

A MITEL PRODUCT GUIDE

# **OpenScape Business V3**

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

#### Disclaimer:

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

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

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

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

Settings and configuration might change due to different Software versions.

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

#### Please note:

Unify offers voice interworking capabilities with Microsoft Teams with a technical description of how to configure the OpenScape Business. Microsoft Teams, AudioCodes SBC, anynode SBC and any other Microsoft certified SBC are 3<sup>rd</sup> 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 <u>https://www.audiocodes.com/library/technical-</u> <u>documents?productFamilyGroup=1637&productGroup=1692&versionGroup=Version+7.2</u>

https://www.audiocodes.com/solutions-products/products/products-for-microsoft-365/directrouting-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 <u>https://www.anynode.de/, https://www.youtube.com/user/TESYSTEMS/featured, https://docs.anynodesbc.com/</u>

## 1. Introduction

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

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

Direct Routing allows the integration of MS Teams infrastructure into existing on-premise telephony system. MS Teams users are enabled to use on-premises telco lines or SIP trunks to make and receive calls instead of using Microsoft Carrier Services via Calling Plans [1].

Certified SBCs are:

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



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

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

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

### 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:

- MS Teams users of Direct Routing must have the following licenses assigned in Microsoft 356 / Office 365: Microsoft 365 / Office 365 Enterprise E3 / E1 (including SfB Online Plan2, Exchange Plan2, and Teams) + Phone System licenses or Microsoft 365 / Office 365 Enterprise E5 (including SfB Online Plan2, Exchange Plan2, Teams, Phone System and Audio Conferencing).
- 2. MS Teams certified SBC (<u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-border-controllers</u>).
- 3. A publicly registered domain name. Public domain name like *onmicrosoft.com* is not a possibility for direct routing.
- 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 (<u>https://docs.microsoft.com/en-us/MicrosoftTeams/direct-routing-plan#public-trusted-certificate-for-the-sbc</u>).
- 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 subsection 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: (<u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan-media-bypass</u>).



# 2. Direct Routing

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

#### 2.1. Setup the Domain

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

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

	Microsoft 365 admin center	Search (Try "passwords" to let users reset their own)	S () Ø	? (мк
≡		Contoso	🕗 Dark	mode
ல்	Home	Domains		
8	Users $\checkmark$			
የድ	Groups $\checkmark$	+ Add domain 🗇 Buy domain () Refresh	lter O Search	] =
<i>₽</i> ≞	Roles			] _
母	Resources $\checkmark$	Domain name 1 Status	TB Choose columns	
	Billing ~	M365x316382.onmicrosoft.com (Default)		
0	Support 🗸			
٢	Settings ^			
1	Domains			
	Search & intelligence			
	Org settings			
	Integrated apps			
	Partner relationships			
Þ	Setup			
k	Reports $\checkmark$			
S	Health $\checkmark$			
Adr	nin centers			
6	Security			0
6	Compliance			Ģ
Þ	Endpoint Manager			



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



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



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

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



Select "Add your own DNS records". Click on **[Continue]**.



	Microsoft 365 admin center		🕸 ? (мк)
≡	Domains > Add domain		
ش بر	Add domain	<ul> <li>MX Records (1)</li> <li>View instructions for MX Records</li> </ul>	•
22	Connect domain	Record Host Name Points to address or value Priority TTL Status	
<sup>7</sup> 個   -		Expected D @ D athdrlabs- xyz.mail.protection.outlook.com D 0 D Hour	
	Add DNS records		
ç	 O Finish	CNAME Records (1)     View instructions for CNAME Records	
٢	-	Record Host Name Points to address or value TTL Status	
		Expected 🗅 autodiscover 🗋 autodiscover.outlook.com 🗋 1 Hour	
S			
۲		<ul> <li>TXT Records (1)</li> <li>View instructions for TXT Records</li> </ul>	
۵		Record TXT name TXT value TTL Status	
Þ		v=spf1	
<b>∲</b>		-all	
\$0 \$			0
ij		Advanced Options	
Ē		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.

	Microsoft 365 admin center	P Search	MK
≡		Contoso 👌 Dark mode	
<u>ش</u>	Home	Domains	
8	Users $\vee$		
^ <u>%</u> ^	Groups $\checkmark$		
2	Roles		
喝	Resources $\checkmark$	Domain name ↑ Status 🖽 Choose columns	
	Billing ~	M365x316382.onmicrosoft.com (Default)	
្ច	Support V	athdriabs.xvz Eelthy	
٢	Settings ^		
	Domains		
	Search & intelligence		
	Org settings		
	Integrated apps		
	Partner relationships		
B	Setup		
Ľ	Reports $\checkmark$		
$\approx$	Health $\checkmark$		
Adı	min centers	6	2
۵	Security		
٢	Compliance		3
Þ	Endpoint Manager		

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: <u>https://docs.microsoft.com/en-us/microsoftteams/teams-powershell-overview</u>.

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

#### Connect-MicrosoftTeams

Provide Teams tenant admin credentials to log in.



Create and pair the SBC SIP trunk in Teams tenant.

Account	Environment Tenant		
nichail.korakis@M365x316382.onmicros	oft.com AzureCloud f4735769-90ce-4c5d-8f4	d-48	
PS C:\Users\Administrator> Get-CsOnl	<pre>inePSTNGateway -Identity sbc01.athdrlabs.x</pre>	yz	
[dentity	: sbc01.athdrlabs.xyz		
InboundTeamsNumberTranslationRules	÷ {}		
InboundPstnNumberTranslationRules	: {}		
OutboundTeamsNumberTranslationRules	: {}		
OutboundPstnNumberTranslationRules	: {}		
qdn	: sbc01.athdrlabs.xyz		
SipSignalingPort	: 5061		
ailoverTimeSeconds	: 10		
orwardCallHistory	: True		
orwardPai	: True		
SendSipOptions	: True		
laxConcurrentSessions	: 24		
nabled	: True		
lediaBypass	: False		
atewaySiteId	:		
atewaySiteLbrEnabled	: False		
atewayLbrEnabledUserOverride	: False		
alloverResponseCodes	: 408,503,504		
eneratekingingwhileLocatingUser	;		
/latLoSupportea	: Faise		
hediakelaykoutingLocationOverride			
roxySDC			
sypassmode	: None		

Run e.g. the command:

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

Parameters that affect current certification:

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

View the newly created "Online PSTN Gateway" (SIP trunk) with the command: Get-CsOnlinePSTNGateway -Identity sbc01.athdrlabs.xyz

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

### 2.3. Enable users for Direct Routing Service

Ensure that the users are homed in Teams Phone System.



Get-CsOnlineUser -Identity MST01@M365x316382.onmicrosoft.com | fl RegistrarPool Get-CsOnlineUser -Identity MST02@M365x316382.onmicrosoft.com | fl RegistrarPool

Configure the phone number and enable enterprise voice and voicemail.

Set-CsUser -Identity MST01@M365x316382.onmicrosoft.com -EnterpriseVoiceEnabled \$true - HostedVoiceMail \$true - OnPremLineURI tel:+ 4989721721001

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

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

Verify phone number assignment with:

Get-CsOnlineUser -Identity MST01@M365x316382.onmicrosoft.com Get-CsOnlineUser -Identity MST02@M365x316382.onmicrosoft.com

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

### 2.4. Configure Voice Routing

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

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

Call routing is made up of the following elements:

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

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

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

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

For all other calls, if a user has both licenses (Microsoft Phone System and Microsoft Calling Plan), **"Automatic Route"** is used. If nothing matches the number patterns in the administratorcreated 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-4799-84f6-402d1b2d6da	a		
DistinguishedName	: CN=06a1ae9b-adbd-4799-84f6-402d1b2d	l6daa,OU=f	4735769	9-9
	0ce-4c5d-8f4d-48044a439de8,OU=OCS			
	Tenants,DC=lync2e001,DC=local			
Identity	: CN=06a1ae9b-adbd-4799-84f6-402d1b2d	l6daa,OU=f	4735769	9-9
	0ce-4c5d-8f4d-48044a439de8,0U=OCS			
	Tenants,DC=1ync2e001,DC=1ocal			
Guid	: cadae485-0f5f-4d51-b9eb-bc159d0d7e5	57		
ObjectCategory	: CN=Person,CN=Schema,CN=Configuratio	on,DC=lynd	2e001,D	C=
	local			
ObjectClass	: {top, person, organizationalPerson,	user}		
WhenChanged	: 3/29/2021 4:17:53 PM			
WhenCreated	: 10/14/2019 4:26:27 PM			
OriginatingServer	: WE02E00ADS02.lvnc2e001.local			
IsBvPassValidation	: True			
IsValid	: True			
ObjectState	: Unchanged			
PS C:\Users\Administrator>				
PS C:\Users\Administrator>				
PS C: (Users (Administrator) Get-Csoni	InerSiNUsage			
Identity : Global				
Usage : {CSL Athens}				
PS C:\Users\Administrator> _				
				· · ·

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

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

🔀 Administrator: Window	s PowerShell	_	×
PS C:\Users\Administra	ator> Get-CsOnlineVoiceRoute -Identity "CSL ATH SBC01"		í
Identity Priority Description NumberPattern OnlinePstnUsages OnlinePstnGatewayList Name	: CSL ATH SBC01 : 0 : .* : .* : {CSL Athens} : {sbc01.athdr1abs.xyz} : CSL ATH SBC01		
5 C:\Users\Administra	ator> _		

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: W	indows PowerShell	—	×
PS C:\Users\Admin	<pre>istrator&gt; Get-CsOnlineVoiceRoutingPolicy -Identity "CSL ATH"</pre>		^
Identity OnlinePstnUsages Description RouteType	: Tag:CSL ATH : {CSL Athens} : : BYOT		ŀ
PS C:\Users∖Admin	istrator> _		

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].

	Microsoft Teams adr	nin cente					¢* @ ? 🚺
		≡	Users \ MST01				
۵ ı	ashboard						
8 <u>0</u> 3 Т	eams	~	MST01		7-DAY QUALITY	7-DAY ACTIVITY	
& C	Devices	~		Phone number +49 89 721721001		2	
۵ ا	ocations	~	Germany	Email MST01@M365x316382.onmicr		Meetings	
<b>ii</b> (	Isers			osoft.com		19 Calir	
۳ ۱	leetings	~		-		Carlo	
	Aessaging policies				🔳 Good 🔳 Poor 🔲 Unknown		
BÊ ⊺	eams apps	~					
@\ _	/oice	~	Account Voice Call history Policies				
1 F	olicy packages						
- A A A A A A A A A A A A A A A A A A A	Inalytics & reports	~	Assigned policies & Edit	Policy package 🖉 Edit			
193 C	Org-wide settings	~	Meeting policy Global (Org-wide default)	Package assigned None			
ا ا	lanning	~	Messaging policy				
9			Global (Org-wide default)				
6	an quanty dashboard in		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)				Give feedback

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:

	Microsoft Teams adm	nin center			Q	٥	?	MK
			Calling policies \ Global					
ඛ	Dashboard							
දීලී	Teams	$\sim$	Global					
\$	Devices	~	Description					
٢	Locations	$\sim$						
දර	Users		Make private calls	On On				
Ē	Meetings	$\sim$	Call forwarding and simultaneous ringing to people in	On On				
Ę	Messaging policies		your organization					
B	Teams apps	$\sim$	Call forwarding and simultaneous ringing to external phone numbers	On On				
ି	Voice	~	Voicemail is available for routing inbound calls	User controlled	$\sim$			
1	Policy packages		Inbound calls can be routed to call groups	On On				
Â	Analytics & reports	~	Allow delegation for inbound and outbound calls	On				
<u>ت</u>	Org-wide settings	$\sim$	Prevent tall bypass and calls through the PSTN	Off				
Ĩ	Planning	$\sim$	revent ton bypass and send cans through the FSTN					
S	Legacy portal 🖸		Busy on busy is available when in a call	• Off				
	Call quality dashboard		Save			Give f	eedbac	:k

**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: <a href="https://www.audiocodes.com/media/13253/connecting-audiocodes-sbc-to-microsoft-teams-direct-routing-enterprise-model-configuration-note.pdf">https://www.audiocodes.com/media/13253/connecting-audiocodes-sbc-to-microsoft-teams-direct-routing-enterprise-model-configuration-note.pdf</a>

### 3.1. LAN and WAN IP Interfaces

faces					
GENERAL			IP ADDRESS		
Index	0		Interface Mode	IPv4 Manual	~
Name	LAN_IF		IP Address	10.8.242.78	
Application Type	OAMP + Media + Control	~	Prefix Length	24	
Ethernet Device	#0 [vlan 1]	▼ View	Default Gateway	10.8.242.1	
DNS					
DNS					
Primary DNS	10.8.251.103				
Secondary DNS	0.0.0.0				
		Cancel	APPLY		

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:

OAMP + Media + Control

LAN\_IF (LAN interface friendly name)

10.8.242.78 (SBC IP - SBC WBM IP)

vlan 1 (dedicated VLAN for LAN interface to OSBiz)

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

- Name:
- Application Type:
- Ethernet Device:
- Primary DNS:
- IP Address:
- Prefix Length:
- Default Gateway:
- 10.8.242.1

24

10.8.251.103

Click on [Apply]

rerfaces					
GENERAL			IP ADDRESS		
Index	1		Interface Mode	IPv4 Manual	~
Name	WAN_IF		IP Address	195.97.14.76	
Application Type	Media + Control	~	Prefix Length	27	
Ethernet Device	#1 [vlan 2]	▼ View	Default Gateway	195.97.14.65	
DNS					
Primary DNS	8.8.8.8				
Secondary DNS	0.0.0.0				
			_		
		Cancel	APPLY		

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

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

- WAN IF (WAN interface friendly name) • Name: **Application Type:** SBC WBM on an interface pointing to internet)
- Ethernet Device:
- Primary DNS:
- IP Address:
- Prefix Length:
- **Default Gateway**:

Click on [Apply].

Media + Control (not recommended to activate OAMP i.e. vlan 2 (dedicated VLAN for WAN interface to Teams) 8.8.8.8 (any known public DNS or according to internet provider's instructions) 195.97.14.76 (DMZ IP address of SBC) 27 195.97.14.65 (router GW IP)

### 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.

Caudiocodes SETUP	MONITOR TROUBLESHOOT		Save Reset	Actions <del>-</del>	<mark>لا</mark>	Admin <del>-</del>
M800B IP NETWORK SIGNALING & MEDIA	ADMINISTRATION			Q Entit	y, paramete	er, value
🗢 🔿 SRD All 💌						
	Time & Date					
	LOCAL TIME	TIME ZONE				
Authentication Server Web Settings	Year         Month         Day         Hours         Minutes         Seconds           2020         2         28         11         41         46	UTC Time UTC Offset	28 Feb, 2020 09:41: Hours: 2	46 Minutes: 0		
Access List		Daylight Saving Time	Disable			~
Additional Management Interfaces (0)	NTP SERVER	DST Mode	Day of year			$\sim$
SNMP	Enable NTP Enable	Start Time	Jan 🗸 01	<ul><li>✓ 0 :</li></ul>	0	
▶ LICENSE	Primary NTP Server Address (IP or FQDN) 10.8.251.104	Offere (min)	jan 🔮 OI	• 0 :	0	
	Secondary NTP Server Address (IP or FQDN)	Oriset (min)	ou	Time .		
	NTP Update Interval Hours: 24 Minutes: 0	Day of Month Start	jan 🗸 Sunday	✓ First	<u> </u>	0
	NTP Authentication Key Identifier 0	Day of Month End	Jan 🚩 Sunday	✓ First	• 0 :	0
	NTP Authentication Secret Key					
	Cancel	APPLY				

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.

ntexts				
GENERAL		OCSP		
Index	1	OCSP Server	Disable	$\checkmark$
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	$\checkmark$
Cipher Client	DEFAULT			
Cipher Server TLS1.3	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SF			
Cipher Client TLS1.3	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SF			
Key Exchange Groups	X25519:P-256:P-384:X448			
Strict Certificate Extension Validation	Disable			
DH key Size	2048			
TLS Renegotiation	Enable			
	Con			

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

Enter the following:

- 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.

MS Teams (Teams TLS context friendly name)

	TROUBLESHOOT				Save	Reset	Actions -	4	Admin <del>-</del>
M800B IP NETWORK SIGNALING & MEDIA ADMI	NISTRATION							ty, parameter	
😧 🕣 SRD All 🔻									
C NETWORK VIEW	TLS Contexts (2)								
CORE ENTITIES	+ New Edit 💼		re ee Page 1 of 1 is in Show 10 V	records per page					Q
IP Interfaces (2)	INDEX 🔶	NAME	TLS VERSION	DTLS VERSI	ION	CIPH	ER SERVER		
Ethernet Devices (2)	0	default	Any TLS1.x	Any		DEFA	ULT		
Physical Ports (12)	1	MS Teams	TLSv1.2	Any		DEFA	JULT		
Static Routes (0)									
HA Settings									
HA Network Monitor (0)									
NAT Translation (0)									
▲ SECURITY	#1[MS Teams]							E	dit
TLS Contexts (2)									
Firewall (8)	GENERAL			OCSP					
Security Settings	Name	<ul> <li>MS Teams</li> </ul>		OCSP Server	Disable				
QUALITY	TLS Version	<ul> <li>TLSv1.2</li> </ul>		Primary OCSP Server	0.0.0.0				
	DTLS Version	Any		Secondary OCSP Server	0.0.0.0				
> DNS	Cipher Server	DEFAULT		OCSP Port	2560				
	Cipher Client	DEFAULT		OCSP Default Response	Reject				
F WED SERVICES	Cipher Server TL\$1.3	TLS_AES_256_GCM_SHA:	384:TLS_CHACHA20_POLY1305_SHA256:TLS						
HTTP PROXY	Cipher Client TLS1.3	TLS_AES_256_GCM_SHA	384:TLS_CHACHA20_POLY1305_SHA256:TLS						
	Key Exchange Groups	X25519:P-256:P-384:X448							
RADIUS & LDAP	Strict Certificate Extension V	Disable							
ADVANCED	DH key Size	2048							
PADANGED	TLS Renegotiation	Enable							
	Certificate Information >> Cha	nge Certificate >> Trus	ted Root Certificates >>						

	MONITOR TROUBLESHOOT	Save	Reset	Actions <del>-</del>	42	Admin <del>-</del>
M800B IP NETWORK SIGNALING & MEDIA	ADMINISTRATION			Ç Enti	ty, paramete	er, value
M8002       IP NETWORK       SIGNALING & MEDIA         Image: SRD       All       Image: SRD       All         Image: SRD       All       Image: SRD       Image: SRD         Image: SRD       CORE ENTITIES       Image: SRD       Image: SRD         Image: SRD       Image: SRD       Image: SRD       Image: SRD<	ADMINISTRATION	re				
	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.

	R TROUBLESHOOT	Save	Reset	Actions -	4	Admin <del>-</del>
M800B IP NETWORK SIGNALING & MEDIA AD	MINISTRATION			🔎 Entity	, parameter,	value
COLLICOCCES     SELUP     MONITO       MOXON     IP NETWORK     SIGMALING & MEDIA     AD       Image: State of the state	R     TRUELESHOOT         MINISTRATION         Image: Context [#1] > Certificate Information         PRUVATE KEY         Manu:         CERTIFICATE   CERTIFICATE Certificate Summer:	Save	Reset	Actions +	La constante	Admin - value
ADVANCED	9744c94873a746c9481754cTFaa3c4 3152c7678463148753683a54c92352537 35996u546479c3332420c7441424643 677219294553c1486461462426166 672234264784322260c7414246436 677219294553c148641464645 67223478478478478478478478478478478 56257847847847847847847847847847847847847847					
	X309-3 extensions: X309-3 Authority Key Identifier: keyid 8D 8C 3E C4-54 AD 8A.E1:77 E9 9B F9-9B 805 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.

	TROUBLESHOOT		Save Reset	Actions - 斗 Admin -
M800B IP NETWORK SIGNALING & MEDIA ADMIN	ISTRATION			
😧 🐨 SRD All 🔻				
CORE ENTITIES	TLS Context [#1] > Trusted Root Certificates			
IP Interfaces (2)	View			Import Export Remove
Ethernet Devices (2)	INDEX SUBJECT	ISSUER	EXPIRES	
Ethernet Groups (12)	0 Sectigo RSA Domain Validation S	USERTrust RSA Certification Aut	12/31/2030	
Physical Ports (12)	1 USERTrust RSA Certification Aut	AAA Certificate Services	12/31/2028	
Static Routes (0) HA Settings HA Network Monitor (0) NAT Translation (0)				
▲ SECURITY		He ee Page 1 of 1		View 1 - 2 of 2
TLS Contexts (2) Firewall (8)	Selected Row #0			
Security Settings	Certificate:			
> QUALITY	Data: Version: 3 (0x2)			
▶ DNS	Serial Wumber 7d 5b.51:26:b4:76:ba:11:db:74:16:0b:bc:53:0d:a7 Signature Algorithm: sha384/WimRSAEncryption Issuer: C2-US, ST=New Jersey, L=Jersey CHY, O=The USERTRUST Network,	CN=USERTrust RSA Certification Authority		
WEB SERVICES	Validity Not Before: Nov 2 00:00:00 2018 GMT Not After : Dec 31 23:59:59 2030 GMT			
HTTP PROXY	Subject: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=S Subject Public Key Info: Public Key Algorithm: rsaEncryption	Sectigo RSA Domain Validation Secure Server CA		
RADIUS & LDAP	RSA Fublic-Key: (2048 bit) Modulus: 00:06:73:33:d6:d7:3c:20:d0:00:d2:17:45:b8:d6:			
> ADVANCED	$\begin{array}{c} 3e\ 07-23\ 0.7\ 41\ ee\ 23\ 30\ ce\ b0\ 5c\ time\ 41\ 61\ 62\ 11\ 71\ 62\ 52\ 52\ 52\ 52\ 52\ 52\ 52\ 52\ 52\ 5$			v

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.

Realms				
GENERAL				
GENEIVE			QUALITY OF EXPERIENCE	
Index	0		QoE Profile	 ▼ View
Name	MR_LAN		Bandwidth Profile	 ▼ View
Topology Location	Down	$\checkmark$		
IPv4 Interface Name	#0 [LAN_IF]	▼ View		
UDP Port Range Start	6000			
Number Of Media Session Legs	100			
UDP Port Range End	6999			
TCP Port Range Start	0			
TCP Port Range End	0			
Default Media Realm	No	$\checkmark$		
		Cancel	APPLY	

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:
- IPv4 Interface Name:
- UDP Port Range Start:
- Number Of Media Session Legs:

Click on [Apply].

MR\_LAN (LAN media realm friendly name) LAN\_IF (see sub-section 3.1) 6000 100 (need to be calculated based on usage)

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

Click on [Apply].

MR\_WAN (WAN media realm friendly name) WAN\_IF (see sub-section 3.1) Up 7000 100 (need to be calculated based on usage)

## 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  $\Leftrightarrow$  MS Phone System and the SBC  $\Leftrightarrow$  OpenScape Business.

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

SIP Inte	rfaces						- x
		SRD	#0 [Def	aultSRD]			
	GENERAL			MEDIA			
	Index	0		Media Realm	#0 [MR_LAN]	View	
	Name	OSBiz_Trunk		Direct Media	Disable	~	
	Topology Location	Down	~				
	Network Interface	#0 [LAN_IF]	View	SECURITY			
	Application Type	SBC	~	TLS Context Name	#0 [default]	View	
	UDP Port	5060		TLS Mutual Authentication		$\checkmark$	
	TCP Port	0		Message Policy	_ v N	View	
	TLS Port	0		User Security Mode	Not Configured	$\checkmark$	
	Additional UDP Ports			Enable Un-Authenticated Registrations	Not configured	~	
	Additional UDP Ports Mode	Always Open	~	Max. Number of Registered Users	-1		
			Cancel	APPLY			

SIP Interfaces					- x			
TCP Port	0	Message Policy		View	^			
TLS Port	0	User Security Mode	Not Configured	$\checkmark$				
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	·			1			
Pre-Parsing Manipulation Set	- Vi	w						
CAC Profile	Vi	w						
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:
- Network Interface:
- Application Type: UDP Port:
- Enable TCP Keepalive:
- Classification Failure response Type:
- Media Realm:

OSBiz\_Trunk (SIP trunk with friendly name) LAN\_IF SBC 5060, as configured in OSBiz (TCP and TLS ports are set to 0, because the connection with OSBiz is UDP) Disable (keep default value) 500 (leave default setting) MR\_LAN

Click on [Apply].	
-------------------	--

SIP Inte	rfaces						– x
		SRD	#0 [De	faultSRD]			^
	GENERAL			MEDIA			
	Index	1		Media Realm	#1 [MR_WAN]	▼ View	
	Name	MS Teams_Trunk		Direct Media	Disable	~	
	Topology Location	Up	~				
	Network Interface	#1 [WAN_IF]	View	SECURITY			
	Application Type	SBC	~	TLS Context Name	#1 [MS Teams]	▼ View	
	UDP Port	0		TLS Mutual Authentication		~	
	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		~
			Cancel	APPLY			

SIP Interfa	ices						– ×
	TCP Port	0		Message Policy	-	View	~
	TLS Port	5061		User Security Mode	Not Configured	$\checkmark$	
	Additional UDP Ports			Enable Un-Authenticated Registrations	Not configured	~	
	Additional UDP Ports Mode	Always Open	$\checkmark$	Max. Number of Registered Users	-1		
	Encapsulating Protocol	No encapsulation	$\checkmark$	2			
	Enable TCP Keepalive	Enable	~				
	Used By Routing Server	Not Used	~				- 1
	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					~
			Ca	ncel			

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

- Name:
- Network Interface:
- Application Type:
- UDP Port:

WAN\_IF SBC 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 Contraction (recommended to prevent DoS attacks) MR\_WAN

System friendly name)

MS Teams\_Trunk (SIP trunk with MS Phone

- Enable TCP Keepalive:
- Classification Failure response Type:
- Media Realm:
- TLS Context Name:

Click on [Apply].

MS Teams
#### 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.

Proxy Sets					- x
	SRD	#0 [Defa	aultSRD]		^
GENERAL			REDUNDANCY		
Index	1		Redundancy Mode		~
Name	ProxySet_OSBiz		Proxy Hot Swap	Disable	~
Gateway IPv4 SIP Interface	-	✓ View	Proxy Load Balancing Method	Disable	~
SBC IPv4 SIP Interface	#0 [OSBiz_Trunk]	✓ View	Min. Active Servers for Load Balanci	ng 1	
TLS Context Name	#1 [MS Teams]	✓ View			
			ADVANCED		
KEEP ALIVE			Classification Input	IP Address only	~
Proxy Keep-Alive	Using OPTIONS	~	DNS Resolve Method		~
Proxy Keep-Alive Time [sec]	60				
Keep-Alive Failure Responses					~
		Cancel	APPLY		

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

- Name:
- SBC IPv4 SIP Interface:
- Proxy Keepalive:
- TLS Context Name:

ProxySet\_OSBiz (OSBiz proxy set friendly name) OSBiz\_Trunk (see sub-section 3.4) Using OPTIONS MS Teams (see sub-section 3.2)

Proxy Address	- x	
	^	
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: •
- Transport Type:

10.8.242.16:5060 (OSBiz IP / FQDN and port) UDP

Click on [Apply].

oxy Sets					-
	SRD	#0 [D	efaultSRD]		
GENERAL			REDUNDANCY		
Index	2		Redundancy Mode		~
Name	ProxySet_MS teams		Proxy Hot Swap	Enable	$\checkmark$
Gateway IPv4 SIP Interface		▼ View	Proxy Load Balancing Method	Random Weights	$\checkmark$
SBC IPv4 SIP Interface	#1 [MS Teams_Trunk]	▼ View	Min. Active Servers for Load Bal	ancing 1	
TLS Context Name	#1 [MS Teams]	▼ View			
			ADVANCED		
KEEP ALIVE			Classification Input	IP Address only	$\checkmark$
Proxy Keep-Alive	Using OPTIONS	~	DNS Resolve Method		$\checkmark$
Proxy Keep-Alive Time [sec]	60				
Keep-Alive Failure Responses					
		Cancel	APPLY		

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

- Name:
- SBC IPv4 SIP Interface:
- TLS Context Name: •
- **Proxy Keepalive:** •
- Proxy Hot Swap:

ProxySet\_MS teams (Teams proxy set friendly name)

- MS Teams\_Trunk (see sub-section 3.4)
- MS Teams (see sub-section 3.2) Using OPTIONS

Enable

Proxy Load Balancing Method: Random Weights

Proxy Addre	ess		- x
			~
G	ENERAL		
h	ndex	0	
F	Proxy Address	sip.pstnhub.microsoft.com:5061	
ד	Fransport Type	TLS 💙	
F	Proxy Priority	1	
P	Proxy Random Weight	1	
			~
		Cancel APPLY	

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

Proxy Address		– x
		~
GENERAL		
Index	2	
Proxy Address	sip3.pstnhub.microsoft.com:5061	
Transport Type	TLS	
Proxy Priority	3	
Proxy Random Weight	1	
		Y
	Cancel APPLY	

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

- Proxy Address:
- Transport Type:
- TLS 1, 2, 3 (for sip, sip2 and sip3 proxy addresses,

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)

- Proxy Priority: correspondingly)
- Proxy Random Weight: 1

#### 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.

	MONITOR TROUBLESHOOT	Save Reset Actions <del>-</del>	Admin <del>-</del>
M800B IP NETWORK SIGNALING & MEDIA	ADMINISTRATIÓN	🔎 Entity, j	parameter, value
🗲 🔿 SRD All 💌			
CORE ENTITIES  CORE S& PROFILES	Coder Group Name 0: AudioCodersGroups_0 v	▼ Delete Group	^
IP Profiles (2)	Coder Name Packetization Time Rate P	Payload Type Silence Suppression Coder Specific	1
Tel Profiles (0)	SILK-NB 20 8 7	103 N/A 🗸	
Coder Settings	SILK-WB V 20 V 16 V	104 N/A Y	
Coder Groups	G.711A-law V 20 V 64 V 8	8 Disabled V	
Allowed Audio Coders Groups (1)	G.7110-law ♥ 20 ♥ 64 ♥	0 Disabled V	
Allowed Video Coders Groups (0)		18 Disabled V	
▶ SBC			
GATEWAY			
▹ SIP DEFINITIONS			
MESSAGE MANIPULATION			
MEDIA			
▶ INTRUSION DETECTION			
	Cancel	APPLY	~

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		x
		~
GENERAL		
Index	0	
Name	AllowedAudioCoders	
		$\sim$
	Cancel APPLY	

acaud	iocodes setup			Save	Reset	Actions <del>-</del>	4 <mark>1</mark> 1	Admin <del>-</del>
M800B IP	NETWORK SIGNALING & ME	EDIA ADMINISTRATION				<i>⊃ Entit</i> y	, parameter	, value
💿 💿 SRD	Ali 👻							
	DGY VIEW	Allowed Audio Coders Gro	ups [#0] > Allowed Audio Coders (4)					
CORE ENTIT	TIES	+ New Edit m	re ee Page 1 of 1 as a	Show 10 V records per page				Q
CODERS & I	PROFILES		CODER	USER-D	FINED CODER			
IP Profiles (2	2)	0	G.711 A-law					
Tel Profiles (	(0)	1	G.711 U-law					
Coder Settin	gs	2	G.722					
Coder Group	DS	3	G.729					
Allowed Aud	lio Coders Groups (1)							
Allowed Vide	eo Coders Groups (0)							
▶ SBC		#0					E	dit
GATEWAY								
SIP DEFINIT	IONS	GENERAL						
		Coder • G	711 A-law					
MESSAGE N	IANIPULATION	User-defined Coder						
MEDIA								
▶ INTRUSION	DETECTION							
		-						

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.

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	$\checkmark$
MEDIA SECURITY			Session Expires Mode	Transparent	$\checkmark$
SBC Media Security Mode	Not Secured	$\checkmark$	SIP UPDATE Support	Supported	$\checkmark$
Gateway Media Security Mode	Preferable	✓	Remote re-INVITE	Supported	$\checkmark$
Symmetric MKI	Disable	~	Remote Delayed Offer Support	Supported	$\checkmark$
MKI Size	0		MSRP re-INVITE/UPDATE	Supported	$\checkmark$
SBC Enforce MKI Size	Don't enforce	~	MSRP Offer Setup Role	ActPass	$\checkmark$
SBC Media Security Method	SDES	~	MSRP Empty Message Format	Default	$\checkmark$
Reset SRTP Upon Re-key	Disable	~	Remote Representation Mode	According to Operation Mode	~
		Cancel	APPLY		
N6		Cancel	APPLY		
25 Remnte Can Play Rinnhack	Yes	Cancel	APPLY		
25 Remote Can Play Ringback Generate RTP	Yes	Cancel	APPLY SBC FORWARD AND TRANSFER	2	
25 Remote Can Play Ringback Generate RTP	Yes None	Cancel	APPLY SBC FORWARD AND TRANSFER Remote REFER Mode	R Handle Locally	
Remote Can Play Ringback Generate RTP SBC MEDIA	Yes None	Cancel	APPLY SBC FORWARD AND TRANSFEI Remote REFER Mode Remote Replaces Mode	R Handle Locally Handle Locally	<b>Y</b>
25 Remote Can Play Ringback Generate RTP SBC MEDIA Mediation Mode	Yes None	Cancel	APPLY SBC FORWARD AND TRANSFER Remote REFER Mode Remote Replaces Mode Play RBT To Transferee	R Handle Locally Handle Locally No	<b>&gt;</b>
Remote Can Play Ringback Generate RTP SBC MEDIA Mediation Mode Extension Coders Group	Yes None RTP Mediation	Cancel	APPLY SBC FORWARD AND TRANSFEI Remote REFER Mode Remote Replaces Mode Play RBT To Transferee Remote 3xx Mode	R Handle Locally Handle Locally No Handle Locally	<b>&gt;</b> <b>&gt;</b> <b>&gt;</b>
25 Remote Can Play Ringback Generate RTP SBC MEDIA Mediation Mode Extension Coders Group Allowed Audio Coders	Yes None RTP Mediation	Cancel	APPLY SBC FORWARD AND TRANSFER Remote REFER Mode Remote Replaces Mode Play RBT To Transferee Remote 3xx Mode	R Handle Locally Handle Locally No Handle Locally	Y Y Y
25 Remote Can Play Ringback Generate RTP SBC MEDIA Mediation Mode Extension Coders Group Allowed Audio Coders Allowed Coders Mode	Yes None RTP Mediation - Restriction	Cancel	APPLY SBC FORWARD AND TRANSFER Remote REFER Mode Remote Replaces Mode Play RBT To Transferee Remote 3xx Mode SBC HOLD	R Handle Locally Handle Locally No Handle Locally	V V V
Remote Can Play Ringback Generate RTP SBC MEDIA Mediation Mode Extension Coders Group Allowed Audio Coders Allowed Coders Mode	Yes None RTP Mediation - Restriction	Cancel	APPLY SBC FORWARD AND TRANSFEI Remote REFER Mode Remote Replaces Mode Play RBT To Transferee Remote 3xx Mode SBC HOLD Remote Hold Format	R Handle Locally Handle Locally No Handle Locally	
25 Remote Can Play Ringback Generate RTP SBC MEDIA Mediation Mode Extension Coders Group Allowed Audio Coders Allowed Coders Mode Allowed Video Coders	Yes None RTP Mediation - Restriction -	Cancel	APPLY SBC FORWARD AND TRANSFEI Remote REFER Mode Remote Replaces Mode Play RBT To Transferee Remote 3xx Mode SBC HOLD Remote Hold Format Reliable Held Tone Source	R Handle Locally Handle Locally No Handle Locally Transparent Yes	

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

~

~

Cancel APPLY

SBC FAX

Fax Coders Group

Name: •

Direct Media Tag

RFC 2833 Mode

RFC 2833 DTMF Payload Type

Alternative DTMF Method

SBC Media Security Mode: •

As Is

0

As Is

**OSBiz** (friendly name for OSBiz) Not Secured

•

- P-Asserted-Identity Header Mode:
- Remote REFER Mode:
- Remote Replaces Mode:
- Remote 3xx Mode:

As Is Handle Locally Handle Locally Handle Locally

IP Profil	es							_ >
	GENERAL			SBC SIGNALING				
	Index	1		PRACK Mode		Transparent	~	
	Name	MS Teams		P-Asserted-Identity Header Mo	ode	As Is	~	
	Created by Routing Server	No		Diversion Header Mode		As Is	$\checkmark$	
				History-Info Header Mode		As Is	~	
	MEDIA SECURITY			Session Expires Mode		Transparent	~	
	SBC Media Security Mode	Secured	-	SIP UPDATE Support		Not Supported	~	
	Gateway Media Security Mode	Preferable		Remote re-INVITE		Supported only with SDP	~	
	Symmetric MKI	Disable	-	Remote Delayed Offer Support	t	Not Supported	~	
	MKI Size	0		MSRP re-INVITE/UPDATE		Supported	~	
	SBC Enforce MKI Size	Don't enforce	-	MSRP Offer Setup Role		ActPass	$\checkmark$	
	SBC Media Security Method	SDES	-	MSRP Empty Message Forma	at	Default	$\checkmark$	
	Reset SRTP Upon Re-key	Disable	-	Remote Representation Mode		According to Operation Mode	~	
		c	ancel	APPLY				
IP Profile	es				_		– x	
	SBC EARLY MEDIA		IS	SUP Body Handling	Transpa	arent	~	<ul> <li></li> </ul>
	Remote Early Media	Supported	IS	SUP Variant	ltu92		$\checkmark$	

			Cancel	APPLY		
	Extension Coders Group	-	•	Remote 3xx Mode	Handle Locally	$\sim$
	Mediation Mode	(TP Mediation	~	Play RBT To Transferee	No	
	SBC MEDIA			Remote Replaces Mode	Standard	
				Remote REFER Mode	Handle Locally	
	Generate RTP	None	$\checkmark$	SBC FORWARD AND TRANSFER		
	Remote Can Play Ringback	Yes	$\checkmark$			_
	Remote RFC 3960 Support	Not Supported	~	NAT TCP Registration Time	-1	
	Remote Early Media RTP Detection Mod	e By Media	$\checkmark$	NAT UDP Registration Time	-1	
	Remote Multiple Answers Mode	Disable	~	User Registration Time	0	
	Remote Multiple Early Dialogs	According to Operation Mode	$\checkmark$	SBC REGISTRATION		
	Remote Early Media Response Type	Transparent	$\checkmark$			
	Remote Multiple 18x	Supported	~	Max Call Duration [min]	0	
£						

IP Profiles					– x
Generate RTP	None	>	SBC FORWARD AND TRANSFER	ł	^
			Remote REFER Mode	Handle Locally	]
SBC MEDIA			Remote Replaces Mode	Standard	]
Mediation Mode	RTP Mediation	$\checkmark$	Play RBT To Transferee	No	]
Extension Coders Group		•	Remote 3xx Mode	Handle Locally	]
Allowed Audio Coders	#0 [AllowedAudioCoders]	View			
Allowed Coders Mode	Preference		SBC HOLD		
Allowed Video Coders	- •	View	Remote Hold Format	Inactive	]
Allowed Media Types			Reliable Held Tone Source	Yes	]
Direct Media Tag			Play Held Tone	No	]
RFC 2833 Mode	As Is	$\checkmark$			
RFC 2833 DTMF Payload Type	0		SBC FAX		
Alternative DTMF Method	As Is	~	Fax Coders Group	- •	]
Send Multiple DTMF Methods	Disable	$\checkmark$	Fax Mode	As Is	1
		Cancel	APPLY		

IP Profiles					-	x
Adapt RFC2833 BW to Voice coder BV	/ Disabled	~	Fax Offer Mode	All coders	$\checkmark$	~
SDP Ptime Answer	Remote Answer	$\checkmark$	Fax Answer Mode	Single coder	$\checkmark$	
Preferred PTime	0		Remote Renegotiate on Fax Detection	Transparent	$\sim$	
Use Silence Suppression	Add	$\checkmark$	Fax Rerouting Mode	Disable	$\checkmark$	
RTP Redundancy Mode	As Is	$\checkmark$				
RTCP Mode	Generate Always	$\checkmark$	MEDIA			
Jitter Compensation	Disable	~	Broken Connection Mode	Disconnect	~	
ICE Mode	Lite		Media IP Version Preference	Only IPv4	$\checkmark$	
SDP Handle RTCP	Don't Care	$\checkmark$	RTP Redundancy Depth	Disable	~	
RTCP Mux	Not Supported	$\checkmark$				
RTCP Feedback	Feedback Off	$\checkmark$	GATEWAY			
Voice Quality Enhancement	Disable	$\checkmark$	Early Media	Disable	$\checkmark$	
Max Opus Bandwidth	0		Early 183	Disable	~	
Generate No-Op Packets	Disable	$\checkmark$	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:
- SBC Media Security Mode: Remote Early Media RTP Detection Mode:
- Allowed Audio Coders: 3.6). Allowed Coders Mode:

MS Teams (friendly name for Teams) Secured

By Media (required, as Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18x response) AllowedAudioCoders (see sub-section

Preference (re-arranges the codecs in SDP for messages coming from Teams side by prioritizing the coders configured in *AllowedAudioCoders* group) Add

• Use Silence Suppression:

- RTCP Mode:
- ICE Mode: Teams)
- Remote Update Support:
- Remote re-INVITE Support:
- Remote Delayed Offer Support:
- Remote REFER Mode:
- Remote 3xx Mode:
- Remote Hold Format: answer

Generate Always (in case RTCP packets aren't generated, but Teams expects them) Lite (required only if Media Bypass enabled on

Not Supported Supported Only With SDP Not Supported Handle Locally Handle Locally Inactive (some SIP trunks with IP-PBXs may

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.

IP Grou	25					-
		SRD	#0 [Defa	ultSRD]		
	GENERAL			QUALITY OF EXPERIENCE		
	Index	1		QoE Profile		r View
	Name	OSBiz		Bandwidth Profile		r View
	Topology Location	Down	$\checkmark$			
	Туре	Server	~	MESSAGE MANIPULATION		
	Proxy Set	#1 [ProxySet_OSBiz]	View	Inbound Message Manipulation Set	1	
	IP Profile	#2 [OSBiz]	View	Outbound Message Manipulation Set	2	
	Media Realm	#0 [MR_LAN]	View	Message Manipulation User-Defined Str	ing 1	
	Internal Media Realm	- •	View	Message Manipulation User-Defined Str	ring 2	
	Contact User			Proxy Keep-Alive using IP Group setting	js Disable	$\checkmark$
	SIP Group Name					
			Cancel	APPLY		

SBC GENERAL					
ODO GENERAL			User UDP Port Assignment	Disable	~
Classify By Proxy Set	Enable	$\checkmark$	Authentication Mode	User Authenticates	~
SBC Operation Mode	Not Configured	$\checkmark$	Authentication Method List		
SBC Client Forking Mode	Sequential	$\checkmark$	SBC Server Authentication Type	According to Global Parameter	~
CAC Profile	-	✓ View	OAuth HTTP Service		▼ View
SIP Source Host Name			Username		
			Password		
ADVANCED					
			GATEWAY		
Local Host Name			SIP Re-Routing Mode		~
UUI Format	Disable	~	Always Use Route Table	No	~
Always Use Src Address	Yes	$\checkmark$			
			GW GROUP STATUS		
SBC ADVANCED			GW Group Registered IP Address		
		0			

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

- Name:
- Proxy Set:
- IP Profile:
- Media Realm:
- Inbound Message Manipulation Set:
- Outbound Message Manipulation Set:
- Classify By Proxy Set:
- Always Use Src Address:

OSBiz (friendly name for OSBiz) ProxySet\_OSBiz (see sub-section 3.5) OSBiz (see sub-section 3.7) MR\_LAN (see sub-section 3.3) 1, (see sub-section 3.11) 2, (see sub-section 3.11) Enable Yes

Click	on	[Apply].
-------	----	----------

IP Grou	ps							-	x
		SRD	#	0 [Defa	aultSRD]				^
	GENERAL				QUALITY OF EXPERIENCE				
	Index	2			QoE Profile		•	View	
	Name	MS Teams			Bandwidth Profile	Bandwidth Profile		View	
	Topology Location	Up							
	Туре	Server			MESSAGE MANIPULATION				
	Proxy Set	#2 [ProxySet_MS teams]	View		Inbound Message Manipulation Set	t	-1		
	IP Profile	#1 [MS Teams]	View		Outbound Message Manipulation S	et	-1		
	Media Realm	#1 [MR_WAN]	View		Message Manipulation User-Defined	String 1			
	Contact User				Message Manipulation User-Defined	String 2	2		
	SIP Group Name				Proxy Keep-Alive using IP Group setti	ings	Enable	~	
	Created By Routing Server	No							~
			Car	ncel	APPLY				

25					
Proxy Set Connectivity	Connected		Max. Number of Registered Users	-1	
			Registration Mode	User Initiates Registration	~
SBC GENERAL			User Stickiness	Disable	~
Classify By Proxy Set	Disable	~	User UDP Port Assignment	Disable	~
SBC Operation Mode	Not Configured	~	Authentication Mode	User Authenticates	~
SBC Client Forking Mode	Sequential	$\sim$	Authentication Method List		
CAC Profile	- *	View	SBC Server Authentication Type	According to Global Parameter	~
			OAuth HTTP Service	-	▼ View
ADVANCED			Username		
	sbc01.athdrlabs.xyz		Password		
Local Host Name					
		NUT2	GATEWAY		
UUI Format	Disable		SIP Re-Routing Mode		×
Always Use Src Address	Yes		Always Use Route Table	No	~
		Cancel	APPLY		

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

- Name:
- Topology Location:
- Type:
- **Proxy Set**: 3.5)
- IP Profile:
- Media Realm:
- Classify By Proxy Set:
- Local Host Name:

Up Server ProxySet\_MS Teams (see sub-section MS Teams (see sub-section 3.7) MR\_WAN (see sub-section 3.3) Disable sbc01.athdrlabs.xyz (public FQDN for SBC in Teams tenant, see sub-section

MS Teams (friendly name for Teams)

2.1) <mark>Yes</mark>

- Always Use Src Address:
- 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.

	MONITOR TROUBLESHOOT		Save Reset	Actions <del>-</del>	, Admin <del>→</del>
M800B IP NETWORK SIGNALING & MEDIA	ADMINISTRATIÓN			🔎 Entity,	parameter, value
🔶 🧼 SRD All 🔻					
CTOPOLOGY VIEW	Media Security				
CORE ENTITIES	GENERAL		AUTHENTICATION & ENCRYPTION		
CODERS & PROFILES	Media Security	Enable	Authentication on Transmitted RTP Packets	Active	~
▶ SBC	Media Security Behavior	Preferable 🗸	Encryption on Transmitted RTP Packets	Active	~
► GATEWAY	Offered SRTP Cipher Suites	All	Encryption on Transmitted RTCP Packets	Active	$\checkmark$
SIP DEFINITIONS	ARIA Protocol Support	Disable 🗸	SRTP Tunneling Authentication for RTP	Disable	$\checkmark$
MESSAGE MANIPULATION			SRTP Tunneling Authentication for RTCP	Disable	$\checkmark$
▲ MEDIA	MASTER KEY IDENTIFIER				
Media Security	Master Key Identifier (MKI) Size	0			
Voice Settings	Symmetric MKI	Disable 🗸			
Fax/Modem/CID Settings					
DSP Settings					
Quality of Experience					
INTRUSION DETECTION					
		Cancel	APPLY		

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.

Message Conditio	ns		– x
			~
GENERA	L		
Index		0	
Name		MS Teams-Contact	
Conditio	'n	header.contact.url.host contains 'pstnhub.microsoft.com'	
			~
		Cancel APPLY	

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.

cation				
	SRD #	0 [DefaultSRD]		
MATCH		ACTION		
Index	0	Action Type	Allow	~
Name	MS Teams	Destination Routing Policy	-	✓ View
Source SIP Interface	#1 [MS Teams_Trunk]	IP Group Selection	Source IP Group	$\checkmark$
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.athdrlabs.xyz			
Message Condition	#0 [MS Teams-Contact] View	r		
	Car	ncel APPLY		

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

MS Teams (rule friendly name)

- Name:
- Source SIP Interface: Source IP Address:
- Destination Host:
- Message Condition:
- Action Type:
- Source IP Group:

52.114.\*.\* (Teams public proxies FQDNs resolve to 52.114.\*.\* IPs; see sub-sections 3.5 and 3.13) sbc01.athdrlabs.xyz (public FQDN for SBC in Teams tenant, see sub-section 2.1) MS Teams-Contact Allow MS Teams (see sub-section 3.8)

MS Teams\_Trunk (see sub-section 3.4)

#### 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:



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 ]

00	audiocodes	SETUP	MONITOR TF	ROUBLESHOOT					Save	Reset	Actions -	4	Admin <del>-</del>
M800B	IP NETWORK	SIGNALING & MEDIA	ADMINISTRA	TION							,⊖ En	tity, parameter,	value
• •	) SRD All	<b>*</b>											
۵1	TOPOLOGY VIEW		Message Ma	anipulations (4)									^
► C	ORE ENTITIES		+ New Edit	Insert 🛧 🖡	Ê	e 🛶 Page 1 of '	⊳ ⊨ Show 10 ∨	records per page					Q
) C	ODERS & PROFILES		INDEX 🚖	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTI	ON VALUE	ROW ROLE	
> SE	BC		1		1	reinvite.request	param.message.sdp.	1 var.call.src.0	Modify	'1'		Use Current	Conditio
			2		1			param.message.sdp.rl	Modify	'send	recv'	Use Previous	s Conditi
) G/	ATEWAY		3		2	reinvite.response.200	var.call.src.0=='1'	param.message.sdp.rf	Modify	'recvo	only'	Use Current	Conditio
> SI	IP DEFINITIONS		4		2			var.call.src.0	Modify	'0'		Use Previou:	s Conditi
Me	essage Manipulations (4) essage Conditions (1)		#1									Edit	Ť
Pre	e-Parsing Manipulation Sets ((	0)	GENERAL				ACT	ION					
		- /	Name				Acti	on Subject	<ul> <li>var.call.src.</li> </ul>	0			
► M	EDIA		Manipulatio	n Set ID	• 1		Acti	on Type	<ul> <li>Modify</li> </ul>				
⇒ IN	ITRUSION DETECTION		Row Role		Use Current Condition		Acti	on Value	• '1'				
			MATCH										
			Message Ty	pe	<ul> <li>reinvite.request</li> </ul>								
			Condition		<ul> <li>param.message.sdp.rtpn</li> </ul>	node=='sendonly'							
													~

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

## $\label{eq:setup} \ensuremath{\mathsf{SETUP}} >> \ensuremath{\mathsf{SIGNALING}} \& \ensuremath{\mathsf{MEDIA}} >> \ensuremath{\mathsf{MESSAGE}} & \ensuremath{\mathsf{MANIPULATION}} >> \ensuremath{\mathsf{Message}} \\ \ensuremath{\mathsf{Manipulations}}. \end{aligned}$

#### 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.

IP-to-IP	Routing						- ×	k		
		Routing Policy #0	[Default_	SBCRoutingPolicy]			,			
	GENERAL			ACTION						
	Index	0		Destination Type	Dest Address	~				
	Name	Terminate OPTIONS		Destination IP Group	- •	View				
	Alternative Route Options	Route Row		Destination SIP Interface		View				
_				Destination Address	internal					
	MATCH			Destination Port	0					
	Source IP Group	Any View		Destination Transport Type		~	- 1			
	Request Type	OPTIONS		IP Group Set		View				
	Source Username Pattern	*		Call Setup Rules Set ID	-1					
	Source Host	*		Group Policy	Sequential	~				
	Source Tag			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:
- Source IP Group:
- Request Type:
- Destination Type:
- Destination Address:

Terminate OPTIONS (friendly name) Any OPTIONS Dest Address internal

IP-to-IP	Routing				-
		Routing Policy #0 [Def	fault_SBCRoutingPolicy]		
	GENERAL				
-	GENERAL		ACTION		
	Index	1	Destination Type	Request URI	$\checkmark$
	Name	REFER from MS Teams	Destination IP Group	#2 [MS Teams]	View
	Alternative Route Options	Route Row	Destination SIP Interface		View
			Destination Address		
	MATCH		Destination Port	0	
	Source IP Group	Any View	Destination Transport Type		$\checkmark$
	Request Type	All	IP Group Set	🔻	View
	Source Username Pattern	*	Call Setup Rules Set ID	-1	
	Source Host	*	Group Policy	Sequential	$\checkmark$
	Source Tag		Cost Group		View
		Cancel	APPLY		

IP-to-IP Routing				– x
Alternative Route Options	Route Row	Destination SIP Interface		View
		Destination Address		
MATCH		Destination Port	0	
Source IP Group	Any <b>view</b>	Destination Transport Type		~
Request Type	All	IP Group Set		View
Source Username Pattern	*	Call Setup Rules Set ID	-1	
Source Host	*	Group Policy	Sequential	~
Source Tag		Cost Group		View
Destination Username Pattern	*	Routing Tag Name	default	
Destination Host	*	Internal Action		Editor
Destination Tag				
Message Condition	View	r		
Call Trigger	REFER	]		
ReRoute IP Group	#2 [MS Teams] View	,		$\checkmark$
	Ca	ncel 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:
- Source IP Group:
- Destination Type:
- Destination IP Group:
- Call Trigger:
- ReRoute IP Group:

Click on [Apply].

REFER from MS Teams (friendly name)

- Any Request URI
- MS Teams (see sub-section 3.8) REFER
- MS Teams (see sub-section 3.8)

P-to-IP Routing				_ >
	Routing Policy #0 [De	fault_SBCRoutingPolicy]		í
GENERAL		ACTION		
Index	2	Destination Type	IP Group	$\sim$
Name	MS Teams to OSBiz	Destination IP Group	#1 [OSBiz] 👻 V	ïew
Alternative Route Options	Route Row	Destination SIP Interface	- <b>v</b>	liew
		Destination Address		
MATCH		Destination Port	0	
Source IP Group	#2 [MS Teams] View	Destination Transport Type		~
Request Type	All	IP Group Set	- • V	liew
Source Username Pattern	*	Call Setup Rules Set ID	-1	
Source Host	*	Group Policy	Sequential	$\checkmark$
Source Tag		Cost Group	- V	liew
	Cance	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:
- Source IP Group:
- Destination Type:
- Destination IP Group:

MS Teams to OSBiz (friendly name) MS Teams (see sub-section 3.8) IP Group OSBiz (see sub-section 3.8)

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

OSBiz to MS Teams (friendly name) OSBiz (see sub-section 3.8) IP Group MS Teams (see sub-section 3.8).

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

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<br="">Server IP&gt; (e.g. 8.8.8.8)</public>	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:
-----	----------	-------	----	-----	------	------	-----	--------	--------

	MONITOR TROUBLESHO			Save	e Reset		<mark>12</mark>	Adm
00B IP NETWORK SIGNALING & MED	IA ADMINISTRATION					₽ Eni	tity, paramete	er, valu
→ SRD All ▼								
	5							
A NETWORK VIEW	Firewall (8)							
CORE ENTITIES		-		7				0
4.555(19)77/	+ New Edit 🛧 🖡	🔲 🔤 😽 Page	1 of 1 ▷ ▷ Show 10 ∨	records per page				$\mathcal{O}$
SECORITY	INDEX 💠	DESCRIPTION	ACTION U	IPON MATCH	MATCH	OUNT		
TLS Contexts (2)	0	8.8.8.8	Allow		317357			
Firewall (8)	1	52.114.148.0	Allow		14676			
Security Settings	2	52.114.132.46	Allow		520773			
QUALITY	3	52.114.75.24	Allow		698337			
	4	52.114.76.76	Allow		40755			
DNS	6	52.114.7.24	Allow		472010			
WEB SERVICES	49	0.000	Block		234857			
HTTP PROXY	#0						Edit	
RADIUS & LDAP								
ADVANCED	MATCH		ACTI	ON				
	Description	• 8.8.8.8	Actio	n Upon Match	Allow			
	Source IP	• 8.8.8.8	Packe	et Size (	0			
	Source Port	0	Byte	Rate	0			
	Prefix Length	• 32	Byte	Burst	0			
	Start Port	0			-			
	End Port	65535						
	Bratesal	65555 Ami	STAT	IISTICS				
		Any a factor	Matc	h Count	317357			
	Use specific interface	- cridble						
	Interface Name	<ul> <li>WAN_IF</li> </ul>	View					

# 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: <u>https://community.te-systems.de/community-download/files?fileId=2587</u>.

#### 4.1. anynode Wizard – Teams / Voice over IP Provider

anynode*			User: a Copyright © 2021 by TE-SYSTED	anadmin (write VIS GmbH, Ge	e access), Sessi ermany, State: c	ion Timed	TE-SYS competence in put: 30 minutes, Co I, License active: y	TEMS e-communications mmitted: yes es, Trace: off
Wizard Configuration - Objects -	My Account - Extras -	Info 👻			Com	nmit	Monitor Mode	Logout
Information         Tracing         Licenses         Network Interfaces         ▼ Configuration         Routing Domains         Nodes         Routing Forward Profiles         Authentication Profiles         Directories         Load Balancers         ▶ Conditions         Time Ranges	Product		anynode 4.2.6 (Release, Windows x86 (64 bit)) Monitor 4.2.6 (Release, Windows x86 (64 bit)) Administration 4.2.6 (Release, Windows x86 (64 bit)) Administration 4.2.6 (Release, Windows x86 (64 bit)) Frontend 4.2.6 (Release, Windows x86 (64 bit)) Java 1.8.0_275 (AdoptOpenJDK) - used by the Frontend web server OpenSSL 11.11 is Dec 2020					Ш
Auxiliary Objects	Copyright		https://www.te-systems.de					
	Virtualization		vmware					
	Firewalls		Windows Advanced Firewall - disabled					Ŧ
Version: 4.2.6				💶 Off	<b>40%</b>	0%	24%	0

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

Click on "Wizard".

Scenarios	X
The assistants below provide easy to use methods to speed up frequently occuring configurat Select one of the following entries to get a detailed description of the tasks that will be handled	ion tasks. d by the respective assistant.
Assistant            Create relationship between         a VoIP Provider and a PBX or VoIP System         two PBXs or VoIP Systems         Microsoft Teams Direct Routing and a VoIP Provider        Microsoft Teams Direct Routing and a PBX or VoIP System        Microsoft Teams Direct Routing, a VoIP Provider and a PBX or VoIP System        Microsoft Teams Direct Routing, a VoIP Provider and a PBX or VoIP System        Microsoft Skype for Business and a VoIP Provider        Microsoft Skype for Business, a VoIP Provider and a PBX or VoIP System        Microsoft UCMA Application Node and XCAPI        a Microsoft UCMA Application Node and a UC Application (SIP)        a Microsoft UCMA Application Node and a SIP Phones Node        a Microsoft UCMA Application Node and a PBX or VoIP System        a Microsoft UCMA Application Node and a PBX or VoIP System        a Microsoft UCMA Application Node and a PBX or VoIP System        a Microsoft SIB Voicemail System and a PBX or VoIP System	This assistant aids you in creating a Microsoft Teams Direct Routing Node and a PBX or VoIP System Node. These new nodes can be interconnected by direct or dial string routing.
Add      Other Scenarios	
	Start Cancel

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.

cenarios » Node Interconnection Assistant			
Microsoft Teams Direct Routing Configuration of Microsoft Teams Dire	and VoIP System		
Microsoft Teams Direct Routing	Please enter your Micros	It Teams Direct Routing configuration.	
Voice over IP System	Node Type	<ul> <li>Microsoft Teams Direct Routing</li> </ul>	
Routing	Name	= Microsoft Teams Direct Routing	
	Network Controller	<ul> <li>Name = Microsoft Teams Direct Root</li> <li>Interface =</li> <li>IP Version = IP version 4</li> <li>IP Address = [Any IP address]</li> <li>Reverse DNS Lookup = Enabled [Default]</li> </ul>	uting
	Port	= 5060 [Default]	
	TLS Port	= 5067	
	Certificate & Private Key	<ul> <li>Certificate and key missing</li> </ul>	
	Certificate chain	= [None]	
	SIP Interconnection	= SIP Trunk	
	Remote SIP Domain	<ul> <li>sip:sip.pstnhub.microsoft.com</li> </ul>	
	Incoming Manipulations	= [None]	
	Outgoing Manipulations	= [None]	
		Ocn	figure
	< Previous	Next > Finish C:	ancel

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

Scenarios » Node Interconnection Assistant » Microsoft Teams Direct Routing X **Create New Node** Choice of Microsoft Teams Node type. 🤣 Microsoft Teams Microsoft Teams Direct Routing This option is the default setup to create a Microsoft Teams Direct Routing connection. For most use-cases Network Controller this is the right choice. Ports O Microsoft Teams Direct Routing Carrier Trunk This option can be used to create an initial and successive connections to Microsoft Teams Direct Routing Certificate & Private Key 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 Certificate Chain during the initial setup. SBC FQDN 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 Name geographically separate locations. In this case the media-flow can be optimized by the network/Teams/anynodeadministrator 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.

	-	~
Create New Node Network Controller selection	L.	
🤣 Microsoft Teams	You may restrict the operation of a node to a specific network controller. The restriction may consist of a spec network interface and/or IP address to be used for SIP and media transport of this node.	ific
Network Controller Ports Certificate & Private Key Certificate Chain SBC FQDN Name	Network Controller © Create new network controller. Name Microsoft Teams Direct Routing Network © Use a fixed IP address ?	
Name	<ul> <li>Use an interface's address ?</li> <li>Intel(R) 82574L Gigabit Network Connection #3</li> <li>IP version 4</li> <li>Currently: 195.97.14.76</li> <li>Advanced configuration ?</li> <li>Open</li> <li>Specify whether reverse DNS lookup is enabled</li> <li>Enabled Disabled</li> <li>Select existing network controller.</li> </ul>	~
	[None]  Sector change include in the initial initia initial initial initial initial	·

Enter the following:

- Name: name).
- Use an interface's address:

Microsoft Teams Direct Routing (common-sense

<*Windows WAN machine ethernet adapter>* IP version 4 (IP Version) 195.97.14.76 (Public IP Address).

#### Click on [Next].

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

### 4.3. anynode Wizard – Teams / Ports

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



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

#### 4.4. anynode Wizard – Teams / Certificate & Private Key

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

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

Scenarios » Node Interconnection As	sistant » Microsoft Teams Direct Routing	×
Create New Node Determination of the certifica	ate and private key.	
<ul> <li>Microsoft Teams</li> <li>Network Controller</li> <li>Ports</li> <li>Certificate &amp; Private Key</li> <li>Certificate Chain</li> </ul>	<ul> <li>Provide a certificate and an associated private key.</li> <li>With these two values anynode can authenticate and open a secure channel to a peer later. Therefore, it important that the peer will accept the offered certificate.</li> <li>Private Key</li> <li>No private key present.</li> </ul>	is
SBC FQDN Name	No certificate present.	
	Configure Remove     I do not want to provide a certificate and an associated private key yet.	
	< Previous Next > Finish Cancel	

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

Scenarios » Node Interconnection Assistant » Microsoft Teams Direct Routing » Certificate and Private Key Assistant		
Configure a certificate a Choice of assistant approa	and a private key ch.	
Select Action	There are <b>several options</b> to choose from, with whom the <b>certificate and the private</b> <b>key</b> can be <b>edited or changed</b> . Please select an option.	
Import Files	Request a certificate from a Microsoft Windows domain.	
	© Generate a certificate signing request (CSR) and an associated private key.	
	Renew a certificate signing request (CSR) and an associated private key.	
	O Generate a self-signed certificate and an associated private key.	
	Renew a self-signed certificate and an associated private key.	
	Import of the certificate and/or private key.	
	C Export the certificate.	
	< Previous Next > Finish Cancel	

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

Scenarios » Node Interconnection Assistant	» Microsoft Teams Direct Ro	uting » Certificate and Private Key Assistant	×
Configure a certificate and a p Import of certificates and/or private	e keys.		
Select Action	Select the files you want to imported if the configuration	o import. If the file contains multiple certificates, then all will n field allows it.	be
✓ Import Files	must be used <u>twice</u> . The following formats are supported: .cer, .crt, .der, .pem, .p7b, .pk7, .p12, .pfx		
	C:\Users\Mike\Deskto	Browse	
	Upload completed.		
	Drivete Key		
	Private Key		_
	Key Type : RSA		
	Key Size : 2048 Bits		
	Certificate		
	Version	: V3	-
	Subject	: CN=sbc01.athdrlabs.xyz	
	Subject Alternative Names	: sbc01.athdrlabs.xyz (DNS) www.sbc01.athdrlabs.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=S ectigo Limited, L=Salford, ST=Greater Manchester, C=GB	
	Serial	: 205090756ee657a975688951230389c2	_
	Signing Algorithm	: RSA with SHA-256	
	Fingerprint Algorithm	: SHA-1	
	Fingerprint	: FC50F8C4AEB74BC67EBB0281BEC7E7B819DDCB98	-
	< Previous	Next > Finish Cancel	

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

Scenarios » Node Interconnection As	sistant » Microsoft Teams Direct Routing	×
Create New Node Determination of the certifica	te and private key.	
<ul> <li>Microsoft Teams</li> <li>Network Controller</li> </ul>	Provide a certificate and an associated private key. With these two values anynode can authenticate and open a secure channel to a peer later. The important that the peer will accept the offered certificate.	herefore, it is
Ports	Private Key	
Certificate & Private Key Certificate Chain	Key Type : RSA Key Size : 2048 Bits	
SBC FQDN	Certificate	
Name	Version:V3Subject:CN=sbc01.athdrlabs.xyzSubject Alternative Names:sbc01.athdrlabs.xyz (DNS) www.sbc01.athdrlabs.xyz (DNS)Valid From:2021-01-18 03:00:00Valid Until:2022-01-19 02:59:59Issuer:CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo L alford, ST=Greater Manchester, C=GBSerial:205090756ee657a975688951230389c2Signing Algorithm:RSA with SHA-256Fingerprint Algorithm:SHA-1Fingerprint:FC50F8C4AEB74BC67EBB0281BEC7E7B819DDCB98Usage:Verification of digital signatures. Enciphering private or secret keys.Extended Usage:Server authentication Client authenticationCertificate Authority:no	.imited, L=S
	Configure      F      O I do not want to provide a certificate and an associated private key yet.	Remove
	< Previous Next > Finish	Cancel

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.

Scenarios » Node Interconnection Assi	stant » Microsoft Teams Direct Routing	9		×
Create New Node				
Determination of an optional of	ertificate chain.			
🤣 Microsoft Teams	If a certificate chain is needed in ad following list.	dition to the single certificate, then the	ese certificates can	be added to the
Network Controller	Cartificate abain			
🤣 Ports				
🤣 Certificate & Private Key	Certificate Issuer	Certificate Subject	Valid From	Valid Until
🤣 Certificate Chain	CN=USERTrust RSA Certification Au	CN=Sectigo RSA Domain Validation	2018-11-02 03:00	2031-01-01 02:59
SBC FQDN				
Name				
				_
	Request Chain	Add	Edit	Remove
	< F	Previous Next >	Finish	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	of the SBC.		
🤣 Microsoft Teams	Determine the name for the FQDN of the SBC.		
🤣 Network Controller	SBC FQDN (for example sbc1.te-systems.com)		
🤣 Ports	sbc01.athdrlabs.xyz		
🤣 Certificate & Private Key			
🤣 Certificate Chain			
🤣 SBC FQDN			
Name			
	< 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.		
<ul> <li>Microsoft Teams</li> <li>Network Controller</li> <li>Ports</li> <li>Certificate &amp; Private Key</li> <li>Certificate Chain</li> <li>SBC FQDN</li> <li>Name</li> </ul>	Enter a meaningful name for your new node. The name is arbitrary. You will use it to uniquely identify this nod later during configuration. Name Microsoft Teams Direct Routing	e
	< 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.

Scenarios » Node Interconnection Assistant		
Microsoft Teams Direct Routing and VoIP System		
Configuration of Voice over IP System	1	
Ø Microsoft Teams Direct Routing	Please enter your Voice over IP System configuration.	
Voice over IP System	Node Type = [None]	
Routing	Hone type - [Hone]	
	U Configure.	
	< Previous Next > Finish Cancel	

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

Scenarios » Node Interconnection Assistant » Voice over IP System

#### **Create New Node**

Selection of PBX or other Voice over IP System.

🤣 PBX / Sys	tem	The list below contains a number of frequently used PBXs and other Voice over IP systems with their preconfigured defaults for your convenience.	
Network C	Controller	If you cannot find your system of choice, you may use another similar system or Other VoIP System as initia	al
Ports		template to create an individual configuration.	
SIP Interc	onnection		
Remote S	IP Domain	PBX or VoIP System Preset	
Notwork E	) oor W/bitalist	NEC Integrated Communications 3000	
INELWOIK P	eer wintenst	NEC UNIVERGE SV8100 R9.0	
Incoming	Manipulations	net Tenor Series Bx	
Outgoing	Manipulations	Nortel Communication Server 1000/2000	
Name		Oracle Communications SBC	
		Patton SmartNode Series	
		Samsung OfficeServ 7200/7400	
		ShoreTel / ShoreGear	
		Sonus SBC 1000/2000	
		SwyxWare	
		Unify HiPath 3000-Serie/HG 1500	
		Unify HiPath 4000-Serie/HG 3500	
		Unify OpenScape 4000	
		Unify OpenScape Business	
		Unify OpenScape Office	Ξ
		Unify OpenScape Voice	
		XCAPI	
		XCAPI (localhost)	-
		< Previous Next > Finish Cancel	
			_

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

 $\left| \times \right|$ 

## 4.9. anynode Wizard – OSBiz / Network Controller

Scenarios » Node Interconnection Ass	sistant » Voice over IP System	X
Create New Node Network Controller selection.		
PBX / System Network Controller	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.	С
Ports SIP Interconnection	Network Controller  Create new network controller.  Name	
Remote SIP Domain	Unify OpenScape Business	
Network Peer Whitelist Incoming Manipulations Outgoing Manipulations Name	Network  Use a fixed IP address ⑦  Use an interface's address ⑦  vmxnet3 Ethernet Adapter #2  Currently: 10.8.242.78  Advanced configuration ⑦  Open  Specify whether reverse DNS lookup is enabled  Enabled Disabled Select avisting network controller	
	[None]	~
	< Previous Next > Finish Cancel	

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

- Name:
- Network:

Unify OpenScape Business (common-sense name). <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	The new node will use the follow	ving local ports. The	ne remote endpoint must be configured accordingly.
Network Controller	Specify the UDP/TCP Port	5060	Specify the TLS Port 5061
<ul> <li>Ports</li> <li>SIP Interconnection</li> <li>Remote SIP Domain</li> <li>Network Peer Whitelist</li> <li>Incoming Manipulations</li> <li>Outgoing Manipulations</li> <li>Name</li> </ul>	Dynamic UDP/TCP Ports		<ul> <li>Unrestricted UDP port range</li> <li>Restrict UDP port range to <ul> <li>10000</li> <li>13000</li> </ul> </li> <li>Sufficient for approximately 1000 sessions.</li> </ul> <li>Unrestricted TCP port range <ul> <li>Restrict TCP port range to</li> <li>10000</li> <li>13000</li> </ul> </li> <li>Sufficient for approximately 1000 sessions.</li>
		< Previous	Next > Finish Cancel

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

Click on [Next].

## 4.11. anynode Wizard – OSBiz / SIP Interconnection

Scenarios » Node Interconnection As	sistant » Voice over IP System	×
Create New Node		
Choice of SIP interconnectio	n type.	
Choice of SIP interconnection          PBX / System         Network Controller         Ports         SIP Interconnection         Remote SIP Domain         Network Peer Whitelist         Incoming Manipulations         Outgoing Manipulations         Name	n 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 I 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.	≥ be
	< 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 As	sistant » Voice over IP System	×
Create New Node		
Determination of remote SIP	domain.	
PBX / System	Please choose the remote SIP URI which will be used in SIP URIs of outgoing calls and which describes where the remote and exists an be reached.	
📀 Network Controller	the remote enupoint can be reached.	
Ports	© Use URI representation	
SIP Interconnection	Edit	1
🤣 Remote SIP Domain	Use separated representation	-
Network Peer Whitelist	Host	
Incoming Manipulations	10.8.242.92	
Outgoing Manipulations	Transport	
Name	UDP v	
	Port	
	< Previous Next > Finish Cancel	

Enter the following:

- Host:
- Transport:

**10.8.242.92** (OpenScape Business IP). 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 Assi	istant » Voice over IP System		×
Create New Node			
Definition of an IP or hostnam	e whitelist.		
PBX / System	If the interconnection to the VoIP peer the IP addresses from which SIP mess	takes place over a public IP access, it is s sages are allowed by this whitelist.	trictly recommended to minimize
Network Controller	Use the network peer whitelist     Include Demote SID Demoin:	40.0.242.02	
SID Interconnection	Include Remote SIP Domain:	10.8.242.92	Developed ID Adds
Remote SIP Domain	Hostname	Interpret as	Resolved IP Addr
Network Peer Whitelist			
Incoming Manipulations			
Outgoing Manipulations			
Name			
		Add	Ait Remove
	Allow only negotiated peers for	r RTP/RTCP	
	Do not use the network peer white messages of the selected provide	elist. It is already ensured by a separate roor r are able to access the anynode.	uter or a firewall that only SIP
	< Pr	evious 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.

Scenario	os » Node Interconnection Ass	sistant » Voice over IP System			×
Crea	ate New Node				
0	ptional conversion of incom	ning dial strings.			
📀 PB	3X / System	It is recommended to convert incoming calling numbers available to archieve this.	into the E.164	number space. Various manipulation	ns are
🤣 Ne	etwork Controller	If the node's remote endpoint has its own number spac	e then simply a	dd one or more manipulations and	
🥑 Po	orts	describe the type of desired conversion.			
🥑 SII	P Interconnection	Incoming Manipulations			
🤣 Re	emote SIP Domain		Filter	Optional	x
🥑 Ne	etwork Peer Whitelist	Condition	Action		
🥑 Inc	coming Manipulations				
Ou	utgoing Manipulations				
Na	ame				
		Up Down Import	Add	Clone Edit Remo	ve
		< Previous	Next >	Finish Cance	\$I

Scenarios » Node Interconnection Ass	sistant » Voice over IP System			×
Create New Node				
Optional conversion of outgo	ing dial strings.			
🥪 PBX / System	Outgoing manipulations can be used if it is necessary to another destination number space.	o reconvert a ca	lling number from E.164 number spa	ice to
Network Controller	If desired add a manipulation and describe the type of o	conversion.		
🤣 Ports				
SIP Interconnection	Outgoing Manipulations			
📀 Remote SIP Domain		Filter	Optional	X
🤣 Network Peer Whitelist	Condition	Action		
Incoming Manipulations				
🤣 Outgoing Manipulations				
Name				
	Up Down Import	Add	Clone Edit Remo	ve
	< Previous	Next >	Finish Cance	1

Click on [Next].

## 4.15. anynode Wizard – OSBiz / Name

Sce	cenarios » Node Interconnection Assistant » Voice over IP System		
с	reate New Node		
	Determination of node name.		
•	PBX / System	Enter a meaningful name for your new node. The name is arbitrary. You will use it to uniquely identify this node later during configuration.	9
9	Network Controller		
9	Ports	Name	_
9	SIP Interconnection	Unity OpenScape Business	
9	Remote SIP Domain		
	Network Peer Whitelist		
9	Incoming Manipulations		
9	Outgoing Manipulations		
	Name		
			_
		< Previous Next > Finish Cancel	
_			

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

Click on [Finish].

Microsoft Teams Direct Routing and VoIP System Configuration of Voice over IP System		
Microsoft Teams Direct Routing	Please enter your Voice	over IP System configuration.
🤣 Voice over IP System	Nada Tura	- Unife OnenCorne Business
Routing	Note Type Name Network Controller	<ul> <li>Only OpenScape Business</li> <li>Unify OpenScape Business</li> <li>Name = Unify OpenScape Business</li> <li>Interface = vmxnet3 Ethernet Adapter #2</li> <li>IP Version = IP version 4</li> <li>IP Address = [Any IP address]</li> </ul>
	Port TLS Port SIP Interconnection Remote SIP Domain Incoming Manipulations Outgoing Manipulations	= 5060 = 5061 [Default] = SIP Trunk = sip:10.8.242.92;transport=udp = [None] = [None]
	< Previous	✓ Configure     Next >   Finish   Cancel

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

X

## 4.16. anynode Wizard – Routing

Scenarios » Node Interconnection Assistant	
Microsoft Teams Direct Routing Determination of routing type.	g and VoIP System
<ul> <li>Microsoft Teams Direct Routing</li> <li>Voice over IP System</li> <li>Routing</li> </ul>	<ul> <li>Please determine if calls should be routed directly from node to node or whether dial string filters should be applied.</li> <li>Ise direct routing without prefix filter When selecting direct routing, all possible destination URIs are forwarded to the other node without restrictions.</li> <li>Use dial string routing</li> </ul>
	< Previous Next > Finish 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:

<b>any</b> node <sup>*</sup>		competence in e communicatio User: anadmin (write access), Session Timeout: 30 minutes, Committed: yu Copyright © 2021 by TE-SYSTEMS GmbH, Germany, State: connected, License active: yes, Trace: o
Wizard Configuration	My Account ▼ Extras ▼ Info ▼	Commit Monitor Mode Logout
Add Routing Domain Remove Routing	g Domain Clone Routing Domain Export Routing Domain	
Information	♦ Object	
Tracing		000
Licenses	This routing domain listens on the following source nodes for incoming calls.	
Network Interfaces	Name	
	Microsoft Teams Direct Routing	
	Unity OpenScape Business	
Routing Domain		Select All Deselect All
Microsoft Teams Direct Routi		000
Unify OpenScape Business	Routes	
Routing Forward Profiles		Filter Optional X
Authentication Profiles	Filters	Establishment
Directories	To Microsoft Teams Direct Routing Source Nodes = Unify OpenScape Business	Route Call Destination Node = Microsoft Teams Direct Routing
Load Balancers		Routing Forward Profile = To Microsoft Teams Direct Routing
Conditions	To Unify OpenScape Business	
Time Ranges	Source Nodes = Microsoft Teams Direct Routing	Route Call Destination Node = Unity OpenScape Business
Auxiliary Objects		Routing Forward Profile = To Unify OpenScape Business

## 4.17. anynode SBC – Additional Configuration

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

anynode <sup>®</sup>	Copyright © 2	User: anadmin (wri 021 by TE-SYSTEMS GmbH, Ge	te access), Session Timeou ermany, State: connected, L	TE-SYS competence in e ut: 26 minutes, Co icense active: ye	TEMS ecommunications ommitted: yes es, Trace: off
Wizard Configuration - Objects - My Acc	ount ▼ Extras ▼ Info ▼		Commit N	Ionitor Mode	Logout
Add Node Remove Node Clone Node	Export Node				
					1.20
Information				Network	
Tracing				Security Profile	
Licenses				Direct Dec	
Network Interfaces	le		MICrosoft learns	Direct Rol	uting
	en All 🚦 🔁				
▶ Routing Domains	Object				
⇒ Nodes	object				
Microsoft Teams Direct Ro	Limits				
Unify OpenScape Business	Policy Based Session Processing				E
▶ Routing Forward Profiles	Tones and Announcements			0	00
Authentication Profiles	Enable tones and announcements 💿				
Directories	Profile 🤊 Custom 🗸				
Load Balancers	Ringback tone 🧑	Belgium Dingback tone	× 0 / 0		
♦ Conditions	Active tone	[None]		, ,	
Time Ranges					
▶ Auxiliary Objects	Music on hold 🧿	[None]	Solution		
	Session successfully terminated tone 💿	[None]	- <b>G</b> // C		
	Error indicator tone 🧿	[None]	· • • / •		
					-
Version: 4.2.6		💶 Off	<b>40%</b> 👼 3%	<b></b> 33%	0

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.

Configuration      Conserve Node     Conce Hode     Extrast Note     Concerve Node     Conce Hode     Extrast Note     Concerve Node     Concerve Node			
zard Configuration - Objects -	My Account - Extras - Info -		Commit Monitor Mode Lo
d Node Remove Node Clone N	lode Export Node		
			000
Information	Use as a basis for the SIP Response code mar	pping the following profile	
Tracing	Standard		
Licenses	Standard		
Network Interfaces	Incoming SIP Response Code Mapping		
Configuration	SIP Response Code	Telephony Status	User-defined or Default
N Pautian Panaina	301 (Moved permanently)	Redirected	Default
P Routing Domains	302 (Moved temporarily)	Redirected	Default
∀Nodes	403 (Forbidden)	No permission	Default
Microsoft Teams Direct R	404 (Not found)	Erroneous dial string	Default
Unify OpenScope Business	406 (Not acceptable)	Media negotiation error	Default
only openocape business	408 (Request timeout)	Domain Specific 0	User-defined
Routing Forward Profiles	480 (Temporarily not available)	Not responding	Default
Authentication Profiles	488 (Busy here)	Busy	Default
Directories	487 (Request terminated)	Terminated	Default
	488 (Not acceptable here)	Media negotiation error	Default
Load Balancers	500 (Internal server error)	Equipment error	Default
♦ Conditions	503 (Service unavailable)	Congestion	Default
Time Ranges	600 (Busy everywhere)	Busy	Default
Time Ranges	603 (Decline)	Rejected	User-defined
Auxiliary Objects	606 (Not acceptable)	Media negotiation error	Default
		Add E	dit
	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
	verminated	467 (Request terminated)	Default
	Domain Securitie 0	466 (Not acceptable nere)	Licerault
		400 (Request timeout)	Oser-dermed

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.

anynode*	User: anadmin (write access), Session Timeout: 28 minutes, Comm Copyright © 2021 by TE-SYSTEMS GmbH, Germany, State: connected, License active: yes, T	EMS nmunications. nitted: yes Trace: off
Wizard Configuration ▼ Objects ▼	My Account   Extras  Info  Monitor Mode I	Logout
Add Node Remove Node Clone	Node Export Node	
Information	this "m=" line as a response to an "m=" line with the same protocol. ☑ Move "c=" lines below "m=" lines up to the SDP session description.	*
Tracing	Security	
Licenses	Establish new media key for each SDP negotiation           Swan the receiving media key setup with the sending media key setup.	
Network Interfaces	Benegotiation	
	When renegotiating RTP to T.38 (UDPTL), keep the local port if possible.	
Routing Domain	Specify the payload specific media negotiation	=
⇒ Nodes	Session	
Microsoft Teams Direct Ro	O Use the configured media setup exclusively, even if (as in forwardings) the negotiation of other media setups is requested	
Linify OpenScape Business	The configured media setup constrains the negotiable setup	
Pouting Convard Profiles	RTP Negotiation	
	Use the same payload types like the other party	
Authentication Profiles	Always oner the telephone-event according to RPC 2833/4733 Invert sending and receiving payload types	
Directories	For calls that are in the HOLD state, switch to	
Load Balancers	inactive mode  receive-only mode  send-only mode  send/receive mode	
▶ Conditions	During media negotiation throw an error, if	
Time Ranges	no comfort noise is negotiated	
Auxiliary Objects	no telephone-event is negotiated	
	Protocol specifics of individual peers  When negotiating the opus codec suppress the number of channels	Ŧ
Version: 4.2.6	📼 Off 🛛 🛄 40% 💭 4% 🚥 33% (	0

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

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

anynode*	User: anadmin (write access), Copyright © 2021 by TE-SYSTEMS GmbH, Germany, Stat	Competence in e-communicat Session Timeout: 26 minutes, Committed: y te: connected, License active: yes, Trace:	tions yes
Wizard Configuration - Objects -	My Account ▼ Extras ▼ Info ▼	Commit Monitor Mode Logou	ut
Add Routing Forward Profile Remove Re	outing Forward Profile Clone Routing Forward Profile Export Routing Forward Pro	ofile	
Information Tracing Licenses Network Interfaces  ✓ Configuration Noting Domains Nature	/ To Unify OpenScape Business / Telephony Forwarding / Media Negotiation Forwarder / Media Transco         Routing         Forward         Profile         Media         Negotiation         Forwarding         Media         Negotiation         Forwarding         Media         To Unify         Open All	oding Options Media Transcoding Options	
▶ Nodes	Object		
	Settings	000	
To Microsoft Teams Direct R	V Jetungs	000	
To Unify OpenScape Busine	How settings for the direction from the calling to the called entity:		
Authentication Profiles	Specify whether passthrough mode is activated. If the passthrough mode is activated same media format, received media will not be converted to an internal format.	I and the remote side expects the	
Directories			
Load Balancers			
Conditions	Specify whether silence processing is activated.		
Time Ranges	● Yes ◎ No		
Auxiliary Objects	Silence Processing Settings  Specify silence processing properties.  Generate nothing Generate silence Generate comfort noise Generate comfort noise volume level.  By By By By By Scale	enerate events	4
Version: 4.2.6	📼 Off 🛛 😂 40%	0% 📟 33% 🔇 0	

anynode*	User: anadmin (write access), Session Timeout: 28 minutes, Committed: yes Copyright © 2021 by TE-SYSTEMS GmbH, Germany, State: connected, License active: yes, Trace: off
Wizard Configuration - Objects -	My Account   Extras  Info  Commit Monitor Mode Logout
Add Routing Forward Profile Remove Re	outing Forward Profile Clone Routing Forward Profile Export Routing Forward Profile
Information Tracing Licenses Network Interfaces	/ To Microsoft Teams Direct Routing / Telephony Forwarding / Media Negotiation Forwarder / Media Transcoding Options          Routing       →       Telephony         Forward       →       Media         Profile       →       Telephony         Media       Negotiation       →         Media       Transcoding       Options
Routing Domains	Open All 💿 🖉 🔁
▶ Nodes	Diect
To Microsoft Teams Direct	✓ Settings     O
To Unify OpenScape Business	Flow settings for the direction from the calling to the called entity:
Authentication Profiles	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.
Directories	® Yes ◎ No
Load Balancers	
▶ Conditions	Specify whether silence processing is activated.
Time Ranges	● Yes ◎ No
Auxiliary Objects	Silence Processing Settings
	Specify silence processing properties.  Generate nothing Generate silence Generate comfort noise Generate events
	Specify the comfort noise volume level.
	-80 dB Full Scale
Version: 4.2.6	🖸 Off 🕒 40% 🔯 0% 🚥 33% 💽 0

# 5. OpenScape Business – Gateway mode

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

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

### 5.1. PABX Location Data

- Wizards - Basic Installatio	on - Basic Installation						
		3	4	5	6		8
System Overview	Central Functions for Stations	Provider configuration and activation for Internet Telephony	Select a station	Configured Stations	Automatic Configuration of Application Suite	Configure MeetMe Conference	Configure E-Mail Forwarding
hanges done in expert mode I t least the configuration of the vant your OpenScape Busines ly, this integration is done by i tandalone OpenScape Busine	nust be reviewed/repeated after 'Country code' is needed for fer is in " OpenScape Business Ner Service Technician. ss clear the 'Network Integratio	r running through the wizard. satures such as 'Internet telephony' ar twork Integration " you should select t n' check box.	nd 'MeetMe conference'. the "Network Integration" check	box and enter a node ID	In this case, make sure that this no	ide ID is unique within the whole	e network integration.
number			Country code: 00	49	(mandatory)		
			Local area code: 0	89	(optional)		
			PABX number:	72172	(optional)		
			E				
eral			International Prefix:	00			
work Parameters							
			Network Integration:				
			Node ID: [	D			
tream of your internet connect	ion		Upstream up to (Kbps):	256	]		
					-		
Holp Abort	Back OK & N	pyt					

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

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

#### 5.2. SIP Interconnection

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

Expert mode - Telephony Server	
Voice Gateway	Native SIP Server Trunk
SIP Parameters	Add Native SID Server Trunk
TSP Loc-ID Settings	
Codec Parameters	Base Template: Native SIP trunk - predefined
Destination Codec Parameters	
Internet Telephony Service Provider	Trunk Name: Teams
P Networking	Enable Trunk: 🗹
SIPQ-Interconnection     Native SID Server Trunk	Trunk Identifier in System: ITSP/NS 1 🗸
FRANCE SIP SOLVEL FLAIR	
	Renible Domain Name. 10.6.242.75
	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) 500
	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	Native SIP Server Trunk	
SIP Parameters	Add Native SIP Server Trank	
► IT SP Loc-ID Settings		
Codec Parameters     Destination Codec Parameters		~
Internet Telephony Service Provider	CLIP outpring in From header - display part.	
Networking	Cell outgoing in From reader - utspirg haire -	
▶ SIPQ-Interconnection	CLIP outgoing in From header - user part. call number V	
Native SIP Server Trunk	Outgoing From Header - domain/host part: domain/Name 🗸	
	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 V	
	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:

<ul> <li>Base Template:</li> </ul>	Native SIP trunk – predefin	ed
Trunk Name:	Teams (a common-sense n	ame)
• Enable Trunk:	Activated	
<ul> <li>Trunk Identifier in System:</li> </ul>	ITSP/NS 1 (choice of 10 ex	ternal Native SIP
• Trank Tuentiner in System.		
	connections; greyed out ite	ans are occupied by
	already configured trunks)	
<ul> <li>Remote Domain Name:</li> </ul>	10.8.242.78 (host name or	IP address of the
	external SIPserver, i.e. the	AudioCodes SBC LAN
	interface IP)	
Transport Protocol	LIDP (as configured in SBC)	
<ul> <li>IP Address / Host Name:</li> </ul>	10.8.242.78 (SBC IP addre	ss / FQDN)
Port:	5060 (as configured in SBC	; default value = 5060;
	enter port 0 for DNSSRV)	
<ul> <li>Show Extended SIP Data:</li> </ul>	Enabled (by enabling this f	ag some additional
	configuration parameters a	re available to control
	the SIPstack and to adapt i	the content of SIP header
	fields)	
CLIP outgoing in From header	- display part:	display name
CLIP outgoing in P-Asserted-T	d 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).

Expert mode - Telephony Server		8
Voice Gateway	Native SIP Server Trunk Liser	
SIP Parameters	Edit Nativo STD Sorver Truck Hear	Delete Nativo SID Conver Trunk Llear
►ITSP Loc-ID Settings		Delete Hauve Str Server Hank OSer
Codec Parameters	User	d' Teams-User
Destination Codec Parameters		
Internet Telephony Service Provider	Authorization nam	e:
Networking	Passwor	d:
SIPQ-Interconnection	Confirm Dessuran	d:
▼Native SIP Server Trunk	Commit Passwor	u.
Circuit UTC (Cloud)		
Native SIP trunk		
▼Teams		
Teams-User		
	Apply Undo 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:

xpert mode - Telephony Server									
unks/Routing	Trunks								
Trunks		displ	y all lines		add line		Change Direct	ion	
▼LAN									
▼Box: 1, Slot: 1	Trunk		Box-SI-Pt-Li	Code	2	Route	Status	Туре	
Port 3 Networking	Line 61	LAN 1-0-7-1		##760	MS_Teams		active	ITSP/NS 1	
Port 4 SIPQ-Interconnection 1	Line 62	LAN 1-0-7-2		##761	MS_Teams		active	ITSP/NS 1	
Port 5 SIPQ-Interconnection 2	Line 63	LAN 1-0-7-3		##762	MS Teams		active	ITSP/NS 1	
Port 7 IT SP/N S 1	Line 64	LAN 1-0-7-4		##763	MS Teams		active	ITSP/NS 1	
•##760 0-7-61	Line 65	LAN 1-0-7-5		##764	MS Teams		active	ITSP/NS 1	
▼##/61 U-/-6Z	Line 66	LAN 1-0-7-6		##765	MS Teams		active	ITSP/NS 1	
•##762 0-7-63	Line 67	LAN 1-0-7-7		##766	MS Teams		active	ITSP/NS 1	
■##764 0.7.65	Line 68	LAN 1-0-7-8		##767	MS Teams		active	ITSP/NS 1	
● <i>MI</i> 765 0.7.66	Line 69	LAN 1-0-7-9		##768	MS Teams		active	ITSP/NS 1	
◆##766 0-7-67	Line 70	LAN 1-0-7-10		##769	MS Teams		active	ITSP/NS 1	
##767 0-7-68	Line ro	L/11 1-0-7-10		##705	mo_reama		acuve	1101/101	
##768 0-7-69									
♦##769 0-7-70									
								_	
runks									
display a	Il lines		add line		Change Dire	ction			
			Number: 10	×					

## 5.3. Routes

The route configuration will be created automatically.

Trunks/Routing Route					
Trunks				Bouto	Trunks/Routing
Loopa Value Control Value Cont	Special Parameter change		Change Politing Parameters	Change Route	Trunks
Koute     Change house     Change h	Special Parameter change		Change Rodding Parameters		▼Route
Trk Grp. 1 Boute Name MS Teams		e MS Teams	Route Name:		Trk Grp. 1
Trk Gp. 2		into_roanto	reado Harro.		Trk Grp. 2
Trk Grp. 3 Seizure code: 0		le: 0	Seizure code:		Trk Grp. 3
Trik Grp. 4 CO code (2nd trunk code): 0		e): 0	CO code (2nd trunk code):		Trk Grp. 4
Trk Gp. 5			, ,	Gateway Location	Trk Grp. 5
Trk Gp. 6 County Ecology		0: 10	Country codo:	Cateria, Econion	Trk Grp. 6
Tirk Gp. 7 County code, 49		le. 49	Country code.		Trk Grp. 7
App. sume Local area code: 89		le: 89	Local area code:		App. Suite
Tit for 10 PABX number: 72172		er: 72172	PABX number:		Trk Grp. 10
Tit Gru 11 PABX number-incoming				PABX number-incoming	Trk Grp. 11
MS Teams		e: /9	Country code:		MS Teams
M0X402		43	obuility code.		MDX4402
Trik Grp. 14 Local area code: 89		le: 89	Local area code:		Trk Grp. 14
Trk Grp. 15 PABX number: 72172		er: 72172	PABX number:		Trk Grp. 15
Networking			Location number:		Networking
		a. 🗆	Location number.		
PABX number-outgoing				PABX number-outgoing	
Country code:		le:	Country code:		
Local area code:		le:	Local area code:		
			DADY		
PABX number:		er:	PABX number:		
Suppress station number:		er:	Suppress station number:		
Overflow route				Overflow route	
		None V	Overflow route :		
				Digit transmission	
Digit transmission: en-bloc sending 🗸		n: en-bloc sending V	Digit transmission:		
Mobile Extension Number (MEX)				Mobile Extension Number (MEX)	
MEX Number		er	MEX Number		
Apply Undo Help			lelp	Apply Undo H	

Expert mode - Telephony Server					×
Trunks/Routing	Route				
Trunks	Change Route	Change Routing Darameters		Special Darameter change	
▼Route	change route			Speak Foreneed change	
Trk Grp. 1	Routing flags				
Trk Grp. 2		Digit repetition on:			
Trk Grp. 3		Analysis of second dial tone / Trunk monitoring:			
Trk Grp. 4		Intercent per direction	7		
Trk Grp. 5		intercept per direction.			
Trk Grp. 6		Over. service 3.1 kHz audio:	$\checkmark$		
Ann Suite		Add direction prefix incoming:			
Trk Grp. 9		Add direction prefix outgoing	-		
Trk Grp. 10		Only Na with international (antional configuration	_		
Trk Grp. 11		Call No. with International / national prefix.			
MS_Teams		Ringback tone to CO:			
MDX4402		Name in CO:	✓		
Trk Grp. 14		Commentation			
Trk Grp. 15		Segmentation.	yes 🗸		
Networking		deactivate UUS per route:			
		Always use DSP:			
		Analog trunk seizure:	no pause 🗸		
		Trunk call pause:	Pause 2 s 🗸		
		Type of seizure:	linear 🗸		
		Route type:	PABX 🗸		
		No. and type, outgoing:	Country code 🗸		
		Call number type:	Direct inward dialing 🗸		
	Rerouting	Change route allowed:	7		
	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
•	CO code (2 <sup>nd</sup> trunk code):	<ul> <li>dialed the code).</li> <li>0 (it is only relevant for networking routes with route type = PABX).</li> </ul>

•	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
		-

### 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.

Expert mode - Telephony Server								×	
LCR	Dial Plan								
LCR Flags	Diarrian	Unit Fran							
Classes Of Service					Dispidy Diari				
Dial Plan	Dial Plan	Name	Dialed digits	Routing Table	Acc. code	Classes of service	Emergency		
▶ Routing table	76	MDX4402	0CZ	$9 \checkmark \rightarrow$		✓			
Dial rule	77	MDX4402	0C0-Z	$9 \checkmark \rightarrow$		$\checkmark$		^	
mulusite	78	MDX4402	0C1Z			$\checkmark$			
	79	MDX4402	0CNZ			$\checkmark$			
	80	MDX4402	000-7			<b>v</b>			
	81			- × →		$\checkmark$			
	82					~			
	83					7			
	84					<b>v</b>			
	85					<b>v</b>			
	86			- <b>X</b> →		<b>v</b>			
	87					$\checkmark$			
	88			- × →		$\checkmark$			
	89					$\checkmark$			
	90			$ \rightarrow $		$\checkmark$			
	91					~			
	92					$\checkmark$			
	93					<b>v</b>			
	94					~	Π	- 10	
	95			- <b>V</b> →		<b>v</b>			
	96					$\checkmark$			
	97			- <b>×</b> →		$\checkmark$			
	98	Teams	0C721721-Z	98 🗸 🔿		$\checkmark$			
	99	Teams	0C0-89721721-7			$\checkmark$			
	100	Teams	0C00-4989721721-7			<b>v</b>		$\sim$	
	Page 1 of 10			11213141516171819			Items per page 10 25 50	0 <b>100</b>	
	Apply	Undo Help							

## 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.

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.



Expert mode - Telephony Server														×
12 - Table		-												
73 - Table	^	Routing	Table											
74 - Table							Change Rou	ting Table						
75 - Table														
76 - Table							R	outing Table:	99		en-b	loc sending		
77 - Table			1	1		1				1				
78 - Table		Index	Dedicated Route	Rot	ite	_	Dial Rule		min. COS		Warning	D	edicated Gateway	GW Node ID
79 - Table		1		MS_Teams	$\sim$	Teams-nat	$\sim \rightarrow$		15 🗸	None	$\sim$	No	$\sim$	
00 - Table 91 Table		2		None	~	None	~		15 🗸	None	$\checkmark$	No	$\sim$	
82 - Table		3		None	~	None	~		15 ¥	None	~	No	~	
83 - Table				Nene		None			15.14	None		No		
84 - Table		4		None	•	None	·		15 •	None	•	NU	•	
85 - Table		5		None	$\sim$	None	$\sim$		15 🗸	None	$\sim$	No	$\sim$	
86 - Table		6		None	$\sim$	None	$\sim$		15 🗸	None	$\sim$	No	$\sim$	
87 - Table		7		None	$\checkmark$	None	$\sim$		15 🗸	None	$\sim$	No	~	
88 - Table		8		None	~	None	×		15 ¥	None	~	No	×	
89 - Table		-		Hone	· .	Hone			10 1	Tione	-		-	
90 - Table		9		None	~	None	$\sim$		15 🗸	None	~	NO	~	
91 - Table		10		None	$\sim$	None	$\sim$		15 🗸	None	$\sim$	No	$\sim$	
92 - Table		11		None	$\checkmark$	None	$\sim$		15 🗸	None	$\sim$	No	~	
93 - Table		12		None	~	None	~		15 🗸	None	~	No	~	
94 - Table		12		None	~	None	~		15 1	None	~	No	V	
06 Table		15		None	•	None	•		15 🕈	None	•	NO	•	
97 - Table		14		None	$\sim$	None	$\sim$		15 🗸	None	~	No	$\sim$	
98 - Table		15		None	$\sim$	None	$\sim$		15 🗸	None	$\sim$	No	$\sim$	
99 - Table		16		None	$\checkmark$	None	$\sim$		15 🗸	None	$\checkmark$	No	~	
100 - Table														
101 - Table														
102 - Table														
103 - Table														
104 - Table														
105 - Table														
106 - Table														
107 - Table														
108 - Table		-	obly Undo	Help										
109 - Table	~	A	ppiy Olido	neip										
L 440 Tablo														

Expert mode - Telephony Server										8
72 - Table	~	Routing	Table							
74 - Table		_				Change Routing Table				
75 - Table										
76 - Table						Routing Table	100	en-bloc se	ndina	
77 - Table						5				
78 - Table		Index	<b>Dedicated Route</b>	Route	Di	al Rule	min. COS	Warning	Dedicated Gateway	GW Node ID
79 - Table		1		MS Teams 🗸	Teams-int	·] →	15 🗸	None	No Y	
80 - Table		2	_	Nono	Nono		15.14	Nono	No	
81 - Table		2		None V	None		15 🗸	None •	NO V	
82 - Table		3		None 🗸	None	·	15 🗸	None V	No V	
83 - Table		4		None 🗸	None N	•	15 🗸	None 🗸	No 🗸	
84 - Table		5		None 🗸	None	•	15 🗸	None V	No V	
96 Table		6		None	None	-	15 ¥	None	No	
87 - Table		7	_	Nono	Nono	-	15.34	Nono	No	
88 - Table		'		None +	None		15 🕈	None 🗸	140 +	
89 - Table		8		None 🗸	None	·	15 🗸	None V	No V	
90 - Table		9		None 🗸	None N	•	15 🗸	None V	No 🗸	
91 - Table		10		None 🗸	None	•	15 🗸	None V	No 🗸	
92 - Table		11		None	None	-	15 🗸	None	No Y	
93 - Table		40	_	hinn hí	hlana	-	45.14	himme bd	No. N.	
94 - Table		12		None 🗸	None		15 🗸	None	ND V	
95 - Table		13		None 🗸	None	·	15 🗸	None V	No V	
96 - Table		14		None 🗸	None N	•	15 🗸	None V	No 🗸	
97 - Table		15		None V	None	•	15 🗸	None V	No V	
90 - Table		16		None	None		15 🗸	None	No	
100 - Table					110110	_	10			
101 - Table										
102 - Table										
103 - Table										
104 - Table										
105 - Table										
106 - Table										
107 - Table										
108 - Table			untra Unada	Unix						
109 - Table	$\sim$	A	undo	neib						
140 Tabla	1									

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

Expert mode - Telephony Server							E		
LCR	Dial	I Pula							
LCR Flags	Diai	Mai Nute (Anana Dial Dula							
Classes Of Service									
Dial Plan		Rule Name	Dial	rule format	Network access	Туре			
Routing table	1	ISDN	A		Main network supplie V	Unknown			
Dial rule	2	SIP	A		Main network supplie V	Unknown			
Multisite	3	SIP lokal	HE2A		Main network supplie V	Unknown			
	4	MEB	E1A		Corporate Network	PABX number V			
	5	IP-Network	A		Corporate Network	Unknown			
	6	Multi-Location	BA		Corporate Network V	Unknown			
	7	Gateway call	E1A		Corporate Network	Unknown			
	8	COInternat	D0E4A		Main network supplie V	Unknown			
	9	Add cc to Canoni	D49E2A		Main network supplie V	Country code V			
	10	National to Cano	D49E3A		Main network supplie V	Country code V			
	11	Internat. to Can	E3A		Main network supplie V	Country code V			
	12	SIP local_Canoni	HE2A		Main network supplie V	Country code V			
	13	Teams-nat	D49E3A		Main network supplie V	Country code 🗸			
	14	Teams-int	E3A		Main network supplie V	Country code 🗸			
	15	Teams-local	D4989E2A		Main network supplie V	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 🗸			
	Page	e 1 of 11		H 11213141	516121819	Ite	ems per page <u>10 25 50 100</u>		
		Apply Undo	Help						

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

Α

For calls to PSTN configure the following:

- Rule Name: • **SIP** (common-sense name)
- Dial rule format:
- Network access:
- Type:

Main network supplier Unknown

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

- Rule Name:
- Dial rule format:
- Network access:
- D4989E2A Main network supplier

Teams-local (common-sense name)

• Type: Country code

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

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

E3A

Country code • Type:

For calls to Teams with international format configure the following:

- Rule Name:
- Dial rule format:
- Network access: •
- Main network supplier

Teams-int (common-sense name)

• Type:

Country code

### 5.5. System Parameter Flags

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



Expert mode - Telephony Server		×
Basic Settings	System Flags	
▼System	Edit System Flags	
System Flags		
Time Parameters	Configurable CLIP: 🗹	~
DISA	Caller list at destination in case of Forward Line:	
Intercept/Attendant/Hotline	Call forwarding after deflect call / single step transfer.	
LDAP	Follow call management in case of deflect call / single step transfer:	
Texts		
Flexible menu	Extended Rey Policionality.	
Service Codes	Calling number in pick-up groups / ringing groups / CFN /RNA: M	
HFA Registration Password	SPE support:	
Gateway	SPE advisory tone:	
Quality of Service	Transparent dialing of * and # on trunk interfaces:	
Port Management	Add seizure code for MEX	
Voicemail / Announcement Player		
Phone Parameter Deployment		
	Restrict indirect trunk group connections according to CON Matrix:	
	Onen numbering scheme	
	active:	
	Node calumber	
	Transit permission	
	Feature transit: 🗹	
	Tie traffic transit. 🗹	
	External traffic transit : 🗹	
	Special switch	
	Automatic, cyclical line seizure: M	~
	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). enabled enabled enabled

- Feature transit:
- Tie traffic transit:
- External traffic transit:

Click on [Apply].

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

# 6. OpenScape Business - Trusted external User mode

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

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

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



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



#### 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	
Voice Gateway	Native SIP Server Trunk
SIP Parameters	Add Native SIP Server Trunk
ITSP Loc-ID Settings	
Codec Parameters	Base Template Trusted SBC - predefined
Destination Codec Parameters	
Internet Telephony Service Provider	Trunk Name: Teams
Networking	Enable Trunk:
SIPQ-Interconnection	
Native SIP Server Trunk	Irunk Identifier in System: IISP/NS1 👻
Circuit UTC (Cloud)	Remote Domain Name: 10.8.242.78
Native SIP trunk	Transition and and a second seco
▼ Irusted SBC	Iransport protoco: uup V
	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: stunt-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	
Voice Gateway	Native SIP Server Trunk
SIP Parameters	Add Native SIP Server Trunk
ITSP Loc-ID Settings	
Codec Parameters	
Destination Codec Parameters	
Networking	CLIP outgoing in From header - display part 🛛 display name 🗸
SIPQ-Interconnection	CLIP outgoing in From header - user part. call number ❤
Native SIP Server Trunk	Outgoing From Header - domain/host part
Circuit UTC (Cloud)	
Native SIP trunk	Diversion: From contains original CallingPartyNumber:
▼Trusted SBC	Diversion: PAI contains original CallingPartyNumber:
	CLIP outgoing in P-Asserted-Id header - display parti 🛛 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: onlt 🗸
	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: v
	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:

Activated

Trusted SBC – predefined

Teams (a common-sense name)

ITSP/NS 1 (choice of 10 external Native SIP

- Base Template:
- Trunk Name:
- Enable Trunk:
- Trunk Identifier in System:
- Remote Domain Name:
- Transport Protocol:
- IP Address / Host Name: Port:
- Show Extended SIP Data:

connections; greyed out items are occupied by already configured trunks) 10.8.242.78 (host name or IP address of the external SIPserver, i.e. the AudioCodes SBC LAN interface IP) UDP (as configured in SBC) 10.8.242.78 (SBC IP address / FQDN) 5060 (as configured in SBC; default value = 5060; enter port 0 for DNSSRV) 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:
- Diversion: PAI contains original CallingPartyNumber:
- CLIP outgoing in P-Asserted-Id header display part:
- CLIP outgoing in Diversion header display part:
- Check Redirection:

display name disabled display name display name 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).

Expert mode - Telephony Server		3
Voice Gateway	Native SIP Server Trunk Liser	
SIP Parameters		
ITSP Loc-ID Settings	curl nauve sup server fruit User	Delete Native SIP Server Trunk User
Codec Parameters	liserid: Teams-liser	
Destination Codec Parameters	Contra Teamb Oder	
Internet Telephony Service Provider	Authorization name:	
Networking	Password	
SIPQ-Interconnection		
Native SIP Server Trunk	Confirm Password:	
Circuit UTC (Cloud)		
Native SIP trunk		
Teams		
Teams-User		
Trusted SBC		
	Apply Undo 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:

Expert mode - Telephony Server									
Trunks/Routing	Trunks								
▼Trunks		display all lines		add line			Change Directi	00	1 C C C C C C C C C C C C C C C C C C C
▼LAN				out mit			change on eco		
▼Box: 1, Slot: 1	Trunk	Box-SI-Pt-Li		Code		Route	Status	Туре	
Port 3 Networking	Line 61	LAN 1-0-7-1	##760	MS	Teams		active	ITSP/NS 1	
Port 4 SIPQ-Interconnection 1	Line 62	LAN 1-0-7-2	##761	MS	Teams		active	ITSP/NS 1	
Port 5 SIPQ-Interconnection 2	Line 63	LAN 1-0-7-3	##762	MS	Teams		active	ITSP/NS 1	
Port 7 ITSP/NS 1	Line 64	LAN 1-0-7-4	##763	MS	Teams		active	ITSP/NS 1	
♦##760 0-7-61	Line 65	LAN 1-0-7-5	##764	MS	Teams		active	ITSP/NS 1	
<b>◆</b> ##761 0-7-62	Line 66	LAN 1 0 7 6	##765	MO	Teams		active	ITODAIC 1	
<b>◆</b> ##762 0-7-63	Line 00	LAN 1-0-7-0	##705	MO	_ Teams		active	ITOP/NO T	
●##763 0-7-64	Line 67	LAN 1-0-7-7	##700	MO	_ Teams		active	ITOPAIC 4	
●##764 U-7-65	Line 66	LAN 1-0-7-8	##/6/	MS	_ reams		active	ITSP/NS 1	
• ##765 0-7-66	Line 69	LAN 1-0-7-9	##/68	MS	_ leams		active	IISP/NS 1	
##765 0-7-67	Line 70	LAN 1-0-7-10	##769	MS	5_Teams		active	ITSP/NS 1	
₩₩761 U-1-00 ₩₩768 0 7 69									
<ul><li>◆##769 0-7-70</li></ul>									

Trunks display all lines	add line	Change Direction				
Number: 10 ×						

#### 6.2. Routes

The route configuration will be created automatically.

Expert mode - Telephony Server				×
Trunks/Routing	Poute			
Trunks	Change Route	Change Deuting Darameters		Consid December change
▼Route	Change Route	Change Routing Parameters		Special Parameter change
ISDN		Poute Name:	MS Teams	
Trk Grp. 2		Note Name.	[mo_reams	
Trk Grp. 3		Seizure code:	80	
Trk Grp. 4		CO code (2nd trunk code):		
Trk Grp. 5		CO code (zild ildik code).		
Trk Grp. 6	Gateway Location			
Trk Grp. 7		Country code:	49	
App. Suite		Local area code:	89	
Trk Grp. 10		PARY number:	70170	
Trk Grp. 11		PADA Itumber.	12112	
MS Teams	PABX number-incoming			
MDX4402	1	Country code:	49	
Trk Grp. 14		Local area code:	89	
Trk Grp. 15				
Networking		PABX number:	72172	
		Location number:		
	PABX number-outgoing			
		Country code:		
		Country code.		
		Local area code:		
		PARY number:		
		PADA number.		The feature "Trusted external users" for this route requires specific steps
		Suppress station number:		to prevent unauthorized access by call number spoofing.
	Overflow route			It is strongly recommended to only use this route within the internal
		Overflow route :	None 🗸	LAN with VLAN. Do not allow this connection to be accessed from the
	Digit transmission			Internet.
	Digit transmission	Diskterensister	[	Press OK to continue. Press Cancel to modify the related settings first.
		Digit transmission:	en-bloc sending 🗸	
	Mobile Extension Number (MEX)			
		MEX Number		
	Trusted External Users			Ok Abbrechen
		Trusted External Users		
	Apply Undo H	lelp		

Expert mode - Telephony Server				C
Trunks/Routing	Davida			
Trunks	Route			
▼Route	Change Route	Change Routing Parameters		Special Parameter change
ISDN	Routing flags			
Trk Grp. 2		Digit repetition on:		
Trk Grp. 3		Analysis of second dial tone / Trunk monitoring:		
Trk Grp. 4			_	
Trk Grp. 5		intercept per direction.	_	
Trk Grp. 7		Over. service 3.1 kHz audio:		
App. Suite		Add direction prefix incoming:		
Trk Grp. 9		Add direction prefix outgoing:	0	
Trk Grp. 10		Call No. with international ( national profiv	0	
Trk Grp. 11		can no. with international / national prenx.		
MS_Teams		Ringback tone to CO:		
MDX4402		Name in CO:		
Trk Grp. 15		Segmentation:	ves 🗸	
Networking		depending to 1000 per control		
		deactivate 003 per foute.	0	
		Always use DSP:	U	
		Analog trunk seizure:	no pause 🖌	
		Trunk call pause:	Pause 2 s 💌	
		Type of seizure:	linear 🗸	
		Route type:	PABX 🗸	
		No. and type, outgoing:	Country code 🗸	
		Call number type:	Internal / DID 🗸	
	Rerouting			
		Change route allowed:		
		Poute ontimize active:	No	
		Route optimize active.		
	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)
٠	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

#### 6.3. Trusted external User

#### Create a Mobility User by entering the "Mobility Phone Integration" wizard

		administrator@system Logoff							
Home Administrators S	Setup Expert mode Data Backup License Management Service Center Networking								
Setup									
▼ Wizards	User Telephony	0							
Basic Installation		<b>•</b>							
Telephones / Subscribers	Eait Class of service Set up classes of service with external call numbers that can be assigned to subscribers, e.g., emergency numbers, allowed numbers, denied numbers and assignment of class of service for night service								
Central Telephony									
User Telephony	Station name and release								
UC Suite	Edit Edit station and group names and reset lock code for individual stations								
Cloud Services	Forth Group Call / Hunt Group								
Mass Data	Set up incoming calls for station group (parallel, linear or cyclical call order)								
	Edit Call Forwarding Set up central system-wide station number assignments, and forwarding "after timeout" and "on busy"								
	Edit Configure stations in a pickup group with the option of answering each other's calls								
	Eiti Team Configuration Set up stations in a team where incoming calls are simultaneously signaled at all stations in parallel with the main station, and outgoing calls can be connected using the main station number								
	Edit Mobile Phone Integration 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)								
Executive / Secretary Setup a link between one or more Executive phones and one or more Secretary phones with the goal of enabling simplified call transfers and ring transfers									
UCD         Set up an automatic intelligent call distribution to a group with selected stations									
	Edit Attendant Console Set up stations as attendant console numbers and station behavior for "on busy, incorrect dialing and no answer"								
	Editi Station Profiles Assign stations to a profile and import/export profile data								

#### Press "Add" to create a new Mobility User

Setup - Wizards - User Telephony - Mobile Phone Integration									
	Select station for Mobility								
DISA	Direct inward dialing:								
Add Mobility User Add	New Mobility User								
	Mobility User callno	Mobility User DID	Display	Trunk access code + Mobile Call number	User name for mobile UC clients	State			
						^			

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

ietup - Wizards - User Telephony - Mobile Phone Integration				
	Change Mobility User allocation			
Mobile phone mode in-house	•			
WLAN Mode	0			
Mobility User				
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			
User name for mobile UC clients:	None 🗸			
Help Abort Back 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				
▼ Station	Station		Educative Acces	r is come lengt	
▶ IP Clients	cuit station parameters		Edit station hags	Edit Group/CPW	
Virtual Stations	Station - 3501				
UC Applications		Type:	Mobility Entry		
Profiles/Templates		Call number:	1001 ×		
DDI Extensions					
Mobility User		First Name:	1001 ×		
3501 1001 MS Teams, 1001		Last Name:	MS Teams ×		
3502 1002 MS Teams, 1002			NO.T. 1001		
Circuit User		Display:	MS leams, 1001 ×		
Trusted Fritane I Have	DI	irect inward dialing:	1001 ×		
Stations Overview		Device Type:	virtual		
Key Programming		Clip/Lin:	- ×		
		Access	-		
	Mobility/Circuit				
	Mooney/Circuit	Tuno	Mobility station		
		type.	Mobility station		
	M	obile Call number :	Virtual station		
		Web Feature ID	Circuit station		
	Deservates		StB station		
	roraneter	Extension Type:	Standard V		
		Language:	German 🗸		
	Cal	Il signaling internal:	Ring type 1 V		
	Call	l signaling external:	Ring type 1 V		
	Clas	is of service (LCR)	15 🗸		
		Hotline Mode:	Off 🗸		
		Hotline	None ¥		
		ITED I an ID:			
		HOP LOCID.			
	Apply Undo Help				< >

Expert mode - Telephony Server						×		
Station Station	Trusted external User							
P Clients			Ealt Subscriber					
Virtual Stations UC Applications	Callno DID Search:	First Name	Last Name	Display	Туре	Trusted external station call number		
Promes/templates DDI Extensions Mobility User Circuit User StB User	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	1001 1002	MS Teams MS Teams	MS Teams, 1001 MS Teams, 1002	Trusted external station V Trusted external station V	80004989721721001 80004989721721002		
Trusted External User 3501 1001 MS Teams, 1001 3502 1002 MS Teams, 1002 Stations Overview Key Programming	Apply Undo He	lp	A 4	1		• Items per page <u>10 25 50 100</u>		

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].

Expert mode - Telephony Server								×
LCR LCR Flags Classes Of Service	Dial Plan Change Dial Plan Display Dial Plan Display Dial Plan							
Dial Plan Pouring table	Dial Plan	Name	Dialed digits	Routing Table	Acc. code	Classes of service	Emergency	у
Notang sale Dial rule Multisite	96 97 98 99 100	[] [] [] Teams	80C00-498972172-XXXX	$\begin{array}{c} \cdot  \mathbf{v} \\ \hline 100  \mathbf{v} \end{array} \rightarrow$				*
	Apply	Undo Help	M d 112131515121812 D D		Items p	er page <u>10 25 50</u> .	• <u>100</u>	

**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.** 

Expert mode - Telephony Server					
Basic Settings	System Flags				
▼ System	Edit System Flags				
System Flags	Distant substitut 1				
Lime Parameters	Kingback protection.				
DISA	Euro-impedance:				
Intercept/Attendant/Hotline	Different phonemail messages Day/Night:				
LDAP	Display international / national code number:				
Texts	Line change for direct call.				
Flexible menu					
Speed Dials	Automatic redial:				
Service Codes	Voice mail Node call number:				
Gateway					
Quality of Service	Apply Undo Help				
Port Management	•				

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 2<sup>nd</sup> 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 2<sup>nd</sup> 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:

පී	Users	~	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						
٨	Teams devices	~							
B	Teams apps	~	Dial plan details	Test d	ial plan				
Ē	Meetings	× .	External dialing prefix (i)	Enter a	phone number to test.				
Ę	Messaging policies		Example: 9	Examp	ple: "4255551234"	Test			
ଟ	Voice	~	Optimized device dialing ①						
	Phone numbers		Off						
	Operator Connect								
	Direct Routing		Normalization rules						
	Calling policies		Normalization rules define how phone numbers expressed in various formats are to be translated. One or more normalization						
	Call park policies		rules must be assigned to the dial plan	and are matched from the top to b	ottom.				
	Caller ID policies		+ Add 🖉 Edit 🕆 Move up	↓ Move down 📋 Delete	1 item				0
			✓ Rank	Name	Description	Pattern	Translation	Is matching?	
	Emergency policies		1	4-Digit	Enable extension dialing on OSBiz	^(4))\$	\$1		
	Voice routing policies								
	Auto attendants								
	Call queues								
	Holidays								
	Resource accounts		Save Cancel						

# 9. Support & Serviceability

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

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

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

### 9.2. Known issues

#### Basic Call (Calls to Teams from SIP stations)

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

#### Call Hold

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

#### Codecs

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

## 9.3. Required trace configuration options for error reporting

OpenScape Business Trace Profiles:

- 1. Basic
- 2. Voice Fax Connections
- 3. SIP\_Interconnection\_Subscriber\_ITSP

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

4. SIP\_Registration

OpenScape Business Trace Components:

- 1. FP\_CP-Port-User: level 9
- 2. FP\_DH-SIP: level 9 (only for OpenScape Business X variant)

### 9.4. Required trace files for error analysis

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

## 10. Security

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

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

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

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

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

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

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



mitel.com

© 2024 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.