

OpenScape Business V3

HowTo
Microsoft Teams Interworking

SIP Trunking and Gateway / Trusted external User

- AudioCodes SBC
- anynode SBC

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

1. Introduction	8
1.1. General Configuration overview	9
2. Direct Routing	11
2.1. Setup the Domain	11
2.2. Pair the SBC to the Direct Routing Service of MS Phone System	19
2.3. Enable users for Direct Routing Service	21
2.4. Configure Voice Routing	22
2.5. Designate to a user the ability to use calling functionality within Teams	25
3. AudioCodes SBC	27
3.1. LAN and WAN IP Interfaces	27
3.2. Teams TLS Context	28
3.3. Media Realms	33
3.4. SIP Signaling Interfaces	34
3.5. Proxy Sets and Proxy Addresses	37
3.6. Coder Groups	41
3.7. IP Profiles	43
3.8. IP Groups	46
3.9. Media Security	49
3.10. Message Condition and Classification Rules	50
3.11. Message Manipulation	52
3.12. IP-to-IP Call Routing Rules	54
3.13. Firewall Settings	58
4. Anynode SBC	61
4.1. anynode Wizard – Teams / Voice over IP Provider	61
4.2. anynode Wizard – Teams / Network Controller	64
4.3. anynode Wizard – Teams / Ports	65
4.4. anynode Wizard – Teams / Certificate & Private Key	66
4.5. anynode Wizard – Teams / Certificate Chain	70
4.6. anynode Wizard – Teams / SBC FQDN	71
4.7. anynode Wizard – Teams / Name	72
4.8. anynode Wizard – OSBiz / Voice over IP System	73
4.9. anynode Wizard – OSBiz / Network Controller	75
4.10. anynode Wizard – OSBiz / Ports	76
4.11. anynode Wizard – OSBiz / SIP Interconnection	77
4.12. anynode Wizard – OSBiz / Remote SIP Domain	78

4.13. anynode Wizard – OSBiz / Network Peer Whitelist	79
4.14. anynode Wizard – OSBiz / Manipulations	80
4.15. anynode Wizard – OSBiz / Name	82
4.16. anynode Wizard – Routing	84
4.17. anynode SBC – Additional Configuration	86
5. OpenScape Business – Gateway mode	91
5.1. PABX Location Data	91
5.2. SIP Interconnection	92
5.3. Routes	94
5.4. LCR Changes	96
5.5. System Parameter Flags	100
6. OpenScape Business - Trusted external User mode	102
6.1. SIP Interconnection	103
6.2. Routes	105
6.3. Trusted external User	107
6.4. Configuration Wizard – Team Configuration	108
6.5. LCR Dial Plan	109
6.6. System Parameter Flags	109
7. Capacities & Feature Interaction	110
8. Best Practise	112
9. Support & Serviceability	113
9.1. Assistance to resolve OSBiz or MS Teams client related issues	113
9.2. Known issues	114
9.3. Required trace configuration options for error reporting	115
9.4. Required trace files for error analysis	115

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

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

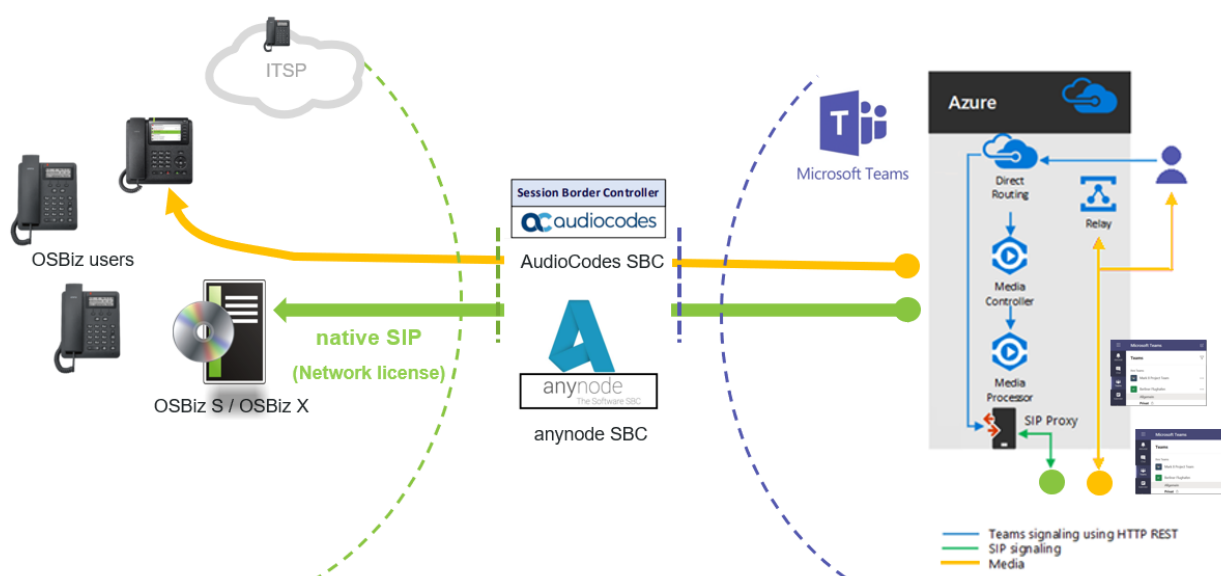
OpenScope Business V3 complements MS Teams with powerful telephony capabilities such as Call Centers, AutoAttendant, DECT, etc.

OpenScope 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 365 / 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.

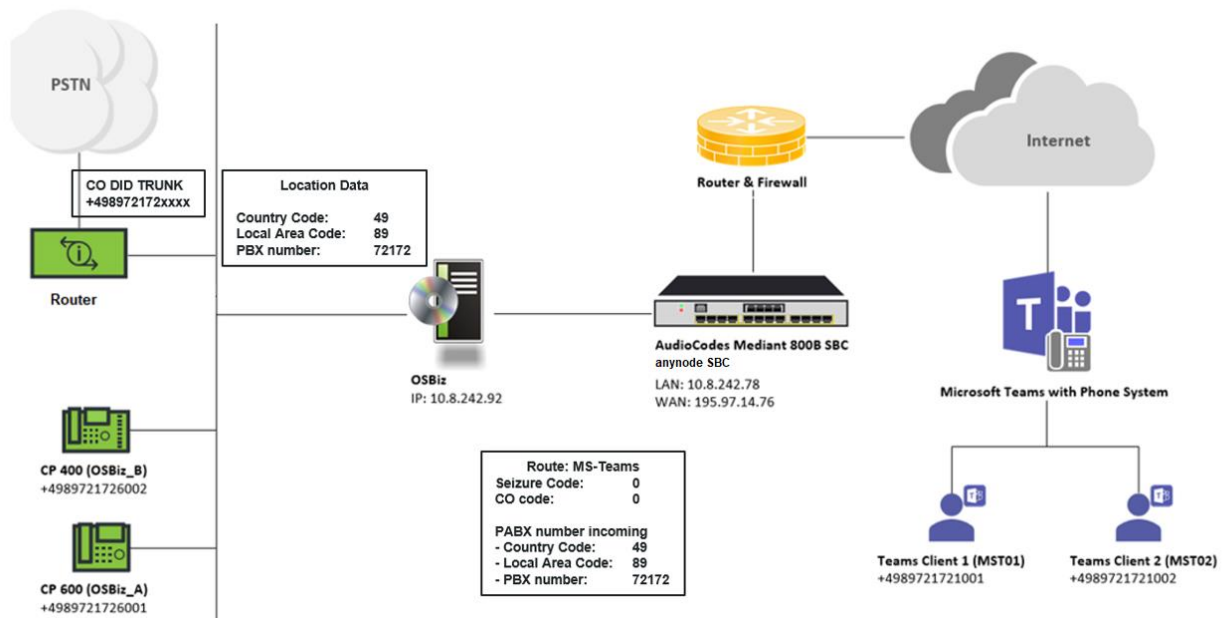
In example environment, Office 365 E5 licenses are available, which are applied to the Teams test users:

- 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>).



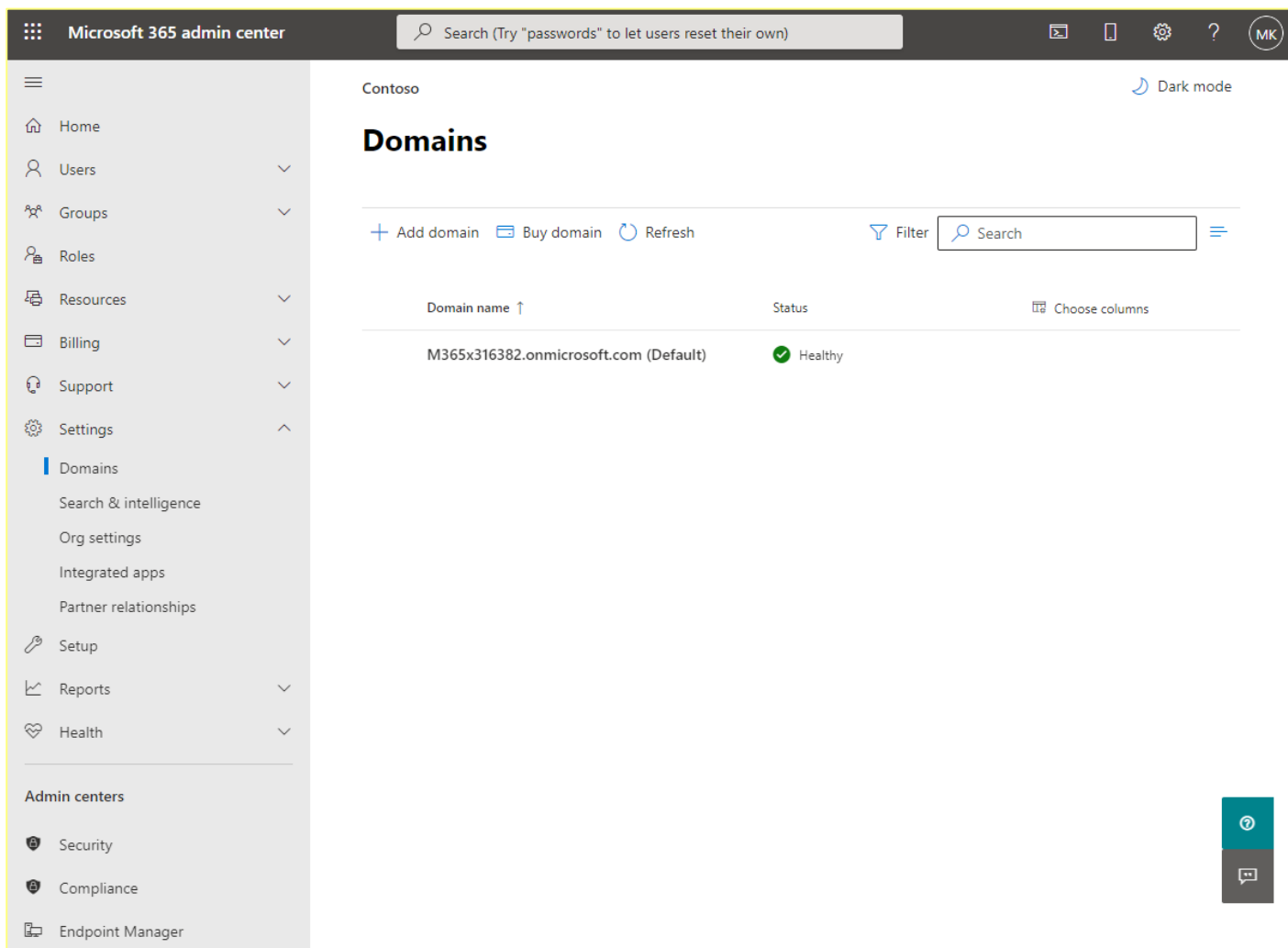
2. Direct Routing

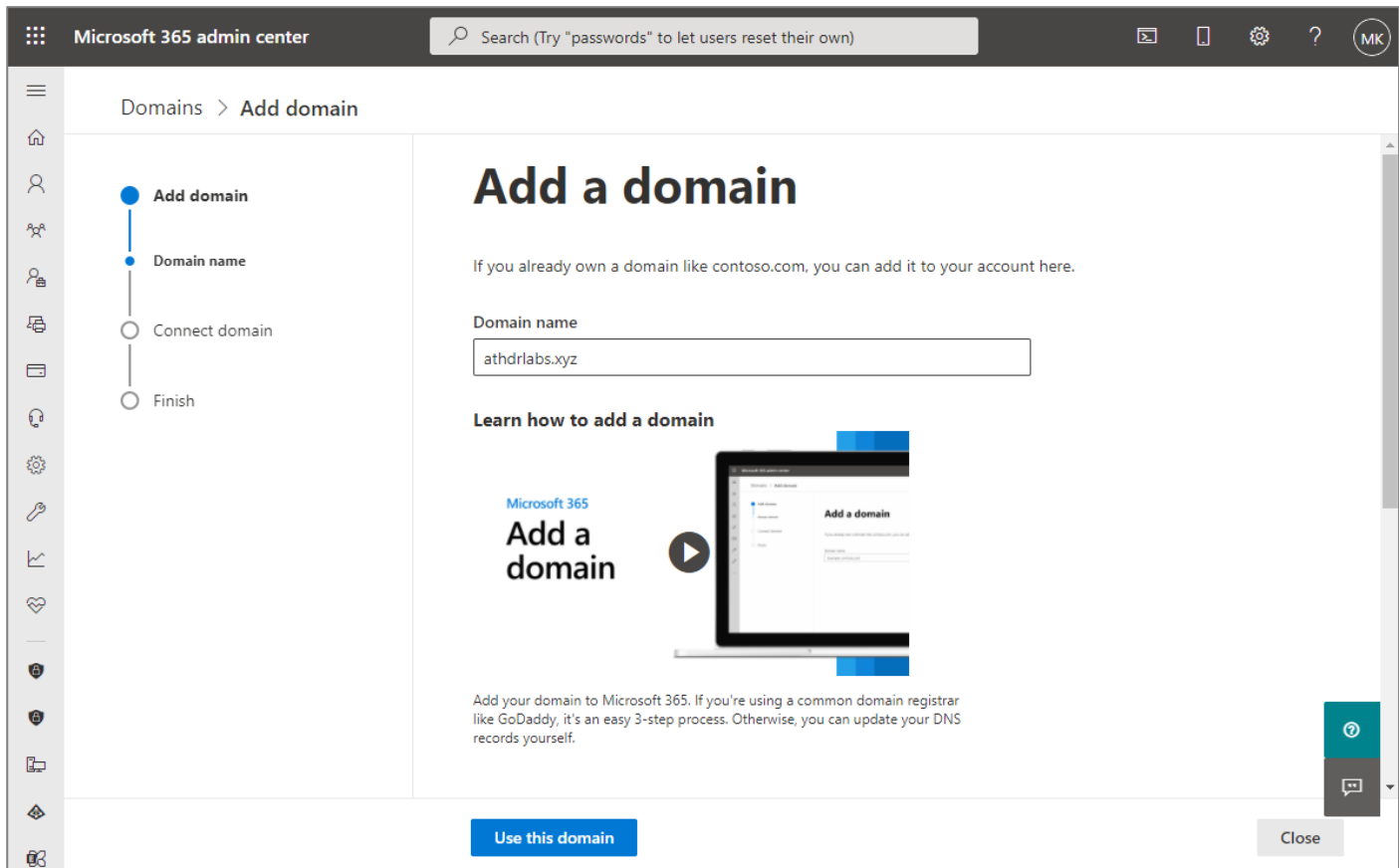
The current section summarizes the example configuration on Microsoft Office 365 tenant for the Direct Routing connection with an AudioCodes or anynode SBC, based on the according certification results [6] & [7]. Default or non-project specific Office 365 tenant configuration will not be referenced in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

2.1. Setup the Domain

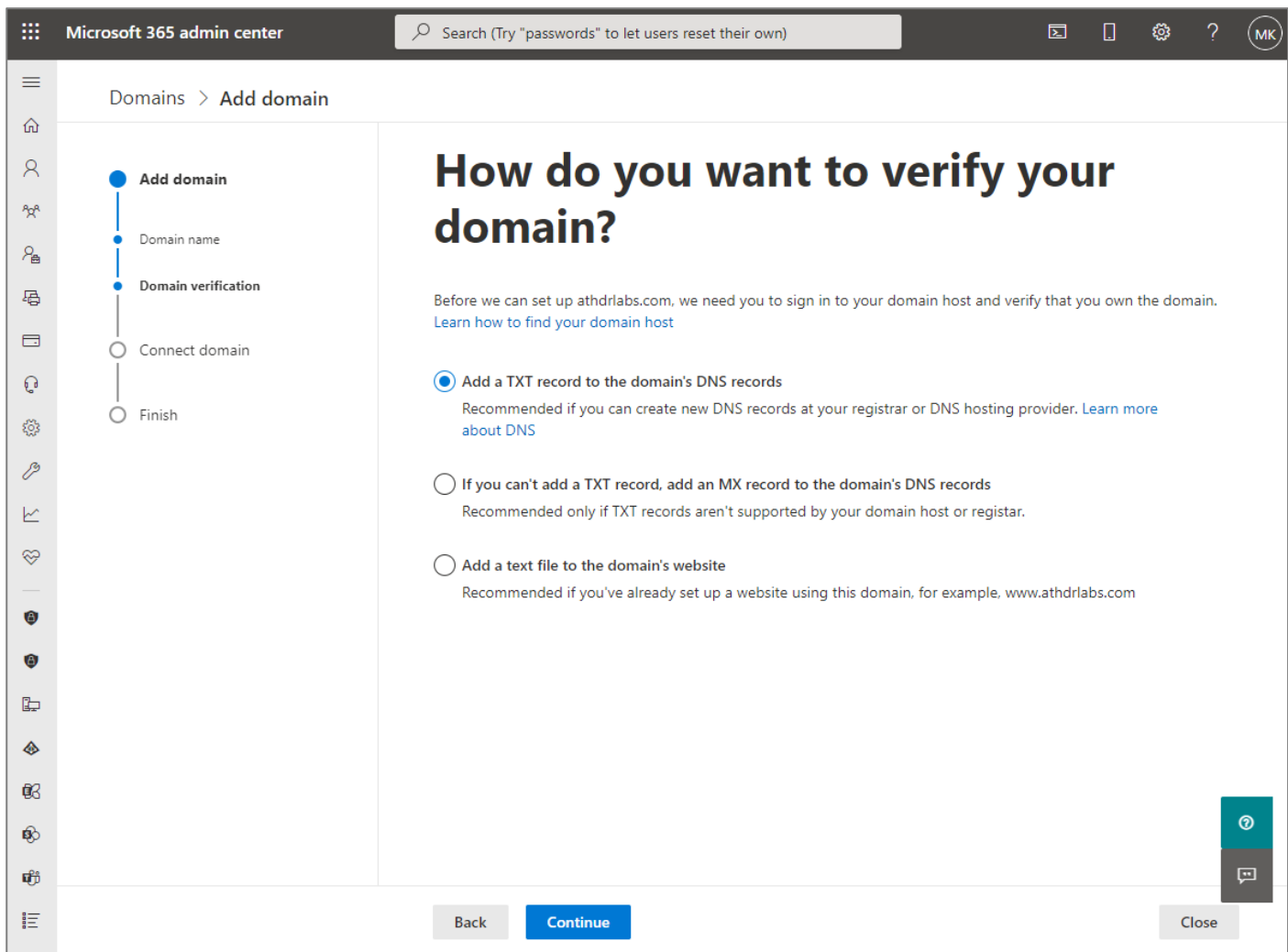
This subsection outlines how to add the SBC domain to the tenant.

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

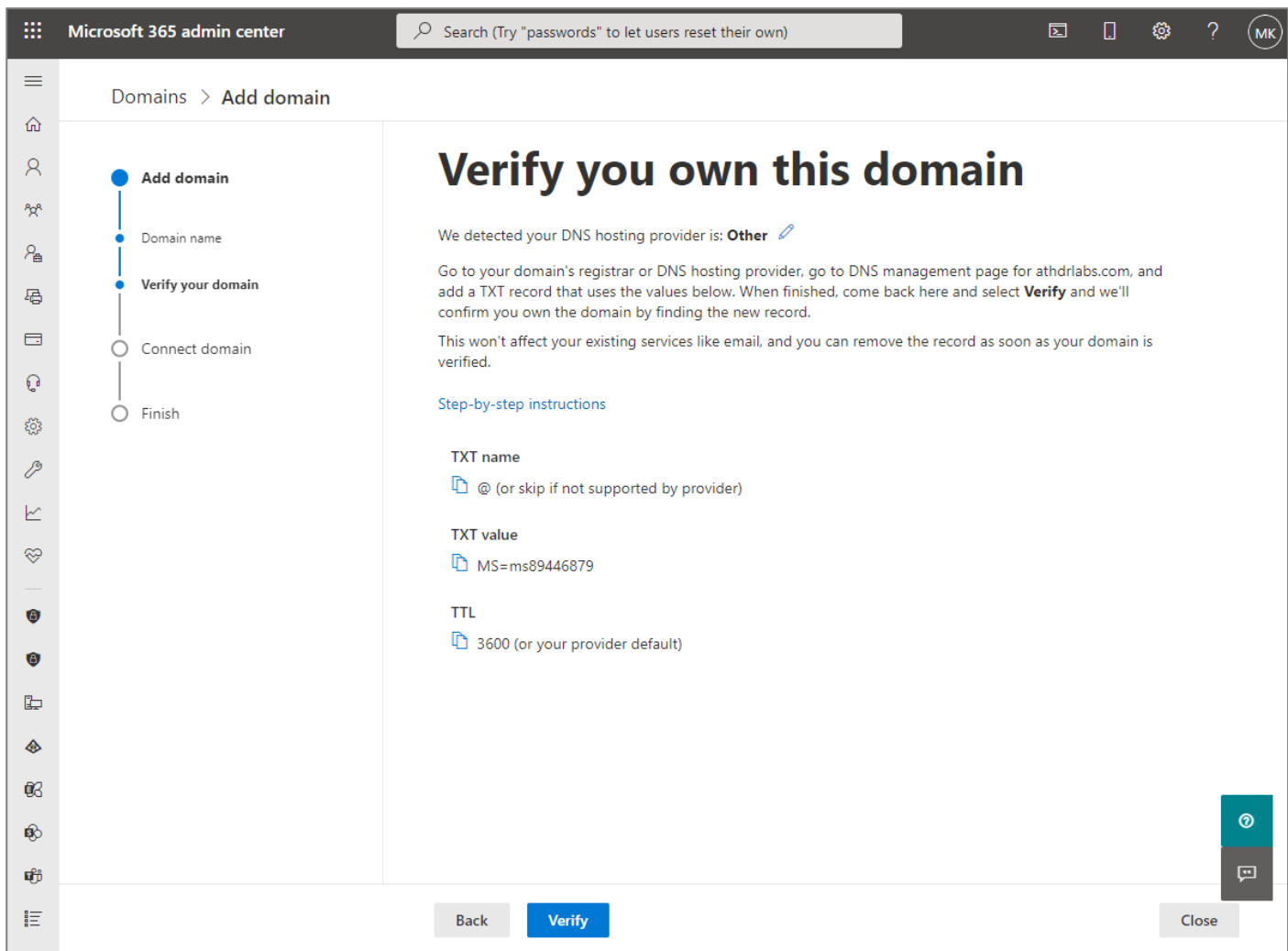




Enter the SBC domain name, e.g. **"athdrllabs.xyz"** in **"Enter a domain you own"** box.
Click on **[Use this domain]**.

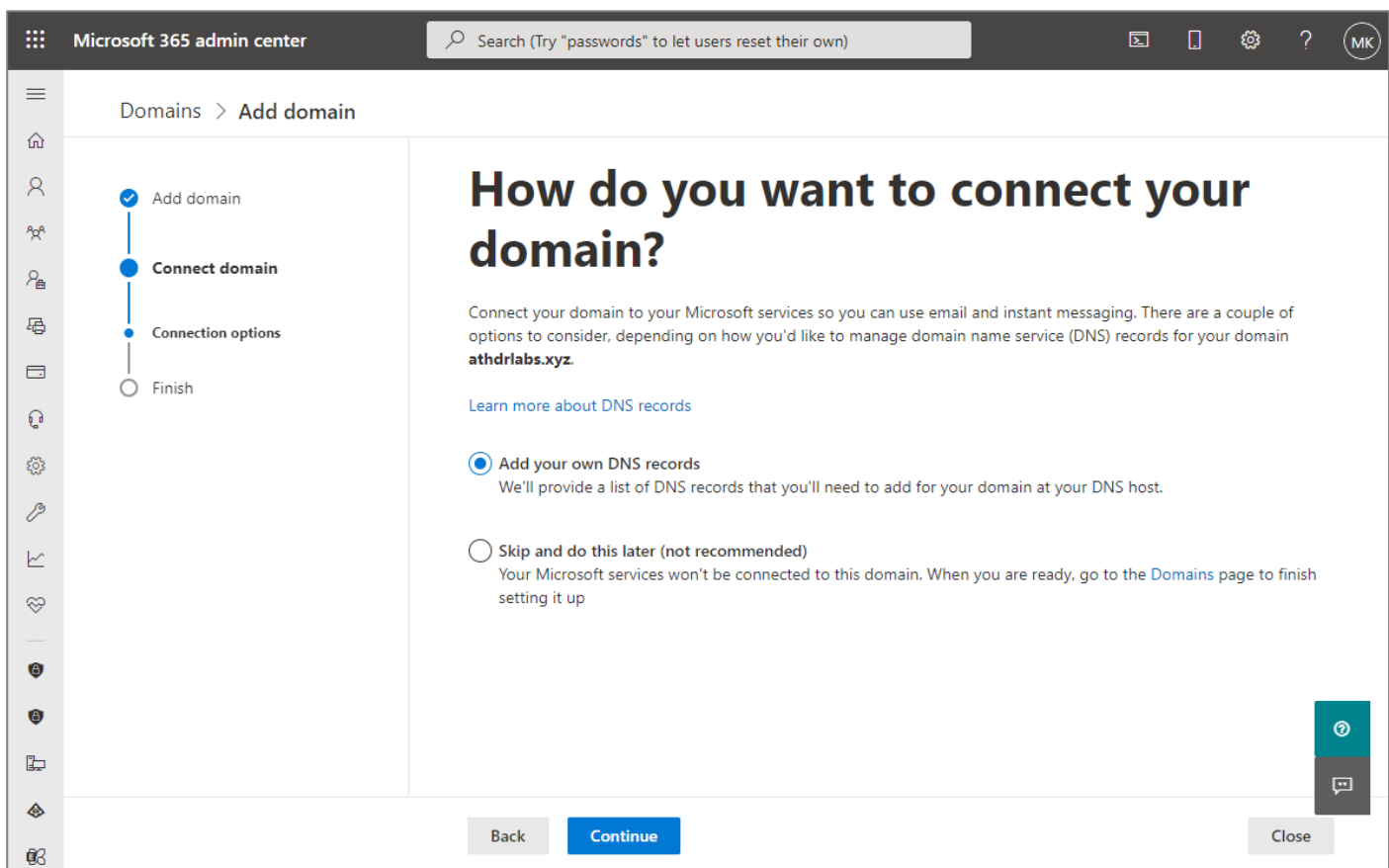


Select "Add a TXT record to the domain's DNS records" and click on **[Continue]**.



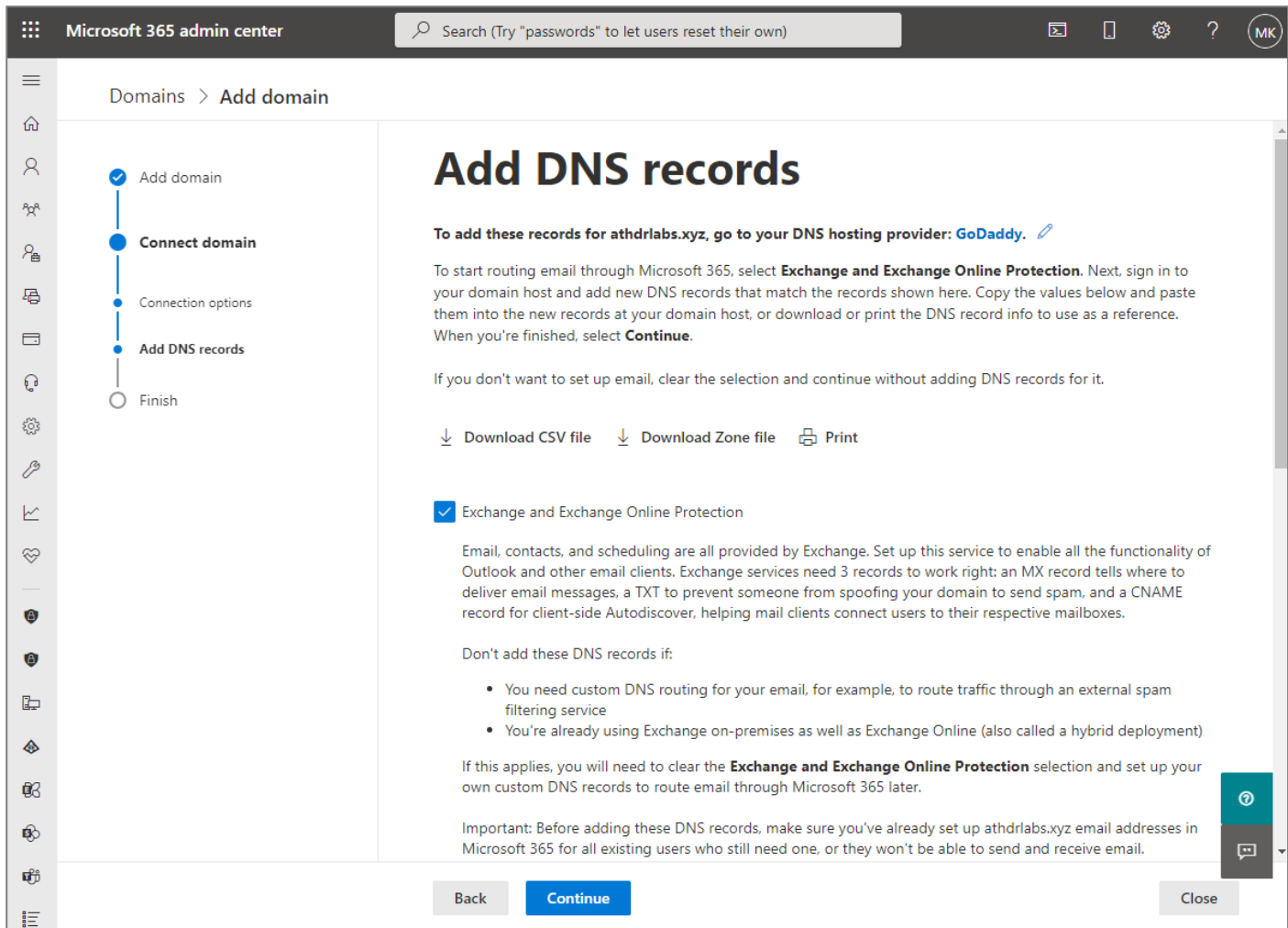
Copy-paste this screen and contact corresponding DNS domain owner to validate domain ownership.

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)

Domains > Add domain

Progress: Add domain (checked), **Connect domain**, Connection options, Add DNS records, Finish

MX Records (1)
View instructions for MX Records

Record	Host Name	Points to address or value	Priority	TTL	Status
Expected	@	athdrlabs-xyz.mail.protection.outlook.com	0	1 Hour	

CNAME Records (1)
View instructions for CNAME Records

Record	Host Name	Points to address or value	TTL	Status
Expected	autodiscover	autodiscover.outlook.com	1 Hour	

TXT Records (1)
View instructions for TXT Records

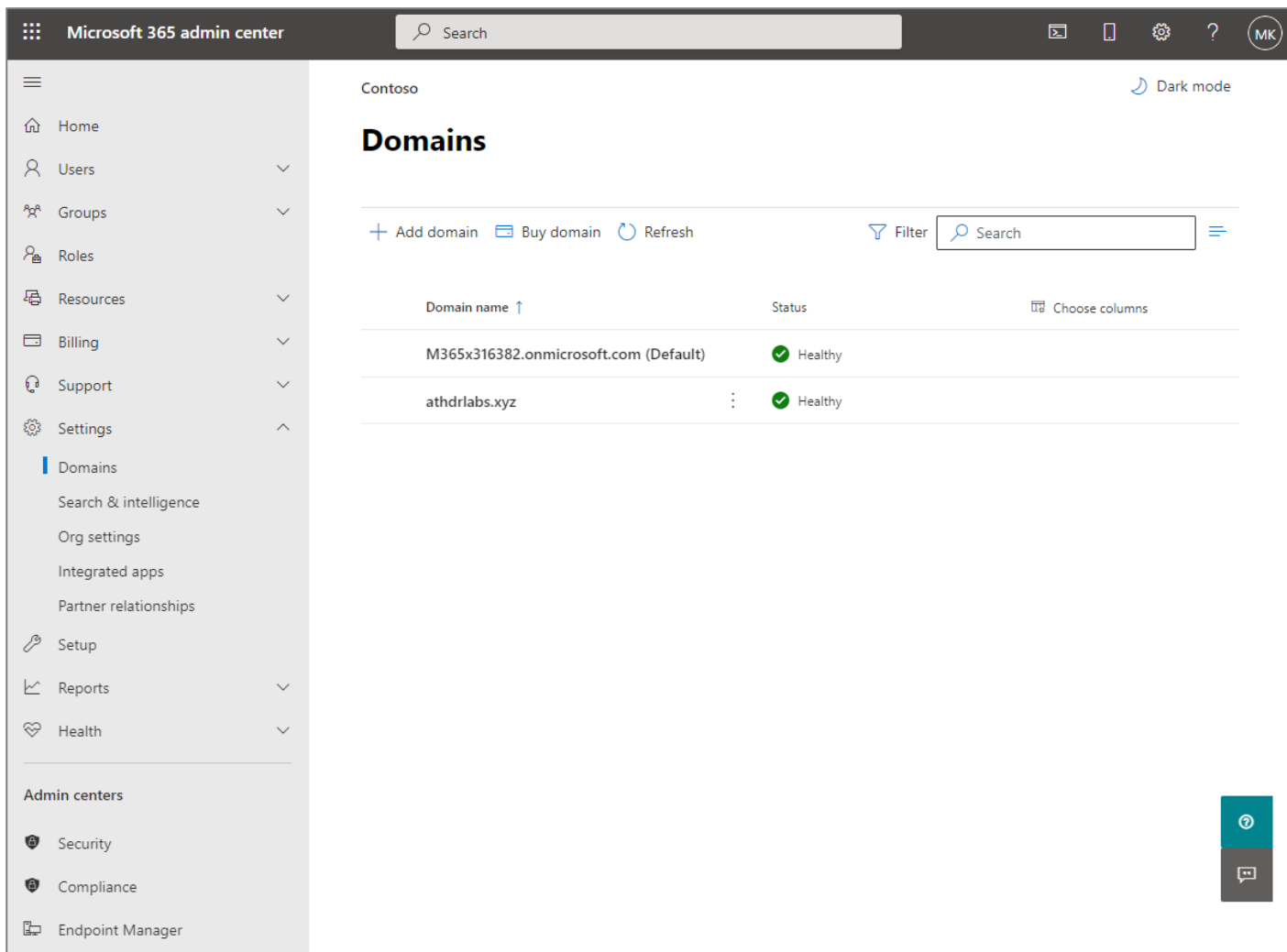
Record	TXT name	TXT value	TTL	Status
Expected	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour	

Advanced Options

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

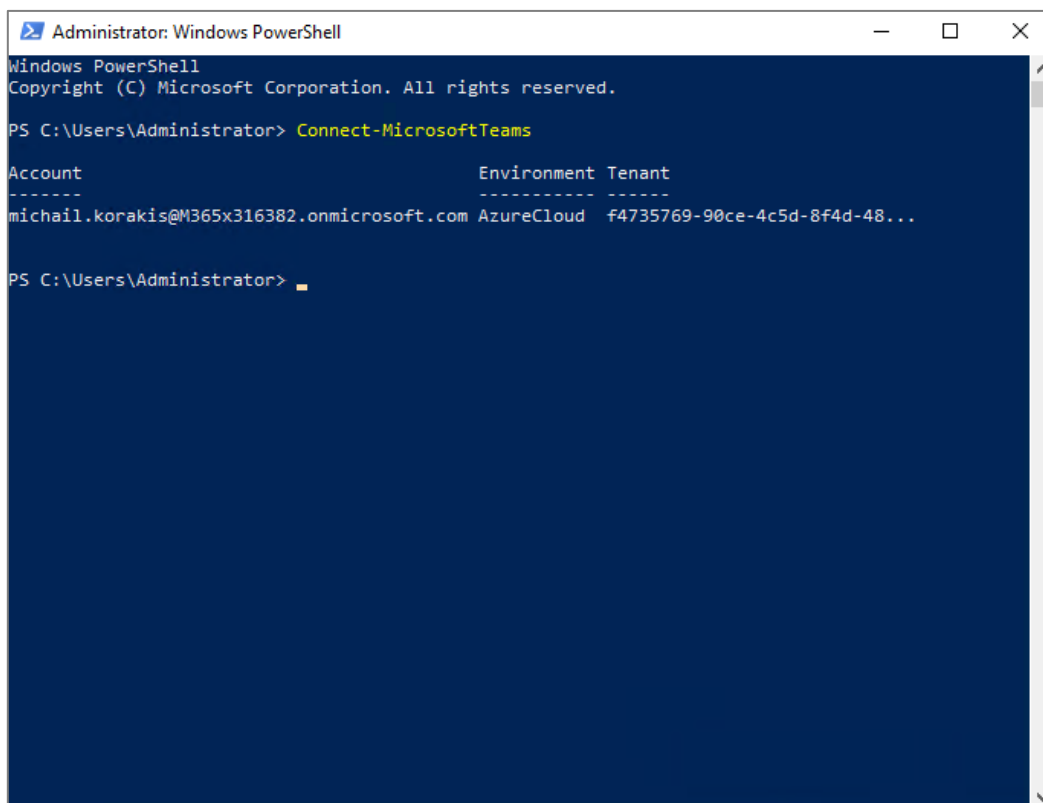
The SBC connection to Microsoft Phone System, routes and routing policies will be configured via PowerShell. Specifically, in the Skype for Business Online PowerShell.

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.



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

PS C:\Users\Administrator> Connect-MicrosoftTeams

Account                                Environment Tenant
-----                                -
michail.korakis@M365x316382.onmicrosoft.com AzureCloud f4735769-90ce-4c5d-8f4d-48...
```

Create and pair the SBC SIP trunk in Teams tenant.

```

Administrator: Windows PowerShell
-----
Account                               Environment Tenant
-----
michail.korakis@M365x316382.onmicrosoft.com AzureCloud f4735769-90ce-4c5d-8f4d-48...

PS C:\Users\Administrator> Get-CsOnlinePSTNGateway -Identity sbc01.athdrlabs.xyz

Identity                               : sbc01.athdrlabs.xyz
InboundTeamsNumberTranslationRules     : {}
InboundPstnNumberTranslationRules      : {}
OutboundTeamsNumberTranslationRules    : {}
OutboundPstnNumberTranslationRules     : {}
Fqdn                                   : sbc01.athdrlabs.xyz
SipSignalingPort                       : 5061
FailoverTimeSeconds                   : 10
ForwardCallHistory                     : True
ForwardPai                             : True
SendSipOptions                         : True
MaxConcurrentSessions                 : 24
Enabled                               : True
MediaBypass                           : False
GatewaySiteId                         : 
GatewaySiteLbrEnabled                 : False
GatewayLbrEnabledUserOverride          : False
FailoverResponseCodes                 : 408,503,504
GenerateRingingWhileLocatingUser      : 
PidfLoSupported                       : False
MediaRelayRoutingLocationOverride     : 
ProxySbc                              : 
BypassMode                            : None

PS C:\Users\Administrator>

```

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.

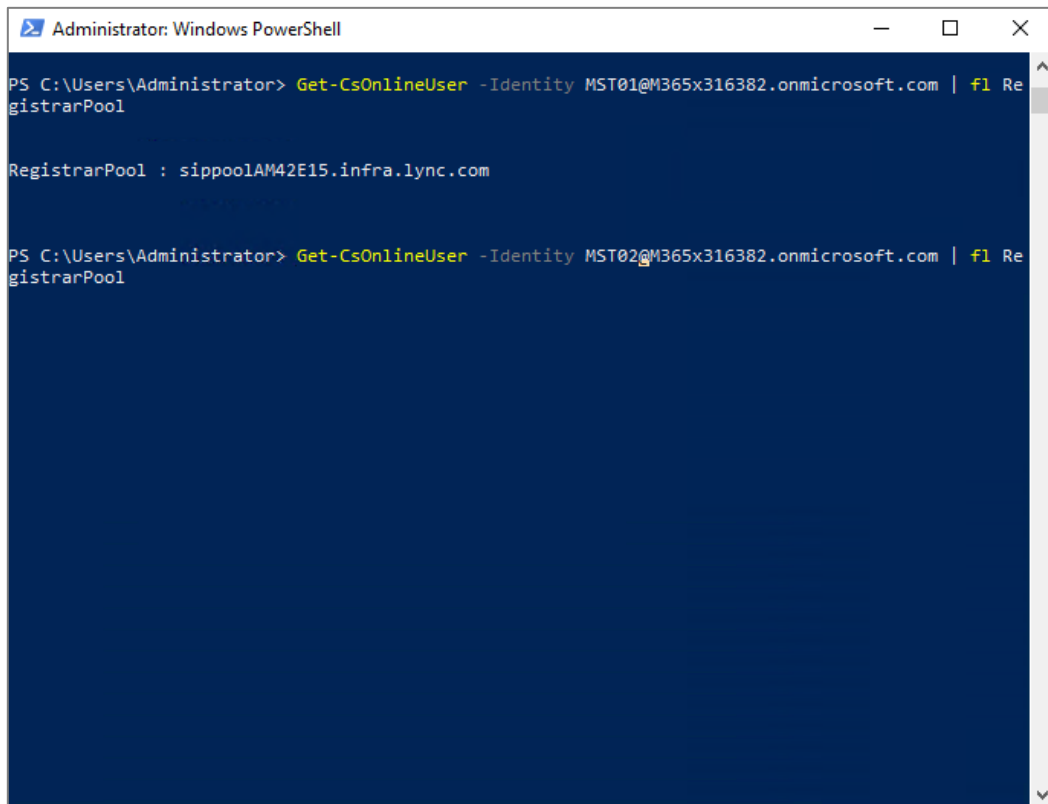
View the newly created "Online PSTN Gateway" (SIP trunk) with the command:

*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.



```
Administrator: Windows PowerShell

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

RegistrarPool : sippoolAM42E15.infra.lync.com

PS C:\Users\Administrator> Get-CsOnlineUser -Identity MST02@M365x316382.onmicrosoft.com | fl RegistrarPool
```

```
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

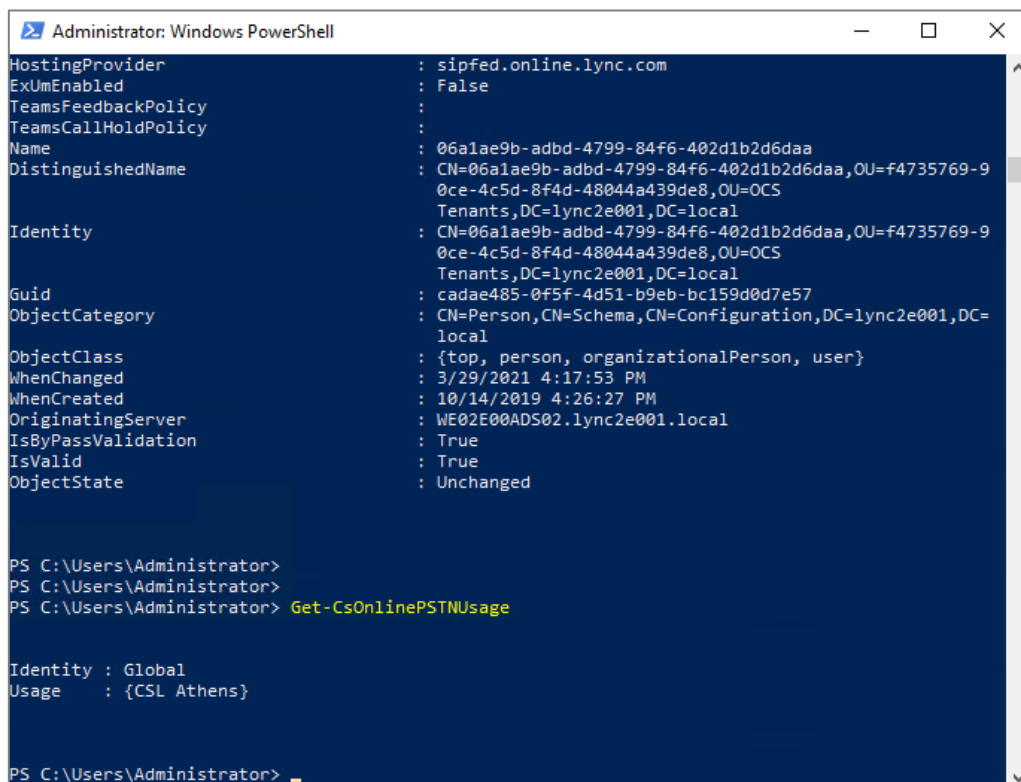
Microsoft Phone System has a routing mechanism that allows a call to be sent to a specific SBC based on:

- 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.



```
Administrator: Windows PowerShell

HostingProvider      : sipfed.online.lync.com
ExUmEnabled          : False
TeamsFeedbackPolicy  :
TeamsCallHoldPolicy  :
Name                 : 06a1ae9b-adbd-4799-84f6-402d1b2d6daa
DistinguishedName     : CN=06a1ae9b-adbd-4799-84f6-402d1b2d6daa,OU=f4735769-9
                     : 0ce-4c5d-8f4d-48044a439de8,OU=OCS
                     : Tenants,DC=lync2e001,DC=local
Identity              : CN=06a1ae9b-adbd-4799-84f6-402d1b2d6daa,OU=f4735769-9
                     : 0ce-4c5d-8f4d-48044a439de8,OU=OCS
                     : Tenants,DC=lync2e001,DC=local
Guid                  : cadae485-0f5f-4d51-b9eb-bc159d0d7e57
ObjectCategory        : CN=Person,CN=Schema,CN=Configuration,DC=lync2e001,DC=
                     : local
ObjectClass            : {top, person, organizationalPerson, user}
WhenChanged           : 3/29/2021 4:17:53 PM
WhenCreated            : 10/14/2019 4:26:27 PM
OriginatingServer      : WE02E00ADS02.lync2e001.local
IsByPassValidation     : True
IsValid                : True
ObjectState            : Unchanged

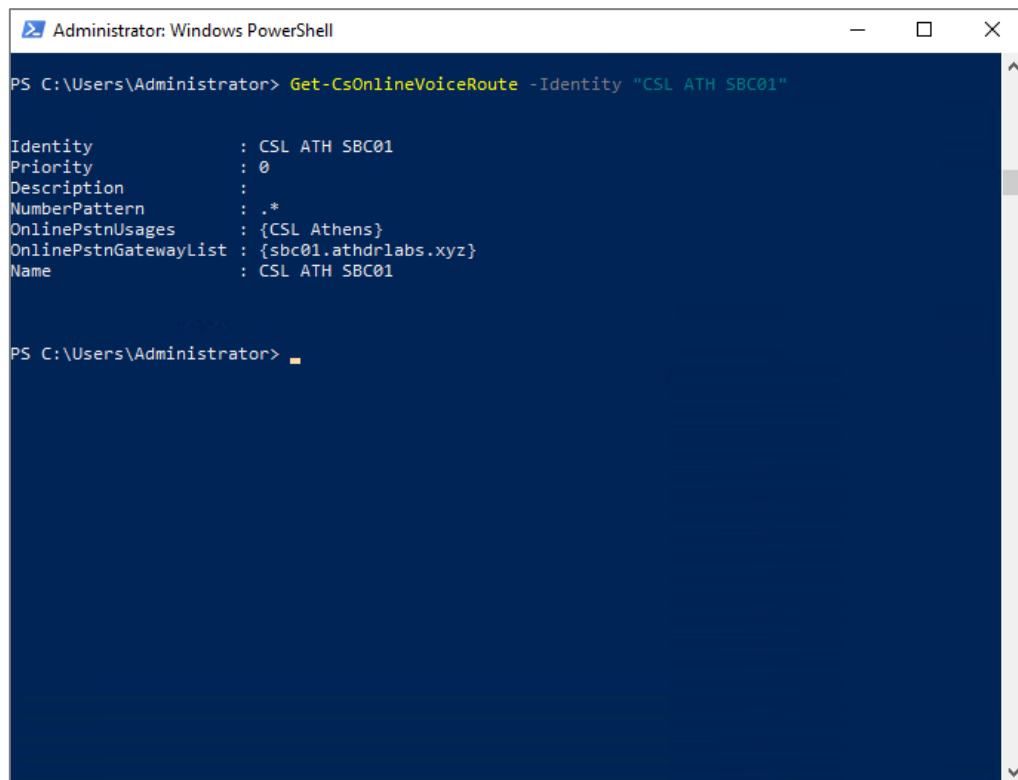
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-CsOnlinePSTNUsage

Identity : Global
Usage     : {CSL Athens}

PS C:\Users\Administrator>
```

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

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



```
Administrator: Windows PowerShell

PS C:\Users\Administrator> Get-CsOnlineVoiceRoute -Identity "CSL ATH SBC01"

Identity           : CSL ATH SBC01
Priority            : 0
Description         :
NumberPattern       : .*
OnlinePstnUsages    : {CSL Athens}
OnlinePstnGatewayList : {sbc01.athdrlabs.xyz}
Name                : CSL ATH SBC01

PS C:\Users\Administrator>
```

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

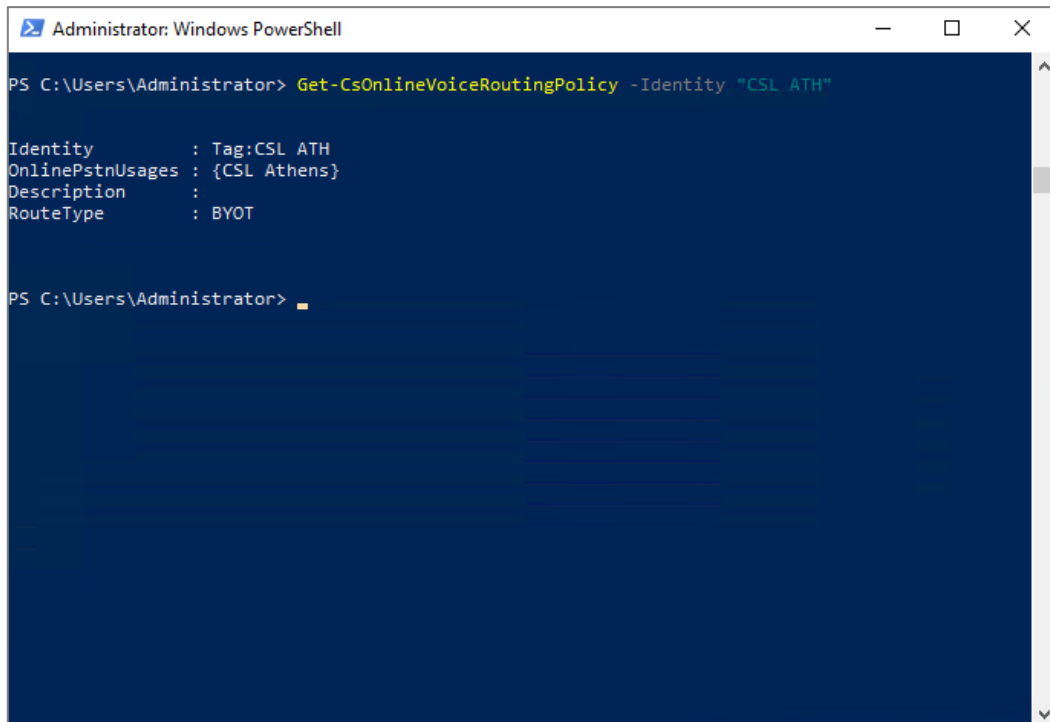
```
New-CsOnlineVoiceRoute -Identity "CSL ATH SBC01" -NumberPattern "^+49(\d{8})$" -  
OnlinePstnGatewayList sbc01.athdrlabs.xyz -Priority 1 -OnlinePstnUsages "CSL Athens"
```

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"
```



```
Administrator: Windows PowerShell

PS C:\Users\Administrator> Get-CsOnlineVoiceRoutingPolicy -Identity "CSL ATH"

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

PS C:\Users\Administrator>
```

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

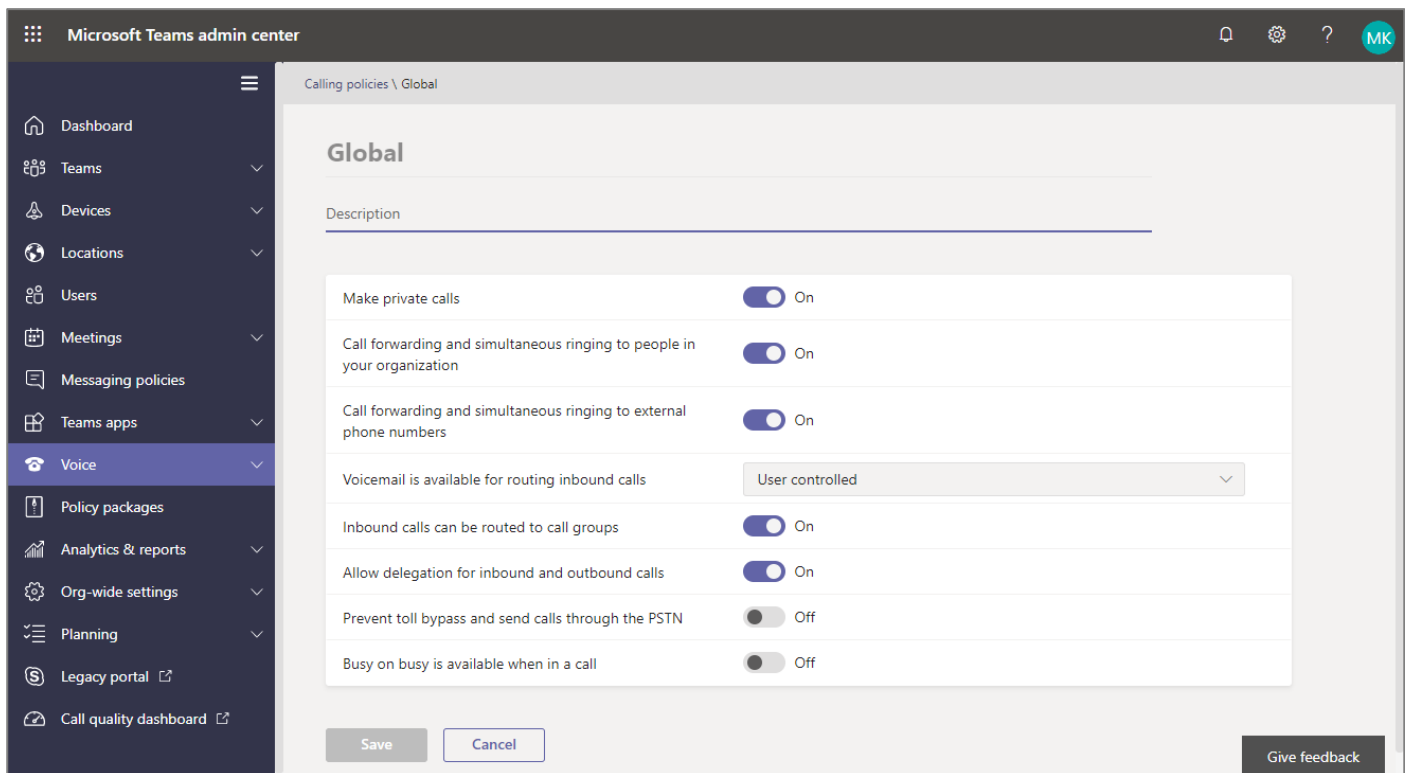
The users in current testing activities have the Global policy assigned where calling functionality is enabled.

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]**.

The screenshot displays the Microsoft Teams Admin Center interface. On the left is a navigation pane with options like Dashboard, Teams, Devices, Locations, Users, Meetings, Messaging policies, Teams apps, Voice, Policy packages, Analytics & reports, Org-wide settings, Planning, Legacy portal, and Call quality dashboard. The 'Users' section is selected, showing a list of users with 'MST01' highlighted. The main area shows the user profile for MST01, including contact information, a 7-day quality donut chart, and 7-day activity statistics. Below the profile, the 'Policies' tab is active, showing a list of assigned policies. The 'Calling policy' is highlighted with a red box, showing it is set to 'Global (Org-wide default)'. Other policies listed include Meeting, Messaging, Live events, App permission, App setup, Call park, and Caller ID, all set to 'Global (Org-wide default)'. A 'Policy package' section shows 'None' is assigned.

Policy Name	Assigned Policy
Meeting policy	Global (Org-wide default)
Messaging policy	Global (Org-wide default)
Live events policy	Global (Org-wide default)
App permission policy	Global (Org-wide default)
App setup policy	Global (Org-wide default)
Call park policy	Global (Org-wide default)
Calling policy	Global (Org-wide default)
Caller ID policy	Anonymous Calling (Direct)

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

The screenshot shows the 'IP Interfaces' configuration window. The 'GENERAL' tab is active, showing fields for Index (0), Name (LAN_IF), Application Type (OAMP + Media + Control), and Ethernet Device (#0 [vlan 1]). The 'IP ADDRESS' tab is also visible, showing Interface Mode (IPv4 Manual), IP Address (10.8.242.78), Prefix Length (24), and Default Gateway (10.8.242.1). The 'DNS' section shows Primary DNS (10.8.251.103) and Secondary DNS (0.0.0.0). The 'APPLY' button is highlighted in blue.

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.

The screenshot shows the Audiocodes M800B web interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar shows the 'ADMINISTRATION' section with a 'TIME & DATE' tab selected. The main content area is titled 'Time & Date' and contains two main sections: 'LOCAL TIME' and 'TIME ZONE'. The 'LOCAL TIME' section includes a date and time picker (Year: 2020, Month: 2, Day: 28, Hours: 11, Minutes: 41, Seconds: 46). The 'TIME ZONE' section includes a UTC Time display (28 Feb, 2020 09:41:46), a UTC Offset (Hours: 2, Minutes: 0), and a Daylight Saving Time dropdown (Disable). The 'NTP SERVER' section is highlighted with a red box and contains the following fields: 'Enable NTP' (dropdown menu set to 'Enable'), 'Primary NTP Server Address (IP or FQDN)' (text field with '10.8.251.104'), 'Secondary NTP Server Address (IP or FQDN)' (empty text field), 'NTP Update Interval' (Hours: 24, Minutes: 0), 'NTP Authentication Key Identifier' (text field with '0'), and 'NTP Authentication Secret Key' (empty text field). At the bottom right of the 'NTP SERVER' section are 'Cancel' and 'APPLY' buttons.

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

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

Click on **[Apply]**.

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

TLS Contexts

GENERAL		OCSP	
Index	1	OCSP Server	Disable
Name	MS Teams	Primary OCSP Server	0.0.0.0
TLS Version	TLSv1.2	Secondary OCSP Server	0.0.0.0
DTLS Version	Any	OCSP Port	2560
Cipher Server	DEFAULT	OCSP Default Response	Reject
Cipher Client	DEFAULT		
Cipher Server TLS1.3	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256		
Cipher Client TLS1.3	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256		
Key Exchange Groups	X25519:P-256:P-384:X448		
Strict Certificate Extension Validation	Disable		
DH key Size	2048		
TLS Renegotiation	Enable		

Cancel APPLY

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.

audiocodes SETUP MONITOR TROUBLESHOOT Save Reset Actions Admin

IP NETWORK SIGNALING & MEDIA ADMINISTRATION Entity, parameter, value

SRD All

NETWORK VIEW

CORE ENTITIES

- IP Interfaces (2)
- Ethernet Devices (2)
- Ethernet Groups (12)
- Physical Ports (12)
- Static Routes (0)
- HA Settings
- HA Network Monitor (0)
- NAT Translation (0)

SECURITY

- TLS Contexts (2)**
- Firewall (0)
- Security Settings

QUALITY

DNS

WEB SERVICES

HTTP PROXY

RADIUS & LDAP

ADVANCED

TLS Contexts (2)

New Edit

Page 1 of 1 Show 10 records per page

INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	default	Any TLS1.x	Any	DEFAULT
1	MS Teams	TLSv1.2	Any	DEFAULT

#1[MS Teams] Edit

GENERAL		OCSP	
Name	MS Teams	OCSP Server	Disable
TLS Version	TLSv1.2	Primary OCSP Server	0.0.0.0
DTLS Version	Any	Secondary OCSP Server	0.0.0.0
Cipher Server	DEFAULT	OCSP Port	2560
Cipher Client	DEFAULT	OCSP Default Response	Reject
Cipher Server TLS1.3	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256		
Cipher Client TLS1.3	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256		
Key Exchange Groups	X25519:P-256:P-384:X448		
Strict Certificate Extension V...	Disable		
DH key Size	2048		
TLS Renegotiation	Enable		

Certificate Information >> **Change Certificate >>** Trusted Root Certificates >>

audiocodes SETUP MONITOR TROUBLESHOOT Save Reset Actions 12 Admin

M8008 IP NETWORK SIGNALING & MEDIA ADMINISTRATION Entity, parameter, value

SRD All

NETWORK VIEW

- CORE ENTITIES
- SECURITY
 - TLS Contexts (2)**
 - Firewall (8)
 - Security Settings
 - QUALITY
 - DNS
 - WEB SERVICES
 - HTTP PROXY
 - RADIUS & LDAP
 - ADVANCED

GENERATE NEW PRIVATE KEY AND SELF-SIGNED CERTIFICATE

Private Key Size: 1024

Private key pass-phrase (optional):

Press the "Generate Private Key" button to create new private key.
Press the "Generate Self-Signed Certificate" button to create self-signed certificate.
Note that the certificate will use the subject name configured in "Certificate Signing Request" box.
Important: generation of private key is a lengthy operation during which the device service may be affected.

Generate Private-Key Generate Self-Signed Certificate

TLS EXPIRY SETTINGS

TLS Expiry Check Start (days): 60

TLS Expiry Check Period (days): 7

Submit TLS Expiry Settings

UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase (optional):

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

Browse... Load File

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

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

Browse... Load File

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.

The screenshot shows the Audiocodes M8008 IP Network configuration page. The left sidebar contains a navigation menu with sections like NETWORK VIEW, CORE ENTITIES, SECURITY, QUALITY, DNS, WEB SERVICES, HTTP PROXY, RADIUS & LDAP, and ADVANCED. The main content area is titled 'TLS Context #1 > Certificate Information'. It displays the PRIVATE KEY (Key size: 2048 bits, Status: OK) and the CERTIFICATE details. The certificate information includes Version: 3 (0x2), Serial Number, Signature Algorithm: sha256WithRSAEncryption, Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Secigo Limited, CN=Secigo RSA Domain Validation Secure Server CA, Validity (Not Before: Jul 10 00:00:00 2020 GMT, Not After: Oct 8 23:59:59 2020 GMT), Subject: CN=bbc.de, Subject Public Key Info (Public Key Algorithm: rsaEncryption, RSA Public-Key: (2048 bit)), and X.509v3 extensions (X.509v3 Authority Key Identifier: keyid:8D:8C:5E:C4:54:AD:8A:E1:77:E9:9B:F9:9B:05:E1:B8:01:8D:61:E1).

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.

The screenshot shows the Audiocodes M8008 IP Network configuration page. The left sidebar is the same as the previous screenshot. The main content area is titled 'TLS Context #1 > Trusted Root Certificates'. It displays a table of trusted root certificates with columns: INDEX, SUBJECT, ISSUER, and EXPIRES. The table contains two rows: Row 0 (Secigo RSA Domain Validation S, USERTrust RSA Certification Aut, 12/31/2030) and Row 1 (USERTrust RSA Certification Aut, AAA Certificate Services, 12/31/2028). Below the table, there is a 'Selected Row #0' section showing the details of the selected certificate, including its Version, Serial Number, Signature Algorithm, Issuer, Validity, Subject, and Subject Public Key Info.

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.

The screenshot shows the 'Media Realms' configuration window. The 'GENERAL' tab is selected. The 'Name' field is set to 'MR_LAN', 'IPv4 Interface Name' is set to '#0 [LAN_IF]', 'UDP Port Range Start' is 6000, and 'Number Of Media Session Legs' is 100. The 'QUALITY OF EXPERIENCE' tab shows 'QoE Profile' and 'Bandwidth Profile' both set to '--'. The 'APPLY' button is highlighted in blue.

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.

SIP Interfaces

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

CLASSIFICATION

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

Cancel **APPLY**

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]**.

SIP Interfaces

SRD: #0 [DefaultSRD]

GENERAL

Index	1
Name	MS Teams_Trunk
Topology Location	Up
Network Interface	#1 [WAN_IF]
Application Type	SBC
UDP Port	0
TCP Port	0
TLS Port	5061
Additional UDP Ports	
Additional UDP Ports Mode	Always Open

MEDIA

Media Realm	#1 [MR_WAN]
Direct Media	Disable

SECURITY

TLS Context Name	#1 [MS Teams]
TLS Mutual Authentication	
Message Policy	--
User Security Mode	Not Configured
Enable Un-Authenticated Registrations	Not configured
Max. Number of Registered Users	-1

Cancel **APPLY**

TCP Port	0	Message Policy	--	View
TLS Port	5061	User Security Mode	Not Configured	▼
Additional UDP Ports		Enable Un-Authenticated Registrations	Not configured	▼
Additional UDP Ports Mode	Always Open	Max. Number of Registered Users	-1	
Encapsulating Protocol	No encapsulation			
Enable TCP Keepalive	Enable			
Used By Routing Server	Not Used			
Pre-Parsing Manipulation Set	--			View
CAC Profile	--			View

CLASSIFICATION	
Classification Failure Response Type	0
Pre-classification Manipulation Set ID	-1
Call Setup Rules Set ID	-1

Cancel [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.

SRD: #0 [DefaultSRD]

GENERAL

Index: 1

Name: ProxySet_OSBiz

Gateway IPv4 SIP Interface: -- View

SBC IPv4 SIP Interface: #0 [OSBiz_Trunk] View

TLS Context Name: #1 [MS Teams] View

REDUNDANCY

Redundancy Mode: [dropdown]

Proxy Hot Swap: Disable

Proxy Load Balancing Method: Disable

Min. Active Servers for Load Balancing: 1

KEEP ALIVE

Proxy Keep-Alive: Using OPTIONS

Proxy Keep-Alive Time [sec]: 60

Keep-Alive Failure Responses: [empty]

ADVANCED

Classification Input: IP Address only

DNS Resolve Method: [dropdown]

Cancel APPLY

Go to **SETUP >> SIGNALING & MEDIA >> CORE ENTITIES >> Proxy Sets** and click on **[New]** to setup the OpenScope 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]**.

GENERAL

Index: 0

Proxy Address: 10.8.242.92:5060

Transport Type: UDP

Proxy Priority: 0

Proxy Random Weight: 0

Cancel 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

The screenshot shows a 'Proxy Address' configuration window. The 'GENERAL' tab is active. The fields are as follows:

Field	Value
Index	2
Proxy Address	sip3.pstnhub.microsoft.com:5061
Transport Type	TLS
Proxy Priority	3
Proxy Random Weight	1

At the bottom of the window are 'Cancel' and 'APPLY' buttons.

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.

The screenshot shows the Audiocodes Management Console interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar shows the 'CODERS & PROFILES' section with 'Coder Groups' selected. The main content area displays the 'Coder Groups' configuration page. At the top, there is a 'Coder Group Name' dropdown menu set to '0 : AudioCodersGroups_0' and a 'Delete Group' button. Below this is a table with the following columns: Coder Name, Packetization Time, Rate, Payload Type, Silence Suppression, and Coder Specific. The table contains six rows of data:

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

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

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**:

Allowed Audio Coders Groups

GENERAL

Index: 0

Name: AllowedAudioCoders

Cancel APPLY

audiocodes SETUP MONITOR TROUBLESHOOT Save Reset Actions Admin

M8008 IP NETWORK SIGNALING & MEDIA ADMINISTRATION Entity, parameter, value

SRD All

TOPOLOGY VIEW

- CORE ENTITIES
- CODERS & PROFILES
 - IP Profiles (2)
 - Tel Profiles (0)
 - Coder Settings
 - Coder Groups
 - Allowed Audio Coders Groups (1)**
 - Allowed Video Coders Groups (0)
- SBC
- GATEWAY
- SIP DEFINITIONS
- MESSAGE MANIPULATION
- MEDIA
- INTRUSION DETECTION

Allowed Audio Coders Groups [#0] > Allowed Audio Coders (4)

+ New Edit

Page 1 of 1 Show 10 records per page

INDEX	CODER	USER-DEFINED CODER
0	G.711 A-law	
1	G.711 U-law	
2	G.722	
3	G.729	

#0 Edit

GENERAL

Coder: G.711 A-law

User-defined Coder

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.

The screenshot shows the 'IP Profiles' configuration window with the 'GENERAL' and 'SBC SIGNALING' tabs selected. The 'GENERAL' tab contains fields for 'Index' (2), 'Name' (OSBiz), and 'Created by Routing Server' (No). The 'SBC SIGNALING' tab contains various signaling parameters. Red boxes highlight the 'Name' field in the GENERAL tab and the 'P-Asserted-Identity Header Mode' field in the SBC SIGNALING tab.

GENERAL	SBC SIGNALING
Index: 2	PRACK Mode: Transparent
Name: OSBiz	P-Asserted-Identity Header Mode: As Is
Created by Routing Server: No	Diversion Header Mode: As Is
	History-Info Header Mode: As Is
	Session Expires Mode: Transparent
	SIP UPDATE Support: Supported
	Remote re-INVITE: Supported
	Remote Delayed Offer Support: Supported
	MSRP re-INVITE/UPDATE: Supported
	MSRP Offer Setup Role: ActPass
	MSRP Empty Message Format: Default
	Remote Representation Mode: According to Operation Mode

The screenshot shows the 'IP Profiles' configuration window with the 'SBC MEDIA' and 'SBC FORWARD AND TRANSFER' tabs selected. The 'SBC MEDIA' tab contains fields for 'Mediation Mode' (RTP Mediation), 'Extension Coders Group' (--), 'Allowed Audio Coders' (--), 'Allowed Coders Mode' (Restriction), 'Allowed Video Coders' (--), 'Allowed Media Types' (empty), 'Direct Media Tag' (empty), 'RFC 2833 Mode' (As Is), 'RFC 2833 DTMF Payload Type' (0), and 'Alternative DTMF Method' (As Is). The 'SBC FORWARD AND TRANSFER' tab contains fields for 'Remote REFER Mode' (Handle Locally), 'Remote Replaces Mode' (Handle Locally), 'Play RBT To Transferee' (No), 'Remote 3xx Mode' (Handle Locally), 'Remote Hold Format' (Transparent), 'Reliable Held Tone Source' (Yes), 'Play Held Tone' (No), and 'Fax Coders Group' (--). Red boxes highlight the 'Remote REFER Mode', 'Remote Replaces Mode', and 'Remote 3xx Mode' fields in the SBC FORWARD AND TRANSFER tab.

SBC MEDIA	SBC FORWARD AND TRANSFER
Mediation Mode: RTP Mediation	Remote REFER Mode: Handle Locally
Extension Coders Group: --	Remote Replaces Mode: Handle Locally
Allowed Audio Coders: --	Play RBT To Transferee: No
Allowed Coders Mode: Restriction	Remote 3xx Mode: Handle Locally
Allowed Video Coders: --	
Allowed Media Types:	
Direct Media Tag:	
RFC 2833 Mode: As Is	
RFC 2833 DTMF Payload Type: 0	
Alternative DTMF Method: As Is	

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

IP Profiles

GENERAL		SBC SIGNALING	
Index	1	PRACK Mode	Transparent
Name	MS Teams	P-Asserted-Identity Header Mode	As Is
Created by Routing Server	No	Diversion Header Mode	As Is
		History-Info Header Mode	As Is
		Session Expires Mode	Transparent
		SIP UPDATE Support	Not Supported
		Remote re-INVITE	Supported only with SDP
		Remote Delayed Offer Support	Not Supported
		MSRP re-INVITE/UPDATE	Supported
		MSRP Offer Setup Role	ActPass
		MSRP Empty Message Format	Default
		Remote Representation Mode	According to Operation Mode

MEDIA SECURITY	
SBC Media Security Mode	Secured
Gateway Media Security Mode	Preferable
Symmetric MKI	Disable
MKI Size	0
SBC Enforce MKI Size	Don't enforce
SBC Media Security Method	SDES
Reset SRTP Upon Re-key	Disable

Cancel **APPLY**

IP Profiles

SBC EARLY MEDIA		ISUP Body Handling	
Remote Early Media	Supported	ISUP Body Handling	Transparent
Remote Multiple 18x	Supported	ISUP Variant	Itu92
Remote Early Media Response Type	Transparent	Max Call Duration (min)	0
Remote Multiple Early Dialogs	According to Operation Mode		
Remote Multiple Answers Mode	Disable		
Remote Early Media RTP Detection Mode	By Media		
Remote RFC 3960 Support	Not Supported		
Remote Can Play Ringback	Yes		
Generate RTP	None		

SBC MEDIA		SBC REGISTRATION	
Mediation Mode	RTP Mediation	User Registration Time	0
Extension Coders Group	--	NAT UDP Registration Time	-1
		NAT TCP Registration Time	-1

SBC FORWARD AND TRANSFER	
Remote REFER Mode	Handle Locally
Remote Replaces Mode	Standard
Play RBT To Transferee	No
Remote 3xx Mode	Handle Locally

Cancel **APPLY**

IP Profiles

Generate RTP: None

SBC MEDIA

Mediation Mode: RTP Mediation

Extension Coders Group: --

Allowed Audio Coders: #0 [AllowedAudioCoders] [View](#)

Allowed Coders Mode: Preference

Allowed Video Coders: -- [View](#)

Allowed Media Types:

Direct Media Tag:

RFC 2833 Mode: As Is

RFC 2833 DTMF Payload Type: 0

Alternative DTMF Method: As Is

Send Multiple DTMF Methods: Disable

SBC FORWARD AND TRANSFER

Remote REFER Mode: Handle Locally

Remote Replaces Mode: Standard

Play RBT To Transferee: No

Remote 3xx Mode: Handle Locally

SBC HOLD

Remote Hold Format: Inactive

Reliable Held Tone Source: Yes

Play Held Tone: No

SBC FAX

Fax Coders Group: --

Fax Mode: As Is

[Cancel](#) [APPLY](#)

IP Profiles

Adapt RFC2833 BW to Voice coder BW: Disabled

SDP PTime Answer: Remote Answer

Preferred PTime: 0

Use Silence Suppression: Add

RTP Redundancy Mode: As Is

RTCP Mode: Generate Always

Jitter Compensation: Disable

ICE Mode: Lite

SDP Handle RTCP: Don't Care

RTCP Mux: Not Supported

RTCP Feedback: Feedback Off

Voice Quality Enhancement: Disable

Max Opus Bandwidth: 0

Generate No-Op Packets: Disable

Fax

Fax Offer Mode: All coders

Fax Answer Mode: Single coder

Remote Renegotiate on Fax Detection: Transparent

Fax Rerouting Mode: Disable

MEDIA

Broken Connection Mode: Disconnect

Media IP Version Preference: Only IPv4

RTP Redundancy Depth: Disable

GATEWAY

Early Media: Disable

Early 183: Disable

Early Answer Timeout [sec]: 0

[Cancel](#) [APPLY](#)

Navigate to **SETUP >> SIGNALING & MEDIA >> CODERS & PROFILES >> IP Profiles** and click 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.

The screenshot shows the 'IP Groups' configuration window. The 'GENERAL' tab is active. The 'Name' field is 'OSBiz'. The 'Type' is 'Server'. The 'Proxy Set' is '#1 [ProxySet_OSBiz]'. The 'IP Profile' is '#2 [OSBiz]'. The 'Media Realm' is '#0 [MR_LAN]'. The 'Internal Media Realm' is '--'. The 'Contact User' and 'SIP Group Name' fields are empty. The 'QUALITY OF EXPERIENCE' tab shows 'QoS Profile' as '--' and 'Bandwidth Profile' as '--'. The 'MESSAGE MANIPULATION' tab shows 'Inbound Message Manipulation Set' as '1' and 'Outbound Message Manipulation Set' as '2'. The 'Message Manipulation User-Defined String 1' and '2' fields are empty. The 'Proxy Keep-Alive using IP Group settings' is set to 'Disable'. The 'APPLY' button is highlighted in blue.

At **SETUP >> SIGNALING & MEDIA >> CORE ENTITIES >> IP Groups** click on **[New]**.
Configure an IP Group for OpenScope 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 OpenScope 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.

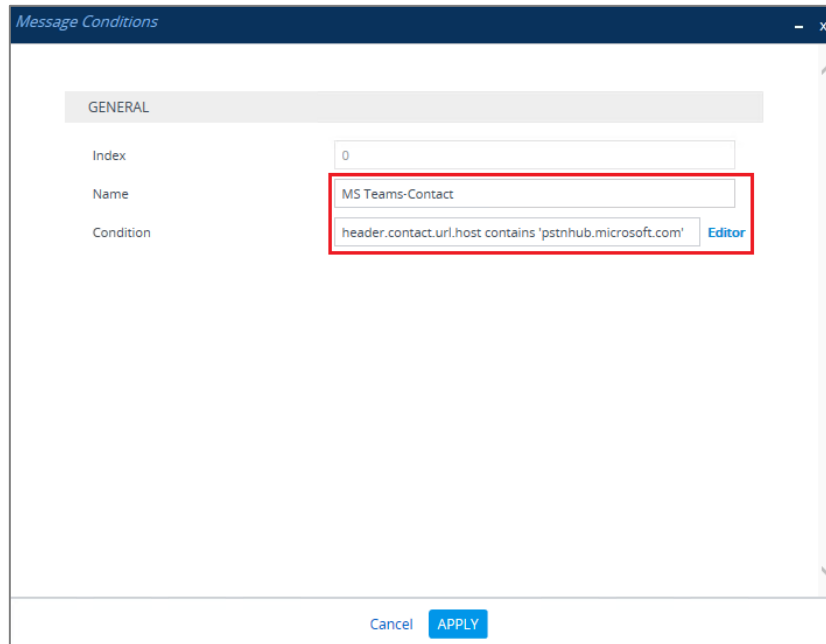
The screenshot shows the Audiocodes M800B configuration interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar shows a 'TOPOLOGY VIEW' with categories like 'CORE ENTITIES', 'CODERS & PROFILES', 'SBC', 'GATEWAY', 'SIP DEFINITIONS', 'MESSAGE MANIPULATION', 'MEDIA', and 'INTRUSION DETECTION'. The 'MEDIA' category is expanded, showing 'Media Security' as the selected option. The main panel displays the 'Media Security' configuration page. It has two tabs: 'GENERAL' and 'AUTHENTICATION & ENCRYPTION'. Under 'GENERAL', the 'Media Security' dropdown is set to 'Enable' (highlighted with a red box), 'Media Security Behavior' is 'Preferable', 'Offered SRTP Cipher Suites' is 'All', and 'ARIA Protocol Support' is 'Disable'. Under 'AUTHENTICATION & ENCRYPTION', 'Authentication on Transmitted RTP Packets' is 'Active', 'Encryption on Transmitted RTP Packets' is 'Active', 'Encryption on Transmitted RTCP Packets' is 'Active', 'SRTP Tunneling Authentication for RTP' is 'Disable', and 'SRTP Tunneling Authentication for RTCP' is 'Disable'. At the bottom, there is a 'MASTER KEY IDENTIFIER' section with 'Master Key Identifier (MKI) Size' set to '0' and 'Symmetric MKI' set to 'Disable'. The bottom right of the panel has 'Cancel' and 'APPLY' buttons.

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.

Classification

SRD #0 [DefaultSRD]

MATCH		ACTION	
Index	0	Action Type	Allow
Name	MS Teams	Destination Routing Policy	-- View
Source SIP Interface	#1 [MS Teams_Trunk] View	IP Group Selection	Source IP Group
Source IP Address	52.114.*.*	Source IP Group	#2 [MS Teams] View
Source Transport Type	Any	IP Group Tag Name	default
Source Port	0	IP Profile	-- View
Source Username Pattern	*		
Source Host	*		
Destination Username Pattern	*		
Destination Host	sbc01.athdrilabs.xyz		
Message Condition	#0 [MS Teams-Contact] View		

Cancel APPLY

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.athdrilabs.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;
```

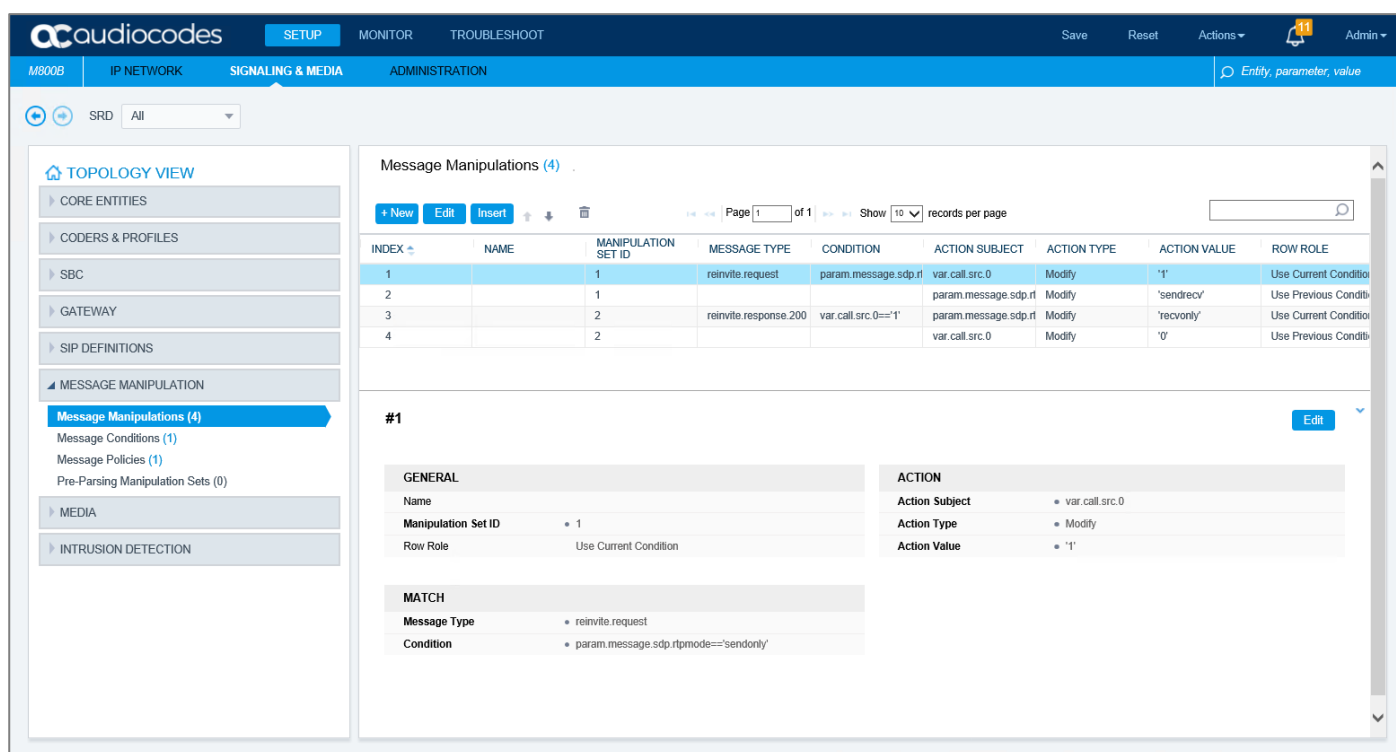
```
MessageManipulations 1 = "", 1, "reinvite.request",  
"param.message.sdp.rtpmode=='sendonly'", "var.call.src.0", 2, "'1'", 0;
```

```
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.

The screenshot shows the 'IP-to-IP Routing' configuration window. At the top, there's a 'Routing Policy' dropdown set to '#0 [Default_SBCRoutingPolicy]'. The window is split into two main sections: 'GENERAL' and 'ACTION'.
In the 'GENERAL' section:
- 'Index' is set to '0'.
- 'Name' is 'Terminate OPTIONS' (highlighted with a red box).
- 'Alternative Route Options' is set to 'Route Row'.
In the 'MATCH' section (under 'GENERAL'):
- 'Source IP Group' is 'Any' (highlighted with a red box).
- 'Request Type' is 'OPTIONS' (highlighted with a red box).
- 'Source Username Pattern' is '*'.
- 'Source Host' is '*'.
- 'Source Tag' is empty.
In the 'ACTION' section:
- 'Destination Type' is 'Dest Address' (highlighted with a red box).
- 'Destination IP Group' is '..'.
- 'Destination SIP Interface' is '..'.
- 'Destination Address' is 'internal' (highlighted with a red box).
- 'Destination Port' is '0'.
- 'Destination Transport Type' is empty.
- 'IP Group Set' is '..'.
- 'Call Setup Rules Set ID' is '-1'.
- 'Group Policy' is 'Sequential'.
- 'Cost Group' is '..'.
At the bottom, there are 'Cancel' and 'APPLY' buttons.

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]**.

IP-to-IP Routing

Routing Policy: #0 [Default_SBCRoutingPolicy]

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

Cancel APPLY

IP-to-IP Routing

Alternative Route Options: Route Row

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

Cancel APPLY

Open 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]**.

IP-to-IP Routing

Routing Policy: #0 [Default_SBCRoutingPolicy]

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

Cancel APPLY

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]**.

IP-to-IP Routing

Routing Policy: #0 [Default_SBCRoutingPolicy]

GENERAL	ACTION
Index: 3	Destination Type: IP Group
Name: OSBiz to MS Teams	Destination IP Group: #2 [MS Teams] View
Alternative Route Options: Route Row	Destination SIP Interface: -- View
MATCH	
Source IP Group: #1 [OSBiz] View	Destination Address:
Request Type: All	Destination Port: 0
Source Username Pattern: *	Destination Transport Type:
Source Host: *	IP Group Set: -- View
Source Tag:	Call Setup Rules Set ID: -1
	Group Policy: Sequential
	Cost Group: -- View

Cancel [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:

The screenshot displays the Audiocodes SBC configuration interface. The top navigation bar includes 'M800B', 'IP NETWORK', 'SIGNALING & MEDIA', and 'ADMINISTRATION'. The 'IP NETWORK' tab is active, showing a search bar with 'Entity, parameter, value' and a 'Save' button. The left sidebar contains a 'NETWORK VIEW' section with a 'SECURITY' tab selected, showing 'Firewall (8)' and 'Security Settings'. The main content area shows a table of Firewall rules with columns: INDEX, DESCRIPTION, ACTION UPON MATCH, and MATCH COUNT. Below the table, the details for rule #0 are shown, including MATCH criteria (Description, Source IP, Prefix Length, Start Port, End Port, Protocol, Use Specific Interface, Interface Name) and ACTION settings (Action Upon Match, Packet Size, Byte Rate, Byte Burst). A STATISTICS section shows the Match Count for rule #0.

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

#0

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

STATISTICS	
Match Count	317357

4. Anynode SBC

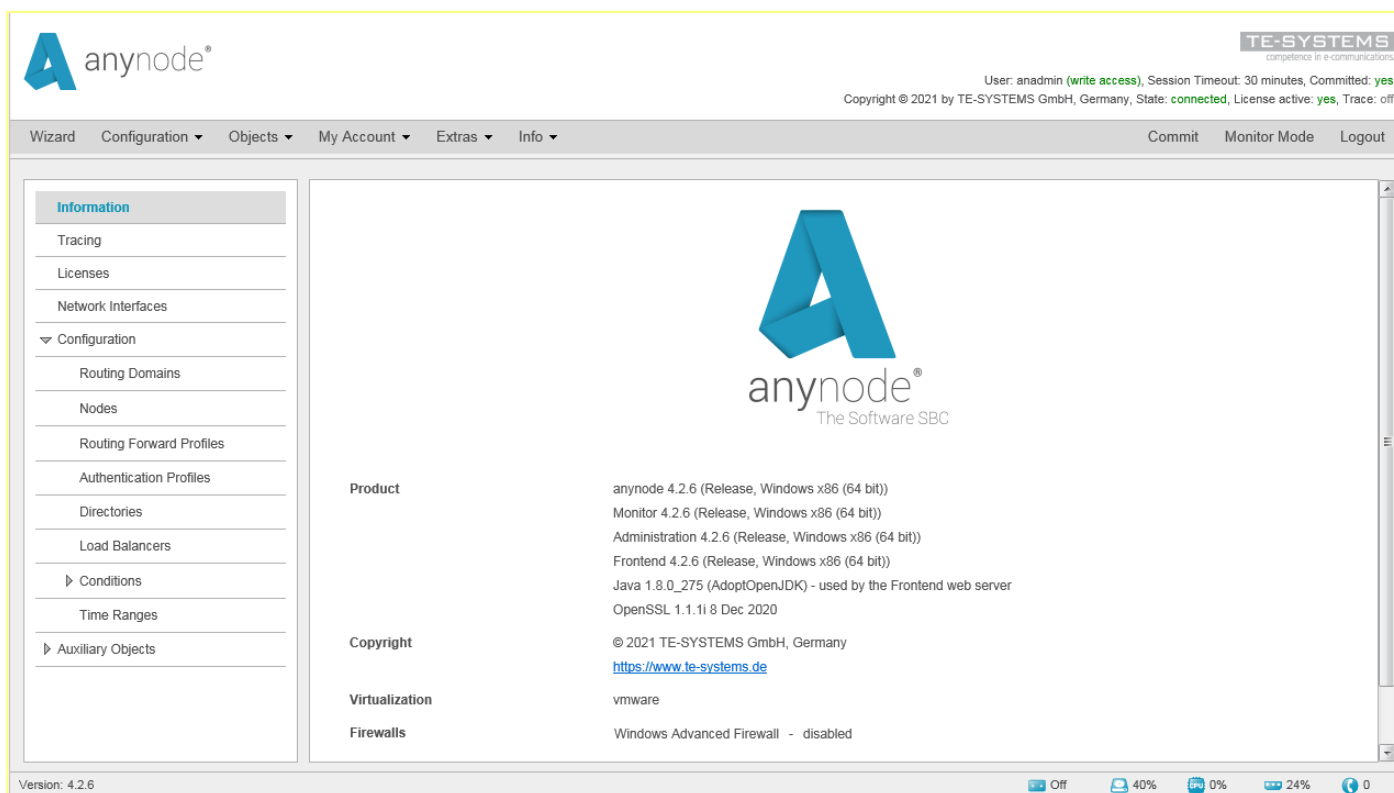
The configuration of anynode SBC for the testing activities needs is performed via "**anynode configuration wizard**". The following sub-sections demonstrate the example configuration utilized in current certification testing activities; default or non-project specific anynode configuration will not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

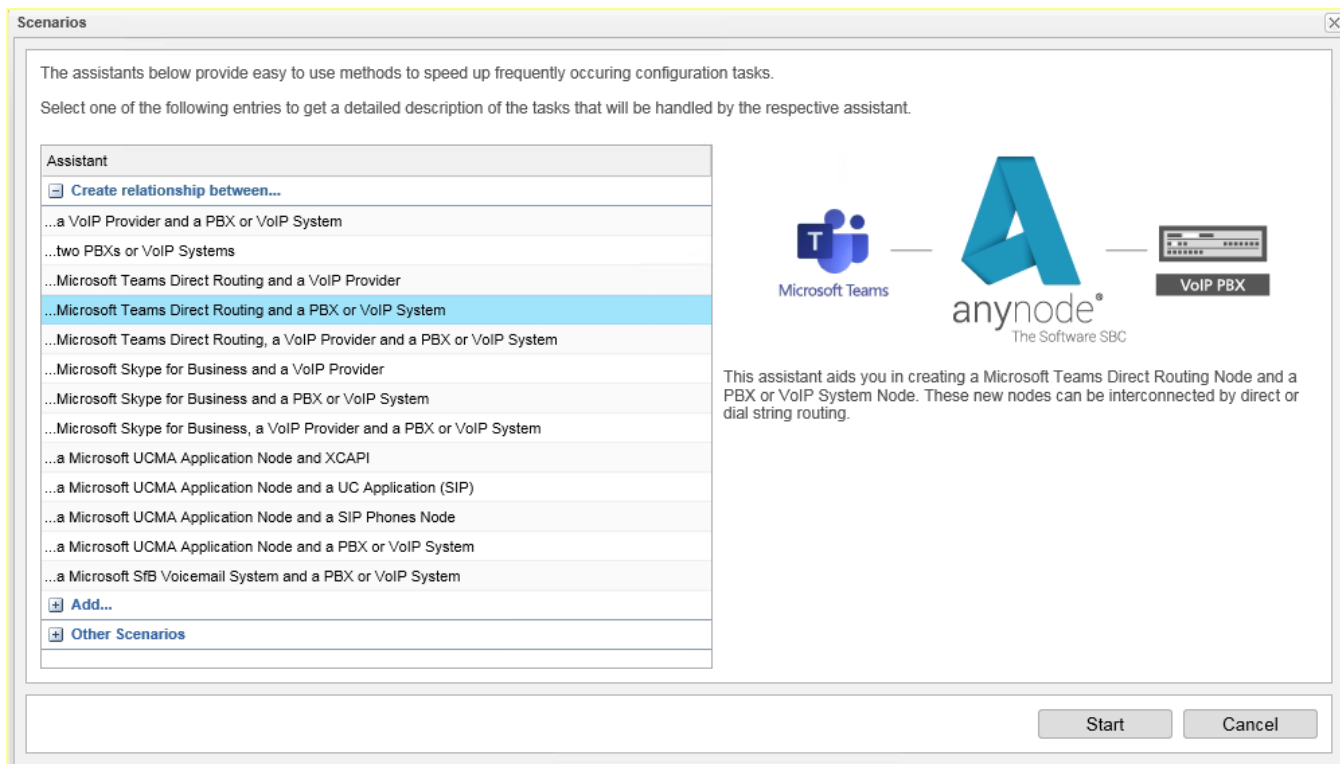
For more information regarding the anynode SBC configuration refer to anynode technote: <https://community.te-systems.de/community-download/files?fileId=2587>.

4.1. anynode Wizard – Teams / Voice over IP Provider

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

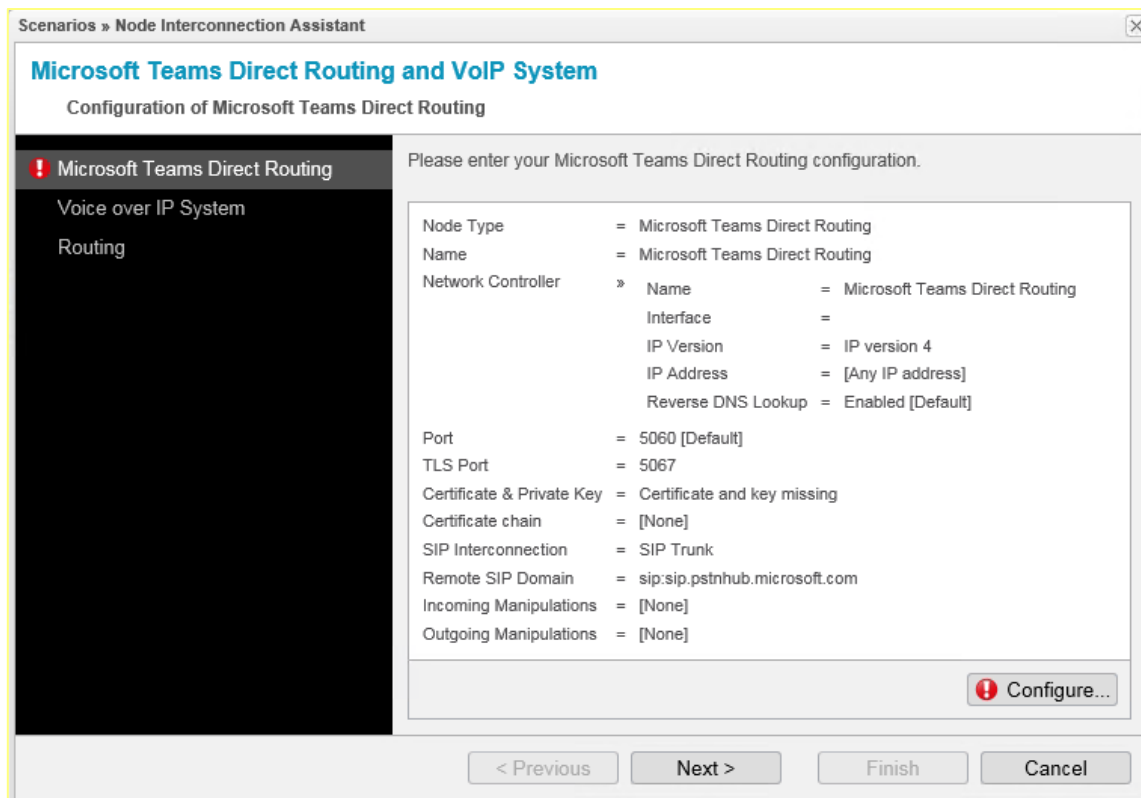


Click on "**Wizard**".



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.

Scenarios » Node Interconnection Assistant » Microsoft Teams Direct Routing

Create New Node

Choice of Microsoft Teams Node type.

☒ Microsoft Teams

Network Controller
 Ports
 Certificate & Private Key
 Certificate Chain
 SBC FQDN
 Name

☒ Microsoft Teams Direct Routing

This option is the default setup to create a Microsoft Teams Direct Routing connection. For most use-cases this is the right choice.

☐ Microsoft Teams Direct Routing Carrier Trunk

This option can be used to create an initial and successive connections to Microsoft Teams Direct Routing using the Carrier Trunk model. The first configuration sets up the connection for the initial tenant. Further tenants can be added by revisiting this option, which then will use the same connection that was configured during the initial setup.

All options below are only intended for use with specific multi-site Enterprise installations. These options implement the anynode-Nodes necessary for the new "Local Media Optimization" feature. It is only of use in scenarios where a single Enterprise Microsoft Teams Direct Routing connection is used from multiple geographically separate locations. In this case the media-flow can be optimized by the network/Teams/anynode-administrator to take the best path possible.

☐ Microsoft Teams Direct Routing (Local Media Optimization)

This option will setup a Microsoft Teams Direct Routing connection in case of "Local Media Optimization" usage. This is the Node that will connect towards the Microsoft Teams Direct Routing cloud service. Together with one or more "Microsoft Teams Direct Routing (Local Media Optimization) Site SBC" Nodes this forms the so-called proxy SBC.

☐ Microsoft Teams Direct Routing with Local Media Optimization Site SBC

This option creates a Node on the proxy SBC that will be used to interact with one remote site-SBCs. One of these Nodes must be configured on the central proxy SBC for each remote site to be connected.

☐ Microsoft Teams Direct Routing with Local Media Optimization Proxy SBC

This option creates the Node on the anynodes deployed in the various remote sites which then will connect to the central proxy SBC.

< Previous Next > Finish Cancel

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.

Scenarios » Node Interconnection Assistant » Microsoft Teams Direct Routing

Create New Node

Network Controller selection.

You may restrict the operation of a node to a specific network controller. The restriction may consist of a specific network interface and/or IP address to be used for SIP and media transport of this node.

Network Controller

☒ Create new network controller.

Name

Microsoft Teams Direct Routing

Network

☐ Use a fixed IP address ?

☒ Use an interface's address ?

Intel(R) 82574L Gigabit Network Connection #3 IP version 4

Currently: 195.97.14.76

☐ Advanced configuration ?

Open...

☐ Specify whether reverse DNS lookup is enabled

☒ Enabled ☐ Disabled

☐ Select existing network controller.

[None]

< Previous Next > Finish Cancel

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.

Scenarios » Node Interconnection Assistant » Microsoft Teams Direct Routing

Create New Node

Assignment of local ports.

- ✓ Microsoft Teams
- ✓ Network Controller
- ✓ Ports
- Certificate & Private Key
- Certificate Chain
- SBC FQDN
- Name

The new node will use the following local ports. The remote endpoint must be configured accordingly.

☒ Specify the TLS Port

Dynamic UDP/TCP Ports

☐ Unrestricted UDP port range

☒ Restrict UDP port range to -
Sufficient for approximately 1000 sessions.

☐ Unrestricted TCP port range

☒ Restrict TCP port range to -
Sufficient for approximately 1000 sessions.

< Previous Next > Finish Cancel

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.

The screenshot shows a window titled "Scenarios » Node Interconnection Assistant » Microsoft Teams Direct Routing". Inside, the "Create New Node" section is active, with the subtitle "Determination of the certificate and private key.".

On the left, a sidebar lists configuration steps: "Microsoft Teams" (checked), "Network Controller" (checked), "Ports" (checked), "Certificate & Private Key" (highlighted with a red exclamation mark), "Certificate Chain", "SBC FQDN", and "Name".

The main area shows two radio button options:

- ☒ **Provide a certificate and an associated private key.**
With these two values anynode can authenticate and open a secure channel to a peer later. Therefore, it is important that the peer will accept the offered certificate.
- ☐ I do not want to provide a certificate and an associated private key yet.

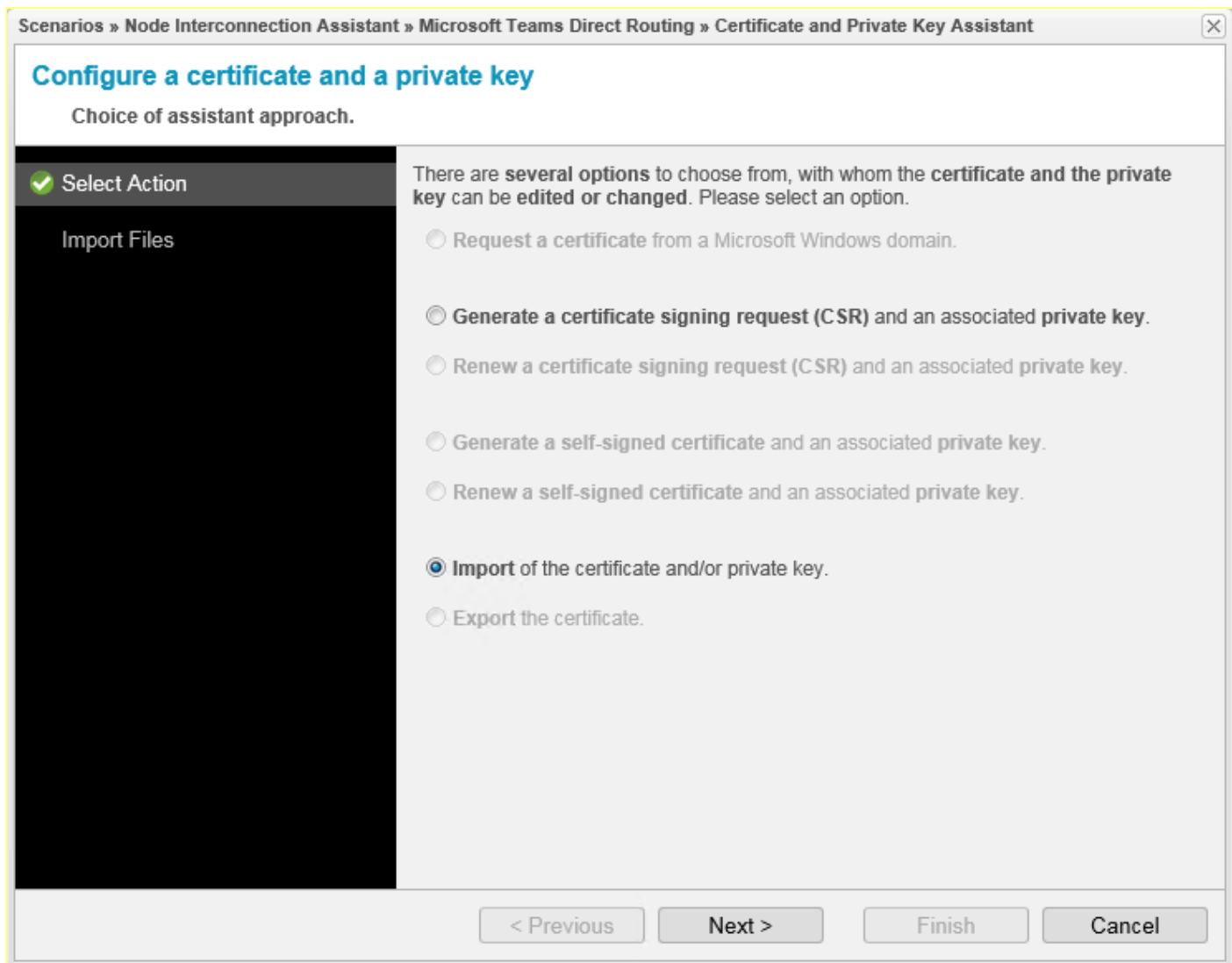
Below the first option, there are two text input fields:

- Private Key:** Contains the text "No private key present."
- Certificate:** Contains the text "No certificate present."

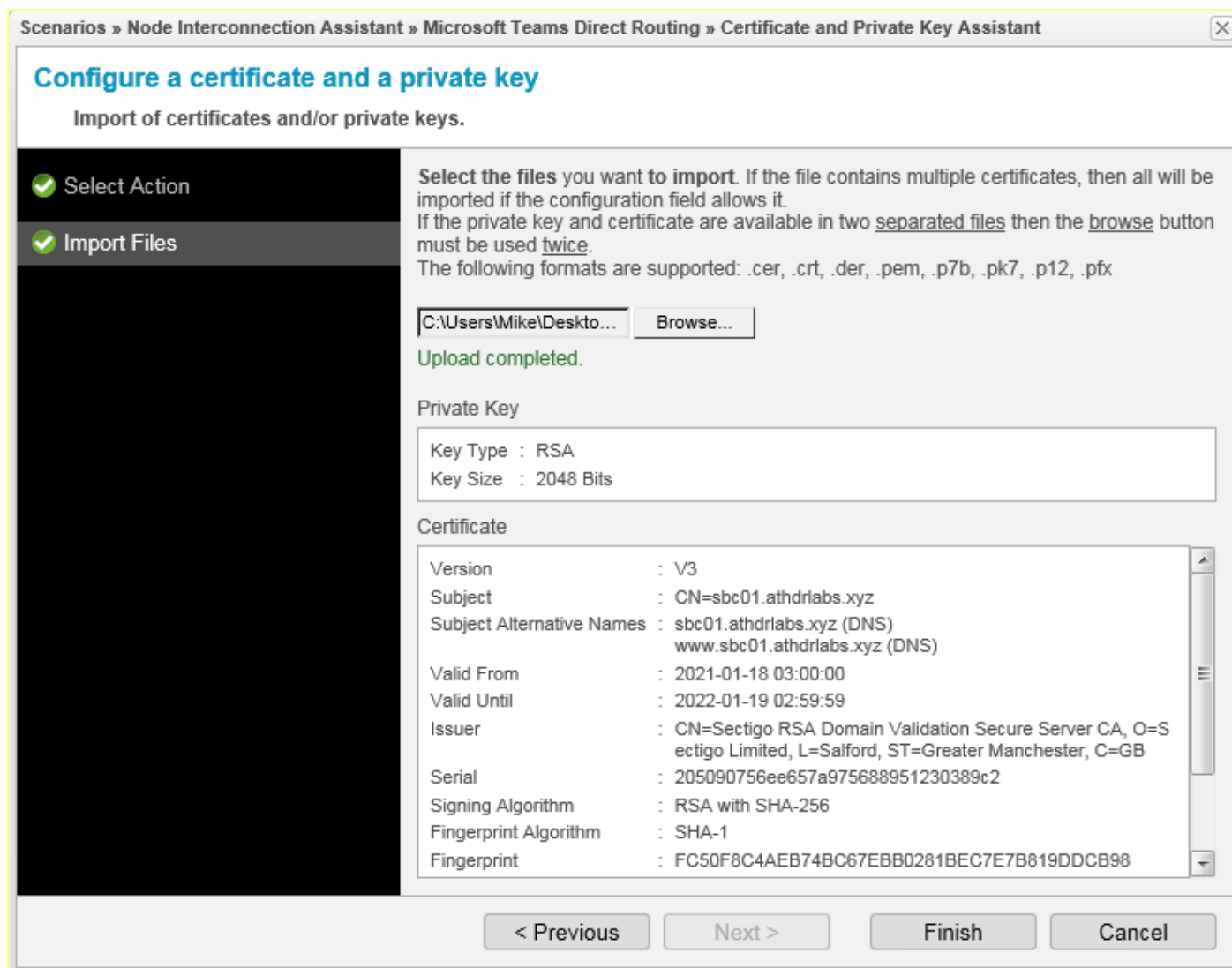
At the bottom right of these fields are two buttons: "Configure..." and "Remove".

At the bottom of the dialog are four navigation buttons: "< Previous", "Next >", "Finish", and "Cancel".

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**". 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]**.

Scenarios » Node Interconnection Assistant » Microsoft Teams Direct Routing

Create New Node

Determination of the certificate and private key.

☒ Microsoft Teams
☒ Network Controller
☒ Ports
☒ Certificate & Private Key
 Certificate Chain
 SBC FQDN
 Name

☒ Provide a certificate and an associated private key.

With these two values anynode can authenticate and open a secure channel to a peer later. Therefore, it is important that the peer will accept the offered certificate.

Private Key

Key Type : RSA
Key Size : 2048 Bits

Certificate

Version : V3
 Subject : CN=sbc01.athdrilabs.xyz
 Subject Alternative Names : sbc01.athdrilabs.xyz (DNS)
 www.sbc01.athdrilabs.xyz (DNS)
 Valid From : 2021-01-18 03:00:00
 Valid Until : 2022-01-19 02:59:59
 Issuer : CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=S alford, ST=Greater Manchester, C=GB
 Serial : 205090756ee657a975688951230389c2
 Signing Algorithm : RSA with SHA-256
 Fingerprint Algorithm : SHA-1
 Fingerprint : FC50F8C4AEB74BC67EBB0281BEC7E7B819DDCB98
 Usage : Verification of digital signatures.
 Enciphering private or secret keys.
 Extended Usage : Server authentication
 Client authentication
 Certificate Authority : no

☐ I do not want to provide a certificate and an associated private key yet.

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.

The screenshot shows a window titled "Scenarios » Node Interconnection Assistant » Microsoft Teams Direct Routing". The main heading is "Create New Node". Below it, the subtitle is "Determination of an optional certificate chain.".

On the left, there is a list of steps with checkboxes:

- ✓ Microsoft Teams
- ✓ Network Controller
- ✓ Ports
- ✓ Certificate & Private Key
- ✓ Certificate Chain

Below the list, there are two input fields: "SBC FQDN" and "Name".

On the right, there is a text box that says: "If a certificate chain is needed in addition to the single certificate, then these certificates can be added to the following list."

Below this text is a table titled "Certificate chain":

Certificate Issuer	Certificate Subject	Valid From	Valid Until
CN=USERTrust RSA Certification Au...	CN=Sectigo RSA Domain Validation...	2018-11-02 03:00	2031-01-01 02:59

At the bottom of the dialog, there are four buttons: "Request Chain", "Add...", "Edit...", and "Remove".

At the very bottom, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

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.

Scenarios » Node Interconnection Assistant » Microsoft Teams Direct Routing

Create New Node

Determination of the FQDN of the SBC.

- ✓ Microsoft Teams
- ✓ Network Controller
- ✓ Ports
- ✓ Certificate & Private Key
- ✓ Certificate Chain
- ✓ SBC FQDN

Name

Determine the name for the FQDN of the SBC.

SBC FQDN (for example sbc1.te-systems.com)

sbc01.athdriabs.xyz

< Previous Next > Finish Cancel

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

Scenarios » Node Interconnection Assistant » Microsoft Teams Direct Routing

Create New Node

Determination of node name.

- ✓ Microsoft Teams
- ✓ Network Controller
- ✓ Ports
- ✓ Certificate & Private Key
- ✓ Certificate Chain
- ✓ SBC FQDN
- ✓ **Name**

Enter a meaningful name for your new node. The name is arbitrary. You will use it to uniquely identify this node later during configuration.

Name

Microsoft Teams Direct Routing

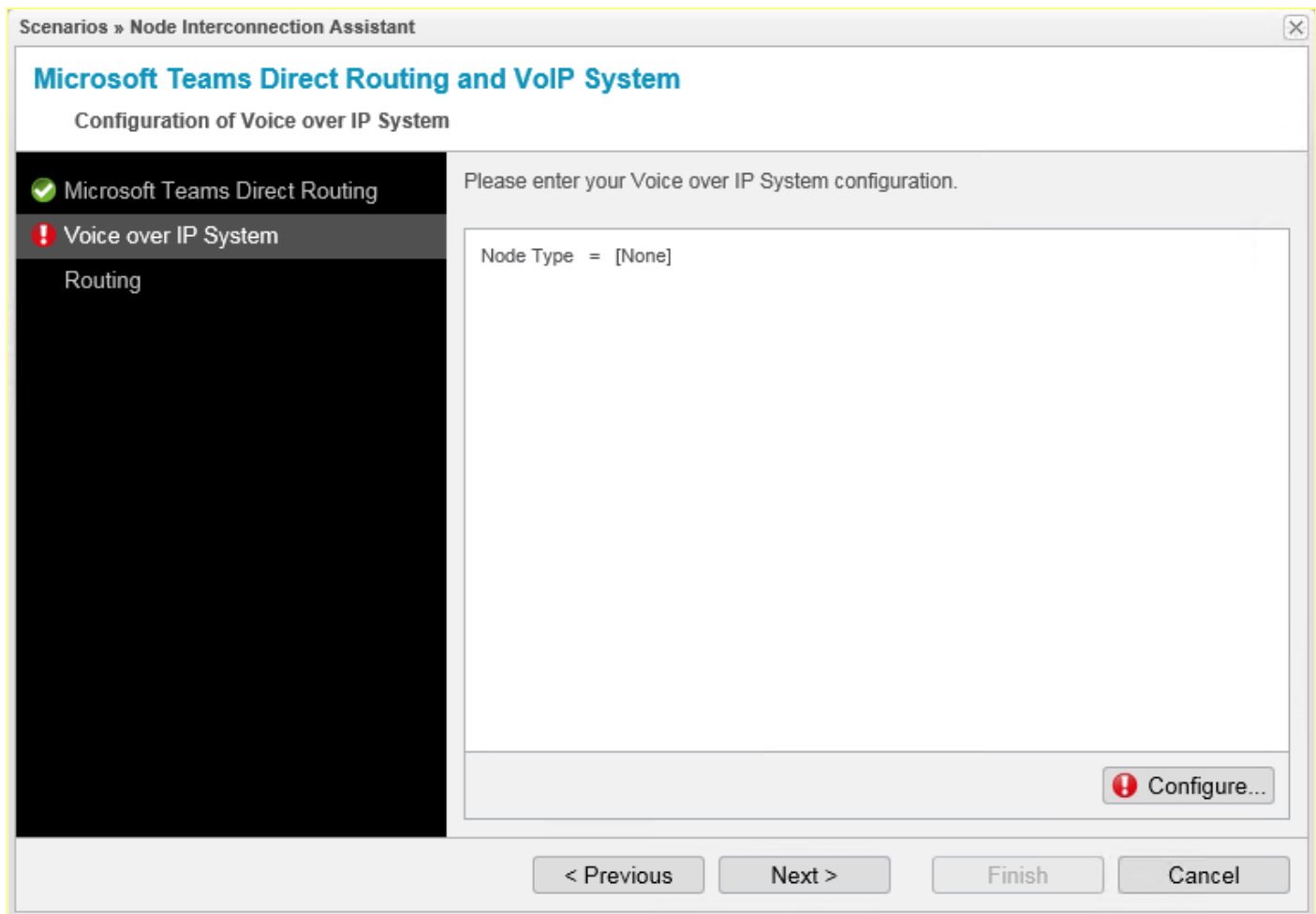
< Previous Next > Finish Cancel

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

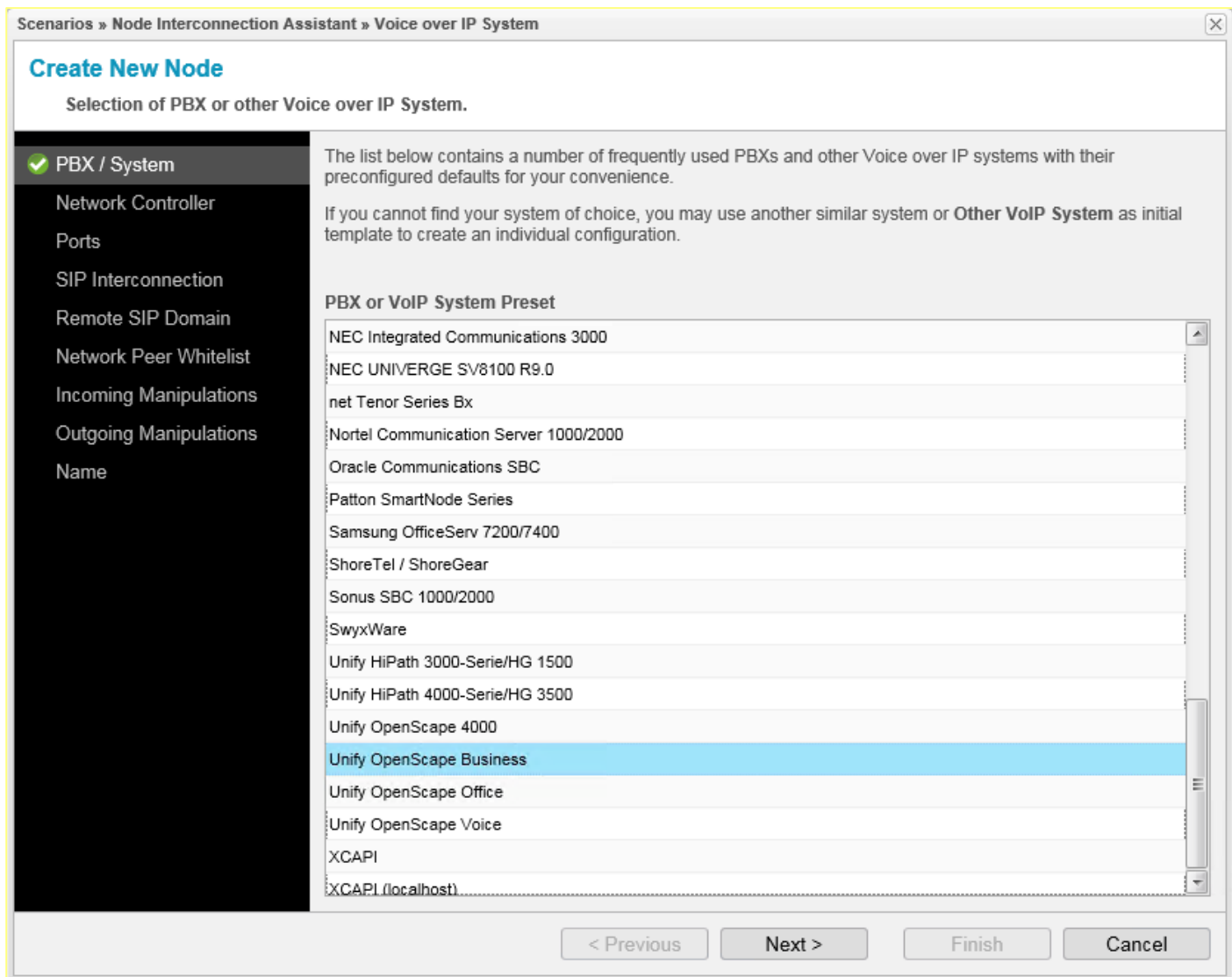
Click on **[Finish]**.

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

Scenarios » Node Interconnection Assistant » Voice over IP System

Create New Node

Network Controller selection.

- ✓ PBX / System
- ✓ Network Controller
- Ports
- SIP Interconnection
- Remote SIP Domain
- Network Peer Whitelist
- Incoming Manipulations
- Outgoing Manipulations
- Name

You may restrict the operation of a node to a specific network controller. The restriction may consist of a specific network interface and/or IP address to be used for SIP and media transport of this node.

Network Controller

☒ Create new network controller.

Name

Unify OpenScape Business

Network

☐ Use a fixed IP address ?

☒ Use an interface's address ?

vmxnet3 Ethernet Adapter #2 IP version 4

Currently: 10.8.242.78

☐ Advanced configuration ?

Open...

☒ Specify whether reverse DNS lookup is enabled

☒ Enabled ☐ Disabled

☐ Select existing network controller.

[None]

< Previous Next > Finish Cancel

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.

Scenarios » Node Interconnection Assistant » Voice over IP System

Create New Node

Assignment of local ports.

- ✓ PBX / System
- ✓ Network Controller
- ✓ Ports
- SIP Interconnection
- Remote SIP Domain
- Network Peer Whitelist
- Incoming Manipulations
- Outgoing Manipulations
- Name

The new node will use the following local ports. The remote endpoint must be configured accordingly.

☒ Specify the UDP/TCP Port ☐ Specify the TLS Port

Dynamic UDP/TCP Ports

☐ Unrestricted UDP port range

☒ Restrict UDP port range to -
Sufficient for approximately 1000 sessions.

☐ Unrestricted TCP port range

☒ Restrict TCP port range to -
Sufficient for approximately 1000 sessions.

< Previous Next > Finish Cancel

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

Scenarios » Node Interconnection Assistant » Voice over IP System

Create New Node

Choice of SIP interconnection type.

It can be determined how a SIP interconnection is realized to a remote station. This also determines which side must authenticate.

SIP Interconnection

- ☒ **Node Interconnection via SIP Trunking**
The node uses SIP trunking to interconnect with the remote station. In this way, full dial string ranges can be linked at once.
- ☐ **Node as SIP Registration Client**
The node registers at a remote station as a client. In this case the remote station has to provide a registrar.
- ☐ **Node as SIP Registrar**
The node provides a registration server (registrar) at which the remote station must register.

< Previous **Next >** Finish Cancel

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.

Scenarios » Node Interconnection Assistant » Voice over IP System

Create New Node

Determination of remote SIP domain.

Please choose the remote SIP URI which will be used in SIP URIs of outgoing calls and which describes where the remote endpoint can be reached.

Remote SIP Domain

☐ Use URI representation

☒ Use separated representation

Host

10.8.242.92

Transport

UDP

Port

☒ Unset ☐ Set to

< Previous Next > Finish Cancel

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.

Scenarios » Node Interconnection Assistant » Voice over IP System

Create New Node

Definition of an IP or hostname whitelist.

- ✓ PBX / System
- ✓ Network Controller
- ✓ Ports
- ✓ SIP Interconnection
- ✓ Remote SIP Domain
- ✓ Network Peer Whitelist**
- Incoming Manipulations
- Outgoing Manipulations
- Name

If the interconnection to the VoIP peer takes place over a public IP access, it is strictly recommended to minimize the IP addresses from which SIP messages are allowed by this whitelist.

☒ Use the network peer whitelist

☒ Include Remote SIP Domain: 10.8.242.92

Hostname	Interpret as	Resolved IP Addr...
----------	--------------	---------------------

☒ Allow only negotiated peers for RTP/RTCP

☐ Do not use the network peer whitelist. It is already ensured by a separate router or a firewall that only SIP messages of the selected provider are able to access the anynode.

< Previous **Next >** Finish Cancel

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.

Scenarios » Node Interconnection Assistant » Voice over IP System

Create New Node

Optional conversion of incoming dial strings.

- ✓ PBX / System
- ✓ Network Controller
- ✓ Ports
- ✓ SIP Interconnection
- ✓ Remote SIP Domain
- ✓ Network Peer Whitelist
- ✓ Incoming Manipulations
- Outgoing Manipulations
- Name

It is recommended to convert incoming calling numbers into the E.164 number space. Various manipulations are available to achieve this.

If the node's remote endpoint has its own number space then simply add one or more manipulations and describe the type of desired conversion.

Incoming Manipulations

Filter: **Optional** X

Condition	Action
-----------	--------

Up Down Import... Add... Clone Edit... Remove

< Previous Next > Finish Cancel

Scenarios » Node Interconnection Assistant » Voice over IP System

Create New Node

Optional conversion of outgoing dial strings.

- ✓ PBX / System
- ✓ Network Controller
- ✓ Ports
- ✓ SIP Interconnection
- ✓ Remote SIP Domain
- ✓ Network Peer Whitelist
- ✓ Incoming Manipulations
- ✓ **Outgoing Manipulations**

Outgoing manipulations can be used if it is necessary to reconvert a calling number from E.164 number space to another destination number space.

If desired add a manipulation and describe the type of conversion.

Outgoing Manipulations

Filter: **Optional** X

Condition	Action

Up Down Import... Add... Clone Edit... Remove

< Previous **Next >** Finish Cancel

Click on **[Next]**.

4.15. anynode Wizard – OSBiz / Name

The screenshot shows a window titled "Scenarios » Node Interconnection Assistant » Voice over IP System". Inside, the "Create New Node" section is active, with the subtitle "Determination of node name.".

On the left, a list of configuration steps is shown with green checkmarks:

- ✓ PBX / System
- ✓ Network Controller
- ✓ Ports
- ✓ SIP Interconnection
- ✓ Remote SIP Domain
- ✓ Network Peer Whitelist
- ✓ Incoming Manipulations
- ✓ Outgoing Manipulations
- ✓ Name** (highlighted)

The main area contains the instruction: "Enter a meaningful name for your new node. The name is arbitrary. You will use it to uniquely identify this node later during configuration." Below this, a text box labeled "Name" contains the text "Unify OpenScape Business".

At the bottom, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

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

Click on **[Finish]**.

Scenarios » Node Interconnection Assistant

Microsoft Teams Direct Routing and VoIP System

Configuration of Voice over IP System

Microsoft Teams Direct Routing

Voice over IP System

Routing

Please enter your Voice over IP System configuration.

Node Type	=	Unify OpenScape Business
Name	=	Unify OpenScape Business
Network Controller	»	<div> Name = Unify OpenScape Business </div> <div> Interface = vmxnet3 Ethernet Adapter #2 </div> <div> IP Version = IP version 4 </div> <div> IP Address = [Any IP address] </div> <div> Reverse DNS Lookup = Enabled [Default] </div>
Port	=	5060
TLS Port	=	5061 [Default]
SIP Interconnection	=	SIP Trunk
Remote SIP Domain	=	sip:10.8.242.92;transport=udp
Incoming Manipulations	=	[None]
Outgoing Manipulations	=	[None]

Configure...

< Previous

Next >

Finish

Cancel

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

4.16. anynode Wizard – Routing

The screenshot shows a window titled "Scenarios » Node Interconnection Assistant" with a close button in the top right corner. The main heading is "Microsoft Teams Direct Routing and VoIP System". Below the heading is the text "Determination of routing type.".

On the left side, there is a list of three options, each preceded by a green checkmark:

- Microsoft Teams Direct Routing
- Voice over IP System
- Routing**

The "Routing" option is highlighted with a dark background. To the right of this list, there is a text area with the following content:

Please determine if calls should be routed directly from node to node or whether dial string filters should be applied.

Below this text are two radio button options:

- ☒ Use direct routing without prefix filter
When selecting direct routing, **all possible destination URIs are forwarded to the other node without restrictions.**
- ☐ Use dial string routing

At the bottom of the window, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

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:

The screenshot displays the anynode web interface. The top navigation bar includes the anynode logo, user information (User: anadmin, Session Timeout: 30 minutes, Committed: yes), and copyright information (Copyright © 2021 by TE-SYSTEMS GmbH, Germany, State: connected, License active: yes, Trace: off). The main menu on the left lists various configuration options, with 'Routing Domains' selected under the 'Configuration' section. The main content area shows the 'Routing Domain' configuration page. It includes a 'Source Nodes' section with a table listing 'Microsoft Teams Direct Routing' and 'Unify OpenScape Business'. Below this is a 'Routes' section with a table showing routes for 'To Microsoft Teams Direct Routing' and 'To Unify OpenScape Business'. The interface also features a sidebar with navigation links, a top bar with user and system status, and a bottom status bar showing version 4.2.6 and various system metrics.

anynode®

TE-SYSTEMS
competence in e-communications

User: anadmin (write access), Session Timeout: 30 minutes, Committed: yes
Copyright © 2021 by TE-SYSTEMS GmbH, Germany, State: connected, License active: yes, Trace: off

Wizard Configuration Objects My Account Extras Info

Add Routing Domain Remove Routing Domain... Clone Routing Domain... Export Routing Domain...

Information
Tracing
Licenses
Network Interfaces
Configuration
Routing Domains
Nodes
Routing Forward Profiles
Authentication Profiles
Directories
Load Balancers
Conditions
Time Ranges
Auxiliary Objects

Object

Source Nodes

This routing domain listens on the following source nodes for incoming calls.

Name
<input checked="" type="checkbox"/> Microsoft Teams Direct Routing
<input checked="" type="checkbox"/> Unify OpenScape Business

Select All Deselect All

Routes

Filter Optional

Filters	Establishment
To Microsoft Teams Direct Routing	
Source Nodes = Unify OpenScape Business	Route Call = Microsoft Teams Direct Routing
	Destination Node = Microsoft Teams Direct Routing
	Routing Forward Profile = To Microsoft Teams Direct Routing
To Unify OpenScape Business	
Source Nodes = Microsoft Teams Direct Routing	Route Call = Unify OpenScape Business
	Destination Node = Unify OpenScape Business
	Routing Forward Profile = To Unify OpenScape Business

Up Down Enable Add... Clone Edit... Remove

Version: 4.2.6

Off 40% 2% 22% 0

4.17. anynode SBC – Additional Configuration

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

The screenshot displays the anynode SBC configuration interface. The top navigation bar includes 'Wizard', 'Configuration', 'Objects', 'My Account', 'Extras', and 'Info'. The left sidebar shows a tree view with 'Configuration' expanded, leading to 'Nodes', and then 'Microsoft Teams Direct Ro...'. The main content area is titled 'Node' and 'Microsoft Teams Direct Routing'. It features a 'Tones and Announcements' section with a checkbox 'Enable tones and announcements' checked. Below this, a 'Profile' dropdown is set to 'Custom'. A table lists various tones with their current settings and edit/delete icons:

Tone Type	Current Setting	Edit	Delete
Ringback tone	Belgium - Ringback tone	+	-
Active tone	[None]	+	-
Music on hold	[None]	+	-
Session successfully terminated tone	[None]	+	-
Error indicator tone	[None]	+	-

The bottom status bar shows system metrics: Version: 4.2.6, CPU 40%, GPU 3%, and other indicators.

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.

anynode®

TE-SYSTEMS
competence in e-communications

User: anadmin (write access), Session Timeout: 23 minutes, Committed: y
Copyright © 2021 by TE-SYSTEMS GmbH, Germany, State: cor, License active: y, Trace: of

Wizard Configuration Objects My Account Extras Info

Add Node... Remove Node... Clone Node... Export Node...

Information
Tracing
Licenses
Network Interfaces

▼ Configuration

► Routing Domains

▼ Nodes

Microsoft Teams Direct R...

Unify OpenScape Business

► Routing Forward Profiles

Authentication Profiles

Directories

Load Balancers

► Conditions

Time Ranges

► Auxiliary Objects

▼ SIP Response Code Mapp

Use as a basis for the SIP Response code mapping the following profile

Standard

Incoming SIP Response Code Mapping

SIP Response Code	Telephony Status	User-defined or Default
301 (Moved permanently)	Redirected	Default
302 (Moved temporarily)	Redirected	Default
403 (Forbidden)	No permission	Default
404 (Not found)	Erroneous dial string	Default
406 (Not acceptable)	Media negotiation error	Default
408 (Request timeout)	Domain Specific 0	User-defined
480 (Temporarily not available)	Not responding	Default
486 (Busy here)	Busy	Default
487 (Request terminated)	Terminated	Default
488 (Not acceptable here)	Media negotiation error	Default
500 (Internal server error)	Equipment error	Default
503 (Service unavailable)	Congestion	Default
600 (Busy everywhere)	Busy	Default
603 (Decline)	Rejected	User-defined
606 (Not acceptable)	Media negotiation error	Default

Add... Edit... Set to Default Remove

Outgoing SIP Response Code Mapping

Telephony Status	SIP Response Code	User-defined or Default
Erroneous dial string	404 (Not found)	Default
No permission	403 (Forbidden)	Default
Congestion	503 (Service unavailable)	Default
Equipment error	500 (Internal server error)	Default
Busy	486 (Busy here)	Default
Redirected	302 (Moved temporarily)	Default
Not responding	480 (Temporarily not available)	Default
Not selected	486 (Busy here)	Default
Rejected	603 (Decline)	User-defined (Overridden Defa...
Terminated	487 (Request terminated)	Default
Media negotiation error	488 (Not acceptable here)	Default
Domain Specific 0	408 (Request timeout)	User-defined

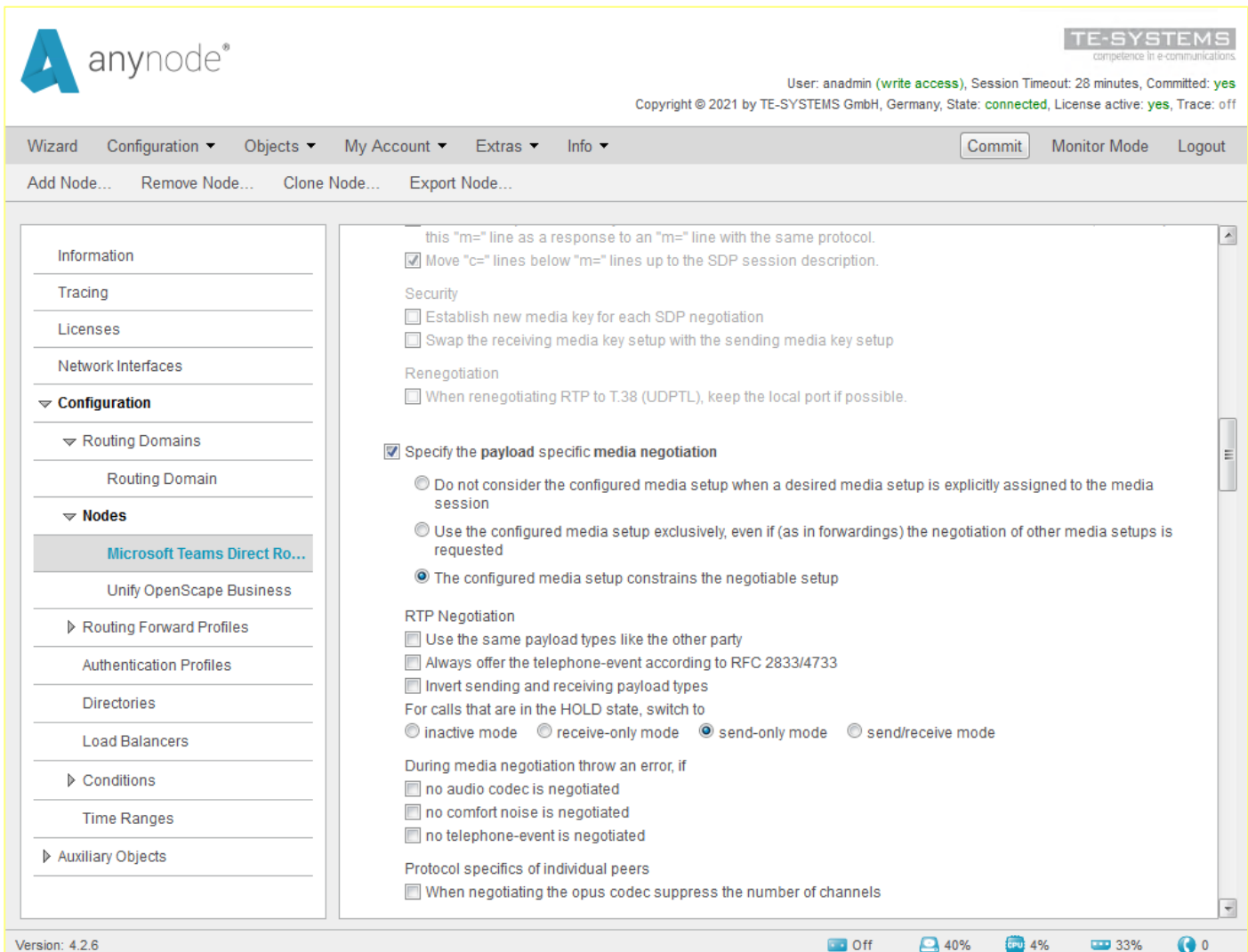
Add... Edit... Set to Default Remove

Version 4.2.6

Off 40% 0% 33% 0

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.



The screenshot shows the anynode® web interface. The left sidebar contains a navigation menu with sections like Information, Tracing, Licenses, Network Interfaces, Configuration, Routing Domains, Nodes, and Auxiliary Objects. The 'Nodes' section is expanded, showing 'Microsoft Teams Direct Ro...' as the selected node. The main content area displays the configuration for this node, including sections for Security, Renegotiation, and RTP Negotiation. The 'Specify the payload specific media negotiation' checkbox is checked. Under 'RTP Negotiation', the 'send-only mode' radio button is selected. The bottom status bar shows system information like Version: 4.2.6 and resource usage (CPU 4%, GPU 4%, etc.).

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:

The screenshot displays the anynode® web interface for configuring Media Transcoding Options. The interface includes a sidebar with navigation options and a main content area with a breadcrumb trail and a flow diagram. The configuration section is titled 'Media Transcoding Options' and includes settings for 'Flow settings for the direction from the calling to the called entity', 'Silence Processing Settings', and 'Comfort noise volume level'.

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**.

dB Full Scale

Information

Tracing

Licenses

Network Interfaces

▼ Configuration

▸ Routing Domains

▸ Nodes

▼ Routing Forward Profiles

To Microsoft Teams Direct ...

To Unify OpenScope Business

Authentication Profiles

Directories

Load Balancers

▸ Conditions

Time Ranges

▸ Auxiliary Objects

/ To Microsoft Teams Direct Routing / 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**.

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

The screenshot displays the 'Setup - Wizards - Basic Installation - Basic Installation' window. The wizard progress bar at the top shows steps 1 through 8, with step 4, 'Select a station', currently active. Below the progress bar, a note states: 'Note: changes done in expert mode must be reviewed/repeated after running through the wizard.' Another note mentions: 'Note: At least the configuration of the 'Country code' is needed for features such as 'Internet telephony' and 'MeetMe conference'. If you want your OpenScape Business in "OpenScape Business Network Integration" you should select the "Network Integration" check box and enter a node ID. In this case, make sure that this node ID is unique within the whole network integration. Normally, this integration is done by a Service Technician. For a standalone OpenScape Business clear the 'Network Integration' check box.'

The configuration fields are as follows:

- PABX number**
 - Country code: 00 49 (mandatory)
 - Local area code: 0 89 (optional)
 - PABX number: 72172 (optional)
- General**
 - International Prefix: 00
- Network Parameters**
 - Network Integration: ☐
 - Node ID: 0
- Upstream of your internet connection**
 - Upstream up to (Kbps): 256

At the bottom of the window, there are buttons for 'Help', 'Abort', 'Back', and 'OK & Next'.

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 OpenScope Business **Networking** license.

Expert mode - Telephony Server

Voice Gateway

- SIP Parameters
- ITSP Loc-ID Settings
- Codec Parameters
- Destination Codec Parameters
- Internet Telephony Service Provider
- Networking
- SIPQ-Interconnection
- Native SIP Server Trunk**

Native SIP Server Trunk

Add Native SIP Server Trunk

Base Template: Native SIP trunk - predefined

Trunk Name: Teams

Enable Trunk: ☒

Trunk Identifier in System: ITSP/NS 1

Remote Domain Name: 10.8.242.78

Transport protocol: udp

SIP Server

IP Address / Host name: 10.8.242.78

Port: 5060

SIP Registrar

Use Registrar: ☐

IP Address / Host name:

Port: 5060

Reregistration interval (sec): 300

STUN Server

Use STUN: ☐

IP Address / Host name:

Port: 3478

Extended SIP Data

Show Extended SIP Data: ☒

Attention: the following parameters are used to adapt the behavior of the SIP stack to a certain trunk implementation. Wrong parameter settings may result in a malfunction of the trunk interface.

Apply Undo Refresh Help

Expert mode - Telephony Server

Voice Gateway

- SIP Parameters
- ITSP Loc-ID Settings
- Codec Parameters
- Destination Codec Parameters
- Internet Telephony Service Provider
- Networking
- SIPQ-Interconnection
- Native SIP Server Trunk**

Native SIP Server Trunk

Add Native SIP Server Trunk

CLIP / CLIR

CLIP outgoing in From header - display part: display name

CLIP outgoing in From header - user part: call number

Outgoing From Header - domain/host part: domainName

Diversion: From contains original CallingPartyNumber: ☒

Diversion: PAI contains original CallingPartyNumber: ☐

CLIP outgoing in P-Asserted-Id header - display part: display name

CLIP outgoing in P-Asserted-Id header - user part: call number

CLIP outgoing in P-Preferred-Id header - display part: omit

CLIP outgoing in P-Preferred-Id header - user part: omit

CLIP outgoing in Diversion header - display part: display name

CLIP outgoing in Diversion header - user part: call number

CLIR outgoing in From header - display part: anonymous

CLIR outgoing in From header - user part: fully anonymous

CLIR outgoing Privacy header: id

COLP / TIP supported for outgoing calls: COLP supported

Call number formatting

Incoming call - Called party number: To header user part

Incoming call - Calling party number: From header user part

Contact URI contains: call number

TCP port used in Contact URI: ephem. src-port

Apply Undo Refresh Help

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).

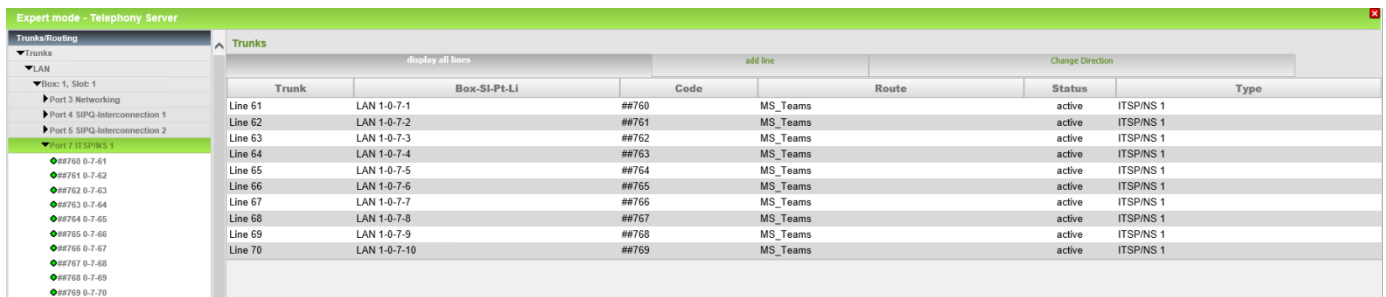
The screenshot shows the 'Expert mode - Telephony Server' window. On the left, a tree view under 'Voice Gateway' has 'Teams' expanded, with 'Teams-User' selected. The main panel is titled 'Native SIP Server Trunk User' and contains a form with the following fields:

- UserId:** Teams-User (highlighted with a red box)
- Authorization name:** (empty text box)
- Password:** (empty text box)
- Confirm Password:** (empty text box)

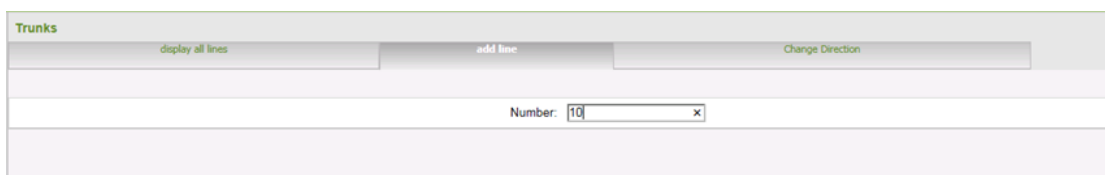
At the bottom of the window are three buttons: 'Apply', 'Undo', and 'Help'.

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:



Trunk	Box-SI-Pt-Li	Code	Route	Status	Type
Line 61	LAN 1-0-7-1	##760	MS_Teams	active	ITSP/NS 1
Line 62	LAN 1-0-7-2	##761	MS_Teams	active	ITSP/NS 1
Line 63	LAN 1-0-7-3	##762	MS_Teams	active	ITSP/NS 1
Line 64	LAN 1-0-7-4	##763	MS_Teams	active	ITSP/NS 1
Line 65	LAN 1-0-7-5	##764	MS_Teams	active	ITSP/NS 1
Line 66	LAN 1-0-7-6	##765	MS_Teams	active	ITSP/NS 1
Line 67	LAN 1-0-7-7	##766	MS_Teams	active	ITSP/NS 1
Line 68	LAN 1-0-7-8	##767	MS_Teams	active	ITSP/NS 1
Line 69	LAN 1-0-7-9	##768	MS_Teams	active	ITSP/NS 1
Line 70	LAN 1-0-7-10	##769	MS_Teams	active	ITSP/NS 1



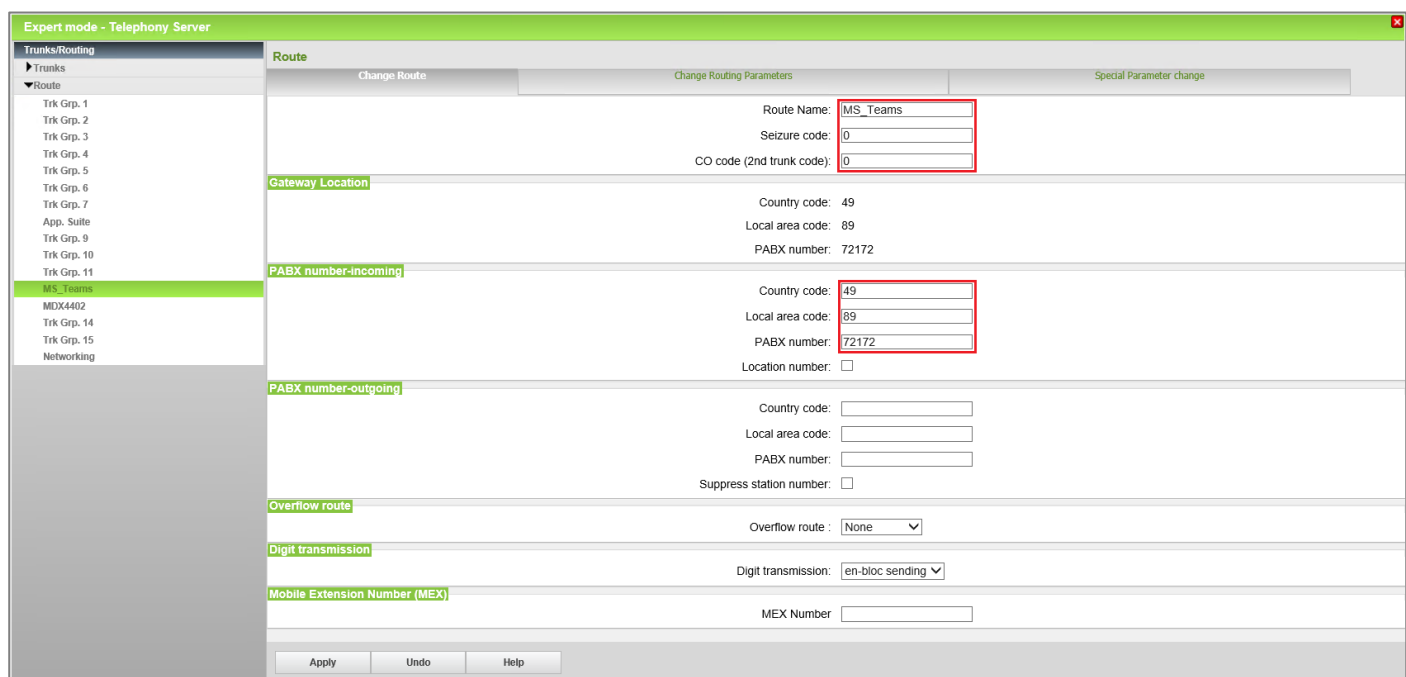
Trunks

display all lines add line Change Direction

Number:

5.3. Routes

The route configuration will be created automatically.



Expert mode - Telephony Server

Trunks/Route

Route

Change Route Change Routing Parameters Special Parameter change

Route Name:

Seizure code:

CO code (2nd trunk code):

Gateway Location

Country code: 49

Local area code: 89

PABX number: 72172

PABX number-incoming

Country code:

Local area code:

PABX number:

Location number:

PABX number-outgoing

Country code:

Local area code:

PABX number:

Suppress station number: ☐

Overflow route

Overflow route:

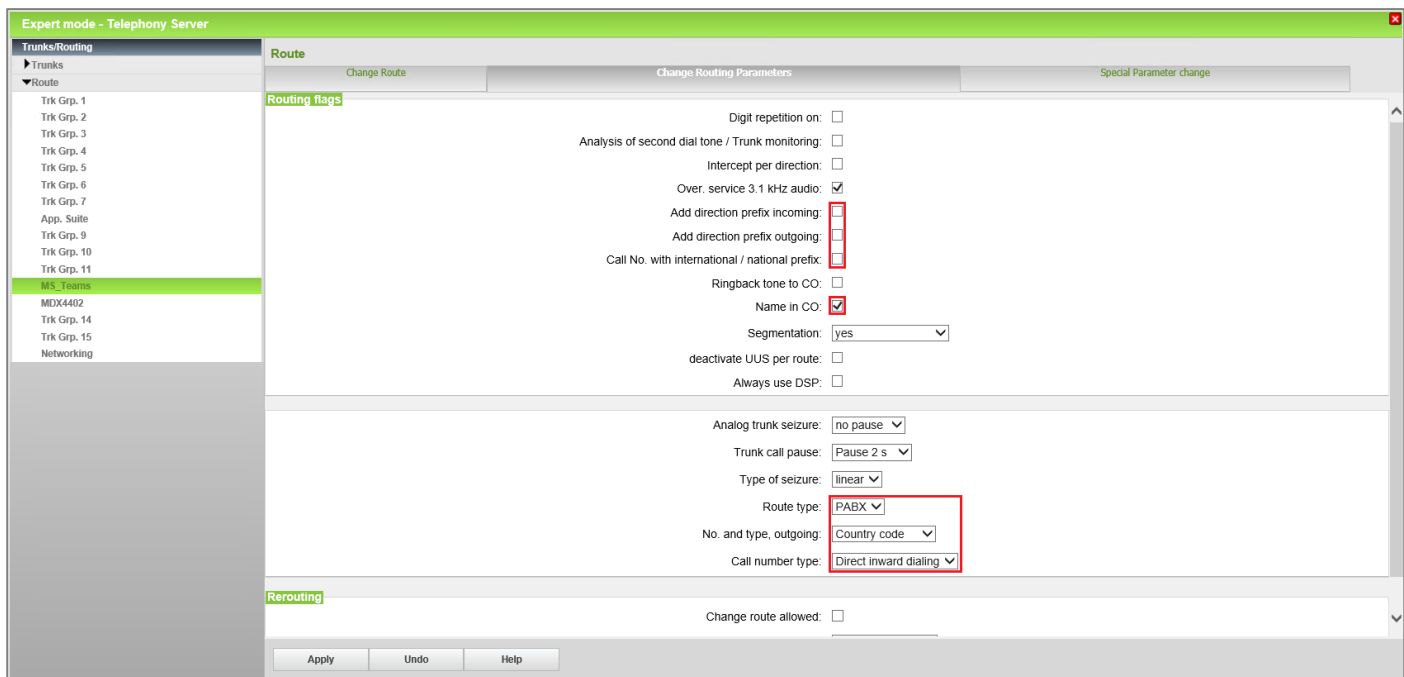
Digit transmission

Digit transmission:

Mobile Extension Number (MEX)

MEX Number:

Apply Undo Help



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.

Dial Plan	Name	Dialed digits	Routing Table	Acc. code	Classes of service	Emergency
76	MDX4402	0CZ	9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
77	MDX4402	0C0-Z	9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
78	MDX4402	0C1Z	9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
79	MDX4402	0CNZ	9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
80	MDX4402	0C00-Z	9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
81			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
82			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
83			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
84			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
85			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
86			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
87			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
88			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
89			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
90			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
91			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
92			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
93			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
94			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
95			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
96			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
97			-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
98	Teams	0C721721-Z	98	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
99	Teams	0C0-89721721-Z	99	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
100	Teams	0C00-4989721721-Z	100	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

Routing Table

Change Routing Table

Routing Table: 98 en-bloc sending

Index	Dedicated Route	Route	Dial Rule	min. COS	Warning	Dedicated Gateway	GW Node ID
1	<input type="checkbox"/>	MS_Teams	Teams-local	15	None	No	
2	<input type="checkbox"/>	None	None	15	None	No	
3	<input type="checkbox"/>	None	None	15	None	No	
4	<input type="checkbox"/>	None	None	15	None	No	
5	<input type="checkbox"/>	None	None	15	None	No	
6	<input type="checkbox"/>	None	None	15	None	No	
7	<input type="checkbox"/>	None	None	15	None	No	
8	<input type="checkbox"/>	None	None	15	None	No	
9	<input type="checkbox"/>	None	None	15	None	No	
10	<input type="checkbox"/>	None	None	15	None	No	
11	<input type="checkbox"/>	None	None	15	None	No	
12	<input type="checkbox"/>	None	None	15	None	No	
13	<input type="checkbox"/>	None	None	15	None	No	
14	<input type="checkbox"/>	None	None	15	None	No	
15	<input type="checkbox"/>	None	None	15	None	No	
16	<input type="checkbox"/>	None	None	15	None	No	

Apply Undo Help

Expert mode - Telephony Server

Routing Table

Change Routing Table

Routing Table: 99 en-bloc sending

Index	Dedicated Route	Route	Dial Rule	min. COS	Warning	Dedicated Gateway	GW Node ID
1	<input type="checkbox"/>	MS_Teams	Teams-nat	15	None	No	
2	<input type="checkbox"/>	None	None	15	None	No	
3	<input type="checkbox"/>	None	None	15	None	No	
4	<input type="checkbox"/>	None	None	15	None	No	
5	<input type="checkbox"/>	None	None	15	None	No	
6	<input type="checkbox"/>	None	None	15	None	No	
7	<input type="checkbox"/>	None	None	15	None	No	
8	<input type="checkbox"/>	None	None	15	None	No	
9	<input type="checkbox"/>	None	None	15	None	No	
10	<input type="checkbox"/>	None	None	15	None	No	
11	<input type="checkbox"/>	None	None	15	None	No	
12	<input type="checkbox"/>	None	None	15	None	No	
13	<input type="checkbox"/>	None	None	15	None	No	
14	<input type="checkbox"/>	None	None	15	None	No	
15	<input type="checkbox"/>	None	None	15	None	No	
16	<input type="checkbox"/>	None	None	15	None	No	

Apply Undo Help

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
110 - 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	<input type="checkbox"/>	MS_Teams	Teams-int	15	None	No	
2	<input type="checkbox"/>	None	None	15	None	No	
3	<input type="checkbox"/>	None	None	15	None	No	
4	<input type="checkbox"/>	None	None	15	None	No	
5	<input type="checkbox"/>	None	None	15	None	No	
6	<input type="checkbox"/>	None	None	15	None	No	
7	<input type="checkbox"/>	None	None	15	None	No	
8	<input type="checkbox"/>	None	None	15	None	No	
9	<input type="checkbox"/>	None	None	15	None	No	
10	<input type="checkbox"/>	None	None	15	None	No	
11	<input type="checkbox"/>	None	None	15	None	No	
12	<input type="checkbox"/>	None	None	15	None	No	
13	<input type="checkbox"/>	None	None	15	None	No	
14	<input type="checkbox"/>	None	None	15	None	No	
15	<input type="checkbox"/>	None	None	15	None	No	
16	<input type="checkbox"/>	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.

Change Dial Rule			
Rule Name	Dial rule format	Network access	Type
1 ISDN	A	Main network supplier	Unknown
2 SIP	A	Main network supplier	Unknown
3 SIP lokal	HE2A	Main network supplier	Unknown
4 MEB	E1A	Corporate Network	PABX number
5 IP-Network	A	Corporate Network	Unknown
6 Multi-Location	BA	Corporate Network	Unknown
7 Gateway call	E1A	Corporate Network	Unknown
8 COInternat	D0E4A	Main network supplier	Unknown
9 Add_cc_to_Canoni	D49E2A	Main network supplier	Country code
10 National_to_Cano	D49E3A	Main network supplier	Country code
11 Internat_to_Can	E3A	Main network supplier	Country code
12 SIP lokal Canoni	HE2A	Main network supplier	Country code
13 Teams-nat	D49E3A	Main network supplier	Country code
14 Teams-int	E3A	Main network supplier	Country code
15 Teams-local	D4989E2A	Main network supplier	Country code
16		Unknown	Unknown
17		Unknown	Unknown
18		Unknown	Unknown
19		Unknown	Unknown
20		Unknown	Unknown
21		Unknown	Unknown
22		Unknown	Unknown
23		Unknown	Unknown
24		Unknown	Unknown
25		Unknown	Unknown

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 *lokal* 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.**

Expert mode - Telephony Server

Basic Settings

System

System Flags

Time Parameters

Display

DISA

Intercept/Attendant/Hotline

LDAP

Texts

Flexible menu

Speed Dials

Service Codes

HFA Registration Password

Gateway

Quality of Service

Port Management

Call Charges

Voicemail / Announcement Player

Phone Parameter Deployment

System flags

Edit System Flags

Through-connection for external FWD on: ☐

Call forwarding to main station interface permitted: ☒

Hunting to external call forwarding destination: ☐

Conference tone: ☐

Warning signal for call pickup groups: ☒

Increase volume for optiPoint/OpenStage terminals: ☐

Relocate allowed: ☐

More than 1 external conference member: ☒

Trunk reservation, automatic: ☐

No. redial with a/c code: ☐

Use only default number for MSN: ☐

Path optimization: ☒

DTMF automatic: ☒

Broadcast with connection: ☒

Tone from CO: ☐

Ringback protection: ☐

Euro-impedance: ☐

Different phonemail messages Day/Night: ☐

Display international / national code number: ☒

Line change for direct call: ☐

Automatic redial: ☐

Voice mail Node call number: ☐

Apply Undo Help

Expert mode - Telephony Server

Basic Settings

System

System Flags

Time Parameters

Display

DISA

Intercept/Attendant/Hotline

LDAP

Texts

Flexible menu

Speed Dials

Service Codes

HFA Registration Password

Gateway

Quality of Service

Port Management

Call Charges

Voicemail / Announcement Player

Phone Parameter Deployment

System flags

Edit System Flags

Configurable CLIP: ☒

Caller list at destination in case of Forward Line: ☐

Call forwarding after defect call / single step transfer: ☐

Follow call management in case of defect call / single step transfer: ☐

Extended Key Functionality: ☐

Calling number in pick-up groups / ringing groups / CFN /RNA: ☒

SPE support: ☐

SPE advisory tone: ☐

Transparent dialing of * and # on trunk interfaces: ☐

Add seizure code for MEX: ☐

CMI MWI Ringer: ☐

Restrict indirect trunk group connections according to CON Matrix: ☐

Open numbering scheme

active: ☐

Node callnumber:

Transit permission

Feature transit: ☒

Tie traffic transit: ☒

External traffic transit: ☒

Special switch

CALL PROC no send: ☐

Automatic, cyclical line seizure: ☒

Apply Undo Help

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]**.

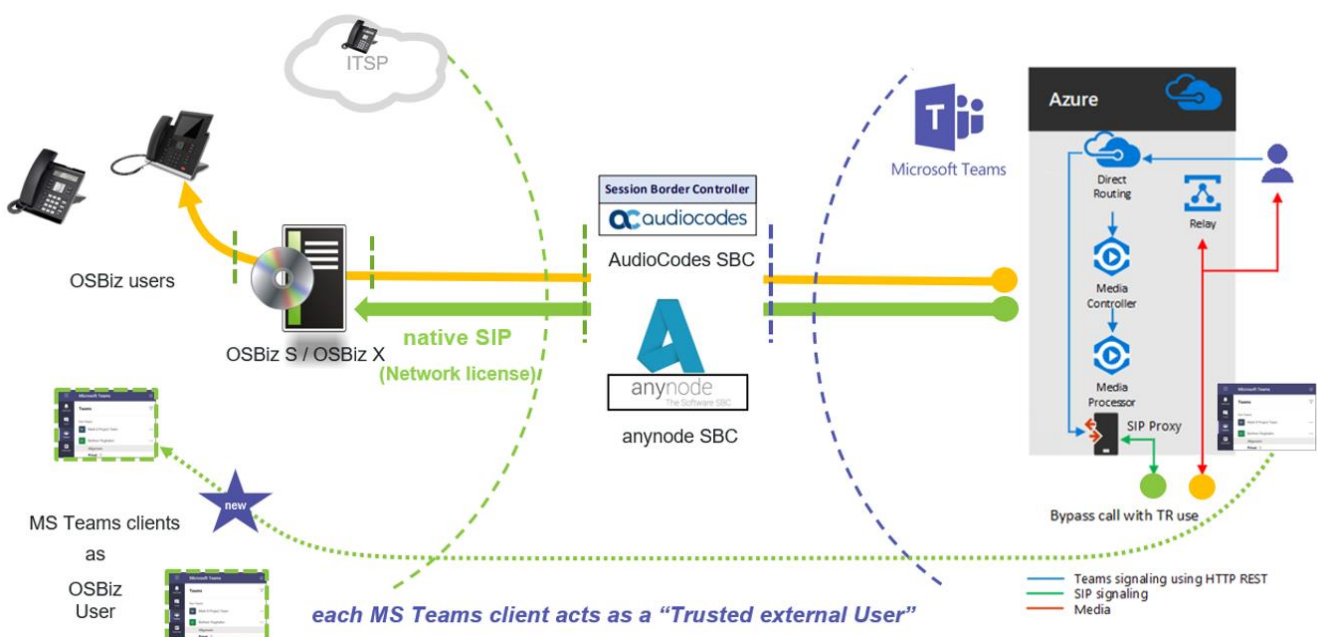
Note: The "**Transit permission**" flags are required because in current environment setup, where OpenScape Business acts as a transit for calls from MS Teams users to PSTN.

6. OpenScape Business - Trusted external User mode

OpenScope 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.

Expert mode - Telephony Server

Native SIP Server Trunk

Add Native SIP Server Trunk

Base Template: **Trusted SBC - predefined**

Trunk Name: **Teams**

Enable Trunk: ☒

Trunk Identifier in System: ITSP/NS 1

Remote Domain Name: 10.8.242.78

Transport protocol: **udp**

Transport security: traditional (udp or tcp)

Media security: RTP only

SIP Server

IP Address / Host name: **10.8.242.78**

Port: **5060**

SIP Registrar

Use Registrar: ☐

IP Address / Host name:

Port: 5060

Reregistration interval (sec): 600

STUN Server

Use STUN: ☐

IP Address / Host name: stun-1-online.de

Port: 3478

Extended SIP Data

Show Extended SIP Data: ☒

Attention: the following parameters are used to adapt the behavior of the SIP stack to a certain trunk implementation. Wrong parameter settings may result in a malfunction of the trunk interface.

Apply Undo Refresh Help

Expert mode - Telephony Server

Native SIP Server Trunk

Add Native SIP Server Trunk

CLIP / CLIR

CLIP outgoing in From header - display part: **display name**

CLIP outgoing in From header - user part: call number

Outgoing From Header - domain/host part: domainName

Diversion: From contains original CallingPartyNumber: ☒

Diversion: PAI contains original CallingPartyNumber: ☐

CLIP outgoing in P-Asserted-Id header - display part: **display name**

CLIP outgoing in P-Asserted-Id header - user part: call number

CLIP outgoing in P-Preferred-Id header - display part: omit

CLIP outgoing in P-Preferred-Id header - user part: omit

CLIP outgoing in Diversion header - display part: **display name**

CLIP outgoing in Diversion header - user part: call number

CLIR outgoing in From header - display part: anonymous

CLIR outgoing in From header - user part: fully anonymous

CLIR outgoing Privacy header: id

COLP / TIP supported for outgoing calls: COLP supported

Call number formatting

Incoming call - Called party number: To header user part

Incoming call - Calling party number: From header user part

Contact URI contains: call number

TCP port used in Contact URI: ephem. src-port

Miscellaneous

Check Redirection: **History-Info + Referred-By**

Apply Undo Refresh Help

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).

The screenshot shows the 'Expert mode - Telephony Server' window. On the left, the 'Voice Gateway' tree has 'Native SIP Server Trunk' expanded, with 'Teams-User' selected. The main panel is titled 'Native SIP Server Trunk User' and contains a form with the following fields:

- UserId:** Teams-User (highlighted with a red box)
- Authorization name:** (empty text box)
- Password:** (empty text box)
- Confirm Password:** (empty text box)

At the bottom of the window are three buttons: 'Apply', 'Undo', and 'Help'.

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:

Trunk	Box-SI-PL-Li	Code	Route	Status	Type
Line 61	LAN 1-0-7-1	##760	MS_Teams	active	ITSP/NS 1
Line 62	LAN 1-0-7-2	##761	MS_Teams	active	ITSP/NS 1
Line 63	LAN 1-0-7-3	##762	MS_Teams	active	ITSP/NS 1
Line 64	LAN 1-0-7-4	##763	MS_Teams	active	ITSP/NS 1
Line 65	LAN 1-0-7-5	##764	MS_Teams	active	ITSP/NS 1
Line 66	LAN 1-0-7-6	##765	MS_Teams	active	ITSP/NS 1
Line 67	LAN 1-0-7-7	##766	MS_Teams	active	ITSP/NS 1
Line 68	LAN 1-0-7-8	##767	MS_Teams	active	ITSP/NS 1
Line 69	LAN 1-0-7-9	##768	MS_Teams	active	ITSP/NS 1
Line 70	LAN 1-0-7-10	##769	MS_Teams	active	ITSP/NS 1

Trunks

display all lines add line Change Direction

Number:

6.2. Routes

The route configuration will be created automatically.

Expert mode - Telephony Server

Route

Change Route Change Routing Parameters Special Parameter change

Route Name:

Seizure code:

CO code (2nd trunk code):

Gateway Location

Country code:

Local area code:

PABX number:

PABX number-incoming

Country code:

Local area code:

PABX number:

Location number: ☐

PABX number-outgoing

Country code:

Local area code:

PABX number:

Suppress station number: ☐

Overflow route

Overflow route:

Digit transmission

Digit transmission:

Mobile Extension Number (MEX)

MEX Number:

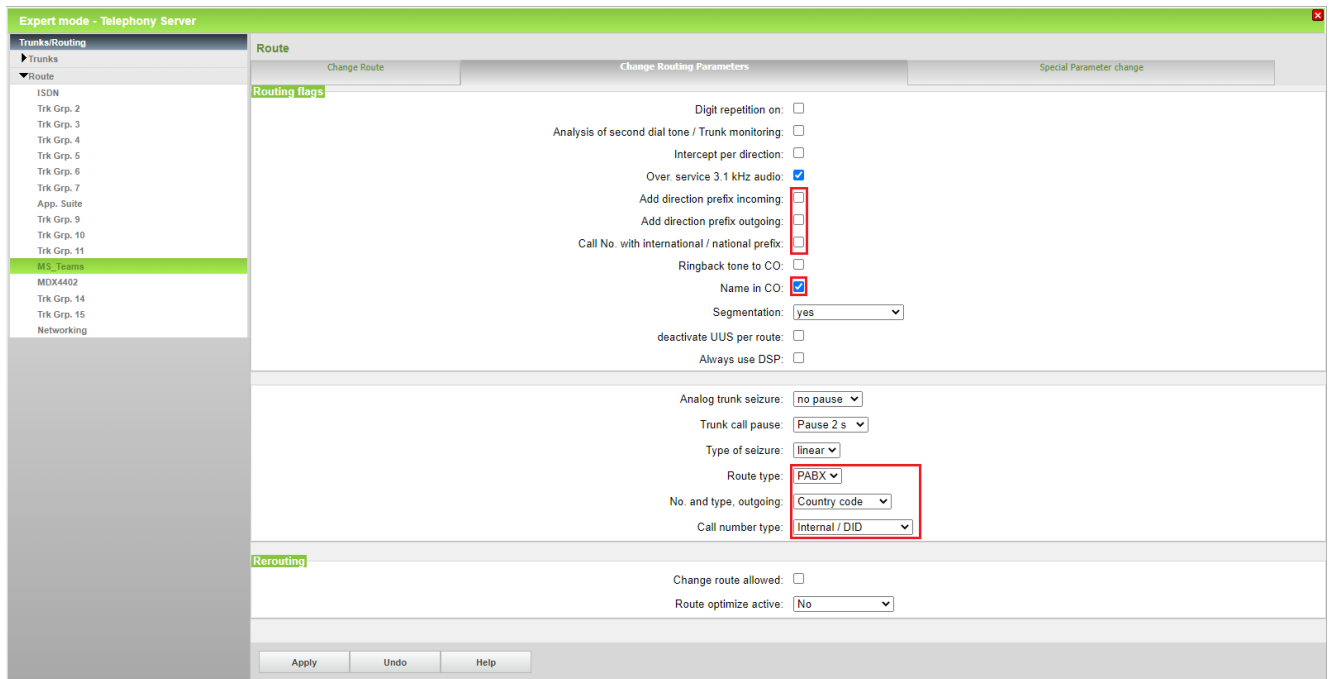
Trusted External Users

Trusted External Users: ☒

Apply Undo Help

The feature "Trusted external users" for this route requires specific steps to prevent unauthorized access by call number spoofing. It is strongly recommended to only use this route within the internal LAN with VLAN. Do not allow this connection to be accessed from the Internet. Press OK to continue. Press Cancel to modify the related settings first.

OK Abbrechen



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

The screenshot shows the 'OpenScape Business Assistant' interface. The top navigation bar includes 'Home', 'Administrators', 'Setup', 'Expert mode', 'Data Backup', 'License Management', 'Service Center', and 'Networking'. The 'Setup' menu is expanded, showing 'Wizards' with sub-items: 'Basic Installation', 'Telephones / Subscribers', 'Central Telephony', 'User Telephony' (highlighted), 'UC Suite', 'Cloud Services', and 'Mass Data'. The main content area is titled 'User Telephony' and contains a list of configuration options, each with an 'Edit' button. The 'Mobile Phone Integration' option is highlighted with a red box. Its description is: 'Set up a link between a mobile phone and an internal station with the goal of enabling incoming and outgoing availability under one station number (One Number Service)'.

Press “Add” to create a new Mobility User

The screenshot shows the 'Add Mobility User' wizard step. The title bar is 'Setup - Wizards - User Telephony - Mobile Phone Integration'. The main content area has a header 'Select station for Mobility'. Below this is a 'DISA' section with a 'Direct inward dialing' input field. The 'Add Mobility User' section is highlighted with a green bar. Below it, the 'Add' button is highlighted with a red box. The 'New Mobility User' section contains a table with the following columns: 'Mobility User callno', 'Mobility User DID', 'Display', 'Trunk access code + Mobile Call number', 'User name for mobile UC clients', and 'State'.

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

The screenshot shows the 'Change Mobility User allocation' wizard step. The title bar is 'Setup - Wizards - User Telephony - Mobile Phone Integration'. The main content area has a header 'Change Mobility User allocation'. Below this is a 'Mobile phone mode in-house' section with two radio buttons: 'GSM Mode' (selected) and 'WLAN Mode'. The 'Mobility User' section is highlighted with a green bar. It contains the following fields: 'Trunk access code+Mobile Call number' (80004989721721001), 'Internal call number of Mobility User' (1001), 'DID of Mobility User' (1001), 'First Name' (1001), 'Last Name' (MS Teams), 'Display' (MS Teams, 1001), and 'User name for mobile UC clients' (None). At the bottom, there are buttons for 'Help', 'Abort', 'Back', and 'OK & Next'.

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

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

Expert mode - Telephony Server

Station

Station - 3501

Type: Mobility Entry

Call number: 1001

First Name: 1001

Last Name: MS Teams

Display: MS Teams, 1001

Direct inward dialing: 1001

Device Type: virtual

Clip/Lin: -

Access: -

Mobility/Circuit

Type: Mobility station

Mobile Call number: -

Web Feature ID: **Trusted external station**

Parameter

Extension Type: Standard

Language: German

Call signaling internal: Ring type 1

Call signaling external: Ring type 1

Class of service (LCR): 15

Hotline Mode: Off

Hotline: None

ITSP Loc-ID: -

Apply Undo Help

Expert mode - Telephony Server

Trusted external User

Edit Subscriber

CallNo	DID	First Name	Last Name	Display	Type	Trusted external station call number
1001	1001	1001	MS Teams	MS Teams, 1001	Trusted external station	80004989721721001
1002	1002	1002	MS Teams	MS Teams, 1002	Trusted external station	80004989721721002

Page 1 of 1

Items per page 10 25 50 100

Apply Undo Help

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.

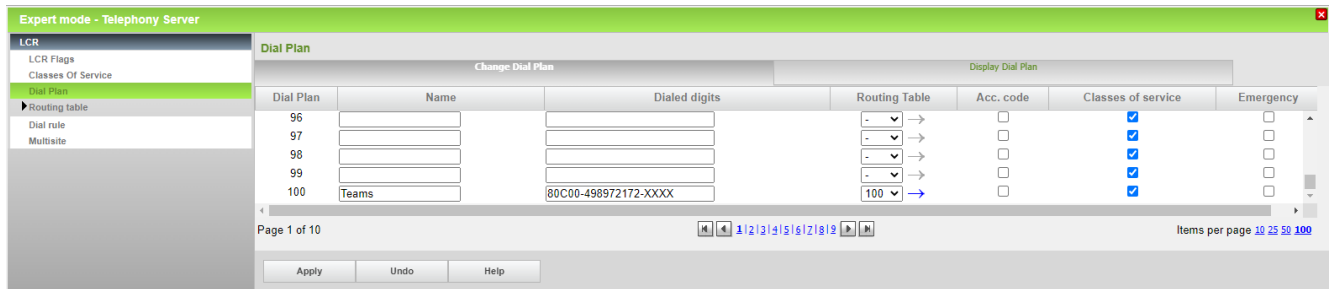
6.5. LCR Dial Plan

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**).

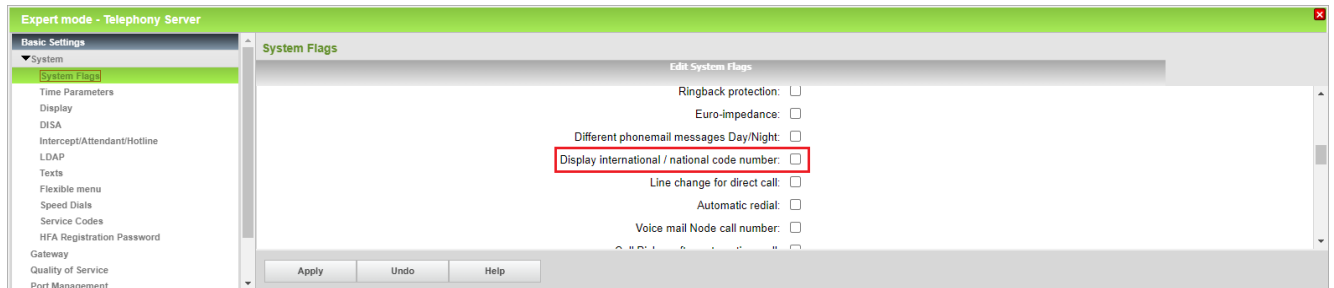
Click on **[Apply]**.



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 independent 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.

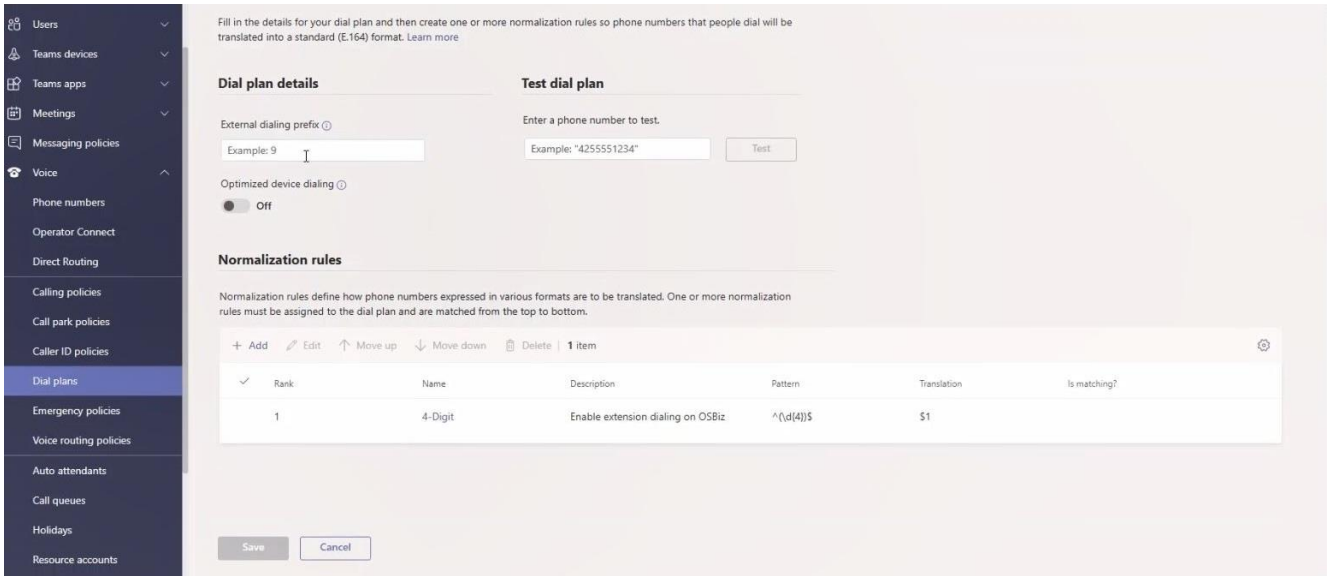
Details are available in [5]: Tutorial VoIP Interfaces.

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:



Fill in the details for your dial plan and then create one or more normalization rules so phone numbers that people dial will be translated into a standard (E.164) format. [Learn more](#)

Dial plan details

External dialing prefix ⓘ
Example: 9

Optimized device dialing ⓘ
☐ Off

Test dial plan

Enter a phone number to test.
Example: "4255551234"

Normalization rules

Normalization rules define how phone numbers expressed in various formats are to be translated. One or more normalization rules must be assigned to the dial plan and are matched from the top to bottom.

+ Add Edit Move up Move down Delete | 1 item

✓	Rank	Name	Description	Pattern	Translation	Is matching?
	1	4-Digit	Enable extension dialing on OSBiz	^(\d{4})\$	\$1	

9. Support & Serviceability

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

no calls with MS Teams client possible	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• see "no calls with MS Teams client possible"
Central Office ITSP calls are not signalled at MS Teams client	<ul style="list-style-type: none">• please check for codecs (e.g. G.711) on Carrier side
desk phone calls are not signalled at MS Teams client	<ul style="list-style-type: none">• please check for codecs (e.g. G.711) on phone side
MS Teams-Client Hold/Park Call <ul style="list-style-type: none">• Feature collision: OSBiz User puts MS Teams client on hold AND MS Teams client puts OSBiz User on hold	<ul style="list-style-type: none">• "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 <ul style="list-style-type: none">• no update on Display	<ul style="list-style-type: none">• update of transferred party information is not supported
MS Teams client Call Forwarding <ul style="list-style-type: none">• Call Forwarding destination is not signalled with original calling party information• display of the forwarded to party does not show the name	<ul style="list-style-type: none">• update of forwarded party information is not supported• name provision is not supported
MS Teams Conference <ul style="list-style-type: none">• OSBiz MoH disturbs the conference call	<ul style="list-style-type: none">• mute the according OSBiz User in the MS Teams conversation - the OSBiz User can unmute himself
Payload issue <ul style="list-style-type: none">• MS Team calling HFA but there	<ul style="list-style-type: none">• activate the flag" always use DSP" for MS Teams

is no payload	Route
Payload issue	
<ul style="list-style-type: none"> Voice interruptions at the beginning of the call 	<p>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</p>

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.

About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and

Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about
us atos.net
atos.net/career

Let's start a discussion together



For more information: osbiz-certification@atos.net

Atos, the Atos logo, Atos|Syntel, and Unify are registered trademarks of the Atos group. April 2020.
© 2020 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.