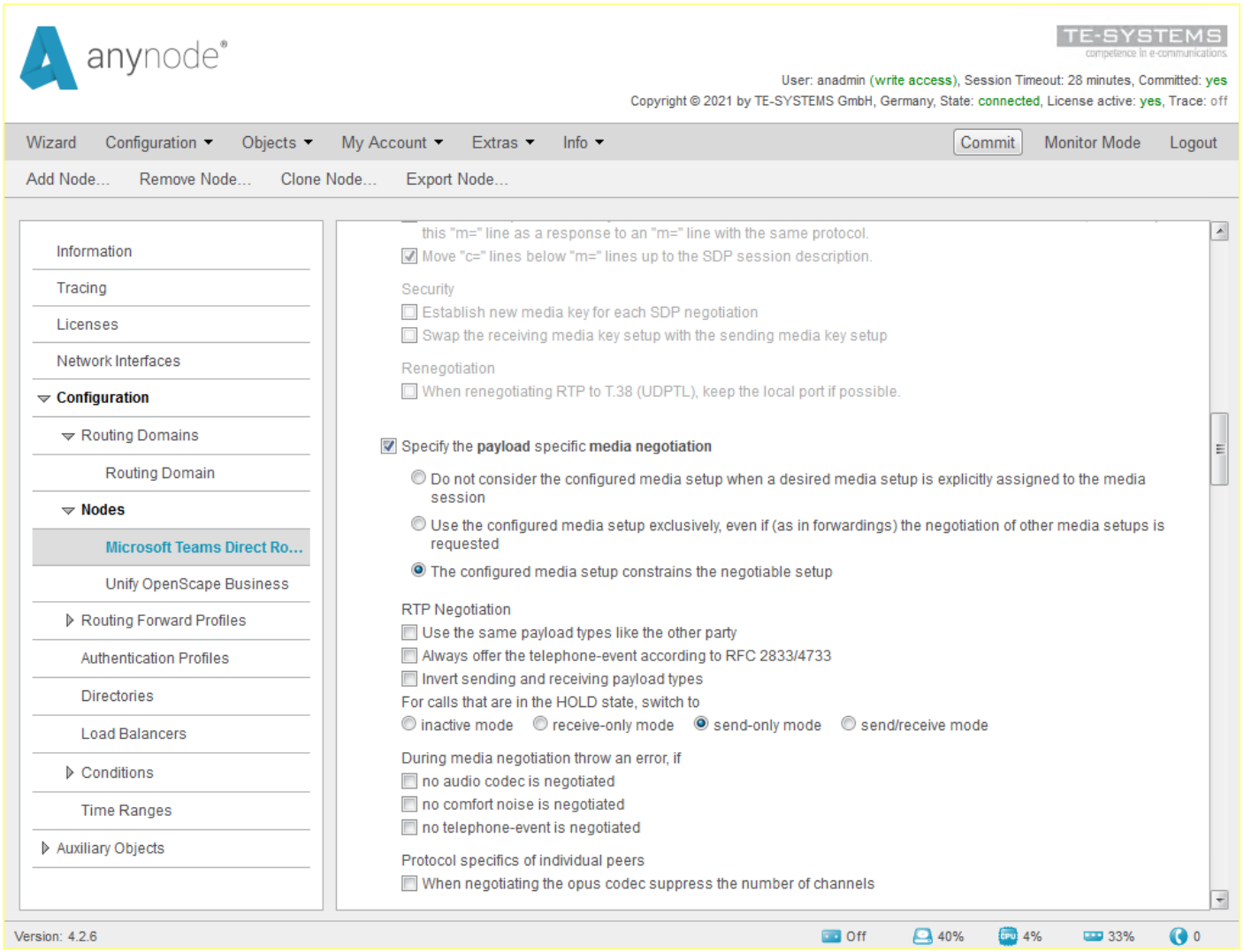
Activate **"Enable tones and announcements"** flag and set e.g. "Belgium - Ringback tone" in **"Ringback tone"** dropdown box.

At **WBM >> Configuration >> Nodes >> <MS Teams DR node> >> SIP Node**, modify the default **"SIP Response Code Mapping"** configuration.



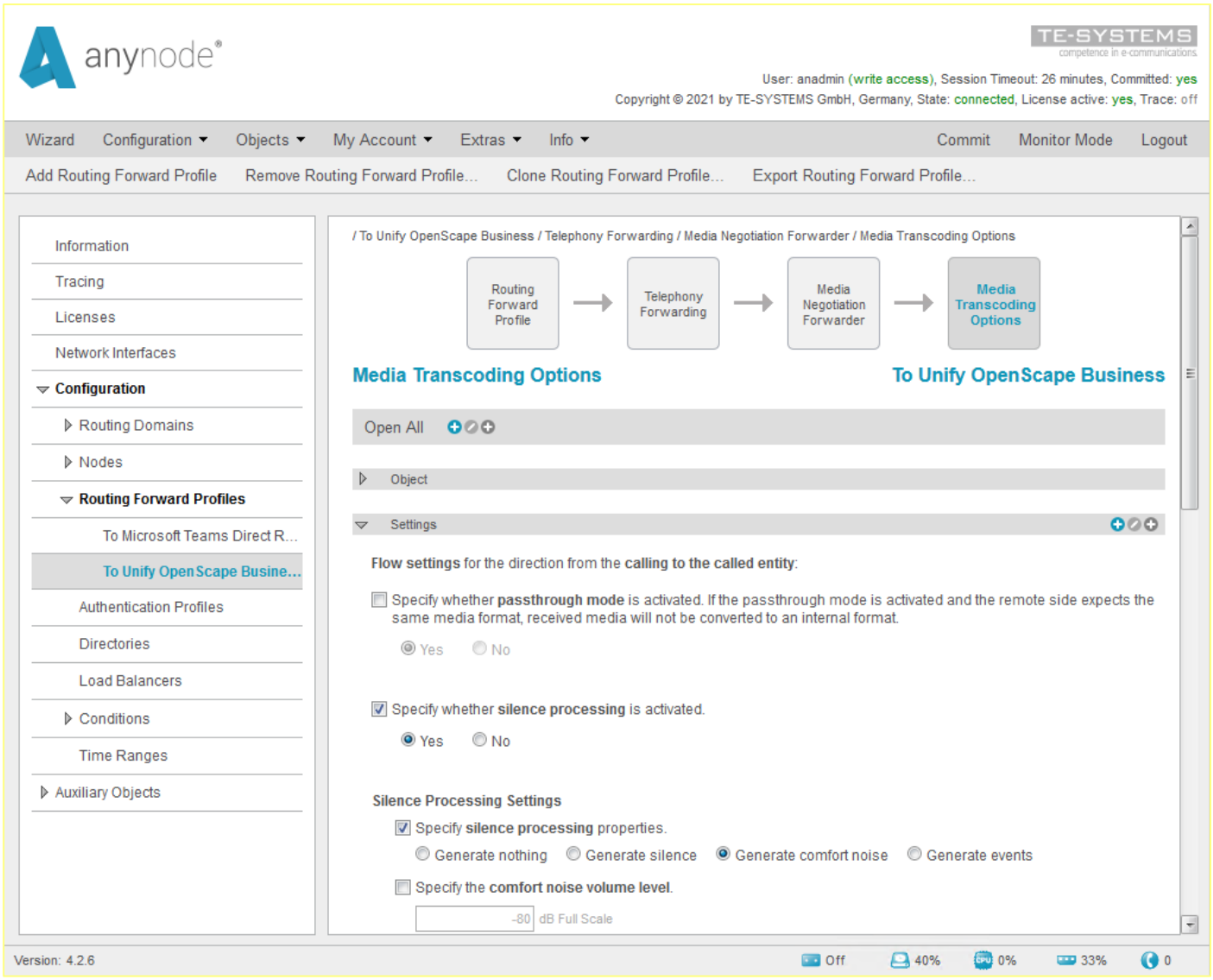
Set the user-defined values "603 (Decline)" and "408 (Request Timeout)" in **"Incoming SIP Response Code Mapping"** and **"Outgoing SIP Response Code Mapping"** configuration areas.

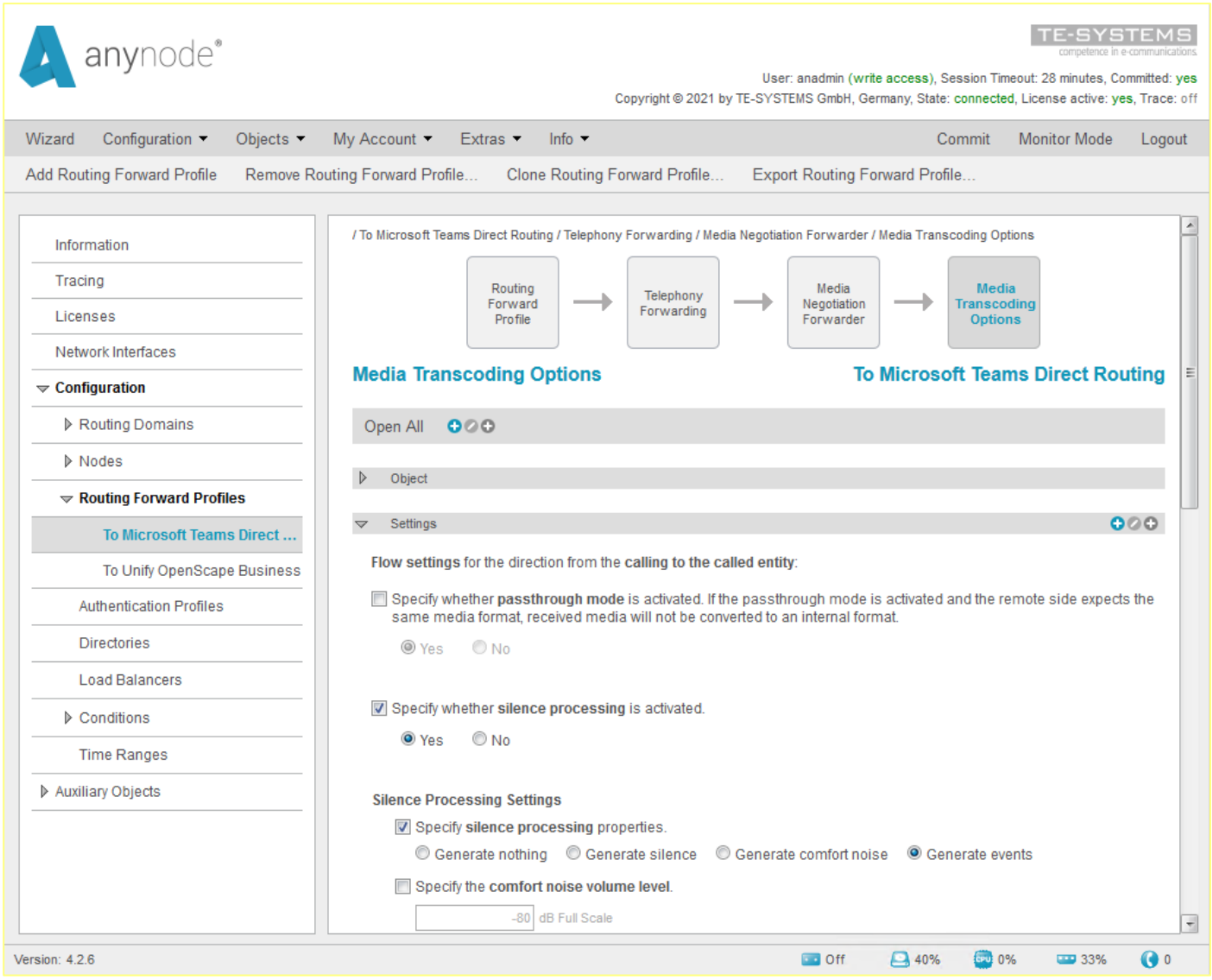
Access **WBM >> Configuration >> Nodes >> <MS Teams DR node> >> Media Negotiation >> Settings** (3rd detail level), change the system default configuration for the **"Specify the payload specific media negotiation"** by enabling the corresponding flag.



Set "send-only mode" (the default is "inactive mode") for the **"RTP Negotiation"** selection options. This configuration affects the call hold behavior.

In regards to the comfort noise observations , at **WBM >> Configuration >> Routing Forward Profiles >> <To MS Teams Profile> / <To OSBiz Profile>>> Media Transcoding Options** webpages, the example configuration used for the testing activities is shown in the pictures below:



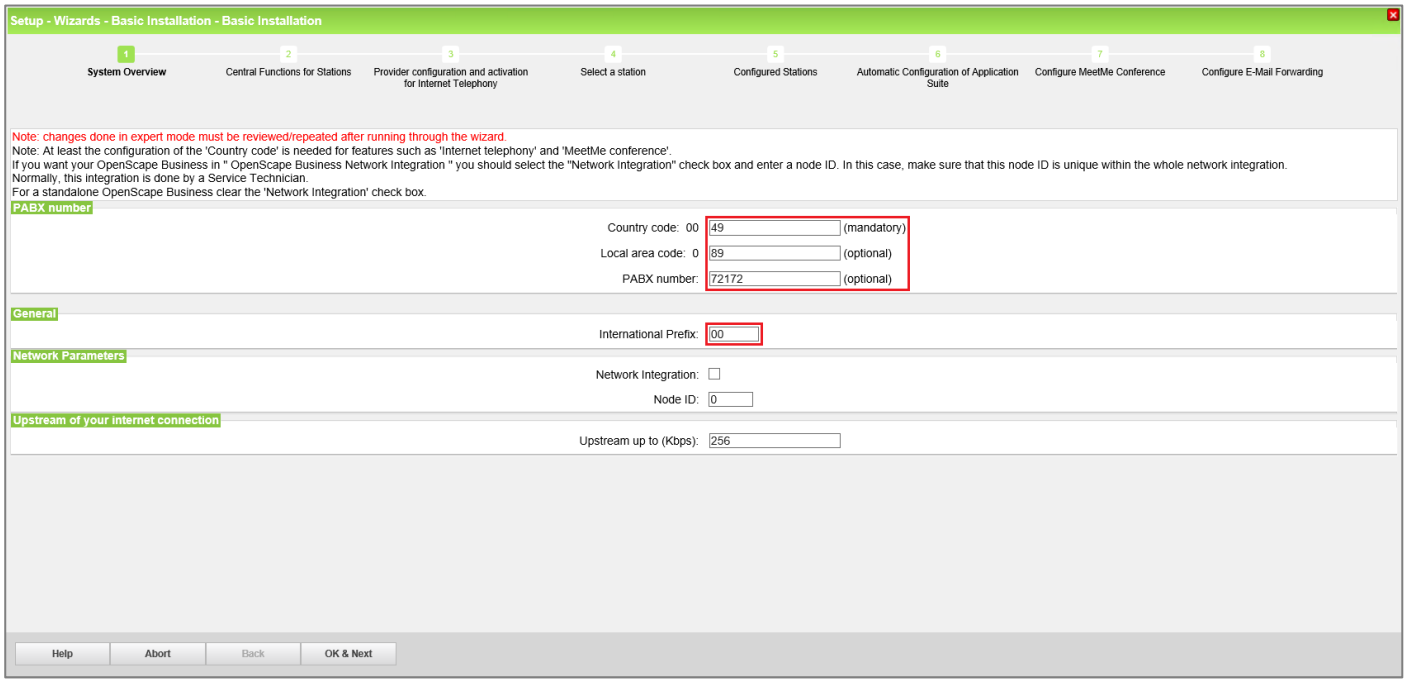

anynode
TE-SYSTEMS
competence in e-communications
User: anadmin (write access), Session Timeout: 28 minutes, Committed: yes
Copyright © 2021 by TE-SYSTEMS GmbH, Germany, State: connected, License active: yes, Trace: off
Wizard
Configuration
Objects
My Account
Extras
Info
Commit
Monitor Mode
Logout
Add Routing Forward Profile
Remove Routing Forward Profile...
Clone Routing Forward Profile...
Export Routing Forward Profile...
Information
Tracing
Licenses
Network Interfaces
Configuration
Routing Domains
Nodes
Routing Forward Profiles
To Microsoft Teams Direct ...
To Unify OpenScape Business
Authentication Profiles
Directories
Load Balancers
Conditions
Time Ranges
Auxiliary Objects
/ To Microsoft Teams Direct Routing / Telephony Forwarding / Media Negotiation Forwarder / Media Transcoding Options
Routing Forward Profile
Telephony Forwarding
Media Negotiation Forwarder
Media Transcoding Options
Media Transcoding Options
To Microsoft Teams Direct Routing
Open All
Object
Settings
Flow settings for the direction from the calling to the called entity:
Specify whether passthrough mode is activated. If the passthrough mode is activated and the remote side expects the same media format, received media will not be converted to an internal format.
Yes
No
Specify whether silence processing is activated.
Yes
No
Silence Processing Settings
Specify silence processing properties.
Generate nothing
Generate silence
Generate comfort noise
Generate events
Specify the comfort noise volume level.
-80
dB Full Scale
Version: 4.2.6
Off
40%
0%
33%
0

5. OpenScape Business – Gateway mode

OpenScape Business supports "Microsoft Teams Interworking" as **simple Gateway** towards a Microsoft certified SBC for Direct Routing and requires a valid **Software Support license**.

This section refers to OpenScape Business related example configuration where OpenScape Business is **routing calls as a simple Gateway** and must be adapted accordingly.

5.1. PABX Location Data

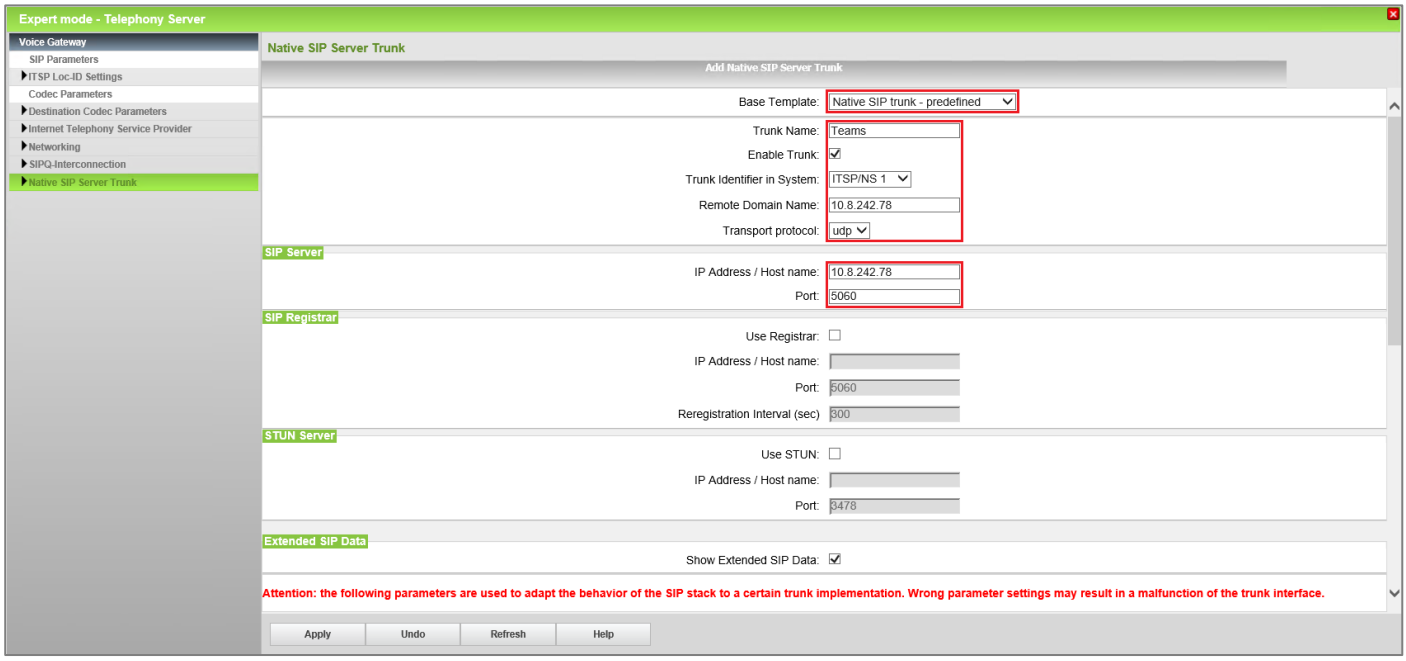


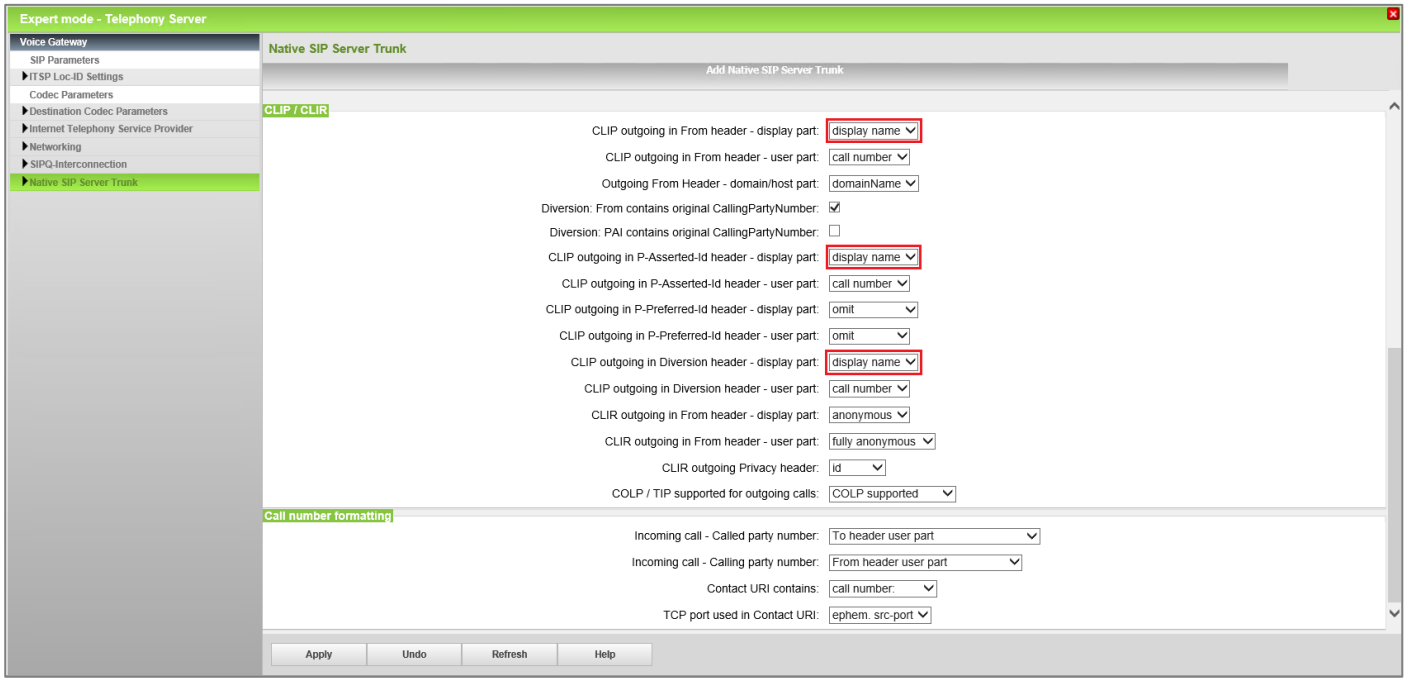
When a new OpenScape Business system is setup, the **Basic Installation Wizard** must be run.

To view the PABX location data for the current test environment, go to **OSBiz Assistant >> Setup >> Wizards >> Basic Installation** and click on **[Edit]**.

5.2. SIP Interconnection

OSBiz is interconnected to MS Teams Cloud PBX via a **Native SIP Trunk** with a Microsoft certified SBC. Please note that native SIP trunking requires an Unify OpenScape Business **Networking** license.



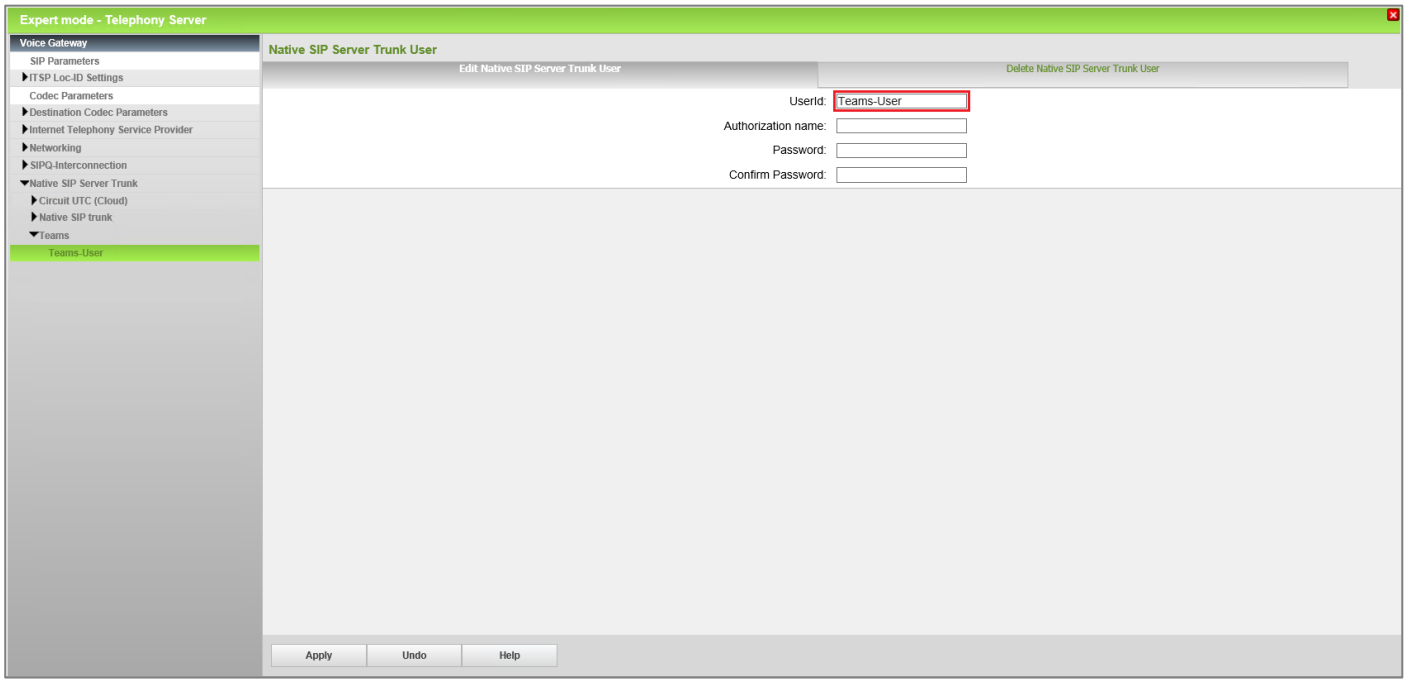


Go to **OSBiz Assistant >> Expert mode >> Telephony Server >> Voice Gateway >> Native SIP Server Trunk** and add a new native SIP server trunk, by entering the following:

- **Base Template:** Native SIP trunk – predefined
- **Trunk Name**: Teams (a common-sense name)
- **Enable Trunk:** Activated
- **Trunk Identifier in System:** ITSP/NS 1 (choice of 10 external Native SIP connections; greyed out items are occupied by already configured trunks)
- **Remote Domain Name:** 10.8.242.78 (host name or IP address of the external SIPserver, i.e. the AudioCodes SBC LAN interface IP)
- **Transport Protocol:** UDP (as configured in SBC)
- **IP Address / Host Name:** 10.8.242.78 (SBC IP address / FQDN)
  Port: 5060 (as configured in SBC; default value = 5060; enter port 0 for DNSSRV)
- **Show Extended SIP Data:** Enabled (by enabling this flag some additional configuration parameters are available to control the SIPstack and to adapt the content of SIP header fields)
- **CLIP outgoing in From header - display part:** display name
- **CLIP outgoing in P-Asserted-Id header - display part:** display name
- **CLIP outgoing in Diversion header - display part:** display name

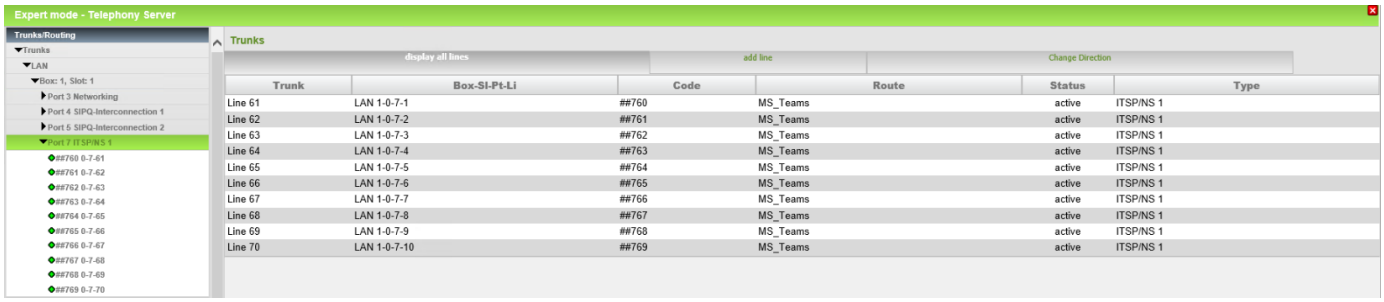
Click on **[Apply]**.

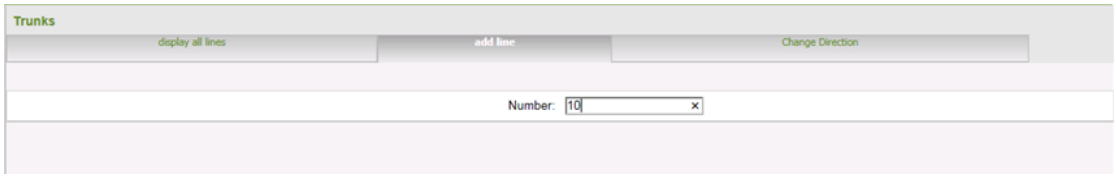
Note: The value "display name" for the extended SIP parameters is required in order Teams client to have the proper OpenScape Business subscriber name presentation when it receives a call from an OpenScape Business station (see sub-section 5 for the name and number display).



Once the trunk is created, return to **Native SIP Server Trunk** webpage, edit the Teams native SIP trunk and add a user e.g. Teams-User (no credentials to connected to SBC are used in current project).

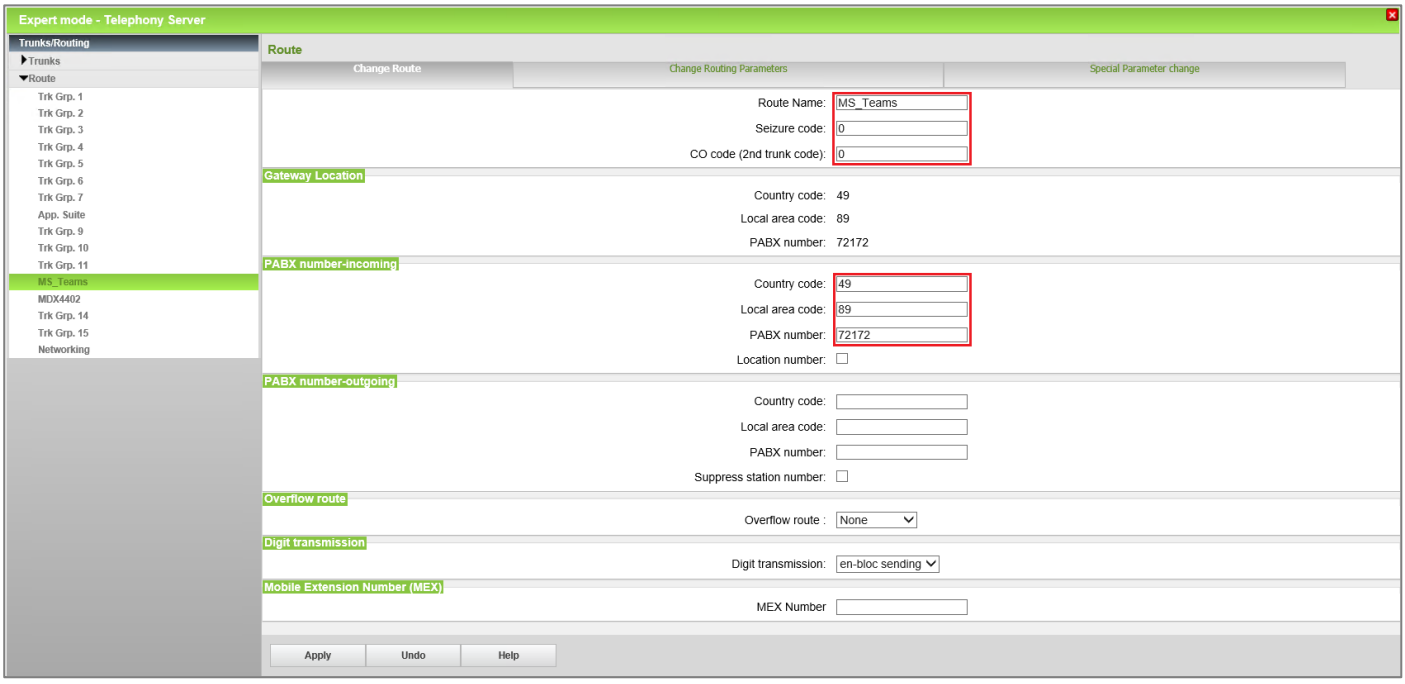
Trunk lines can be added via:

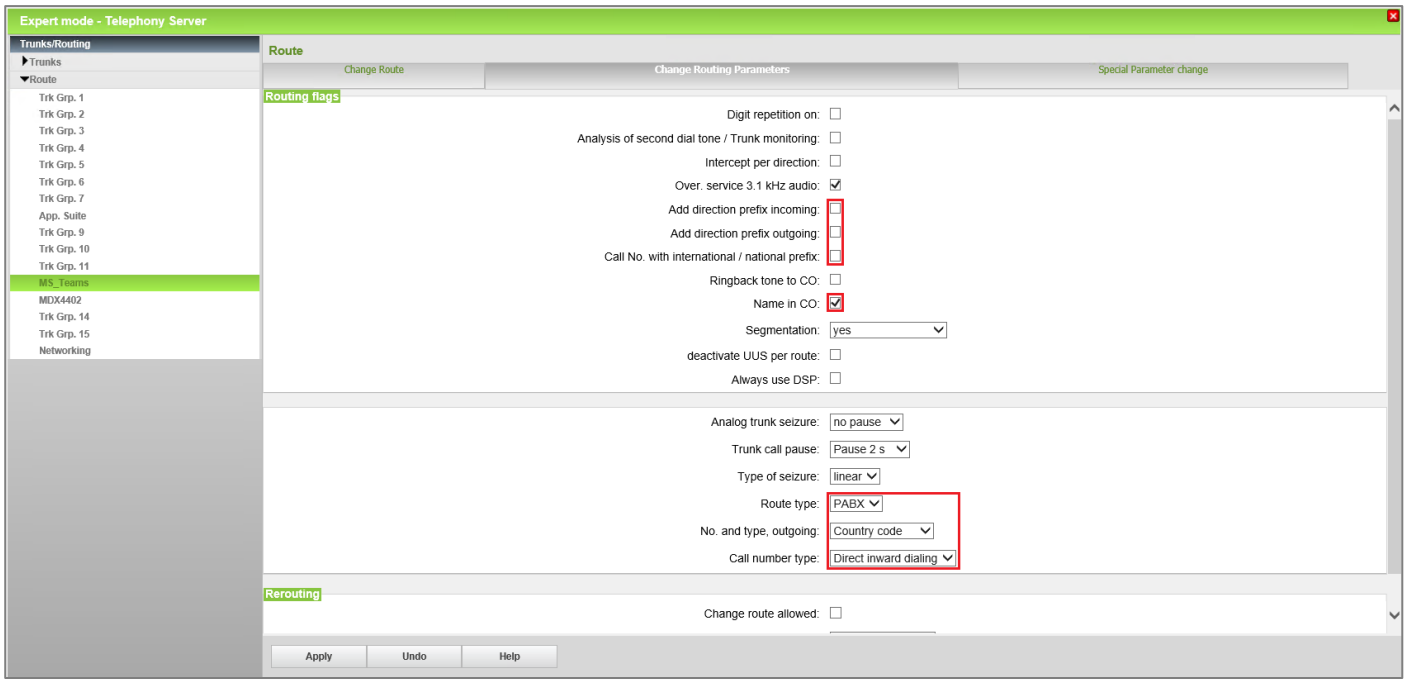




5.3. Routes

The route configuration will be created automatically.





Navigate to **OpenScape Business Assistant >> Expert mode >> Telephony Server >> Trunks/Routing >> Route** and select the route created for the SBC native SIP trunk.

For the **Change Route** and **Change Routing Parameters** tabs, enter the following:

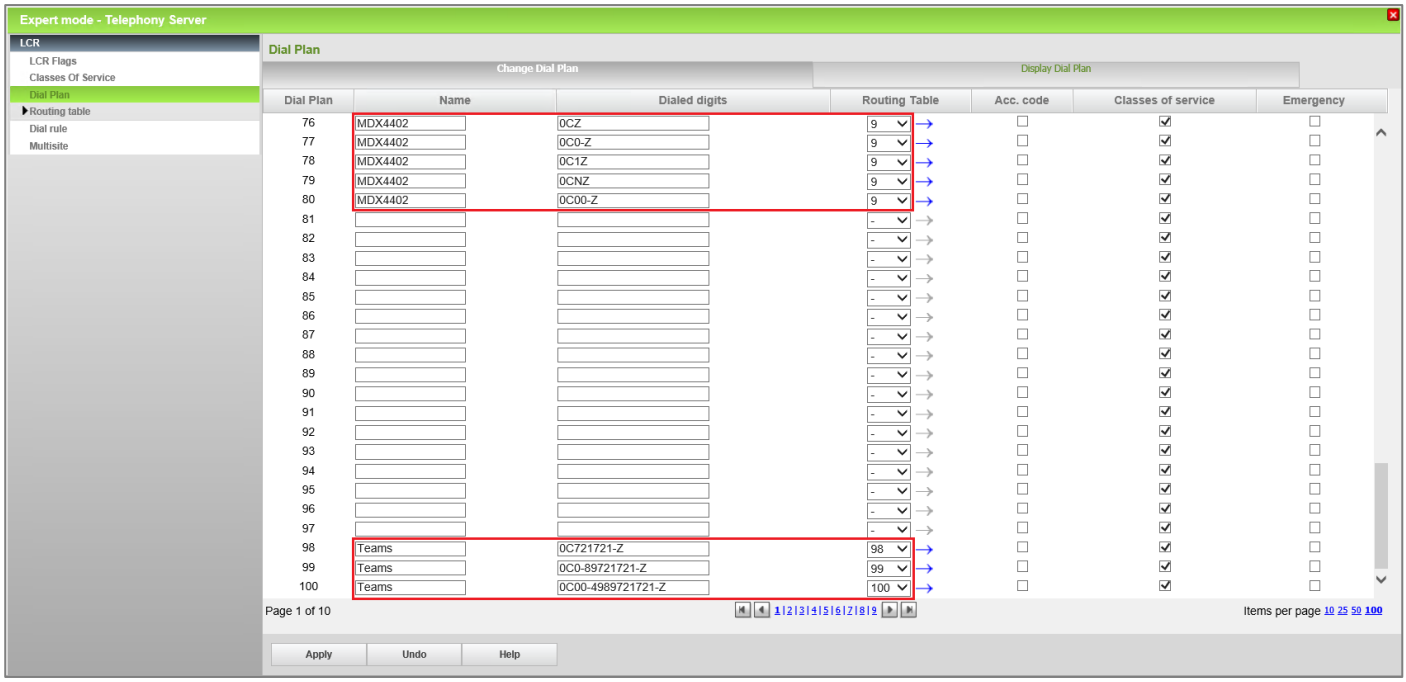
- **Route Name:** MS_Teams (friendly name; the entered name replaces the default route number in the Routes list)
- **Seizure code:** 0 (the seizure code is the code that causes the switchingsystem to provide a line to the station that dialed the code).
- **CO code (2nd trunk code):** 0 (it is only relevant for networking routes with route type = PABX).

- **PABX number – incoming / Country code:** 49
- **PABX number – incoming / Local area code:** 89
- **PABX number – incoming / PABX number:** 72172
- **Add direction prefix incoming:** Disabled
- **Add direction prefix outgoing:** Disabled
- **Call No. with international / national prefix:** Disabled
- **Name in CO:** Enabled
- **Route type:** PABX
- **No. and type, outgoing:** Country code
- **Call number type:** Direct inward dialing

Click on **[Apply]**.

5.4. LCR Changes

The **Dial Plan** is searched for patterns that match the dialed digits. The result is used as a criterion for selecting the **Routing Table**. Of course, the dial plan must be configured up to the local requirements. At the same time, the system checks if the subscriber's class of service matches for this route. For external connections, each call number including the code (up to a maximum of 24 characters incl. field separators) is checked in the dial plan. The dial plan then determines a route table for the station; the station is assigned this table for the connection setup. Up to 16 routes are created via a single route table.



Go to: **OpenScape Business Assistant >> Expert mode >> Telephony Server >> LCR >> Dial Plan.**

The dial plan for the current testing environment is used with some variations of 0CZ, where 0 is the line seizure code.

To reach a Teams user through OpenScape Business, the following dialed digits patterns must be matched:

- 0C721721-Z (local format, related to routing table 98).

- 0C0-89721721-Z (national format, related to routing table 99) .

- 0C00-4989721721-Z (international format, related to routing table 100).

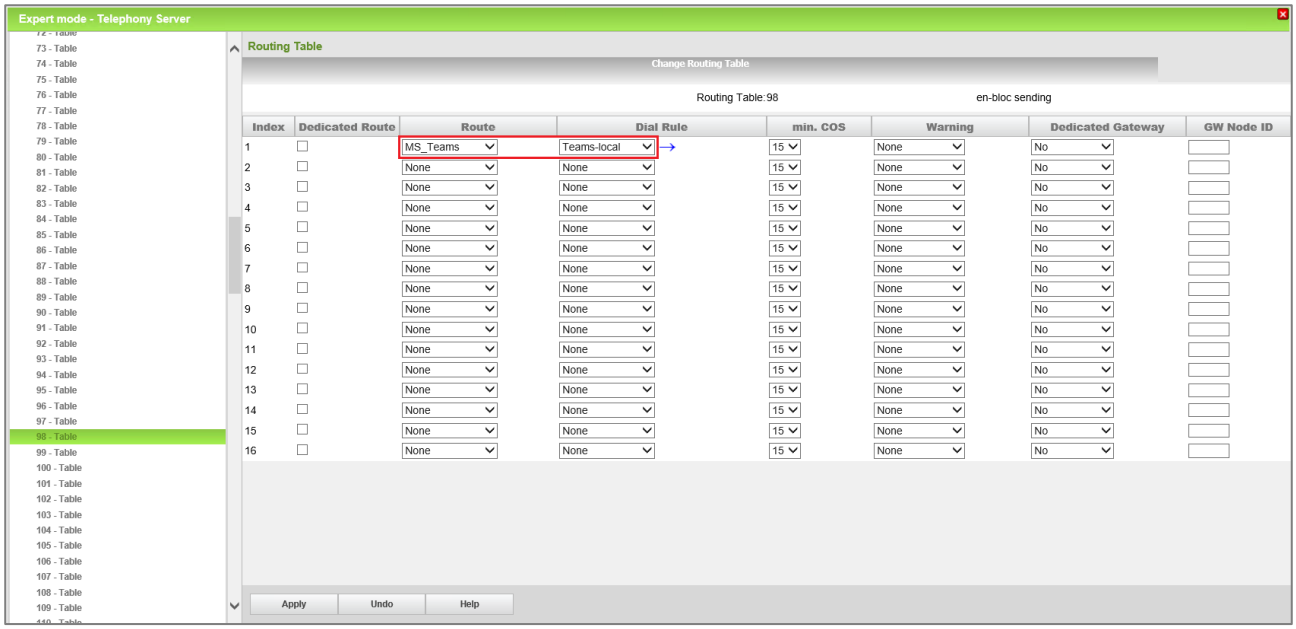
Any other call (either from an OpenScape Business station or a MS Teams user) starting from digit 0, not matching to the above patterns is routed to PSTN (related to routing table 9 – here in this example MDX4402).

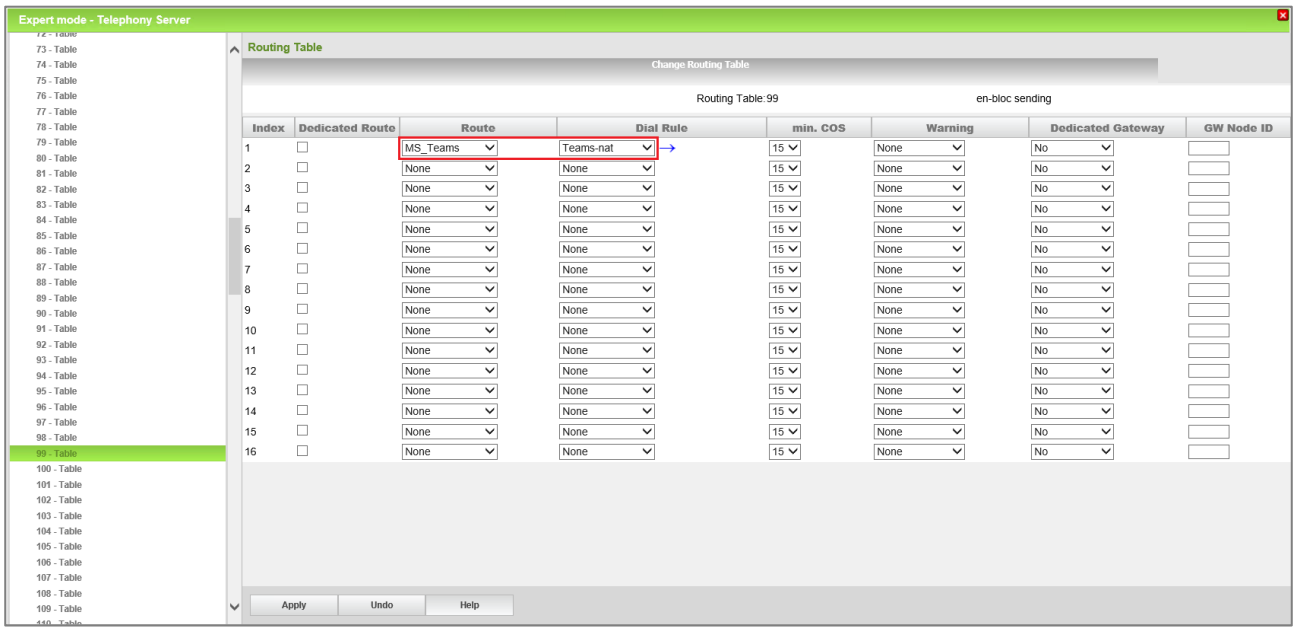
Note: For calls from PSTN subscribers to MS Teams users (through OpenScape Business), the Mediatrix ISDN BRI gateway must be configured to deliver +49xxxx (E.164) in FROM header. The TO number should be delivered in OpenScape Business dialable format as if an OpenScape Business station makes the call to a MS Teams user.

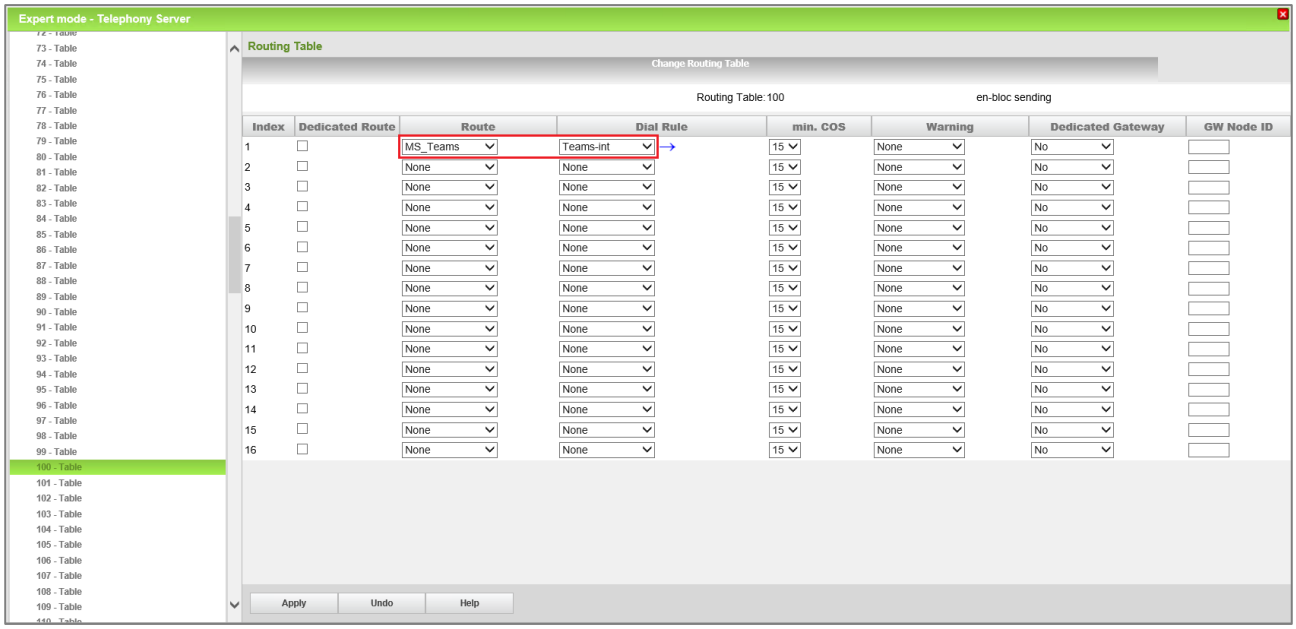
Click on **[Apply].**

Navigate to **OpenScape Business Assistant >> Expert mode >> Telephony Server >> LCR >> Routing table** and assign each routing table (e.g. 98, 99, 100) to the corresponding dial rule.

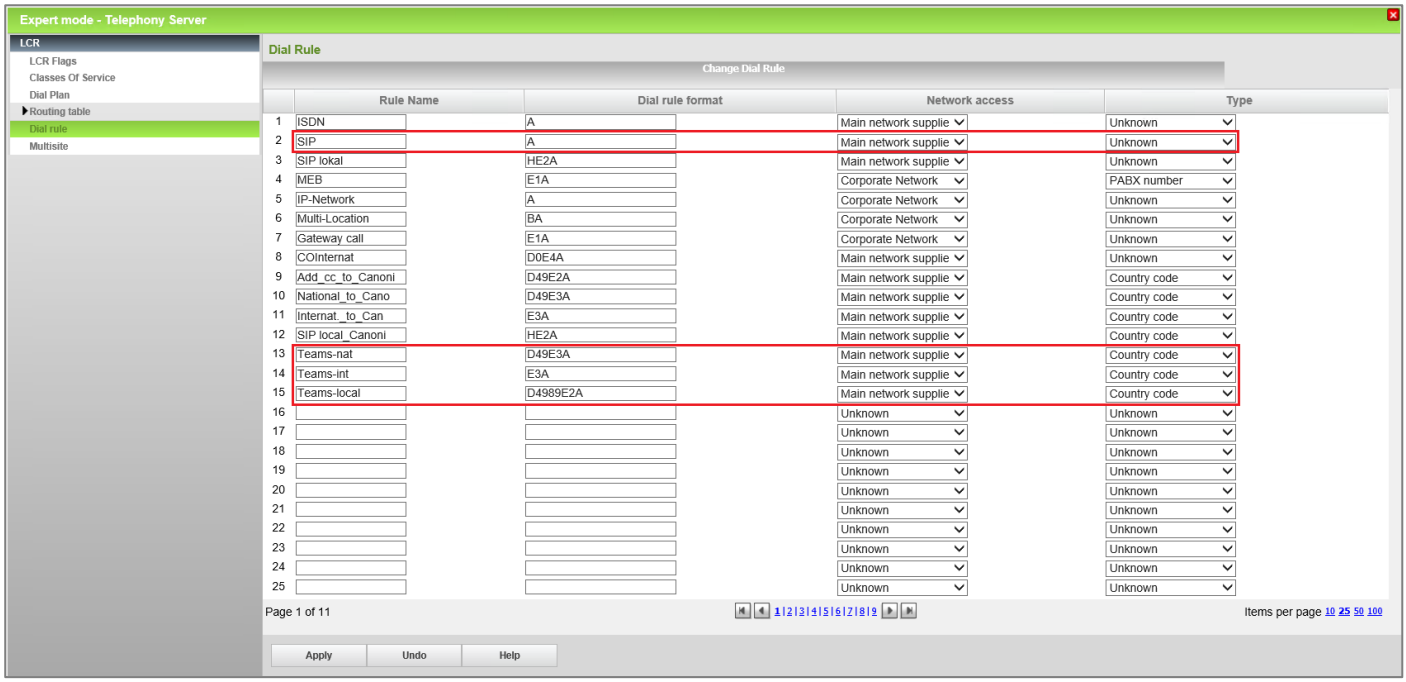
Click on **[Apply].**






Expert mode - Telephony Server
73 - Table
74 - Table
75 - Table
76 - Table
77 - Table
78 - Table
79 - Table
80 - Table
81 - Table
82 - Table
83 - Table
84 - Table
85 - Table
86 - Table
87 - Table
88 - Table
89 - Table
90 - Table
91 - Table
92 - Table
93 - Table
94 - Table
95 - Table
96 - Table
97 - Table
98 - Table
99 - Table
100 - Table
101 - Table
102 - Table
103 - Table
104 - Table
105 - Table
106 - Table
107 - Table
108 - Table
109 - Table
Routing Table
Change Routing Table
Routing Table: 100
en-bloc sending
Index
Dedicated Route
Route
Dial Rule
min. COS
Warning
Dedicated Gateway
GW Node ID
1 MS_Teams Teams-int 15 None No
2 None None 15 None No
3 None None 15 None No
4 None None 15 None No
5 None None 15 None No
6 None None 15 None No
7 None None 15 None No
8 None None 15 None No
9 None None 15 None No
10 None None 15 None No
11 None None 15 None No
12 None None 15 None No
13 None None 15 None No
14 None None 15 None No
15 None None 15 None No
16 None None 15 None No
Apply
Undo
Help

The **Dial Rule** table defines how the digits selected by the station are converted and dialed by the communication system.



Navigate to **OpenScape Business Assistant >> Expert mode >> Telephony Server >> LCR >> Dial rule.**

For calls to PSTN configure the following:

- **Rule Name:** SIP (common-sense name)
- **Dial rule format:** A
- **Network access:** Main network supplier
- **Type:** Unknown

For calls to Teams in *local* format configure the following:

- **Rule Name:** Teams-local (common-sense name)
- **Dial rule format:** D4989E2A
- **Network access:** Main network supplier
- **Type:** Country code

For calls to Teams in *national* format configure the following:

- **Rule Name:** Teams-nat (common-sense name)
- **Dial rule format:** D49E3A
- **Network access:** Main network supplier
- **Type:** Country code

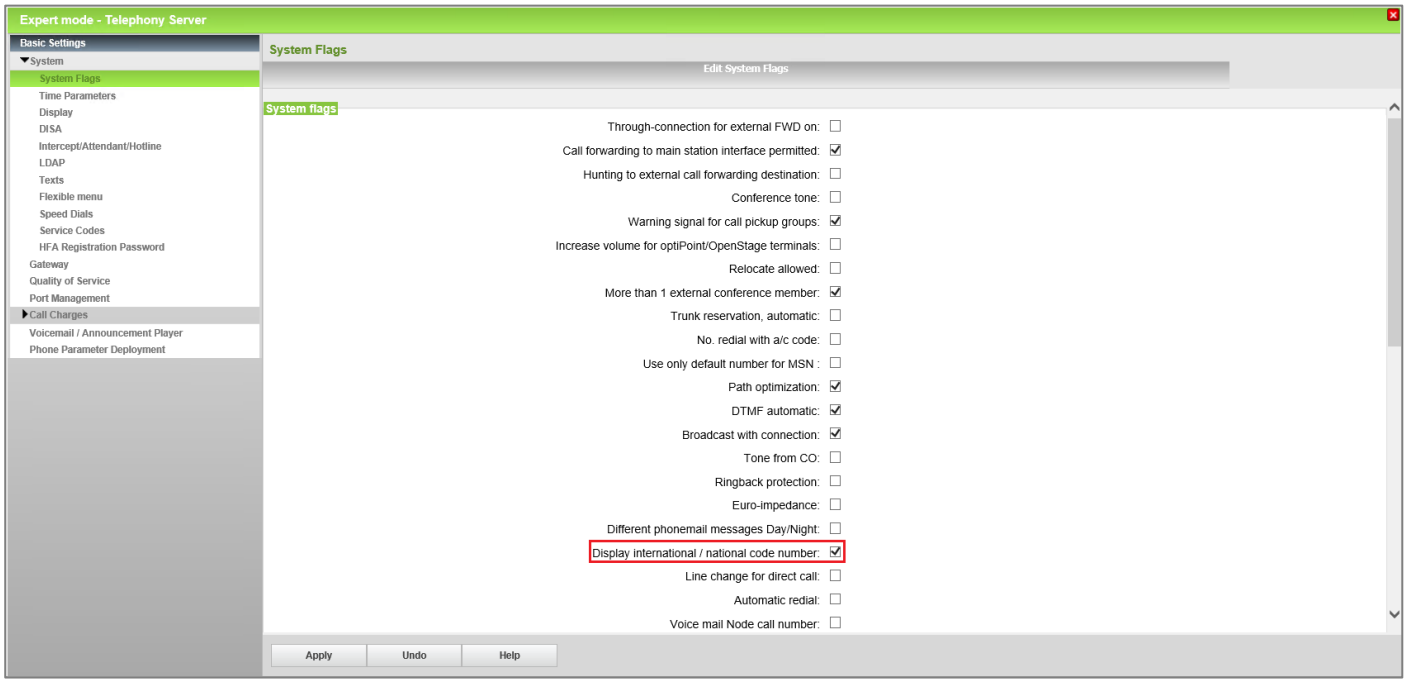
For calls to Teams with international format configure the following:

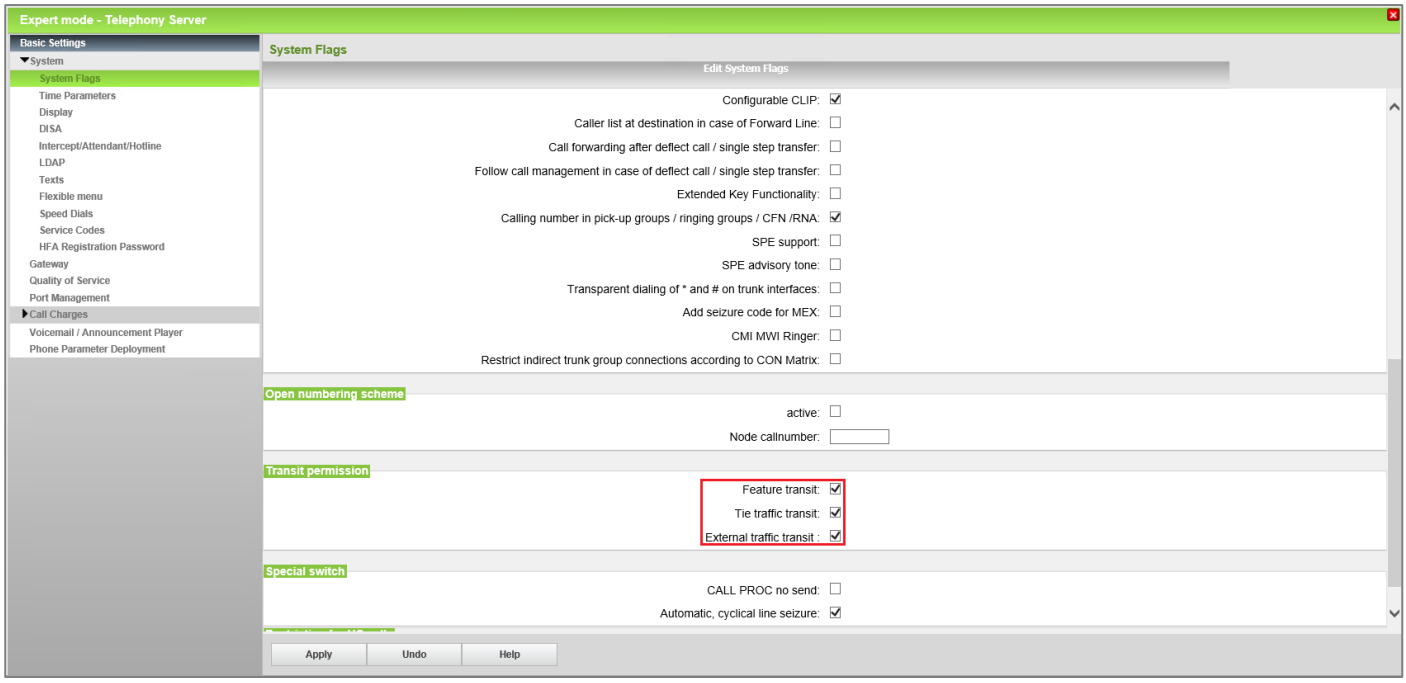
- **Rule Name:** Teams-int (common-sense name)
- **Dial rule format:** E3A
- **Network access:** Main network supplier
- **Type:** Country code

Click on **[Apply].**

5.5. System Parameter Flags

Navigate to **OpenScape Business Assistant >> Expert mode >> Basic Settings >> System.**





Select **"System Flags"** and configure the following:

- **Display international / national code number:** enabled (the complete phone number (PABX number + Direct Inward Dialing (DID) number, including the local area code and country code, if available) is shown on the display of the phone).
- **Feature transit:** enabled
- **Tie traffic transit:** enabled
- **External traffic transit:** enabled

Click on **[Apply]**.

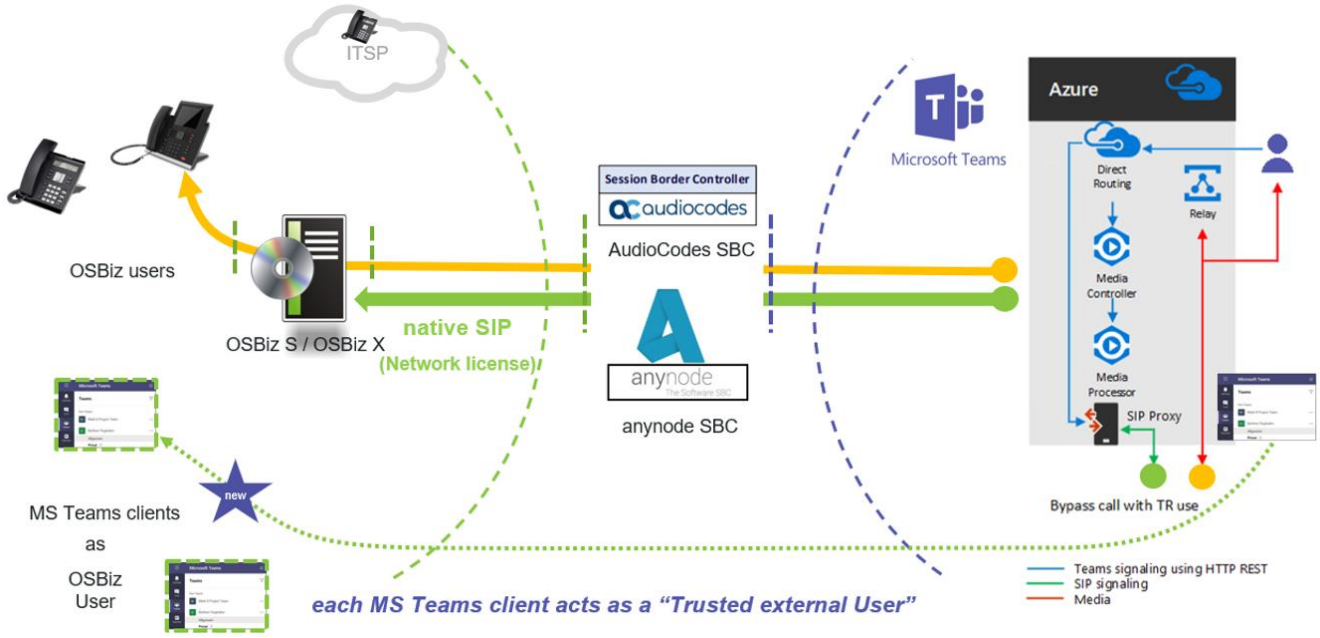
Note: The **"Transit permission"** flags are required because in current environment setup, where OpenScape Business acts as a transit for calls from MS Teams users to PSTN.

6. OpenScape Business - Trusted external User mode

OpenScape Business supports "Microsoft Teams Interworking" via "Trusted SBC" trunking towards a Microsoft certified SBC for Direct Routing and requires a valid **Software Support license**.

On top of the "regular" approach where OpenScape Business is routing calls as a simple Gateway additional features are be offered with "**Trusted external User**". In this scenario each MS Teams User can be assigned to an User within OpenScape Business:

- MS Teams users are configured as virtual OpenScape Business users of new type „Trusted external station"
- IP User license required per "Trusted external User" which is assigned to a MS Teams user
- same feature set as known from Skype for Business interworking
- the "Trusted external User" can operate standalone or can be added to a Mobility group / MULAP (One Number Service)
- integration into OpenScape Business Call Management
- Busy Lamp Indication for voice calls via OpenScape Business (DSS key / UC application)
- outgoing calls from MS Teams user use OpenScape Business ONS number
- Class of Service / traffic restrictions are checked by OpenScape Business
- parallel ringing to desk phone and MS Teams user for inbound calls
- internal calls: just dial short numbers in both directions

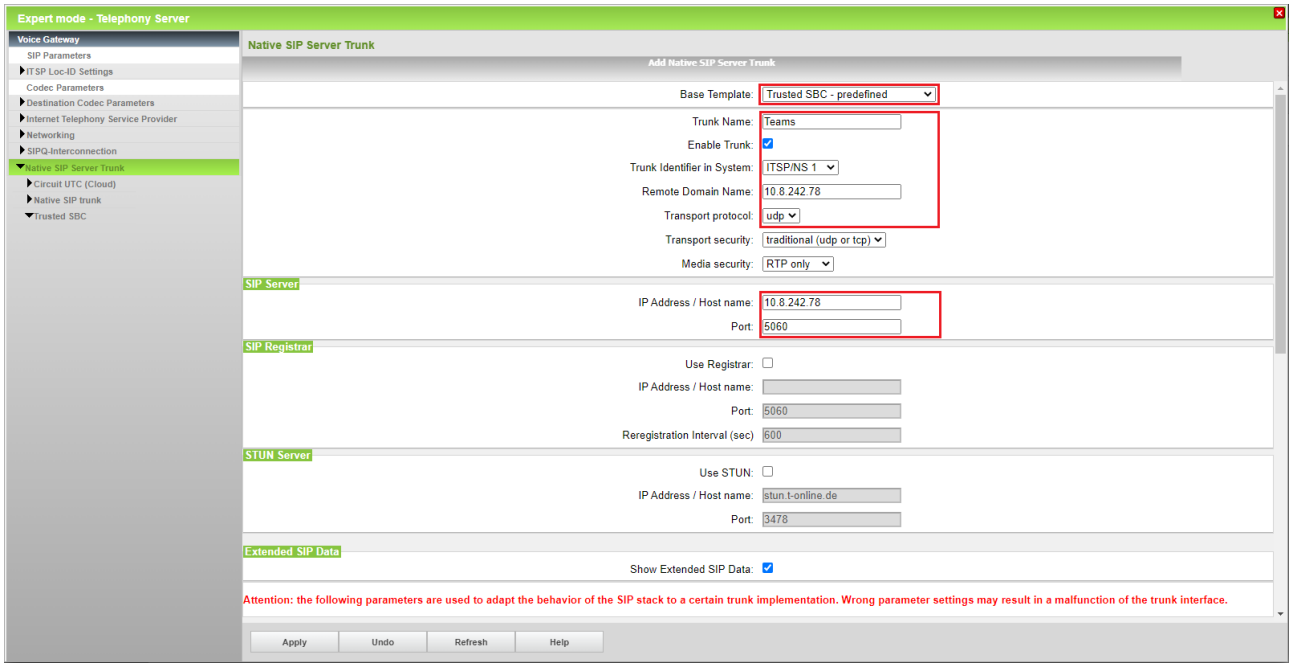


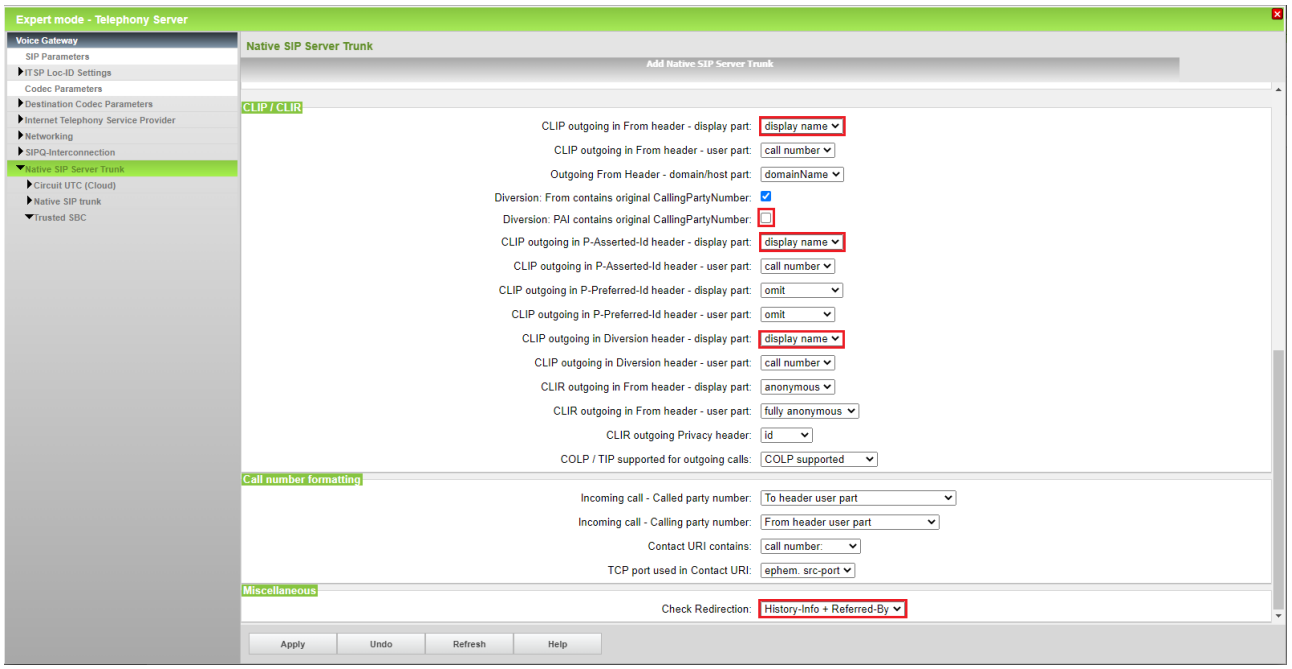
Trusted external User scenario: MS Teams Interworking via Direct Routing with Office 365

	The following paragraphs require the configuration settings of the previous chapters - OpenScape Business as simple Gateway - and describe how the "Trusted external User" is linked to an according route and profile.

6.1. SIP Interconnection

OpenScape Business is interconnected to MS Teams Cloud PBX via the **Native SIP Trunk** category **Trusted SBC** with a Microsoft certified SBC. Please note that native SIP trunking requires an Unify OpenScape Business **Networking** license.



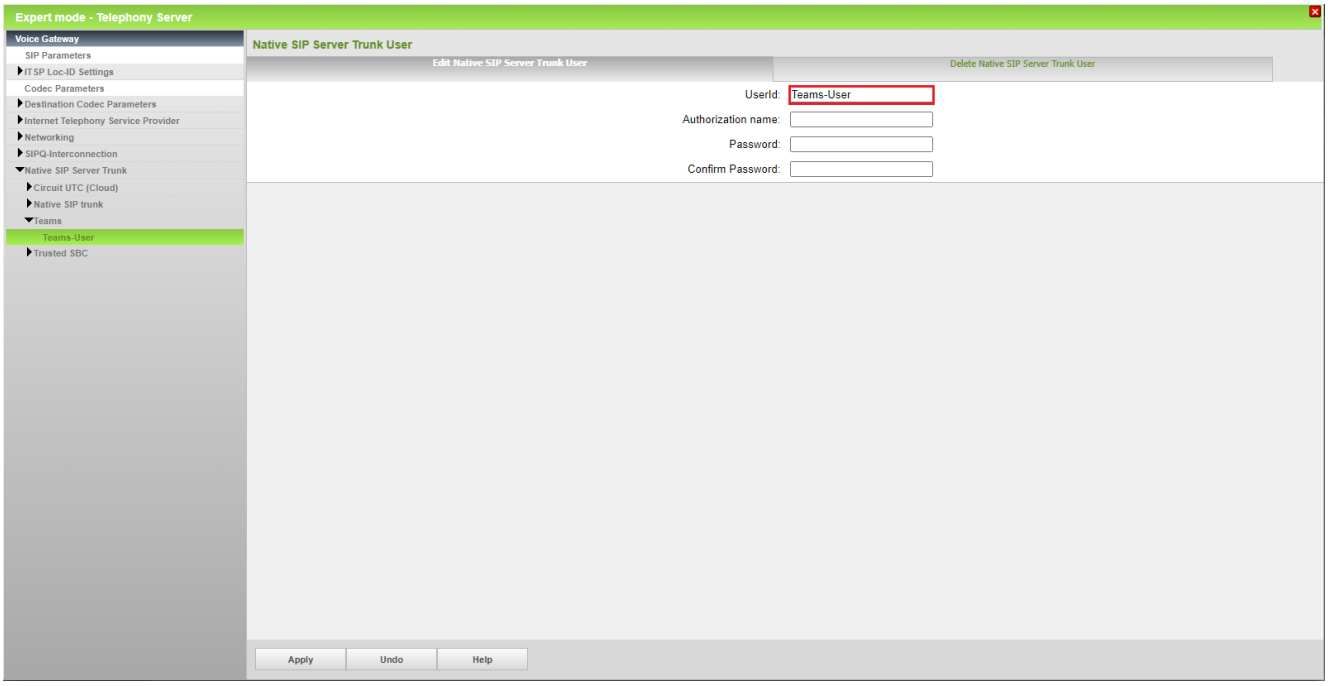


Go to **OpenScape Business Assistant >> Expert mode >> Telephony Server >> Voice Gateway >> Native SIP Server Trunk** and add a new native SIP server trunk, by entering the following:

- **Base Template:** Trusted SBC – predefined
- **Trunk Name**: Teams (a common-sense name)
- **Enable Trunk:** Activated
- **Trunk Identifier in System:** ITSP/NS 1 (choice of 10 external Native SIP connections; greyed out items are occupied by already configured trunks)
- **Remote Domain Name:** 10.8.242.78 (host name or IP address of the external SIPserver, i.e. the AudioCodes SBC LAN interface IP)
- **Transport Protocol:** UDP (as configured in SBC)
- **IP Address / Host Name:** 10.8.242.78 (SBC IP address / FQDN)
  Port: 5060 (as configured in SBC; default value = 5060; enter port 0 for DNSSRV)
- **Show Extended SIP Data:** Enabled (by enabling this flag some additional configuration parameters are available to control the SIPstack and to adapt the content of SIP header fields)
- **CLIP outgoing in From header - display part:** display name
- **Diversion: PAI contains original CallingPartyNumber:** disabled
- **CLIP outgoing in P-Asserted-Id header - display part:** display name
- **CLIP outgoing in Diversion header - display part:** display name
- **Check Redirection:** History-Info + Referred-By

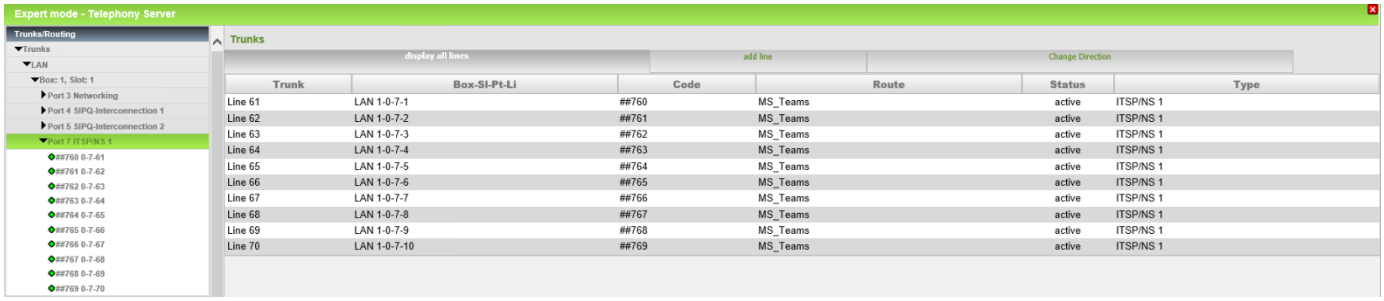
Click on **[Apply]**.

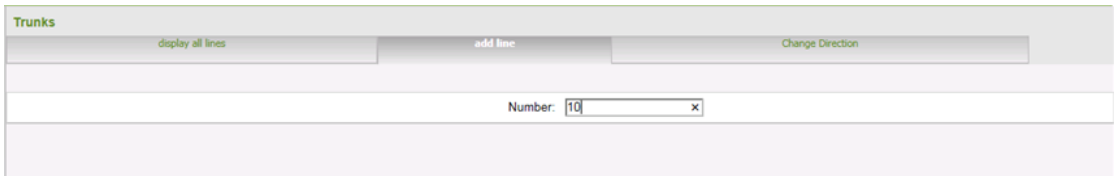
Note: The value "display name" for the extended SIP parameters is required in order Teams client to have the proper OpenScape Business subscriber name presentation when it receives a call from an OpenScape Business station (see sub-section 5 for the name and number display).



Once the trunk is created, return to **Native SIP Server Trunk** webpage, edit the **Teams** Trusted SBC trunk and add a user e.g. Teams-User (no credentials to connected to SBC are used in current project).

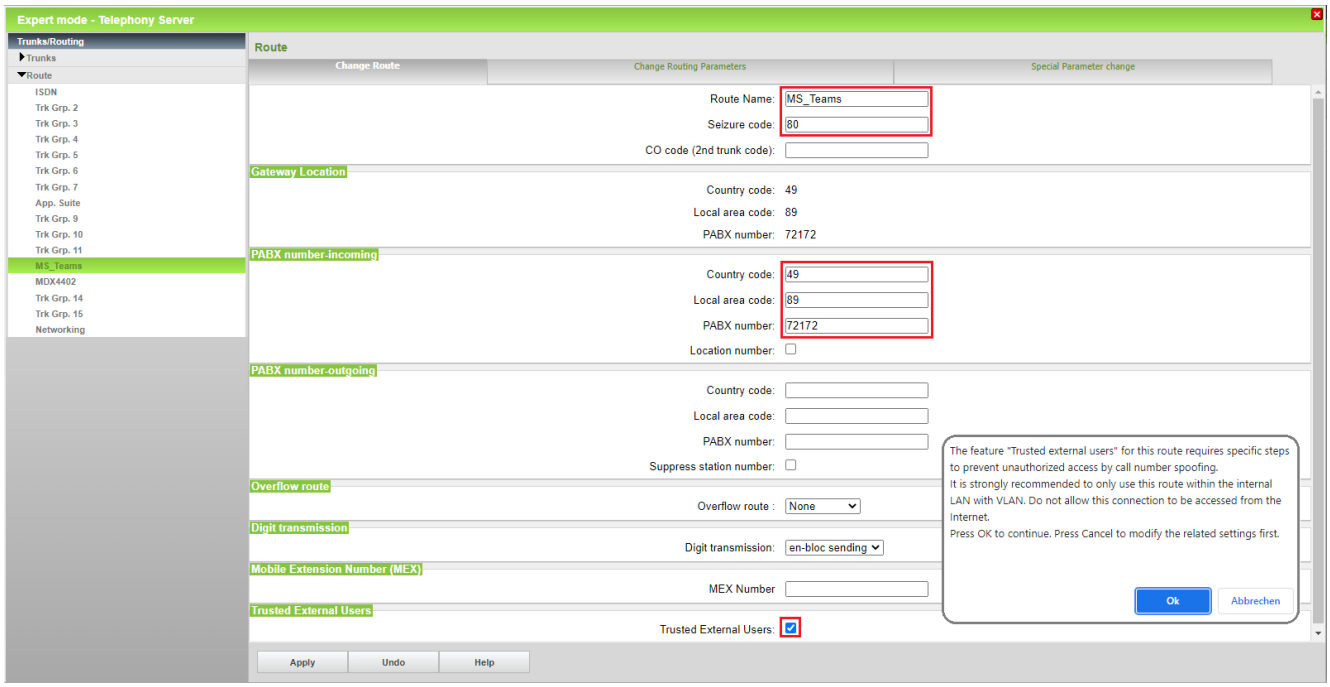
Trunk lines can be added via:

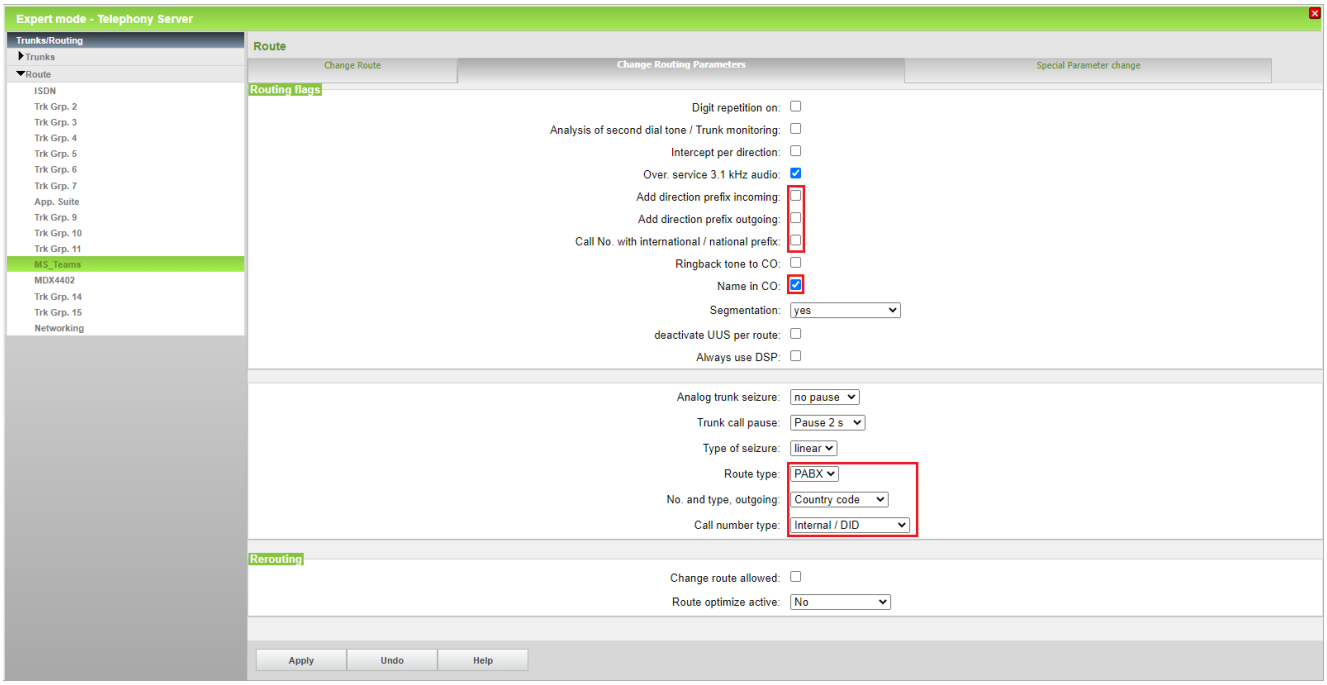




6.2. Routes

The route configuration will be created automatically.





Navigate to **OpenScape Business Assistant >> Expert mode >> Telephony Server >> Trunks/Routing >> Route** and select the route created for the SBC native SIP trunk.

For the **Change Route** and **Change Routing Parameters** tabs, enter the following:

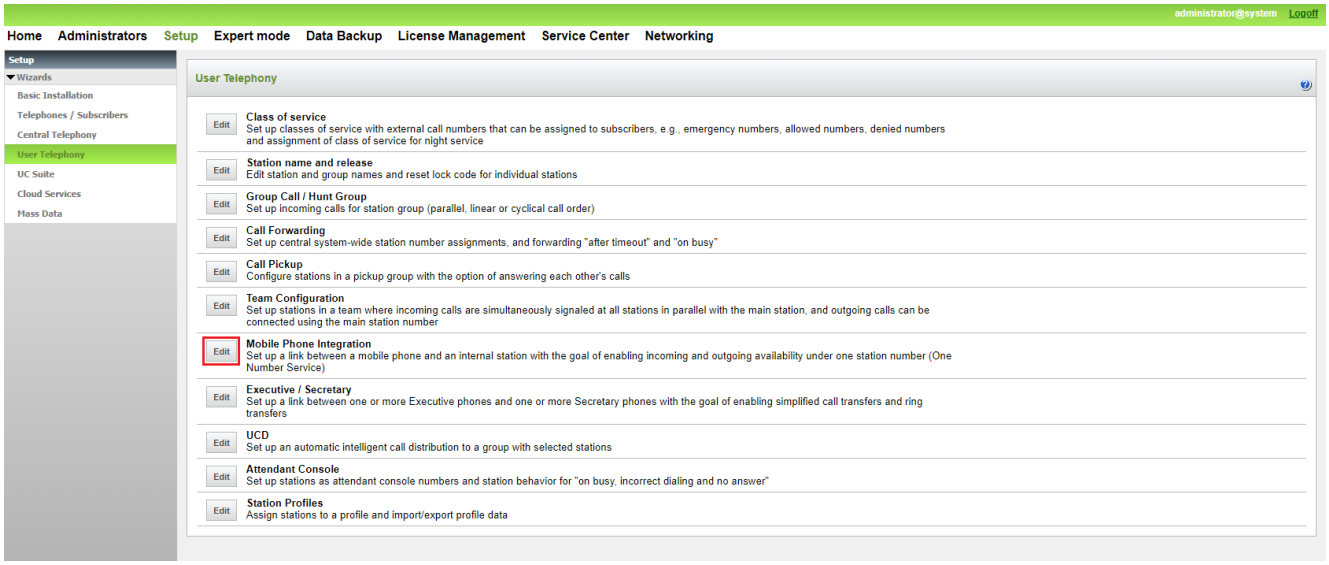
- **Route Name:** MS_Teams (friendly name; the entered name replaces the default route number in the Routes list)
- **Seizure code:** 80 (the seizure code is the code that causes the switchingsystem to provide a line to the station that dialed the code).
- **Trusted External Users:** Enabled (requires confirmation of the disclaimer)

- **PABX number – incoming / Country code:** 49
- **PABX number – incoming / Local area code:** 89
- **PABX number – incoming / PABX number:** 72172
- **Add direction prefix incoming:** Disabled
- **Add direction prefix outgoing:** Disabled
- **Call No. with international / national prefix:** Disabled
- **Name in CO:** Enabled
- **Route type:** PABX
- **No. and type, outgoing:** Country code
- **Call number type:** Internal / DID

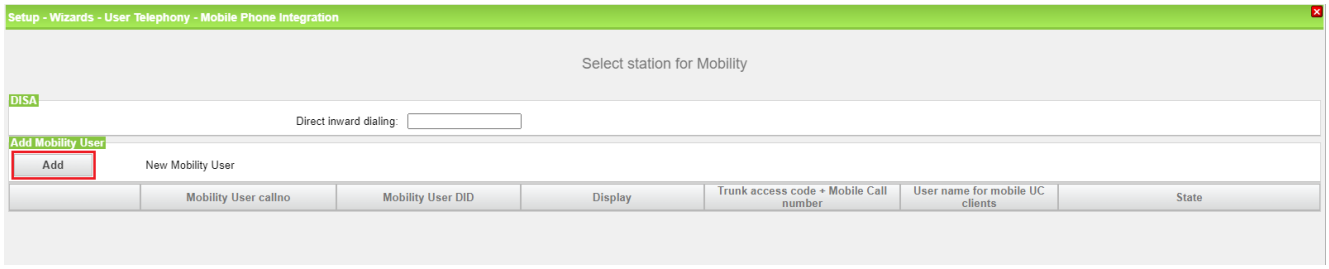
Click on **[Apply].**

6.3. Trusted external User

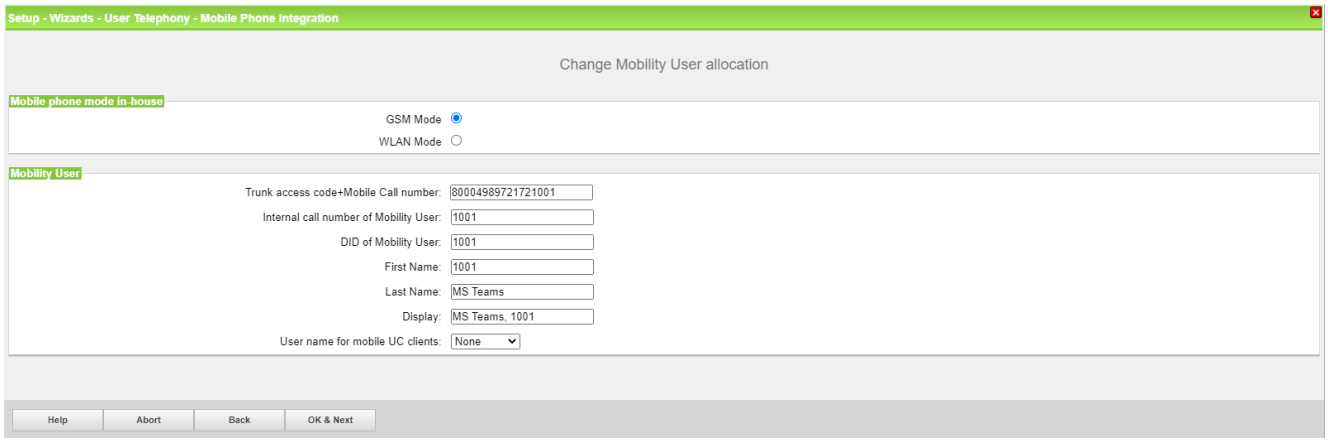
Create a Mobility User by entering the „Mobility Phone Integration“ wizard



Press “Add” to create a new Mobility User

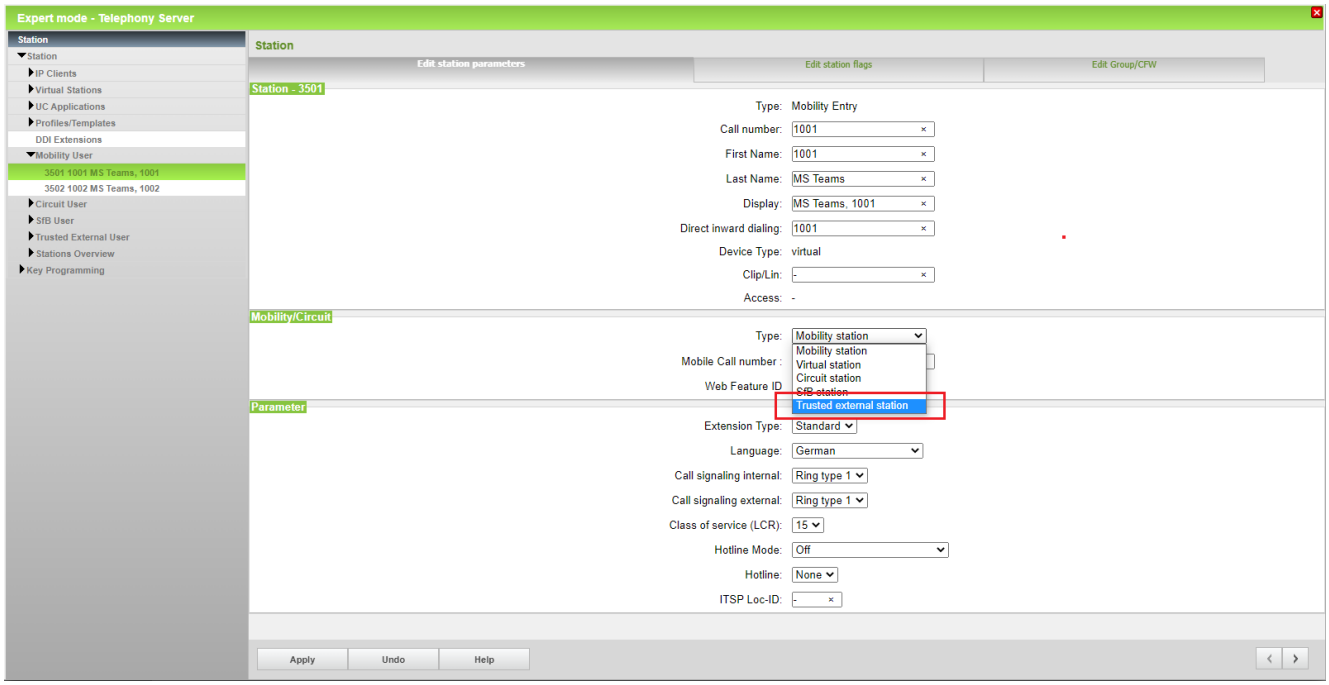


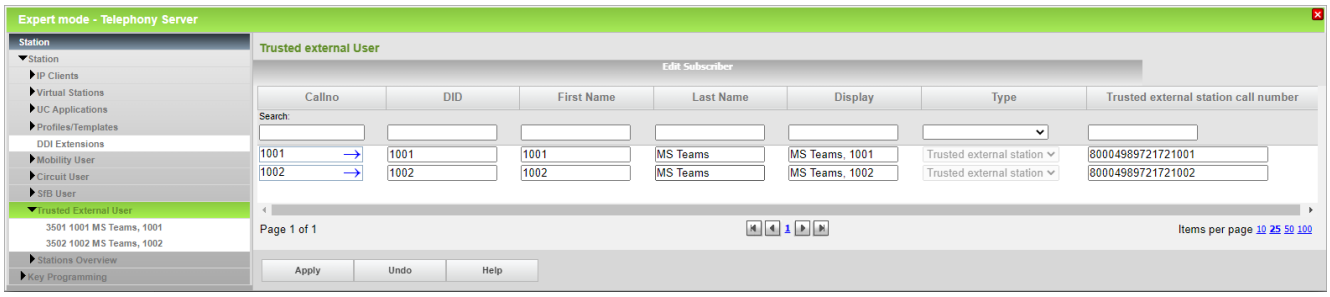
Microsoft Teams numbering plan is in standard E.164 format:



Click [OK & Next] and on the next page [Finish]

Change in Expert Mode the Virtual Station Type to: “Trusted external station”:





Hint: Depending on the use case standalone Mobility User or Mobility MULAP the Mobility User will have a DID. The station flag: “DTMF-based feature activation” – available in OSBiz X - is ignored for Mobility User type “Trusted external Station”. A Mobility User of type “Trusted external Station” sends DTMF transparently through the system.

6.4. Configuration Wizard – Team Configuration

The “Trusted External User” can be added to a Team / MULAP through the „Team Configuration“ wizard.

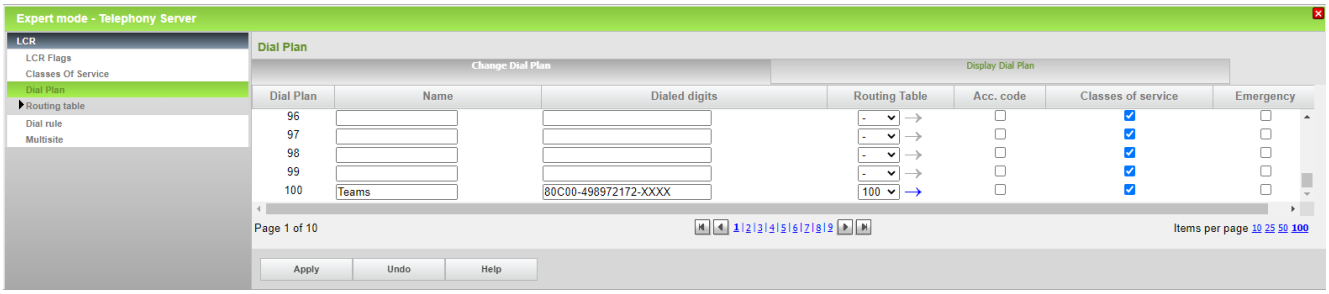
6.5. LCR Dial Plan

Go to: **OpenScape Business Assistant >> Expert mode >> Telephony Server >> LCR >> Dial Plan.**

To reach a Teams user through OpenScape Business, the following dialed digits patterns must be matched:

- 80C00-498972172-1XXX (international format, related to routing table 100).

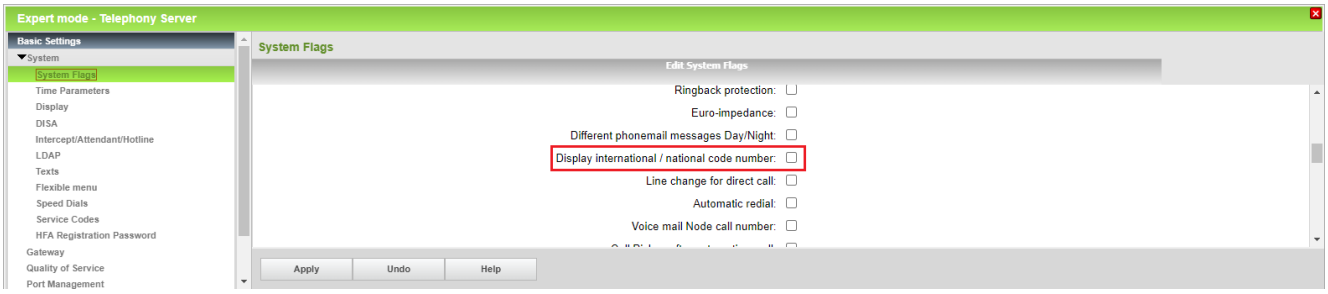
Click on **[Apply].**



Note: LCR Routing Tables and Dial Rules are the same as in the Gateway mode configuration.

6.6. System Parameter Flags

Navigate to **OpenScape Business Assistant >> Expert mode >> Basic Settings >> System.**



Display international / national code number: disabled

Note: "Display international / national code number" setting is different compared to the Gateway mode configuration (chapt. 5.5).

7. Capacities & Feature Interaction

Codec support

OpenScape desk phones or other calling devices must be configured to offer at least a G.711 codec. In SBC Teams IP profile configure an "Allowed Coders Group" including e.g. the codecs G.711, G.722 and G.729 with "Allowed Coders Mode = Preference".

Basic Call

Because MS Teams Phone System doesn't send SIP header P-Asserted-Identity in 180 or 200 messages to convey connected party information no name information will be displayed on OpenScape business. Display names may be converted by OpenScape Business via directory entries. Make sure that in SBC the OpenScape Business IP profile configuration that "P-Asserted-Identity Header Mode = As Is".

Trusted External User: name support via MS Teams Client User assignment.

Parallel Ringing

Gateway mode: in the case of incoming calls, the MS Teams client can ring in parallel via an external ringing group (* 81) or a group call with an external destination.

Trusted External User: via Teams / MULAP pairing with deskphone.

Call Hold/Retrieve

The OpenScape Business feature held call is not to displayed on MS Teams Client and vice versa.

Consultation

A consultation call claims another native SIP Trunk line.

Trusted External User: although the consultation call inherits Calling Number and Calling Name and according Class of Service of the Trusted external User, the consultation call is not assigned to the Trusted external User.

Call Forward

Call Forwarding settings in OpenScape Business and MS Teams Client are indepenedent from each other. A forwarding setting of OpenScape Business might overrule a forwarding setting of MS Teams and vice versa.

The forwarded-to party's display won't show that the call had been forwarded, when the call is forwarded from the OpenScape Business to the MS Teams domain and vice versa. A forwarded call of a MS Teams client stays active in a trombone connection until the forwarded call is released.

Trusted External User: the 2nd call leg is handled like in the consultation call scenario.

Call Transfer

In call transfer (Attended/Blind) scenarios, user devices (OpenScape Business/MS Teams) display the original connected party and not the transferred-to party. A call transferred by a MS Teams client stays active in a trombone connection until the transferred call is released.

Trusted External User: the 2nd call leg is handled like in the consultation call scenario.

Busy signaling for Voice Calls

Gateway mode: there is no busy signaling (LED, CFB, …) in OpenScape Business if MS Teams user is busy during a call and vice versa.

Trusted External User: Voice Call busy signaling in OpenScape Business via MS Teams Client user assignment within OpenScape Business (DSS Key, LED, CFB, UC applications, …).

Conference

There is no conference display indication on OpenScape Business user's phone who has been invited to a Teams conference. On the other hand, at the MS Teams client there will be no conference indication display when participating in a conference started in OpenScape Business.

When an OpenScape Business subscriber invokes call hold, while being a member of a MS Teams conference, MOH is played into the conference by the OpenScape Business.

Encryption

OpenScape Business does not support secure media interworking with the SBC.

Class of Service

Gateway mode: external calls of MS Teams Clients via the native SIP trunk are restricted by Denied List 1.

Trusted External User: external calls of MS Teams Clients are restricted by OpenScape Business User assigned COS list.

LAN/WAN Interface

As MS Teams Interworking is possible via the LAN interface only, the WAN interface is not available as a TCP/IP connection for an ITSP. The ITSP must be connected via LAN interface as well.

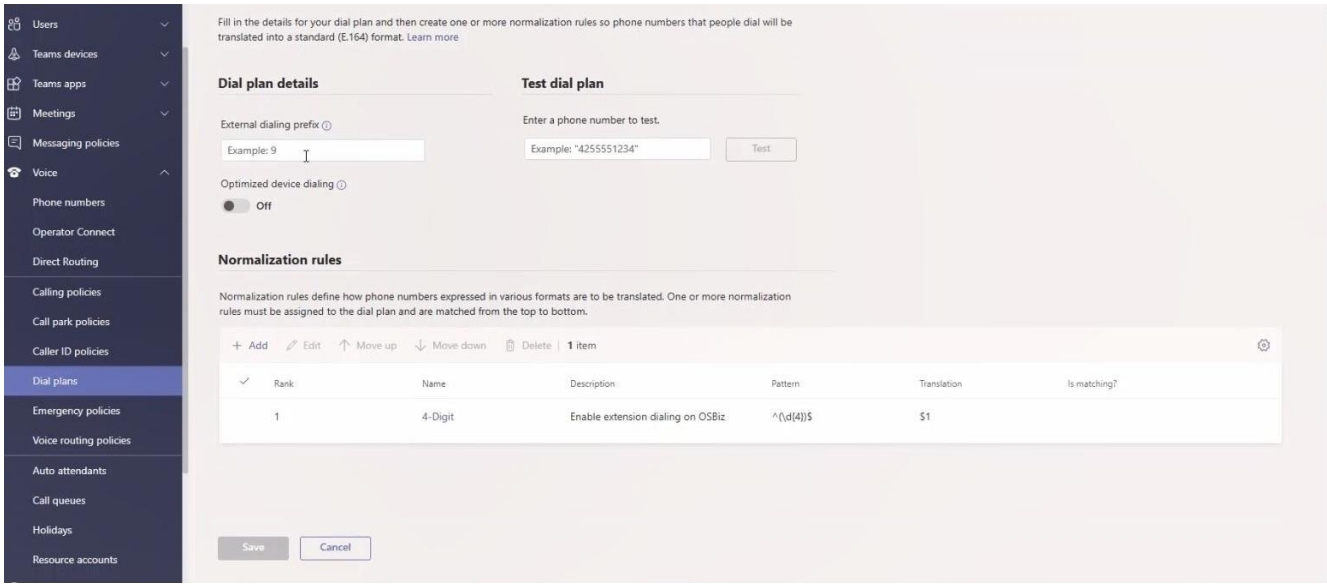
Details are available in [5]: Tutorial VoIP Interfaces.

8. Best Practise

Information and useful hints from customer installations.

Internal Call number for MS Teams client

Instead of using the complete E.164 format a MS Teams clients can be addressed by a short number (e.g. 4 digits corresponding to the internal number) via an according Dial plan entry:



9. Support & Serviceability

9.1. Assistance to resolve OSBiz or MS Teams client related issues

no calls with MS Teams client possible	• no natives SIP lines are configured or all lines are busy • external calls might be restricted by according entries in Denied List 1
no outbound calls to MS Teams client possible	• depending on Teams numbering plan the called party number in E.164 requires LCR dialing rule type "Country code"
no inbound calls from MS Teams client possible	• see "no calls with MS Teams client possible"
Central Office ITSP calls are not signalled at MS Teams client	• please check for codecs (e.g. G.711) on Carrier side
desk phone calls are not signalled at MS Teams client	• please check for codecs (e.g. G.711) on phone side
MS Teams-Client Hold/Park Call • Feature collision: OSBiz User puts MS Teams client on hold AND MS Teams client puts OSBiz User on hold	• "on hold" indication for Display is not supported • MS Teams client is unable to resume the call if OSBiz User hasn't resumed first
MS Teams client Transfer • no update on Display	• update of transferred party information is not supported
MS Teams client Call Forwarding • Call Forwarding destination is not signalled with original calling party information • display of the forwared to party does not show the name	• update of forwarded party information is not supported name provision is not supported
MS Teams Conference • OSBiz MoH disturbs the conference call	• mute the according OSBiz User in the MS Teams conversation - the OSBiz User can unmute himself
Payload issue • MS Team calling HFA but there	• activate the flag" always use DSP" for MS Teams

is no payload	Route
Payload issue	
• Voice interruptions at the beginning of the call	Microsoft recommends to check whether the network is ready for Teams requirements, for example see: https://docs.microsoft.com/en-us/microsoftteams/3-envision-evaluate-my-environment#network-readiness

9.2. Known issues

- **Basic Call (Calls to Teams from SIP stations)**

  Gateway mode: When a SIP station makes a call to MS Teams user, after the call is established the number shown on SIP station is not in the correct format according to system configuration.

- **Call Hold**

  In double call hold scenarios for calls between MS Teams users and OpenScape Business subscribers, it has been observed that the Teams user is unable to resume the call if the OpenScape Business subscriber hasn't resumed the call first; if OpenScape Business subscriber resumes first, then the MS Teams user is able to resume the call.

- **Codecs**

  In a codec mismatch scenario where a MS Teams user makes a call to an OpenScape Business subscriber, even if the PBX responds with a SIP 488 Not Acceptable Here message, the OpenScape Business station rings; when the call is answered there is no speechpath.

9.3. Required trace configuration options for error reporting

OpenScape Business Trace Profiles:

1. Basic
2. Voice Fax Connections
3. SIP_Interconnection_Subscriber_ITSP

In case of registration issue please activate the OpenScape Business Trace Profile in addition:

4. SIP_Registration

OpenScape Business Trace Components:

1. FP_CP-Port-User: level 9
2. FP_DH-SIP: level 9 (only for OpenScape Business X variant)

9.4. Required trace files for error analysis

- OpenScape Business Diagnosis Logs and Wireshark traces
- each SBC has his own trace instructions and capabilities

10. Security

In a scenario that integrates MS Teams via a 3rd-pty SBC particular care needs to be taken to avoid misconfiguration that facilitates toll fraud. The reason is that there is no authentication of the MS Teams subscriber when connecting to the SBC. The security mainly relies on a trust relationship that is established between MS Teams and the SBC during the TLS connection.

As Microsoft teams does not check any class of service for the telephony clients, toll fraud is possible by dialing premium service numbers from MS Teams Clients using OpenScape Business as a gateway to the public telephone network.

If the SBC cannot be installed in the customer LAN a VPN between OpenScape Business and SBC must be used.

The following measures are strongly recommended to reduce the risk for toll fraud when connecting to MS Teams:

- Import the Trusted CA's proposed by Microsoft.
- Restrict import of additional CA's to the minimum required for additional SBC Trunk connections (Note: Support of a wide range of Trusted CA's increases the risk of compromise through spoofed certificates).
- Always use mTLS with full certificate validation of the certificates.
- Restrict access from MS Teams in the SBC firewall to IP address ranges for MS Teams as published by Microsoft.

To prevent calls to premium services or toll fraud, the numbers that are not allowed to be dialed from the MS Teams client via the SBC trunk line must be entered the Denied List 1 within the OpenScape Business configuration.

As an additional measure, the MS-Teams Client can be configured as a "Trusted mobile User" within OpenScape Business. In this case, the OpenScape Business Class of Service (COS) lists can be applied to the associated user within OpenScape Business.