



A MITEL
PRODUCT
GUIDE

Unify OpenScape Solution Set V10

OpenScape Voice with MS Teams and OpenScape SBC,
Configuration Guide

Administrator Documentation

10/2025

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

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

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Contents

History of Changes	3
1 Introduction	4
1.1 Additional Support Information	4
1.2 Network Topology	4
1.3 Microsoft Teams & AudioCodes SBC	6
2 OpenScape Voice Configuration	7
2.1 Endpoints	8
2.1.1 SBC Endpoint.....	8
2.1.2 Teams Endpoints.....	19
2.1.3 SSP Endpoint.....	30
2.1.4 Endpoint Main Page	40
2.2 Destinations & Routes.....	42
2.2.1 Teams Destination.....	42
2.2.2 SSP Destination.....	46
2.2.3 Destinations Overview.....	48
2.3 Translation.....	49
2.3.1 Teams Numbers Routing.....	49
2.3.2 PSTN Numbers Routing	51
2.3.3 Domain Codes	53
2.4 SIP UA Forking	55
2.5 Display Number Modification (optional)	56
3 Configuring OpenScape SBC.....	61
3.1 Connect to OpenScape Voice Server	62
3.1.1 Core Realm Interface	62
3.1.2 SIP Server.....	63
3.2 Certificates	64
3.3 Media.....	68
3.3.1 Codec Manipulation Options	68
3.3.2 Teams Media Profile	70
3.3.3 PSTN Service Provider Media Profile.....	71
3.3.4 OpenScape Voice Media Profile	72
3.3.5 General Media Settings.....	73
3.4 Remote Endpoints	74
3.4.1 Teams Remote Endpoints	74
3.4.2 PSTN Remote Endpoint.....	79

History of Changes

Issue	Date	Summary
1	03/2017	First issue of the guide
2	03/2021	Minor Changes
3	01/2022	v1.8 Updates
4	02/2022	v1.9 Updates
5	11/2022	Minor Change
6	06/2023	Minor Change
7	08/2023	Minor Change
8	03/2024	Added Chapter 1.3 Microsoft Teams & AudioCodecs SBC
9	09/2025	Improvements and enhancements throughout the document. Added RTP parameter configurations for Non-Media Bypass Mode and Media Bypass Mode .

1 Introduction

Microsoft Teams Direct Routing solution with Unify OpenScape SBC (and OpenScape Voice) is available and released for both Media Bypass ON and OFF Teams tenant configurations.

This document describes how to connect the Unify OpenScape SBC (with OpenScape Voice) to Microsoft Teams Direct routing configuration. Microsoft Teams Direct Routing configuration isn't included in current document and may be found under <https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure>.

Product	SW Version	Media Bypass OFF Support	Media Bypass ON Support
OpenScape Voice	V10R2.13.1	✓	✓
OpenScape SBC	V10R1.2.0	✓	
OpenScape SBC	V10R2.2.0	✓	✓
OpenScape Apps	V10 R3.10.1	✓	✓

1.1 Additional Support Information

In the current Unify product software implementation:

- OpenScape SBC with OpenScape Voice solution is supported.
- OpenScape SBC with OpenScape 4000 solution is supported.
- SBC standalone (without PBX) is not currently supported.
- Domain-based MS Teams multi-tenancy is supported.
- Comfort Noise generation is not currently supported by OpenScape SBC.
- The History-Info header is not currently supported by OpenScape Voice & OpenScape 4000.
- The OSEE environment with SBC-THIG and Teams is not currently supported.

1.2 Network Topology

The block diagrams in **fig.1** and **fig.2** below show the Teams Direct Routing connection topology along with the SIP / Media flows for Media Bypass OFF and Media Bypass ON cases.

While Teams Phone System is directly connected to OpenScape SBC, the PSTN access is possible to be available through OpenScape Voice, too.

The example configuration presented in current document covers the PSTN (SSP) SIP trunk connectivity to OS SBC directly; PSTN access through OS Voice is out of scope.

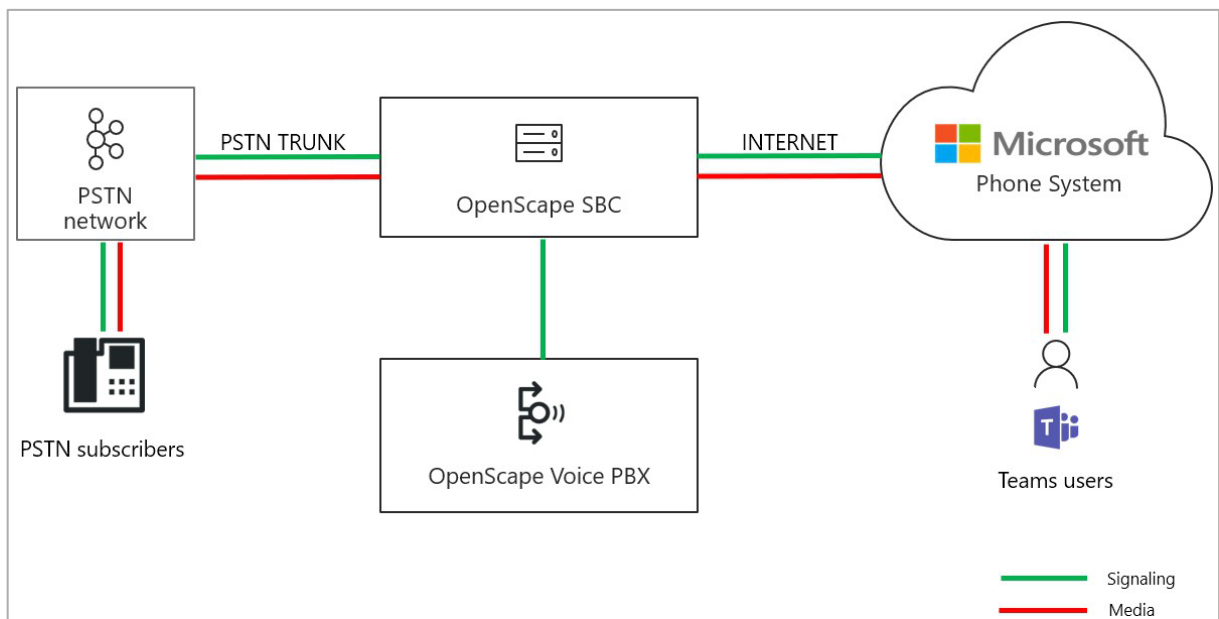


Figure 1: Topology Block Diagram SIP and Media Flows – Media Bypass OFF

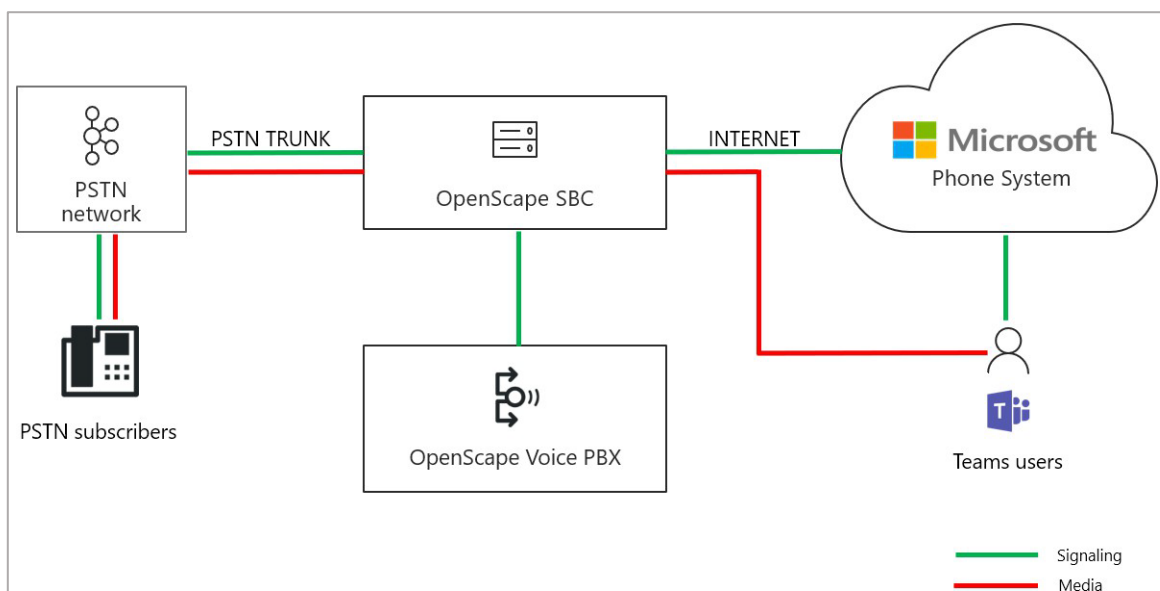


Figure 2: Topology Block Diagram SIP and Media Flows – Media Bypass ON

When media bypass is deactivated and a Teams client makes or receives a call, both signaling and media flow between the SBC, the Microsoft Phone System, and the Teams client, as shown in **fig.1**.

On the other hand, when media bypass is activated and a Teams client makes or receives a call, the signaling continues to flow between the SBC, the Microsoft Phone System, and the Teams client, as in the case of Media Bypass OFF. However, in the Media Bypass ON case, the media flow is kept directly between the Teams client and the SBC, as shown in **fig.2**.

The OpenScape SBC isn't a B2BUA, and it has limited SIP message manipulation capabilities. The OpenScape Voice IP-PBX provides call routes, enhanced SIP message manipulation, and number modification facilities. Thus, SIP signaling for incoming and outgoing calls to the Teams client will always pass through the OS Voice service.

1.3 Microsoft Teams & AudioCodes SBC

For the current certification, Microsoft Teams Direct Routing configuration is utilized to set up the testing environment.

The prerequisites for Direct Routing are:

1. MS Team's users of Direct Routing must have the following licenses assigned in Office 365:
 - *Office 365 Enterprise E3 (including SfB Online Plan2, Exchange Plan2, and Teams)*
 - *Phone System licenses or Office 365 Enterprise E5 (including SfB Online Plan2, Exchange Plan2, Teams, Phone System, and Audio Conferencing).*
2. MS Teams certified SBC (<https://docs.microsoft.com/en-us/microsoftteams/direct-routing-border-controllers>).
3. A publicly registered domain name. A public domain name, such as *onmicrosoft.com*, is not a possibility for direct routing.
4. Public trusted certificate for the SBC with a SAN record with the host name of the SBC. The certificate must be from one Microsoft's approved root CAs (<https://docs.microsoft.com/en-us/MicrosoftTeams/direct-routing-plan#public-trusted-certificate-for-the-sbc>).
5. Public IP address for SBC WAN connection and appropriate firewall rules for signaling.
6. "SBC MS Direct Routing" License should be obtained and applied to OpenScape SBC.

2 OpenScape Voice Configuration

This chapter describes the OpenScape Voice configuration for connecting to OpenScape SBC. The purpose of this connectivity is to enable OpenScape Voice to provide the necessary SIP message manipulation and call routing functions to OpenScape SBC, allowing it to interconnect with Teams Direct Routing and facilitate calls between Teams clients and PSTN subscribers.

In OpenScape Voice, the connection to the OpenScape SBC must be set up, along with the signaling paths to Microsoft Teams datacenters and the SSP (PSTN provider).

In addition, call routing must be configured according to the numbering plan of Teams users and PSTN subscribers.

As an example:

Items	Example
SBC IP	10.8.242.72 TCP 5060
Signaling path to Teams FQDN 1: sip.pstnhub.microsoft.com	10.8.242.72 TCP 50001
Signaling path to Teams FQDN 2: sip2.pstnhub.microsoft.com	10.8.242.72 TCP 50002
Signaling path to Teams FQDN 3: sip3.pstnhub.microsoft.com	10.8.242.72 TCP 50003
Signaling path to Teams FQDN ALL: sip- all.pstnhub.microsoft.com see note	10.8.242.72 TCP 50004
Signaling path to PSTN provider: BCOM	10.8.242.72 TCP 50010
Teams user number ranges (reachable from PSTN)	31850080xxx
PSTN subscriber number ranges	498970072xxxx

For OS Voice installation or General configuration, refer to the [Unify customer documentation site](#).

Important:

Per Microsoft's announcement, support for the *"sip-all.pstnhub.microsoft.com"* FQDN will end in March 2022.

Although Microsoft recommends using the three FQDNs for Direct Routing connection points — **"sip.pstnhub.microsoft.com"**, **"sip2.pstnhub.microsoft.com"**, and **"sip3.pstnhub.microsoft.com"** — the **"sip-all.pstnhub.microsoft.com"** FQDN was originally used in Unify component configurations due to DNS resolution issues in some

countries.

However, there have been reported cases where the "**sip-all.pstnhub.microsoft.com**" FQDN can cause incorrect certificate negotiation between OpenScape SBC and the Microsoft Teams tenant.

Therefore, do NOT configure the SIP trunk to point to "sip-all.pstnhub.microsoft.com" in Unify components unless explicitly recommended by Unify support.

For completeness, this document still presents the configuration of the "**sip-all.pstnhub.microsoft.com**" SIP trunk.

Configuring the Endpoints

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

2.1.1 SBC Endpoint Configuration

1. Go to **OpenScape Common Management Platform > Configuration > OpenScape Voice > Business Group > Profiles > Endpoint** to configure the Endpoint Profile.
2. Click **Add**.
3. In the **General** tab, configure the following:
 - **Name:** **EPP_Teams**
(a common-sense name)
 - **SIP Privacy Support:** **Full**

[OdysseusC] - [BG_GR] - Add Endpoint Profile

Please enter the profile data.

General Endpoints Services

Endpoint Profile

Please enter a unique name to identify this profile.

Name: EPP_SBC01

Remark:

Numbering Plan: NP_BG_GR

Management Information

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

Class of Service:

Routing Area:

Calling Location:

SIP Privacy Support: Full

Failed Calls Intercept Treatment: Disabled

Impact Level: Unclassified

Save Cancel

4. In the **Services** tab, from the **Call Transfer** drop-down menu, select **Yes**.
5. Click **Save**.
6. Navigate to **OpenScape Common Management Platform > Configuration > OpenScape Voice > Business Group > Members > Endpoints** to configure the **Endpoint**.
7. Click **Add**.
8. In the **General** tab, enter the following:
 - **Name:** **EP_SBC01**
(a common-sense name).
 - **Profile:** **EPP_SBC01**
(select previously created endpoint profile).
 - **Endpoint Template:** **Central SBC** (set of pre-configured endpoint attributes)

The screenshot shows a web-based configuration interface for adding a new endpoint. The title bar indicates the context: '[OdysseusC] - [BG_GR] - [Main Office] - Add Endpoint : EP_SBC01'. The 'General' tab is active, showing a list of tabs: General, SIP, Attributes, Aliases, Routes, and Accounting. Below the tabs, a header bar reads 'Endpoint' followed by an information icon and the text 'Define the connection data of an endpoint, e.g. you may use this to add a gateway to a switch.' The main form contains the following fields:

- Name:** EP_SBC01
- Remark:** (empty text area with up/down arrows)
- Registered:** ☐
- Profile:** EPP_SBC01 (with a selection button '...')
- Branch Office:** (empty text field with a selection button '...')
- Associated Endpoint:** (empty text field with a selection button '...')
- Default Home DN:** (empty text field with a selection button '...')
- Location Domain:** (empty text field)
- Endpoint Template:** Central SBC (with a selection button '...')
- Endpoint Type:** Central SBC
- Max number of users:** (empty text field)
- Last Update:** (empty text field)

At the bottom right, there are 'Save' and 'Cancel' buttons.

9. Select the **SIP** tab and configure the following:

- **SIP Trunking:** **Activated**
- **Type:** **Static**
(it can be enabled only if the **SIP Proxy** attribute is enabled)
- **Signaling Address Type:** **IP Address or FQDN** (route the calls via proxy)
- **Endpoint Address:** **10.8.242.72** (SBC LAN interface)
- **Port:** **5060**
- **Transport protocol:** **TCP** (UDP, TLS or MTLS are also possible)
- **SRTP media mode:** **Disabled**
- **Trusted Ports:** **All** (click **Edit** and **Add** all Ports)

[OdysseusC] - [BG_GR] - [Main Office] - Add Endpoint : EP_SBC01

General SIP Attributes Aliases Routes Accounting

Endpoint Type

SIP Private Networking: ☐

SIP Trunking: ☒

SIP-Q Signaling: ☐

SIP Signaling

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

Type: Static

Signaling Address Type: IP Address or FQDN

Endpoint Address: 10.8.242.72

Port: 5060

Transport protocol: TCP

Endpoint does not accept incoming TLS connections: ☐

SRTP media mode: Disabled

Key Exchange Mechanisms Supported: None

AMAT Support: Disabled

Save Cancel

[OdysseusC] - [BG_GR] - [Main Office] - Add Endpoint : EP_SBC01?

General

SIP

Attributes

Aliases

Routes

Accounting

Key Exchange Mechanisms Supported:

None

ANAT Support:

Disabled

ICE Support:

Enabled

DTLS Support:

Enabled

SIP UA Forking Support:

None

Use Proxy/SBC Best-Effort SRTP settings for calls to subscribers:

AS-SIP Interface

Management Address:

Red Sky E911 Manager node:

Outgoing Call Supervision Timer(ms):

Proxy Bypass Supervision Timer (ms):

Treat endpoint as secure

Security

?

Set the Realm, Username and Password for digest authentication or configure the signaling address as a trusted one.

Trusted

Ports:

Edit...

Save

Cancel

10. The **Attributes** tab is populated automatically since the "Central SBC" template was selected in the **General** tab. Make sure that the following are selected:

- **SIP Proxy:** Activated
- **Central SBC:** Activated
- **Route via Proxy:** Activated
- **Enable Session Timer:** Activated

[OdysseusC] - [BG_GR] - [Main Office] - Add Endpoint : EP_SBC01

General SIP **Attributes** Aliases Routes Accounting

Attributes

Attributes available for this SIP endpoint

Supports SIP UPDATE Method for Display Updates	<input type="checkbox"/>
UPDATE for Confirmed Dialogs Supported	<input type="checkbox"/>
Survivable Endpoint	<input type="checkbox"/>
SIP Proxy	<input checked="" type="checkbox"/>
Central SBC	<input checked="" type="checkbox"/>
Route via Proxy	<input checked="" type="checkbox"/>
Allow Proxy Bypass	<input type="checkbox"/>
Public/Offnet Traffic	<input type="checkbox"/>
Accept Billing Number	<input type="checkbox"/>
Use Billing Number for Display Purposes	<input type="checkbox"/>
Allow Sending of Insecure Referred-By Header	<input type="checkbox"/>
Override IRM Codec Restriction	<input type="checkbox"/>
Transfer HandOff	<input type="checkbox"/>

Save Cancel

[OdysseusC] - [BG_GR] - [Main Office] - Add Endpoint : EP_SBC01

General SIP Attributes Aliases Routes Accounting

Set NPI/TON to Unknown ☐

Include Restricted Numbers in From Header ☐

SIPQ Truncated MIME ☐

Enable Session Timer ☒

Ignore Answer for Announcement ☐

Enable TLS RFC5626 Ping ☐

Enable TLS Dual Path Method ☐

Ignore Receipt of 181 Call is Being Forwarded ☐

Use extended max. count for loop prevention ☐

Do Not Audit Endpoint ☐

Use Proxy/SBC ANAT settings for calls to subscribers ☐

Support for Callback Path Reservation ☐

Send Progress to Stop Call Proceeding Supervision Timer ☐

Limited PRACK Support ☐

Support Media Redirection ☐

Save Cancel

11. Select the **Aliases** tab and click **Add**. Enter the following:

- **Name:** 10.8.242.72
(the SBC LAN interface for incoming SIP traffic; if there is a need to restrict the port 5060, the value 10.8.242.72:5060 should be entered, instead).

[OdysseusC] - Add Alias

The Alias name can be 1 to 49 characters long.

Name: 10.8.242.72:5060

OK Cancel

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

2.1.2 MS Teams Endpoint Configuration

1. Go to **OpenScape Common Management Platform > Configuration > OpenScape Voice > Business Group > Profiles > Endpoint** to configure the Endpoint Profile.
2. Click **Add**.

[OdysseusC] - [BG_GR] - Add Endpoint Profile

Please enter the profile data.

General Endpoints Services

Endpoint Profile

Please enter a unique name to identify this profile.

Name: EPP_Teams

Remark:

Numbering Plan: NP_BG_GR

Management Information

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

Class of Service:

Routing Area:

Calling Location:

Time Zone:

SIP Privacy Support: Full Receive

Failed Calls Intercept Treatment: Disabled

Save Cancel

3. In the **General** tab, configure the following:
 - **Name:** EPP_Teams (a common-sense name)
 - **Numbering Plan:** NP_BG_GR
(All translations, destinations and routes regarding MS teams should be assigned to the Numbering Plan of Teams Endpoint Profiles)
 - **SIP Privacy Support:** Full Receive
(the OS Voice does not send a P-Asserted-Identity header field in the messages (requests or responses) to the endpoint. However, the OS Voice SHALL accept any received P-Asserted-Identity header fields)

4. In the **Services** tab, from the **Call Transfer** drop-down menu, select **Yes**.

The screenshot shows a software window titled "[OdysseusC] - [BG_GR] - Add Endpoint Profile". It has three tabs: "General", "Endpoints", and "Services", with "Services" currently selected. A message at the top says "Please enter the profile data." The "Services" tab contains several configuration options, each with a radio button and a dropdown menu:

- Message Waiting:** Set to "No".
- Call Transfer:** Set to "Yes".
- Call Forward Invalid Destination:** Set to "No".
- Toll and Call Restrictions:** Set to "No".
- Park to Server:** Set to "No".
- CSTA Network Interface Device:** Set to "No".

Below these, there is a checkbox labeled "Enable Name Provider and Limited Call Control" which is unchecked. A section titled "What to do if Application fails to handle inbound calls:" contains a dropdown menu set to "Allow call to proceed as normal" and an empty text input field. At the bottom right, there are "Save" and "Cancel" buttons.

5. Click **Save**.

6. Go to **OpenScape Common Management Platform > Configuration > OpenScape Voice > Business Group > Members > Endpoints** to configure the Endpoint.
7. Click **Add**.

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

General | SIP | Attributes | Aliases | Routes | Accounting

Endpoint

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

Name: EP_Teams_SP1

Remark: [Text Area]

Registered: ☐

Profile: EPP_Teams [...]

Branch Office: [Text Field] [...]

Associated Endpoint: [Text Field] [...]

Default Home DN: [Text Field] [...]

Location Domain: [Text Field]

Endpoint Template: [Text Field] [...]

Endpoint Type: [Text Field]

Max number of users: [Text Field]

Last Update: [Text Field]

CSTA Device ID: [Text Field]

Save **Cancel**

8. In the **General** tab, enter the following:
 - **Name:** EP_Teams_SP1 (a common-sense name).
 - **Profile:** EPP_Teams (select previously created endpoint profile).

9. Select the **SIP** tab and enter the following:

- **SIP Trunking:** **Activated**
- **Type:** **Static**
- **Signaling Address Type:** **IP Address or FQDN**
- **Endpoint Address:** **10.8.242.72** (SBC LAN interface)
- **Port:** **50001**
(will be configured in SBC for sip.pstnhub.microsoft.com trunk)
- **Transport protocol:** **TCP** (UDP, TLS or MTLS are also possible)
- **SRTP media mode:** **Disabled**
- **ICE Support:** **Enabled** (default value for static endpoints)
- **SIP UA Forking Support:** **Full**
(If activated, SIP UA fully complies with RFC3261 SDP offer/answer rules)
- **Trusted Ports:** **All**
(click **Edit** and **Add** all Ports)

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

General SIP Attributes Aliases Routes Accounting

Endpoint Type

SIP Private Networking: ☐

SIP Trunking: ☒

SIP-Q Signaling: ☐

SIP Signaling

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

Type: Static

Signaling Address Type: IP Address or FQDN

Endpoint Address: 10.8.242.72

Port: 50001

Transport protocol: TCP

Endpoint does not accept incoming TLS connections: ☐

SRTP media mode: Disabled

Key Exchange Mechanisms Supported: None

ANAT Support: Disabled

Save Cancel

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

General

SIP

Attributes

Aliases

Routes

Accounting

Key Exchange Mechanisms Supported:

None

ANAT Support:

Disabled

ICE Support:

Enabled

DTLS Support:

Enabled

SIP UA Forking Support:

Full

Use Proxy/SBC Best-Effort SRTP settings for calls to subscribers:

AS-SIP Interface

Management Address:

Red Sky E911 Manager node:

Outgoing Call Supervision Timer(ms):

Proxy Bypass Supervision Timer (ms):

Treat endpoint as secure

Security

Set the Realm, Username and Password for digest authentication or configure the signaling address as a trusted one.

Trusted

 Ports:

Edit...

Save

Cancel

10. Go to the **Attributes** tab and configure the following:

For both **Non-Media Bypass Mode** and **Media Bypass Mode**, select the following attributes to activate them:

- **SIP Proxy:** **Activated**
- **Route via Proxy:** **Activated**
(route the calls via proxy)
- **Allow Sending of Insecure Referred-By Header:** **Activated**
(this attribute makes sure, that to the right call account)
- **Do not Send Invite without SDP:** **Activated**
(SIP re-INVITE requests that do not include SDP will not be sent during redirection procedures; OSV will reuse the SDP previously received from the endpoint to send as an SDP offer to the new partner endpoint; when the SDP answer is received the new SDP will be sent in a re-INVITE and the 200 OK answer will be consumed by OS Voice)
- **Send International Numbers in GNF:** **Activated**
(the OS Voice adds a '+' in front of all numbers which have NPI = PUBLIC / NOA = INTERNATIONAL and to do this, both the Translation and the Display Number Modification tables MUST be provisioned to send numbers with NPI = PUBLIC / NOA = INTERNATIONAL to this endpoint)
- **Enable Session Timer:** **Activated**
- **Limited PRACK Support:** **Activated**
(the PRACK-Lite feature provides a limited form of RFC3262 PRACK within OS Voice, supporting PRACK on a half-call basis and only for SIP network-network interfaces)
- **Ignore Receipt/Do not send Privacy Header:** **Activated**
(when PAI is activated in Teams Direct Routing configuration for the SBC endpoint, Teams sends a "Privacy:id" header which causes anonymous call display at called party and with this attribute OS strips this header from PAI)

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

General SIP Attributes Aliases Routes Accounting

Attributes

Attributes available for this SIP endpoint

Supports SIP UPDATE Method for Display Updates	<input type="checkbox"/>
UPDATE for Confirmed Dialogs Supported	<input type="checkbox"/>
Survivable Endpoint	<input type="checkbox"/>
SIP Proxy	<input checked="" type="checkbox"/>
Central SBC	<input type="checkbox"/>
Route via Proxy	<input checked="" type="checkbox"/>
Allow Proxy Bypass	<input type="checkbox"/>
Public/Offnet Traffic	<input type="checkbox"/>
Accept Billing Number	<input type="checkbox"/>
Use Billing Number for Display Purposes	<input type="checkbox"/>
Allow Sending of Insecure Referred-By Header	<input checked="" type="checkbox"/>
Override IRM Codec Restriction	<input type="checkbox"/>
Transfer HandOff	<input type="checkbox"/>
Send P-Preferred-Identity rather than P-Asserted-Identity	<input type="checkbox"/>

Save Cancel

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

General **SIP** **Attributes** **Aliases** **Routes** **Accounting**

Send domain name in From and P-Preferred-Identity headers	<input type="checkbox"/>
Send Redirect Number instead of calling number for redirected calls	<input type="checkbox"/>
Do not send Diversion header	<input type="checkbox"/>
Do not Send Invite without SDP	<input checked="" type="checkbox"/>
Send International Numbers in Global Number Format (GNF)	<input checked="" type="checkbox"/>
Rerouting Direct Incoming Calls	<input type="checkbox"/>
Rerouting Forwarded Calls	<input type="checkbox"/>
Enhanced Subscriber Rerouting	<input type="checkbox"/>
Automatic Collect Call Blocking supported	<input type="checkbox"/>
Send Authentication Number in P-Asserted-Identity header	<input type="checkbox"/>
Send Authentication Number in Diversion Header	<input type="checkbox"/>
Send Authentication Number in From Header	<input type="checkbox"/>
Use SIP Endpoint Default Home DN as Authentication Number	<input type="checkbox"/>
Use Subscriber Home DN as Authentication Number	<input type="checkbox"/>
Set NPI/TON to Unknown	<input type="checkbox"/>
Include Restricted Numbers in From Header	<input type="checkbox"/>

Save **Cancel**

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

General **SIP** **Attributes** **Aliases** **Routes** **Accounting**

SIPQ Truncated MIME	<input type="checkbox"/>
Enable Session Timer	<input checked="" type="checkbox"/>
Ignore Answer for Announcement	<input type="checkbox"/>
Enable TLS RFC5626 Ping	<input type="checkbox"/>
Enable TLS Dual Path Method	<input type="checkbox"/>
Ignore Receipt of 181 Call is Being Forwarded	<input type="checkbox"/>
Use extended max. count for loop prevention	<input type="checkbox"/>
Do Not Audit Endpoint	<input type="checkbox"/>
Use Proxy/SBC ANAT settings for calls to subscribers	<input type="checkbox"/>
Support for Callback Path Reservation	<input type="checkbox"/>
Send Progress to Stop Call Proceeding Supervision Timer	<input type="checkbox"/>
Limited PRACK Support	<input checked="" type="checkbox"/>
Support Media Redirection	<input type="checkbox"/>
Voice Mail Server	<input type="checkbox"/>
Disable Long Call Audit	<input type="checkbox"/>
Send/Receive Impact Level	<input type="checkbox"/>

Save **Cancel**

Attribute	Value
Do Not Allow URNs in R-URI/TO Header for NG911 Calls	<input type="checkbox"/>
Reserve 8	<input type="checkbox"/>
Accept x-channel header	<input type="checkbox"/>
Suppress SPE in SIPQ	<input type="checkbox"/>
Record All Calls	<input type="checkbox"/>
SRC Capable	<input type="checkbox"/>
Add Endpoint Name in Sip URI	<input type="checkbox"/>
Reserved 11	<input type="checkbox"/>
Do not send Conference Indication (Hide isFocus)	<input type="checkbox"/>
Do Not Allow Geolocation Info	<input type="checkbox"/>
Ignore Location by Value on SIP INVITE/REINVITE	<input type="checkbox"/>
Support Foreign Peer Domain	<input type="checkbox"/>
Suppress Alert Info Auto Answer	<input type="checkbox"/>
Support Replaces Header	<input checked="" type="checkbox"/>
Ignore Receipt/Do not send Privacy Header	<input checked="" type="checkbox"/>
Enable REFER Notifications	<input checked="" type="checkbox"/>

Buttons: Save, Cancel

For **Media Bypass Mode** only:

- Select the **Enable REFER Notifications** attribute.
- Go to **OpenScape Common Management Platform > Configuration > OpenScape Voice > Administration > General Settings > RTP**.
- Click on the name of the "*Srx/Sip/PassiveForkingEnable*" parameter.

The **Edit RTP parameter** window opens.

- Set the value of the "*Srx/Sip/PassiveForkingEnable*" parameter to **True**.

For **Non-Media Bypass Mode** only:

- Select the **Support Replaces Header** attribute.
- Go to **OpenScape Common Management Platform > Configuration > OpenScape Voice > Administration > General Settings > RTP**.
- Click on the name of the "*Srx/Sip/MSTeamsMediaBypassMode*" parameter.

The **Edit RTP parameter** window opens.

- Set the value of the "*Srx/Sip/MSTeamsMediaBypassMode*" parameter to **"one" (1)**.

[grdv222c] - Edit RTP parameter - Google Chrome

Not secure https://10.14.255.100/management/portal/Applications/Operation/OSV/Administration/GeneralSettings/PopUps/m...

[grdv222c] - Edit RTP parameter

RTP Parameter Data

Name: Srx/Sip/MSTeamsMediaBypassMode

Type: Integer

Unit: int

Range: [0-2]

Process restart is required: false

Value: 1

Suggested Value: 0

Description: OSV-19257 This parameter is used to handle different call handling based upon the media bypass mode. Setting this parameter to 0, MS Teams functionality over SIP Trunk is disabled. Setting this parameter to 1, OSV works on non-media bypass mode. Setting this parameter to 2, OSV works on media bypass mode.

Save Cancel

11. Select the **Aliases** tab and click **Add**.

- In the **Name** field, enter **10.8.242.72:50001** (the SBC LAN interface for incoming SIP traffic restricted for port 50001, that corresponds to Teams SIP Proxy 1 related traffic)

[OdysseusC] - Add Alias

The Alias name can be 1 to 49 characters long.

Name: 10.8.242.72:50001

OK Cancel

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

13. Repeat the same procedure to create the endpoints for the remaining Teams

FQDNs:

- **EP_Teams_SP2** with port **50002**
(for sip2.pstnhub.microsoft.com)
- **EP_Teams_SP3** with port **50003**
(for sip3.pstnhub.microsoft.com)
- **EP_Teams_ALL** with port **50004**
(for sip-all.pstnhub.microsoft.com)

2.1.3 SSP Endpoint Configuration

1. Go to OpenScape Common Management Platform > Configuration > OpenScape Voice > Business Group > Profiles > Endpoint to configure the Endpoint Profile.
2. Click **Add**.

[OdysseusC] - [BG_GR] - Add Endpoint Profile

Please enter the profile data.

General Endpoints Services

Endpoint Profile

Please enter a unique name to identify this profile.

Name: EPP_BCOM

Remark:

Numbering Plan: NP_BG_GR ...

Management Information

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

Class of Service: ...

Routing Area: ...

Calling Location: ...

Time Zone: ...

SIP Privacy Support: Full

Failed Calls Intercept Treatment: Disabled

Save Cancel

3. In the **General** tab, enter the following:
 - **Name:** **EPP_BCOM** (a common-sense name)
 - **SIP Privacy Support:** **Full**

[OdysseusC] - [BG_GR] - Add Endpoint Profile ?

Please enter the profile data.

General **Endpoints** **Services**

● Message Waiting: No ▼

● Call Transfer: Yes ▼

● Call Forward Invalid Destination: No ▼

● Toll and Call Restrictions: No ▼

● Park to Server: No ▼

● CSTA Network Interface Device: No ▼ ☐ Enable Name Provider and Limited Call Control

What to do if Application fails to handle inbound calls:

Allow call to proceed as norm: ▼

4. In the **Services** tab, from the **Call Transfer** drop-down menu, select **Yes**.
5. Click **Save**.

6. Go to **OpenScape Common Management Platform > Configuration > OpenScape Voice > Business Group > Members > Endpoints** to configure the Endpoint.
7. Click **Add**.

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

General SIP Attributes Aliases Routes Accounting

Endpoint

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

Name: EP_BCOM

Remark:

Registered: ☐

Profile: EPP_BCOM

Branch Office:

Associated Endpoint:

Default Home DN

Location Domain

Endpoint Template:

Endpoint Type:



Max number of users:

Last Update:

CSTA Device ID:

Save Cancel

8. In the **General** tab, enter the following:
 - **Name:** EP_BCOM (a common-sense name).
 - **Profile:** EPP_BCOM (select previously created endpointprofile).



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


General
SIP
Attributes
Aliases
Routes
Accounting

Endpoint Type

SIP Private Networking: ☐
SIP Trunking: ☒
SIP-Q Signaling: ☐

SIP Signaling


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

Type:

Signaling Address Type:

Endpoint Address:

Port:

Transport protocol:

Endpoint does not accept incoming TLS connections: ☐

SRTP media mode:

Key Exchange Mechanisms Supported:

ANAT Support:

Save

Cancel

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

General SIP Attributes Aliases Routes Accounting

Key Exchange Mechanisms Supported: None

ANAT Support: Disabled

ICE Support: Enabled

DTLS Support: Enabled

SIP UA Forking Support: None

Use Proxy/SBC Best-Effort SRTP settings for calls to subscribers: ☐

AS-SIP Interface ☐

Management Address:

Red Sky E911 Manager node: ☐

Outgoing Call Supervision Timer(ms):

Proxy Bypass Supervision Timer (ms):

Treat endpoint as secure ☐

Security

Set the Realm, Username and Password for digest authentication or configure the signaling address as a trusted one.


Trusted ☒ Ports:

9. Select the **SIP** tab and configure the following:

- **SIP Trunking:** Activated
- **Type:** Static
- **Signaling Address Type:** IP Address or FQDN
- **Endpoint Address:** 10.8.242.72 (SBC LAN interface)
- **Port:** 50010
- (will be configured in SBC for sip.pstnhub.microsoft.com trunk)
- **Transport protocol:** TCP (UDP, TLS or MTLS are also possible)
- **SRTP media mode:** Disabled
- **ICE Support:** Enabled (default value for static endpoints)
- **SIP UA Forking Support:** None
- (if activated, SIP UA fully complies with RFC3261 SDP offer/answer rules)
- **Trusted** Ports: All (click on **[Edit]** and **[Add]** all Ports)

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

- **SIP Proxy:** Activated
- **Route via Proxy:** Activated
(route the calls via proxy)
- **Allow Sending of Insecure Referred-By Header:** Activated
(this attribute makes sure, that calls get charged to the right call account)
- **Do not Send Invite without SDP:** Activated
(SIP re-INVITE requests that do not include SDP will not be sent during redirection procedures; OSV will reuse the SDP previously received from the endpoint to send as an SDP offer to the new partner endpoint; when the SDP answer is received the new SDP will be sent in a re-INVITE and the 200 OK answer will be consumed by OS Voice)
- **Send International Numbers in GNF:** Activated
(the OS Voice adds a '+' in front of all numbers which have NPI = PUBLIC / NOA = INTERNATIONAL and to do this, both the Translation and the Display Modification tables MUST be provisioned to send numbers with NPI = PUBLIC / NOA = INTERNATIONAL to this endpoint)
- **Enable Session Timer:** Activated
- **Limited PRACK Support:** Activated
(the PRACK-Lite feature provides a limited form of RFC3262 PRACK within Voice, supporting PRACK on a half-call basis and only for SIP network-network interfaces)
- **Support Replaces Header:** Activated
- **Ignore Receipt/Do not send Privacy Header:** Deactivated
- **Enable REFER Notifications:** Activated

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

?

General

SIP

Attributes

Aliases

Routes

Accounting

Attributes

i

Attributes available for this SIP endpoint

Supports SIP UPDATE Method for Display Updates

☐

UPDATE for Confirmed Dialogs Supported

☐

Survivable Endpoint

☐

SIP Proxy

☒

Central SBC

☐

Route via Proxy

☒

Allow Proxy Bypass

☐

Public/Offnet Traffic

☐

Accept Billing Number

☐

Use Billing Number for Display Purposes

☐

Allow Sending of Insecure Referred-By Header

☒

Override IRM Codec Restriction

☐

Transfer HandOff



☐

Send P-Preferred-Identity rather than P-Asserted-Identity

☐

Save

Cancel


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


General

SIP

Attributes

Aliases

Routes

Accounting

Send domain name in From and P-Preferred-Identity headers	<input type="checkbox"/>
Send Redirect Number instead of calling number for redirected calls	<input type="checkbox"/>
Do not send Diversion header	<input type="checkbox"/>
Do not Send Invite without SDP	<input checked="" type="checkbox"/>
Send International Numbers in Global Number Format (GNF)	<input checked="" type="checkbox"/>
Rerouting Direct Incoming Calls	<input type="checkbox"/>
Rerouting Forwarded Calls	<input type="checkbox"/>
Enhanced Subscriber Rerouting	<input type="checkbox"/>
Automatic Collect Call Blocking supported	<input type="checkbox"/>
Send Authentication Number in P-Asserted-Identity header	<input type="checkbox"/>
Send Authentication Number in Diversion Header	<input type="checkbox"/>
Send Authentication Number in From Header	<input type="checkbox"/>
Use SIP Endpoint Default Home DN as Authentication Number	<input type="checkbox"/>
Use Subscriber Home DN as Authentication Number	<input type="checkbox"/>
Set NPI/TON to Unknown	<input type="checkbox"/>
Include Restricted Numbers in From Header	<input type="checkbox"/>

Save

Cancel

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

General
SIP
Attributes
Aliases
Routes
Accounting

SIPQ Truncated MIME	<input type="checkbox"/>
Enable Session Timer	<input checked="" type="checkbox"/>
Ignore Answer for Announcement	<input type="checkbox"/>
Enable TLS RFC5626 Ping	<input type="checkbox"/>
Enable TLS Dual Path Method	<input type="checkbox"/>
Ignore Receipt of 181 Call is Being Forwarded	<input type="checkbox"/>
Use extended max. count for loop prevention	<input type="checkbox"/>
Do Not Audit Endpoint	<input type="checkbox"/>
Use Proxy/SBC ANAT settings for calls to subscribers	<input type="checkbox"/>
Support for Callback Path Reservation	<input type="checkbox"/>
Send Progress to Stop Call Proceeding Supervision Timer	<input type="checkbox"/>
Limited PRACK Support	<input checked="" type="checkbox"/>
Support Media Redirection	<input type="checkbox"/>
Voice Mail Server	<input type="checkbox"/>
Disable Long Call Audit	<input type="checkbox"/>
Send/Receive Impact Level	<input type="checkbox"/>

Save
Cancel

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

?

General

SIP

Attributes

Aliases

Routes

Accounting

Reserve 8

Accept x-channel header

Suppress SPE in SIPQ

Record All Calls

SRC Capable

Add Endpoint Name in Sip URI

Reserved 11

Do not send Conference Indication (Hide isFocus)

Do Not Allow Geolocation Info

Ignore Location by Value on SIP INVITE/REINVITE

Support Foreign Peer Domain

Suppress Alert Info Auto Answer

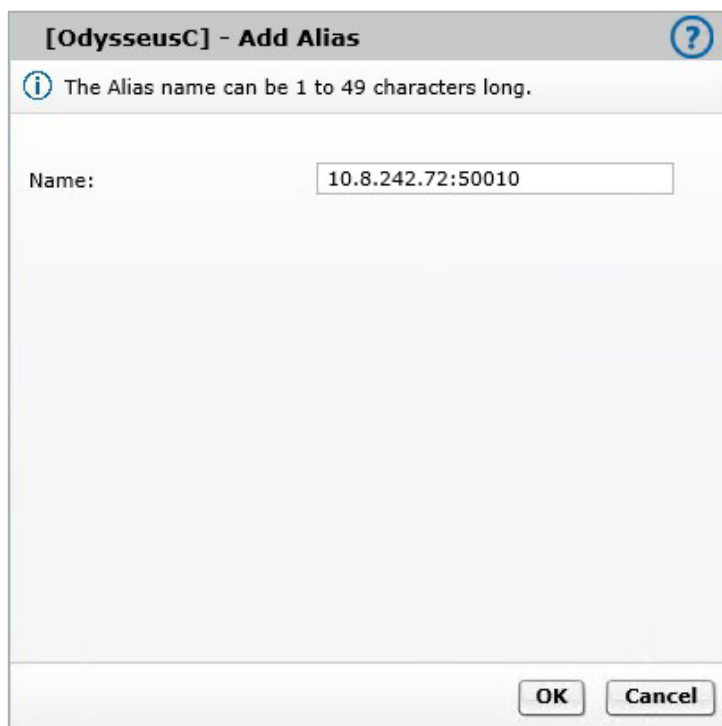
Support Replaces Header

Ignore Receipt/Do not send Privacy Header

Enable REFER Notifications

Save

Cancel



11. Select the **Aliases** tab and click **Add**.

- In the **Name** field, enter **10.8.242.72:50010**
(the SBC LAN interface for incoming SIP traffic restricted for port 50010, that corresponds to BCOM ITSP related traffic)

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

2.2. Enabling the Registration flag

1. Go to OpenScape Common Management Platform > Configuration > OpenScape Voice > Business Group > Members > Endpoints window. A list of all the configured endpoints in OS Voice is displayed.

The registration flag for the newly created endpoints needs to be activated.

2. Select an endpoint and click **Edit**. As an example:

[OdysseusC] - [BG_GR] - [Main Office] - Edit Endpoint : EP_Teams_SP1

General | SIP | Attributes | Aliases | Routes | Accounting

Endpoint

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

Name: EP_Teams_SP1

Remark:

Registered: ☒

Profile: EPP_Teams

Branch Office:

Associated Endpoint:

Default Home DN:

Location Domain:

Endpoint Template:

Endpoint Type:

Max number of users:

Last Update: 2021-10-13 12:59:48.0

CSTA Device ID:

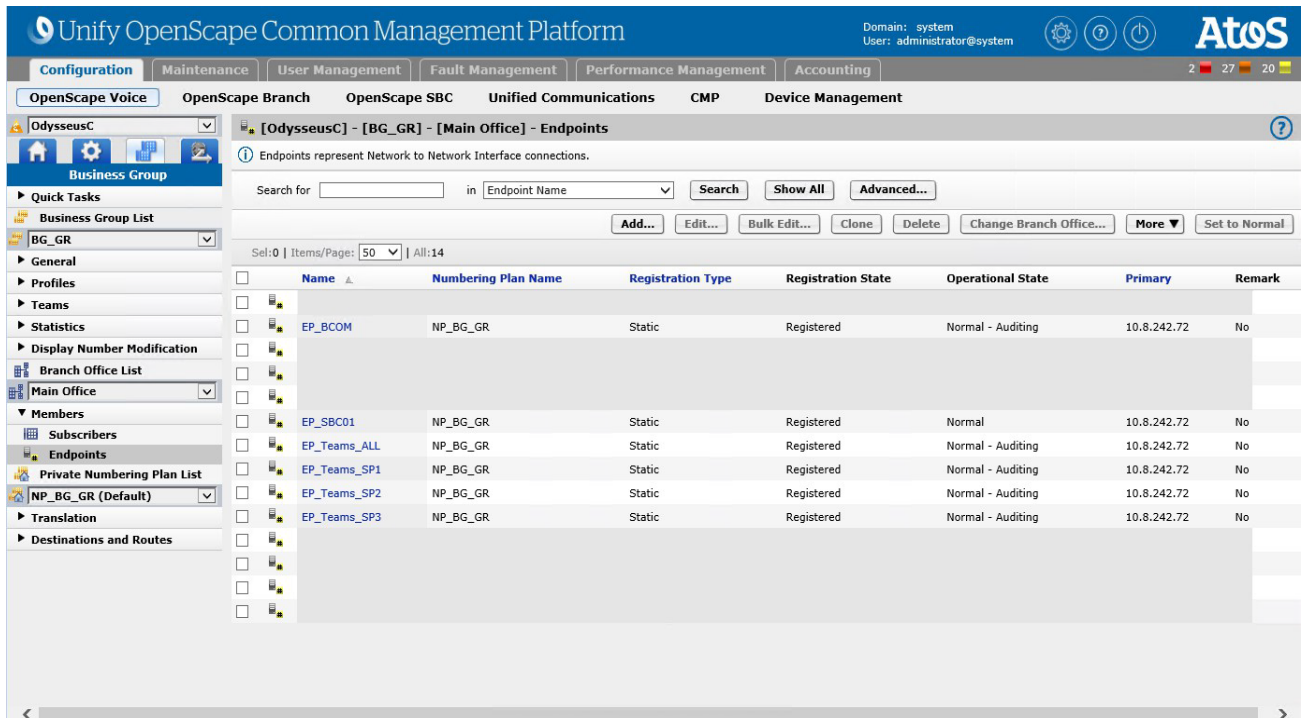
Save **Cancel**

- In the **General** tab, select the **Registered** checkbox.

Note: The *Registered* checkbox can only be enabled if the SIP Type under the SIP tab is set to *Static*. This option specifies the registration state for the endpoint.

- To activate the sending of **SIP OPTIONS** messages for the Teams and SSP endpoints, select the endpoint and click **More**.
- Select the **"Periodic Audit Enable"** option from the drop-down menu.

The newly created endpoints in the CMP endpoint overview window are shown below as an example:




2.3 Configuring Destinations & Routes

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

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

2.3.1 MS Teams Destination Configuration

1. Navigate to OpenScope Common Management Platform > Configuration > OpenScope Voice > Business Group > Destinations and Routes > Destinations.
2. Click **Add**.

 [OdysseusC] - [BG_GR] - [NP_BG_GR] - Add Destination ?

i Destinations are used for routing a call to an endpoint.

General Routes Route Lists Destination Codes

Name:

is a Media Server: ☐

is Conference Focus Server : ☐

3. In the **General** tab enter the following:
 - **Name:** **DST_Teams** (a common-sense name).
4. Click **Save**.
5. Select the "**DST_Teams**" destination and click **Edit**.

[OdysseusC] - [BG_GR] - [NP_BG_GR] - Add Route

A route connects the destination with an endpoint representing a gateway.

The Route ID indicates the priority level.

ID:

Type:

SIP Endpoint:

Originator Attributes

Restricts the traffic according to specified settings. Routes with the same restrictions can be prioritized.

Signaling Type:

Bearer Capability:

Destination Directory Number

*Number of digits to delete: Leading digits are cut off from the Directory Number.
Digits to insert: the digit string is added to the beginning of the remaining digits.*

Modification Type:

Number of digits to delete:

Digits to insert:

Nature of Address:

6. Configure the associated **"Route"**, by clicking in **"Routes"** tab and entering the following:
 - **ID:** 1
 - (the priority of the route; if there are multiple routes to a destination and route prioritization is selected, the route with the lowest numbered route ID has the highest priority, and will be selected first)
 - **SIP Endpoint:** EP_Teams_SP1
 - **Modification Type:** Number Manipulation
 - **Nature of Address:** International
7. Repeat the same procedure for the remaining Teams endpoints, but different ID should be assigned per endpoint:
 - "EP_Teams_SP2 → ID = 2"
 - "EP_Teams_SP3 → ID = 3"
 - "EP_Teams_ALL → ID = 4"
8. To populate the **"SIP Endpoint"** box with e.g., the "EP_Teams_SP1" endpoint:
 - a. Click the corresponding button, then select **"Main Office"** in the pop-up window.
 - b. Click **Next**.
 - c. Select "EP_Teams_SP1" from the list.
 - d. Click **OK**.

9. To enable the MS Teams route prioritization:

- Go to the **"Route Lists"** tab
- Select the **"Prioritized"** checkbox.
- Click **Save**.

[OdysseusC] - [BG_GR] - [NP_BG_GR] - Edit Destination: DST_Teams

Destinations are used for routing a call to an endpoint.

General | Routes | **Route Lists** | Destination Codes

Route Lists

This list provides an overview of all routes with the same originating signaling type and bearer capability. Prioritization is possible.

Items/Page: 10 | All: 1

Originating Signaling Type	Originating Bearer Capability	Prioritized	Fallback to Local Numbering Plan
Unassigned	Unassigned	<input checked="" type="checkbox"/>	w Dialed Number <input type="checkbox"/> w Modified Number <input type="checkbox"/>

Save Cancel

After saving the configuration, the **"Routes"** tab should appear as shown below:

[OdysseusC] - [BG_GR] - [NP_BG_GR] - Edit Destination: DST_Teams

Destinations are used for routing a call to an endpoint.

General | **Routes** | Route Lists | Destination Codes

Routes

Multiple routes can be used for prioritizing the routes to the gateways.

Add... Edit... Delete

Sel: 0 | Items/Page: 10 | All: 4

ID	Endpoint	Route Type	Delete	Insert	Nature of Address
1	EP_Teams_SP1	SIP-Endpoint	0		International
2	EP_Teams_SP2	SIP-Endpoint	0		International
3	EP_Teams_SP3	SIP-Endpoint	0		International
4	EP_Teams_ALL	SIP-Endpoint	0		International

Save Cancel

2.3.2 SSP Destination Configuration

1. Go to **OpenScape Common Management Platform > Configuration > OpenScape Voice > Business Group > Destinations and Routes > Destinations.**
2. Click **Add.**

The screenshot shows the 'Add Destination' window for the configuration path [OdysseusC] - [BG_GR] - [NP_BG_GR]. The window has a title bar with a help icon. Below the title bar is a tabbed interface with four tabs: 'General' (selected), 'Routes', 'Route Lists', and 'Destination Codes'. A message icon with an 'i' is followed by the text 'Destinations are used for routing a call to an endpoint.' The 'General' tab contains the following fields:

- Name:** A text box containing 'DST_BCOM'.
- is a Media Server:** A checkbox that is currently unchecked.
- is Conference Focus Server :** A checkbox that is currently unchecked.

At the bottom right of the window are 'Save' and 'Cancel' buttons.

3. In the **General** tab enter the following:
 - **Name:** **DST_BCOM** (a common-sense name).
4. Click **Save.**
5. Select the "**DST_BCOM**" destination and click **Edit.**

The screenshot shows the 'Add Route' window for the configuration path [OdysseusC] - [BG_GR] - [NP_BG_GR]. The window has a title bar with a help icon. Below the title bar is a message icon with an 'i' followed by the text 'A route connects the destination with an endpoint representing a gateway.' The window is divided into several sections:

- ID:** A section with a message icon and the text 'The Route ID indicates the priority level.' Below this is a text box for 'ID:' containing the value '1'.
- Type:** A dropdown menu currently set to 'SIP Endpoint'.
- SIP Endpoint:** A text box containing 'EP_BCOM' and a button with three dots '...'.
- Originator Attributes:** A section with a message icon and the text 'Restricts the traffic according to specified settings. Routes with the same restrictions can be prioritized.' Below this are two dropdown menus: 'Signaling Type' set to 'Undefined' and 'Bearer Capability:' set to 'Unassigned'.
- Destination Directory Number:** A section with a message icon and the text 'Number of digits to delete: Leading digits are cut off from the Directory Number. Digits to insert: the digit string is added to the beginning of the remaining digits.' Below this is a dropdown menu for 'Modification Type:' set to 'None'.

At the bottom right of the window are 'Save' and 'Cancel' buttons.

6. Configure the associated **Route**, by clicking in **Routes** tab and entering the following:

- **ID:** 1
- SIP Endpoint: EP_BCOM
- Modification Type: None

6. Click **Save**.

The **Route** tab should appear as shown below:

[OdysseusC] - [BG_GR] - [NP_BG_GR] - Edit Destination: DST_BCOM

Destinations are used for routing a call to an endpoint.

General Routes Route Lists Destination Codes

Routes

Multiple routes can be used for prioritizing the routes to the gateways.

Add... Edit... Delete

Sel:0 | Items/Page: 10 | All:1

	ID	Endpoint	Route Type	Delete	Insert	Nature of Address
<input type="checkbox"/>	1	EP_BCOM	SIP-Endpoint	0		Undefined

Save Cancel

2.3.3 Viewing Destinations

Go to OpenScope Common Management Platform > Configuration > OpenScope Voice > **Business Group > Destinations and Routes > Destinations** window.

The MS Teams and SSP (BCOM) destinations are displayed:

The screenshot displays the Unify OpenScope Common Management Platform interface. The top navigation bar includes tabs for Configuration, Maintenance, User Management, Fault Management, Performance Management, and Accounting. The main menu on the left lists various management areas, with 'Business Group' selected. The central pane shows the 'Destinations' window for the 'OdysseusC' system, specifically for the '[BG_GR] - [NP_BG_GR] - Destinations' view. A search bar is present above a table of destinations. The table has columns for 'Name', 'Media Server', and 'Number of Routes'. Two destinations are listed: 'DST_BCOM' with 1 route and 'DST_Teams' with 4 routes. The interface also includes a sidebar with 'Quick Tasks' and a bottom status bar.

Name	Media Server	Number of Routes
DST_BCOM	False	1
DST_Teams	False	4

2.4 Configuring Translation

With **Translation**, the administrator configures where outgoing calls from OpenScape Voice subscribers are routed based on the dialed digits.

A call can only be routed if the dialed digits match a **PAC (Prefix Access Code)**.

The **Destination Code** feature provides destination codes for basic telephone service. A destination code is used for a call if the dialed (or PAC-modified) digits and the address match.

2.4.1 MS Teams Numbers Routing Configuration

1. Navigate to OpenScape Common Management Platform > Configuration > OpenScape Voice > Business Group > Translation > Prefix Access Codes.

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

Identification

① If the dialed digits match this code, the specified modification to these dialed digits is executed.

Prefix Access Code: 3185008

Remark:

Minimum Length: 11

Maximum Length: 20

Digit Position: 0

Digits to insert:

Settings

① Specify additional parameters to determine how the call will be routed.

Prefix Type: Off-net Access

Nature of Address: Unknown

Destination Type: None

Destination:

Save Cancel

2. Click **Add** and configure the following:

- **Prefix Access Code:** 3185008
(the starting digits of Teams subscriber numbers)
- **Minimum Length:** 11
(minimum expected length of Teams numbers)
- **Maximum Length:** 20
(maximum expected length of Teams numbers)
- **Digit Position:** 0

- (don't remove any digits from dialed number before sending them to destination)
- **Prefix Type:** **Off-net Access**
(a prefix access code to permit access to remote destinations)
 - **Nature of Address:** **Unknown**
 - **Destination Type:** **None**

The resulting digits will be processed in the user's numbering plan's destination codes table.

3. Click **Save**.
4. Go to **OpenScape Common Management Platform > Configuration > OpenScape Voice > Business Group > Translation > Destination Codes**.

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

Identification

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

Destination Code: 3185008

Remark:

Nature Of Address: Unknown

Originator Attributes

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

Class Of Service:

Routing Area:

Traffic Type

Specify the traffic type for this destination code.

None ☒

Use Local Toll Table ☐

Select Traffic Type ☐

Destination

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

Destination Type: Destination

Destination: DST_Teams

DN Office Code:

Save **Cancel**

5. Click **Add** and enter the following:
 - **Destination Code:** 3185008 (select the previously created PAC).
 - **Nature of Address:** Unknown
 - **Destination Type:** Destination
 - **Destination:** DST_Teams
6. Click **Save**.

2.4.2 PSTN Numbers Routing Configuration

1. Go to **OpenScape Common Management Platform > Configuration > OpenScape Voice > Business Group > Translation > Prefix Access Codes**.

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

Identification

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

Prefix Access Code: 498970072

Remark:

Minimum Length: 13

Maximum Length: 13

Digit Position: 0

Digits to insert:

Settings

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

Prefix Type: Off-net Access

Nature of Address: International

Destination Type: None

Destination:

Save **Cancel**

2. Click **Add**.



The **Add Prefix Access Code** window opens.

3. Configure the following settings:
 - **Prefix Access Code:** 498970072
(the starting digits of PSTN subscriber numbers).
 - **Minimum Length:** 13 (minimum expected length of PSTN numbers).
 - **Maximum Length:** 13 (maximum expected length of PSTN numbers).


- **Digit Position:** 0
(don't remove any digits from dialed number before sending them to destination).
- **Prefix Type:** Off-net Access
(a prefix access code to permit access to remote destinations).
- **Nature of Address:** International.
- **Destination Type:** None
(the resulting digits will be processed in the user's numbering plan's destination codes table).


4. Click **Save**.

5. Go to **OpenScape Common Management Platform > Configuration > OpenScape Voice > Business Group > Translation > Destination Codes**.


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


Identification


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


Destination Code: 


Remark:

Nature Of Address:


Originator Attributes

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

Class Of Service: 


Routing Area: 

Traffic Type


 Specify the traffic type for this destination code.

None ☒


Use Local Toll Table ☐


Select Traffic Type ☐ 



Destination

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

Destination Type:

Destination: 

DN Office Code: 

6. Click **Add** and enter the following:

- **Destination Code:** 498970072 (select the previously created PAC).
- Nature of Address: International
- Destination Type: Destination
- Destination: DST_BCOM

6. Click **Save**.

2.4.3 Domain Codes Configuration

1. Go to **OpenScape Common Management Platform > Configuration > OpenScape Voice > Business Group > Translation > Domain Codes**.

The screenshot shows a web-based configuration window titled "[OdysseusC] - [BG_GR] - [NP_BG_GR] - Add Domain Code". The window has a "General" tab selected. It is divided into several sections: "Identification", "Translation Redirect", "Code Processing", and "Traffic Type".

Identification Section:

- An information icon and text: "This domain code will be used for a call if the dialed domain or part of the dialed domain matches".
- Domain Code:** A text input field containing "10.8.242.72".
- Class Of Service:** A text input field, followed by a "...", and a "Clear" button.
- Routing Area:** A text input field, followed by a "...", and a "Clear" button.
- Remark:** A text input field with up and down arrow icons on the right.

Translation Redirect Section:

- Prefix Type:** A dropdown menu with "Off-net Access" selected.
- Redirect To:** A dropdown menu with "None" selected.

Code Processing Section:

- Retranslate:** A checkbox, currently unchecked.
- Number:** A text input field.

Traffic Type Section:

- An information icon and text: "Specify the traffic type for this domain code."

At the bottom right of the window are "Save" and "Cancel" buttons.

[OdysseusC] - [BG_GR] - [NP_BG_GR] - Add Domain Code

General

Translation Redirect

Prefix Type: Off-net Access

Redirect To: None

Code Processing

Retranslate: ☐

Number:

Traffic Type

Specify the traffic type for this domain code.

None ☒

Select Traffic Type ☐ ...

Destination

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

Destination Type: Destination

Destination Name: DST_Teams ... Clear

Save Cancel

2. Click **Add** and configure the following:

- **Domain Code:** 10.8.242.72 (SBC core IP)
- **Prefix Type:** Off-net Access
- **Redirect To:** None
- **Destination Name:** DST_Teams

3. Click **Save**.

2.5 Activating SIP UA Forking

OSV Passive Forking (UAC) provides an interworking function which essentially merges multiple Microsoft Teams downstream early dialogs into a single upstream SIP dialog. This functionality shields upstream SIP clients (SIP UAC) establishing sessions with the MS Teams network from being exposed to the full RFC 3261/RFC3264 forking SIP Proxy server behavior of the MS Teams Phone System. The SIP UA Forking tab is used to enable the feature and list all devices configured with their respective SIP forking capability.

1. To activate the OSV Passive Forking feature, go to **OpenScape Common Management Platform > Configuration > OSV > Administration > Signaling Management > SIP**.

[OdysseusC]- SIP Settings

SIP Settings

General Rerouting Audit SIP Timers DTLS Interworking SRTP Interworking

ICE Support AEI Support FQDN ANAT Interworking Responsible Domains **SIP UA Forking**

SIP UA Forking Configuration

OSV Passive Forking: Enabled

SIP UA Forking Devices

List of device identifiers that, when present in the UA header will cause the registering device be accounted as compatible with the SIP UA Proxy Capability setting.

Add... Edit... Delete

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

<input type="checkbox"/>	Device Identifier	SIP UA Forking Capability
--------------------------	-------------------	---------------------------

Save Cancel

2. From the **OSV Passive Forking** drop-down menu, select **Enabled**.
3. Click **Save**.

2.6 Configuring Display Number Modification (optional)

If there is a requirement to manipulate the **FROM** header of an INVITE message (e.g., from the SBC to SSP), the header manipulation is performed in the OS Voice **Display Number Modification** configuration area.

In the following example, the FROM header will be manipulated to include the number in **national format** instead of the international format (E.164).

1. To add the Dutch office code to OS Voice, go to **OpenScape Common Management Platform > Configuration > OSV > Global Translation and Routing > Directory Numbers > Office Codes**.
2. Click **Add**.

The **Add Office Code** window opens.

[OdysseusC]-Add Office Code

Add Office Code

An external caller must dial the Office Code plus the extension number.

Country Code: 31

Area Code: 85

Local Office Code: 0080

Directory Number Range

Optionally a Directory Number Range can be created and reserved for a Business Group.

Directory Number Start: 31850080 990

Directory Number End: 31850080

Business Group Name: ...

Save Cancel

3. Configure the following:

- Country Code: 31
- Area Code: 85
- Local Office Code: 0080
- Directory Number Start: 990 (starting extension).

4. Click **Save**.

4. Go to **OpenScope Common Management Platform > Configuration > OSV > BG > Display Number Modification > Definitions.**
5. Click **Add.**

[OdysseusC]- Display Number Definition

Context Settings

Select a numbering plan from the list.

Business Group: BG_GR

Numbering Plan: ANY

Number Definition

To define a public number, enter country code, area code, local office code and possibly a skip position that defines the numbers of digits to skip in the Local Office Code to create an extension. To define a private number, enter the L2 code, the L1 code, the L0 code and possibly a skip position that defines the number of digits to skip in the L0 code to create an extension. If known, also enter the minimum and maximum number of digits in the fully qualified number definition.

Numbering plan indicator: Public

Country/L2 Code: 31

Area/L1 Code: 85

Local Office/L0 Code: 0080

Number of digits to skip: 3

Min. Digits: 11

Max. Digits: 11

Local Toll

A Local Toll table may define the format of public network numbers as seen by subscribers that match this office code.

Local Toll:

Save Cancel

6. Add the Dutch office code by entering the following:
 - Numbering plan indicator: **Public**
 - Country/L2 Code: **32**
 - Area/L1 Code: **85**
 - Local Office/L0 Code: **0080**
 - Number of digits to skip: **3**
(indicates the numbers of digits to skip in the Local Office Code (NPI = Public) or L0 Code (NPI = Private) to create an extension).
 - Min. Digits: **11**
 - Max. Digits: **11**
7. Click **Save.**

8. Go to **OpenScape Common Management Platform > Configuration > OSV > BG > Display Number Modification > Modifications.**
9. Click **Add.**

[OdysseusC]-Display Number Modification

Create/Edit the "calling party display number" to a specific format

Originating Context Setting

Selected business group and/or numbering plan.

Business Group ANY

Numbering Plan ANY

Terminating Context Setting

Selected numbering plan and/or endpoint.

Business Group BG_GR

Numbering Plan NP_BG_GR

Endpoint EP_BCOM

Modification Rule

Select Input Type of Number, Priority and define which number needs to be put out (Number Source), what the format is (Output TON), how to optimize it (Optimize TON) and whether a prefix needs to be added and whether presentation is restricted.

Input Type Of Number: International

Priority: 1

Output Type Of Number: International

Number Source: Input Number

Presentation Restricted: ☐

Prefix Required: ☐

Optimize Type Of Number: National

Save **Cancel**

10. Add the Dutch office code by configuring the following:

- **Endpoint:** EP_BCOM
- **Input Type Of Number:** International
- **Priority:** 1 (highest priority)
- **Output Type Of Number:** International
- **Number Source:** Input Number
(defines the input format of the "presenter number" when it comes into the OpenScape Voice)

- **Optimize Type Of number:** **National**
(defines the conversion by call processing of an explicit "*calling number*" to a desired format before the number is transmitted to the destination)

11. Click **Save**.

12. Go to **OpenScape Common Management Platform > Configuration > OSV > BG > Members > Endpoints** and select the "**EP_BCOM**" endpoint.

13. Click **Edit**.

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

General | SIP | Attributes | Aliases | Routes | Accounting

Name: EP_BCOM

Remark:

Registered: ☒

Profile: EPP_BCOM ...

Branch Office: ...

Associated Endpoint: ...

Default Home DN 31(85)0080991 ...

Location Domain

Endpoint Template: ...

Endpoint Type:

Max number of users:

Last Update: 2021-11-04 11:05:03.0

CSTA Device ID:

Associated Subscriber DN 31(85)0080991 ...

Save **Cancel**

14. Set the "**Default Home DN**" (set the location of the endpoint in Dutch) to "**31850080990**" (provided by the SSP).

Note: With current OS Voice implementation, the PAI header modification is not possible from the **Display Number Modification** configuration.

15. If the international number format is not desired in PAI header for calls from Teams to PSTN, you can configure the following in the **Attributes** tab:

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

General SIP Attributes Aliases Routes Accounting

Send Redirect Number instead of calling number for redirected calls ☐

Do not send Diversion header ☐

Do not Send Invite without SDP ☒

Send International Numbers in Global Number Format (GNF) ☒

Rerouting Direct Incoming Calls ☐

Rerouting Forwarded Calls ☐

Enhanced Subscriber Rerouting ☐

Automatic Collect Call Blocking supported ☐

Send Authentication Number in P-Asserted-Identity header ☒

Send Authentication Number in Diversion Header ☐

Send Authentication Number in From Header ☐

Use SIP Endpoint Default Home DN as Authentication Number ☒

Use Subscriber Home DN as Authentication Number ☐

Set NPI/TON to Unknown ☐

Include Restricted Numbers in From Header ☐

Save Cancel

When "**Send Authentication Number in P-Asserted-Identity header**" is "**Activated**", the PAI header contains the calling party's name and the dialable number.

When enabled, the display rules that are usually used for populating the PAI header are overridden, apart from the **Display Number Modification** rules.

When "**Use SIP Endpoint Default Home DN as Authentication Number**" is "**Activated**", the Default Home DN provisioned for the SIP endpoint is used to populate the authenticated number.

3 Configuring OpenScape SBC

This chapter outlines the configuration of OpenScape SBC for interworking with Teams Direct Routing.

The OpenScape SBC will be configured with the connection to OS Voice, SSP (BCOM) and Teams Phone System (remote) endpoints.

As an example:

Items	Example
SBC Core (LAN) IP	10.8.242.72
SBC Access (WAN) IP	195.97.14.76
SBC Public FQDN	sbc01.athdrlabs.xyz
OS Voice node 1 (SIP Signaling) IP	10.8.242.16 TCP 5060
OS Voice node 2 (SIP Signaling) IP	10.8.242.26 TCP 5060
Teams FQDN 1 SIP trunk	sip.pstnhub.microsoft.com TLS 5061 (LAN port for OS Voice trunk 50001)
Teams FQDN 2 SIP trunk	sip2.pstnhub.microsoft.com TLS 5061 (LAN port for OS Voice trunk 50002)
Teams FQDN 3 SIP trunk	sip3.pstnhub.microsoft.com TLS 5061 (LAN port for OS Voice trunk 50003)
Teams FQDN ALL SIP trunk	sip-all.pstnhub.microsoft.com ^{see note} TLS 5061 (LAN port for OS Voice trunk 50004)
SSP (BCOM) SIP trunk	Remote URL: sip.bcom.nl Default Home DN: 31850080990 (LAN port for OS Voice trunk 50010)

Routine or not MS Teams Direct Routing specific OS SBC configuration will be omitted. OpenScape SBC installation and administration documentation can be found in the [Unify customer documentation site](#).

Important:

Per Microsoft's announcement, support for the *"sip-all.pstnhub.microsoft.com"* FQDN will end in March 2022.

Although Microsoft recommends using the three FQDNs for Direct Routing connection points — **"sip.pstnhub.microsoft.com"**, **"sip2.pstnhub.microsoft.com"**, and **"sip3.pstnhub.microsoft.com"** — the **"sip-all.pstnhub.microsoft.com"** FQDN was originally used in Unify component configurations due to DNS resolution issues in some countries.

However, there have been reported cases where the **"sip-all.pstnhub.microsoft.com"** FQDN can cause incorrect certificate negotiation between OpenScape SBC and the Microsoft Teams tenant.

Therefore, do NOT configure the SIP trunk to point to "sip-all.pstnhub.microsoft.com" in Unify components unless explicitly recommended by Unify support.

For completeness, this document still presents the configuration of the “**sip-all.pstnhub.microsoft.com**” SIP trunk.

3.3 Connecting to OpenScape Voice Server

3.3.1 Core Realm Interface Configuration

Use the TCP port number from **subsection 2.1.1** for the connection of OS SBC’s eth0 (core) interface to OS Voice.

1. Go to **OS SBC Management Portal > Network/Net Services > Settings**.

The screenshot shows the 'Network/Net Services' configuration window. It has tabs for 'Settings', 'DNS', 'NTP', 'Traffic Shaping', and 'QoS'. The 'Settings' tab is active. Under 'Physical Network Interface', there is a table with columns: Interface, Enabled, MTU, Speed (Mbps), and Duplex mode. The table lists 'eth0' and 'eth1', both with 'Enabled' checked, 'MTU' of 1500, 'Speed' of 'Auto', and 'Duplex mode' of 'Auto'. Below this, there are checkboxes for 'Single armed' and 'Interface bonding', both of which are unchecked. The 'Interface Configuration' section contains a 'Core realm configuration' area with an 'Add' and 'Delete' button. Below this is a table with columns: Type, Network ID, Interface, IP address, Subnet mask, Signaling, Media, SIP-UDP, SIP-TCP, and SIP-TLS. The table contains one entry: Type 'Main IPv4', Network ID 'Main-Core-IPv4', Interface 'eth0', IP address '10.8.242.72', Subnet mask '255.255.255.0', Signaling checked, Media checked, SIP-UDP '5060', SIP-TCP '5060', and SIP-TLS '5061'. At the bottom right are 'OK' and 'Cancel' buttons.

Interface	Enabled	MTU	Speed (Mbps)	Duplex mode
eth0	<input checked="" type="checkbox"/>	1500	Auto	Auto
eth1	<input checked="" type="checkbox"/>	1500	Auto	Auto

Type	Network ID	Interface	IP address	Subnet mask	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS
Main IPv4	Main-Core-IPv4	eth0	10.8.242.72	255.255.255.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5060	5060	5061

2. In the **Core realm configuration** area, ensure that for the **eth0** interface, the “**SIP-TCP**” value is “**5060**”.
3. Click **OK**.
3. Click **Apply Changes** on OS SBC main page.

3.3.2 SIP Server Configuration

The SIP connectivity to OS Voice is configured in **OS SBC Management Portal > VOIP** window.

VOIP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Sip Server Settings | Port and Signaling Settings | Media | QoS Monitoring

General

Comm System Type: Active-Standby

☐ Allow Register from SERVER

Other trusted servers

Node 1

Target type: Binding

Primary server: 10.8.242.16 Transport: TCP Port: 5060

Backup server: Transport: TCP Port:

SRV record: Transport: TCP

Node 2

Target type: Binding

Primary server: 10.8.242.26 Transport: TCP Port: 5060

Backup server: Transport: TCP Port:

SRV record: Transport: TCP

Timers and Thresholds

Failure threshold (pings): 2 OPTIONS interval (sec): 60

Success threshold (pings): 1 OPTIONS timeout (sec): 4

OK Cancel

1. In the **Sip Server Settings** tab, enter the following:

- **Comm System Type:** Active-Standby

(OS Voice is a Duplex system i.e., two nodes in active-standby mode)

- **Target Type:** Binding (for both **OS Voice Node1** and **Node2**)
- **Primary Server:** 10.8.242.16
(OSV SIPSM address over TCP for **OS Voice Node1**)
- **Transport:** TCP (for both OS Voice Node 1 and Node 2)
- **Port:** 5060 (listening port for both **OS Voice Node 1** and **Node 2**).

2. Click **OK**.

3. Click **Apply Changes** on OS SBC main page.

Note: The OS Voice SIP Signaling Manager addresses for UDP/TCP/TLS can be found in OS Voice node's **node.cfg** file located in the **/etc/hq8000** folder (parameters: "**sipsm1_vip**" for **OS Voice Node1** and "**sipsm2_vip**" for **OS Voice Node 2**).

Alternatively, the OS Voice SIPSM IP addresses can be retrieved from CMP.

3.4 Configuring Certificates

Microsoft Phone System Direct Routing interface allows only TLS connections for SIP traffic from SBCs with a certificate signed by one of Microsoft's trusted Certification Authorities.

The certificate needs to have the SBC FQDN as the common name (CN) in the subject field. Certificates with a wildcard in the certificate Subject Alternate Name field conforming to RFC2818 are also supported.

For more information about the certificate and current Microsoft supported Certification Authorities, refer to Microsoft site:

<https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc>.

For the OpenScape SBC TLS interconnection to Microsoft Phone System, 3 files in *"pem"* format are required from the Certification Authority:

- CA certificate (e.g., *"ca_chain.pem"*)
- Server certificate for OS SBC (e.g., *"certificate.pem"*)
- OS SBC server certificate private key used for the CSR to CA (e.g., *"privatekey.pem"*)

The files above must be uploaded to OS SBC and used for the TLS connection with the Microsoft Phone System interface.

1. Go to OS SBC **Management Portal > Security > General** and click on **Certificate Management**.
2. Upload "**ca_chain.pem**" to **CA Certificates**, "**certificate.pem**" to "**X.509**" and "**privatekey.pem**" to "**Key Files**" areas correspondingly, as shown in figure below:

The screenshot shows the 'Certificate Management' window with the following sections:

- CA Certificates:**
 - Upload CA certificate file: No file selected.
 - CA certificates list:
 - ca_chain.pem
 - serverCA.pem
- X.509 Certificates:**
 - Upload X.509 certificate file: No file selected.
 - X.509 certificates list:
 - certificate.pem
 - servercert.pem
- Key Files:**
 - Upload key file: No file selected.
 - Key files list:
 - privatekey.pem
 - serverkey.pem
 - OSMO_Pro_VoIP_APN_cert.p12
 - OpenScapeProVoIPAndroidKey.json

At the bottom right, there are and buttons.

3. Click **Add** to create the certificate profile.

Certificate Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Certificate Profile configuration

Certificate profile name: Teams_Cert_Profile

Certificate service: SIP-TLS

Local client certificate file: [Empty] **Show**

Local server certificate file: certificate.pem **Show**

Local CA file: ca_chain.pem **Show**

Remote CA file: [Empty] **Show**

Local key file: privatekey.pem

EC param: secp256r1

Attach to Config file: ☐

Validation

Certificate Verification: None

☐ Revocation status

☐ Identity Check

Renegotiation

☐ Enforce TLS session renegotiation

TLS session renegotiation interval (minutes): 60

TLS version

Minimum TLS version: TLS V1.2

OK **Cancel**

4. Enter the following:

- **Certificate profile name:** Teams_Cert_Profile (friendly name)
- **Certificate service:** SIP-TLS
- **Local server certificate file:** certificate.pem
- **Local CA file:** ca_chain.pem
- **Local key file:** privatekey.pem
- **Minimum TLS version:** TLS V1.2

5. Click **OK**.

Note: In case of MTLS is required, the "**Remote CA file**" should be selected (i.e., the Teams "**Baltimore**" CA certificate should have been uploaded to "**CA Certificates**" store) and a proper value should be selected for "**Certificate Verification**".

Certificate Management

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

System Certificate

System TLS Certificate: OSV Solution

HTTPS certificate profile: HTTPS System Default

Media DTLS certificate profile:

IOS Push certificate profile: IOS Push Default

Android Push certificate profile: Android Push Default

Certificate Profiles

Add Edit Delete

Name	Certificate service	Client certificate file	Server certificate file	Local CA file	Remote CA file	Local Key file	Attach to Cfg file
OSV Solution	SIP-TLS		servercert.pem	serverCA.pem		serverkey.pem	NO
HTTPS System Default	HTTPS		server.crt			server.key	NO
IOS Push Default	IOS Push					OSMO_Pro_VoIP_APN_cert.1	NO
Android Push Default	Android Push					OpenScapeProVoIPAndroidK	NO
Teams_Cert_Profile	SIP-TLS		certificate.pem	ca_chain.pem		privatekey.pem	NO

Certificate Creation

Create New TLS Certificates

Name: CA file: Self signed Create

OK Cancel

5. Click **OK** in the **Certificate Management** window and then click **OK** in the **Security** window.

6. Click **Apply Changes** on OS SBC main page.

3.5 Configuring Media

With **Media Profiles** settings, various parameters regarding the SDP messages and audio (RTP) traffic may be configured for the OS SBC SIP endpoints to Teams Phone System, SSP (PSTN provider) and OS Voice.

3.5.1 Codec Manipulation Options

In case transcoding or certain codec prioritization for audio is required for the OS SBC – Teams Phone System & OS SBC – SSP media profiles for the corresponding SIP trunks, it is required to enable the codec configuration options first for the media profile setup.

1. Go to the **OS SBC Management Portal > Features** window.
2. Select the "**Enable Codec Support for transcoding**" checkbox.

Features

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

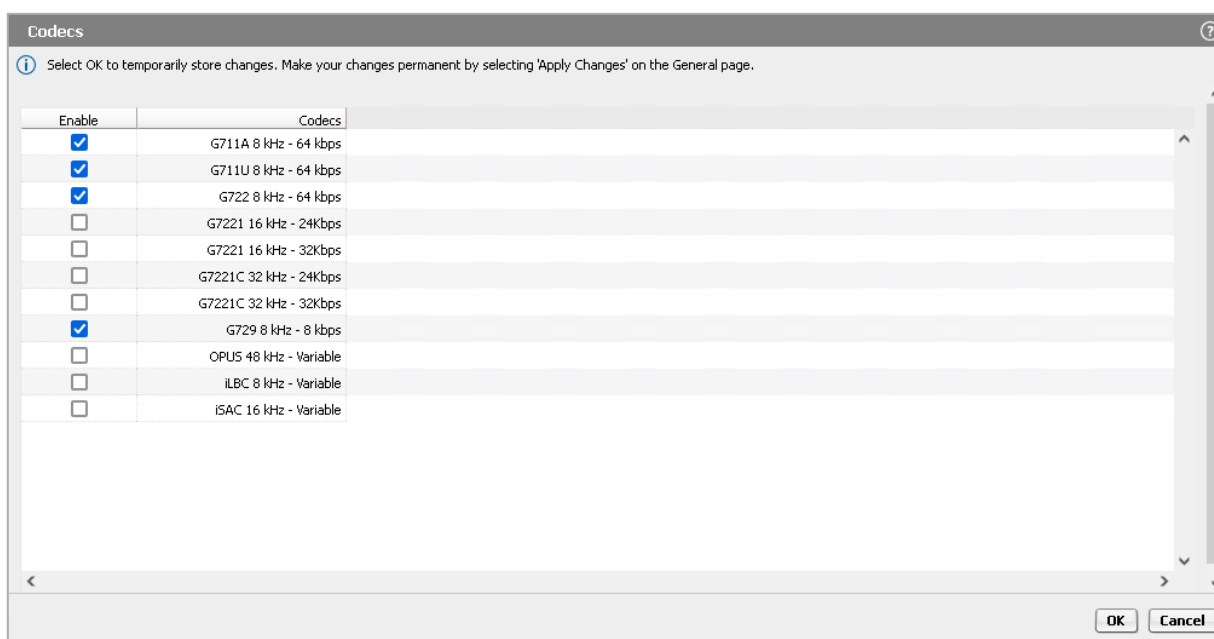
Features configuration

<input type="checkbox"/> Enable Remote Subscribers	Configure
<input type="checkbox"/> Enable Remote Endpoints	Configure
<input checked="" type="checkbox"/> Enable Codec Support for transcoding	Configure
<input type="checkbox"/> Enable TURN Server	Configure
<input type="checkbox"/> Enable Circuit Telephony Connector	Configure
<input type="checkbox"/> Enable Sip Load Balancer	Configure
<input type="checkbox"/> Enable Push Notification Service	Configure
<input type="checkbox"/> Enable Ganglia Monitoring Daemon	
<input type="checkbox"/> Enable Circuit Zookeeper Client	
<input type="checkbox"/> Enable THIG	
<input type="checkbox"/> Enable Standalone	

[OK](#) [Cancel](#)

3. Click **Configure**.

4. In the **Codecs** window, select the codecs to be available for the media profiles (for e.g., transcoding, prioritization), as shown in the example below:



5. Click **OK** on all the open windows.

6. Click **Apply Changes**.

3.5.2 MS Teams Media Profile Configuration

The communication between Teams Phone System is secure with secure audio (SRTP).

In the example presented in current sub-section, it's supposed that the PSTN doesn't support G.711 and transcoding to G.711 is required for calls between PSTN subscribers and Teams clients on OS SBC – Teams Phone System SIP trunks.

1. Go to **OS SBC Management Portal > VOIP > Media**.

Media Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Name: Teams

Media protocol: SRTP only ☐ Direct Media Support

☒ Support ICE Lite

☐ Enable TURN Client

☒ RTP/RTCP Multiplex in offer

☐ SDP Compatibility Mode

☐ Support Mid Attribute

☐ Do not set port to zero on session timer answer SDP

SRTP configuration

SRTP crypto context negotiation: ☐ MIKEY ☒ SDES ☐ DTLS SDES AES-128 only

☒ Mark SRTP Call-leg as Secure

RTCP configuration

RTCP Mode: Always generate

RTCP generation timeout: 4

Codec configuration

☐ Allow unconfigured codecs

☐ Enforce codec priority in profile

☐ Send Telephony Event in Invite without SDP

☐ Use payload type 101 for telephony event/8000

☐ Enforce Packetization Interval

Codec: G722 8 kHz - 64 kbps Add

Move up Move down Delete

Priority	Codec	Packetization interval
1	G711A 8 kHz - 64 kbps	Auto
2	G711U 8 kHz - 64 kbps	Auto

OK Cancel

2. In the **Media Profiles** area click on **[Add]** to create the media profile for OS SBC - Teams connections by entering the following:

- **Name:** Teams (friendly name)
- **Media protocol:** SRTP only
- **Support ICE:** Deactivated (for MB = OFF case)
/ Activated – Lite (for MB = ON case)
- **RTP/RTCP Multiplex in offer:** Activated
(adds rtcp-mux support to outgoing SDP)
- **SRTP crypto context negotiation:** SDES
- **Mark SRTP Call-leg as Secure:** Activated

- **rtcpMode:** **Bypass** or **Always Generate**
(with **Bypass** RTCP, messages from the SSP will be forwarded to Teams;
with **Always Generate** RTCP messages will be generated from OS SBC to
Teams, unless RTCP is received from SSP.)
 - **Allow unconfigured codecs:** **Deactivated**
3. Click **Add** to add the desired codecs (with priority) for transcoding, e.g., G711A, G711U.
 4. Click **OK** to return to the **Media** window.
 5. Click **OK** in the **VOIP** window.
 6. Click **Apply Changes**.

3.5.3 PSTN Service Provider Media Profile Configuration

In this sub-section, as an example, it is assumed that certain codecs need to be prioritized on the OS SBC – SSP (BCOM) SIP trunk for calls between Teams clients and PSTN subscribers.

1. Go to **OS SBC Management Portal > VOIP > Media**.

Media Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Name: BCOM

Media protocol: RTP only ☐ Direct Media Support

☐ Support ICE

☐ Enable TURN Client

☒ RTP/RTCP Multiplex in offer

☐ SDP Compatibility Mode

☐ Support Mid Attribute

☐ Do not set port to zero on session timer answer SDP

SRTP configuration

SRTP crypto context negotiation: ☐ MIKEY ☐ SDES ☐ DTLS ☐ SDES Both

☐ Mark SRTP Call-leg as Secure

RTCP configuration

RTCP Mode: Bypass

RTCP generation timeout: 4

Codec configuration

☒ Allow unconfigured codecs

☐ Enforce codec priority in profile

☐ Send Telephony Event in Invite without SDP

☐ Use payload type 101 for telephony event/8000

☐ Enforce Packetization Interval

Codec: Add

Move up Move down Delete

Priority	Codec	Packetization interval
1	G711A 8 kHz - 64 kbps	Auto
2	G711U 8 kHz - 64 kbps	Auto
3	G722 8 kHz - 64 kbps	Auto
4	G729 8 kHz - 8 kbps	Auto

OK Cancel

2. In the **Media Profiles** area, click **Add** to create the media profile for OS SBC - SSP trunk:

- **Name:** BCOM (friendly name)
- **Media protocol:** RTP only
- **RTP/RTCP Multiplex in offer:** Activated
- **rtcpMode:** Bypass or Always Generate
- **Allow unconfigured codecs:** Activated

3. If codec prioritization is required on the trunk over the other codecs ("**Enforce codec priority in profile**" is "**Activated**"), click **Add** to add the desired codecs to be prioritized (e.g., G711A, G711U, G722, G729).
4. Click **OK** to return to the **Media** window.
5. Click **OK** in the **VOIP** window.
6. Click **Apply Changes**.

3.5.4 OpenScape Voice Media Profile Configuration

1. Go to **OS SBC Management Portal > VOIP > Media**.

Media Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Name OSV

Media protocol RTP only ☐ Direct Media Support

☐ Support ICE Full

☐ Enable TURN Client

☐ RTP/ RTCP Multiplex in offer

☐ SDP Compatibility Mode

☐ Support Mid Attribute

☐ Do not set port to zero on session timer answer SDP

SRTP configuration

SRTP crypto context negotiation ☐ MIKEY ☐ SDES ☐ DTLS SDES Both

☐ Mark SRTP Call-leg as Secure

RTCP configuration

RTCP Mode Bypass

RTCP generation timeout 4

Codec configuration

☒ Allow unconfigured codecs

☐ Enforce codec priority in profile

☐ Send Telephony Event in Invite without SDP

☐ Use payload type 101 for telephony event/8000

☐ Enforce Packetization Interval

Codec G711A 8 kHz - 64 kbps **Add**

Move up Move down Delete

Priority	Codec	Packetization interval

OK Cancel

2. In the **Media Profiles** area click on **[Add]** to create the media profile for OS SBC – OS Voice connection by entering the following:

- **Name:** OSV (friendly name)
- **Media protocol:** RTP only
- **RTP/RTCP Multiplex in offer:** Deactivated
- **Allow unconfigured codecs:** Activated

3. Click **OK** to return to the **"Media"** window.
4. Click **OK** in the **"VOIP"** window.
5. Click **Apply Changes**.

3.5.5 General Media Settings

After creating the media profiles, configure the General media settings.

1. Go to the **OS SBC Management Portal > VOIP > Media** window.

VOIP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Sip Server Settings | Port and Signaling Settings | **Media** | QoS Monitoring

Media Handling

- ☐ Allow multiple media lines for the same media type
- ☒ Replace the SDP Origin (o) field
- ☒ Reset SRTP context upon key change
- ☐ Use single bridge/port for audio media

Core Side Media Configuration

Media profile: OSV

Add Delete

User agent mediaProfile

Media Profiles

Name	Codecs	Media protocol	SRTP crypto context negotiation	Mark SRTP Call-leg as Secure
webrtc_default		SRTP only	dtls	✓
WE_Phone_default		Best Effort SRTP	mikey + sdes	
OSV		RTP only	none	
Teams	G711A, G711U	SRTP only	sdes	✓
BCOM	G711A, G711U, G722, G729	RTP only	none	

Cloud Support

☒ Support OpenScape Cloud

OK Cancel

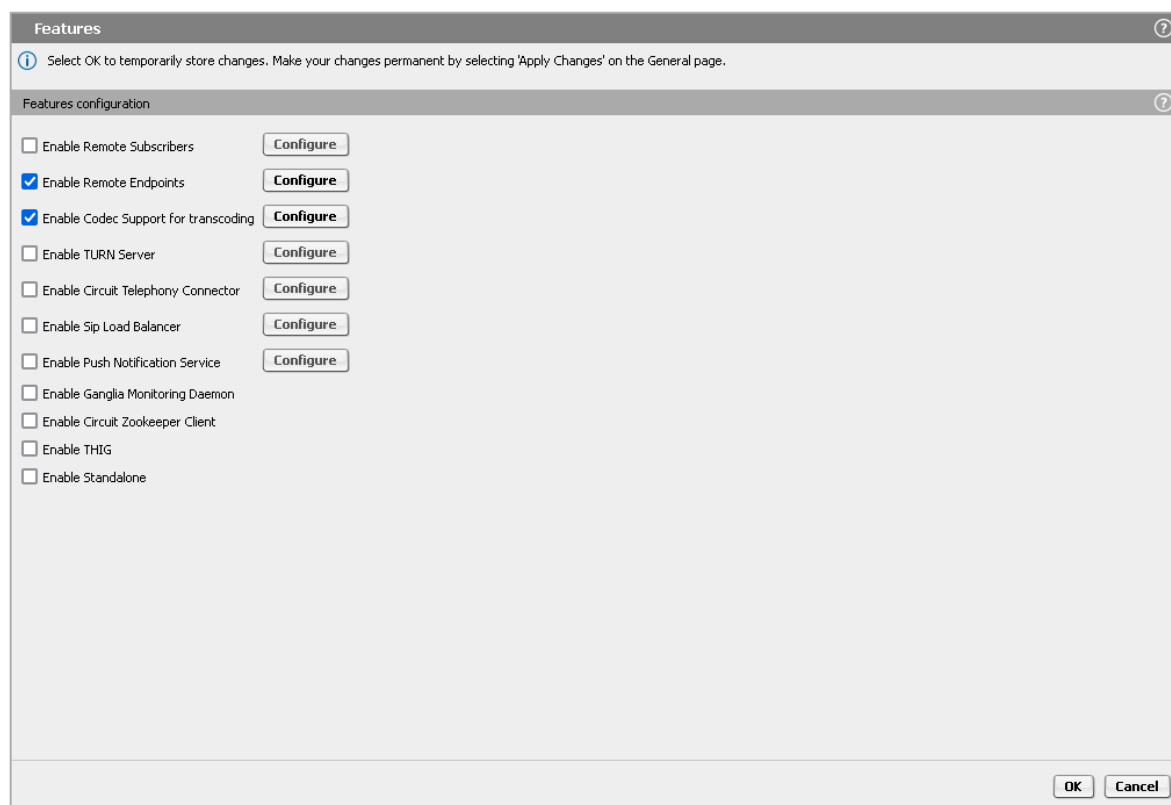
2. In the **"Core Side Media Configuration"** area, select **"OSV"** from the **"Media profile"** drop-down list for the media profile used for the OS SBC – OS Voice SIP trunk.
3. Locate the **Cloud Support** area and select the **"Support OpenScape Cloud"** checkbox.
4. Click **OK**.
5. Click **Apply Changes**.

3.6 Configuring Remote Endpoints

You can set up the OS SBC with Teams Phone System and the PSTN (BCOM SSP) SIP trunks in the **Remote Endpoint** configuration area.

3.6.1 MS Teams Remote Endpoints Configuration

1. Go to the **OS SBC Management Portal > Features** window.
2. Select the **Enable Remote Endpoints** checkbox.



3. Click **Configure**.

The **Remote Endpoints** window opens.

4. Click **Add** in the **"SIP Service Provider Profile"** area to add the endpoint profile for the OS SBC – Teams Phone System endpoint.
5. In the **SIP Service Provider** window, configure the following:
 - **Name:** **TeamsCloud** (friendly name)
 - **Default SSP Profile:** **MS Teams**
(by selecting the MS Teams profile all the required flags are selected automatically)
 - **SIP service address:** **sb01.athdrlabs.xyz**
(SBC public FQDN)
 - Ensure that the checkboxes shown in the following images are selected:

SIP Service Provider Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Name TeamsCloud Default SSP profile MS Teams

☒ Use SIP Service Address for identity headers

SIP service address sbc01.athtdrlabs.xyz

☐ Use SIP Service Address in Request-URI header

☒ Use SIP Service Address in From header

☐ Use SIP Service Address in To header

☒ Use SIP Service Address in P-Asserted-Identity header

☒ Use SIP Service Address in Diversion header

☒ Use SIP Service Address in Contact header

☒ Use SIP Service Address in Via header

☐ Use SIP Service Address in P-Preferred-Identity header

SIP User Agent

SIP User Agent towards SSP Passthru SIP User Agent

Registration

☐ Registration required

Registration interval (sec) 3600

Business Identity

☐ Business identity required

Business identity DN

OK Cancel

SIP Service Provider Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

☐ Do not send Invite without SDP

☐ Do not send Re-Invite when no media type change

☐ Do not send Re-Invite

☐ Remove Silence Suppression parameter from SDP

☐ Enable pass-through of Optional parameters

☐ Force direction attribute to sendrcv

☐ Send default Home DN in PAI

☐ Send default Home DN in PPI

☒ Preserve To and From headers per RFC2543

☐ Disable FQDN pass-through in FROM header

☐ Keep Digest Authentication Header

☒ Send Contact header in OPTIONS

☐ Do not send Privacy header in response messages

☐ Remove bandwidth (b) lines from SDP

☐ Keep P-Asserted-Identity from access side

TLS

TLS Signaling Transport=tl

Sip Connect

☐ Use tel URI

☒ Send user=phone in SIP URI

☐ Registration mode

☐ ITR118

OK Cancel

6. Click **OK** to return to the **Remote Endpoints** window.
7. In the **Remote endpoint configuration** area, click **Add**.
8. In the **Remote endpoint configuration** window, configure the following:
 - **Name:** TeamsSP1 (friendly name)
 - **Type:** SSP
 - **Profile:** TeamsCloud
 - **Signaling address type:** IP address or FQDN
 - **Core realm port:** 50001 (refer to sub-section 2.1.2)

The screenshot shows the 'Remote endpoint configuration' window. At the top, there is a header bar with the title 'Remote endpoint configuration' and a help icon. Below the header, a message states: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' The main configuration area is divided into three sections: 'Remote Endpoint Settings', 'Remote Location Information', and 'Remote Location domain list'.

Remote Endpoint Settings: This section contains several fields and checkboxes. The 'Name' field is set to 'TeamsSP1'. The 'Type' dropdown is set to 'SSP'. The 'Profile' dropdown is set to 'TeamsCloud'. The 'Access realm profile' dropdown is set to 'Main-Access-Realm - ipv4'. The 'Core realm profile' dropdown is set to 'Main-Core-Realm - ipv4'. The 'Associated Endpoint' dropdown is empty. There are checkboxes for 'Enable Call Limits', 'Maximum Permitted Calls' (set to 0), and 'Reserved Calls' (set to 0).

Remote Location Information: This section contains checkboxes for 'Support Peer Domains', 'Support Foreign Peer Domains' (with a 'White list' button), and 'Enable access control'. The 'Signaling address type' dropdown is set to 'IP address or FQDN'.

Remote Location domain list: This section contains a table with columns: Row, Remote URL, Remote port, Remote transport, Media IP, Media profile, TLS mode, Certificate profile, and TLS keep-alive. The table is currently empty. There are 'Add', 'Edit', and 'Delete' buttons above the table. At the bottom right of the window, there are 'OK' and 'Cancel' buttons.

Remote endpoint configuration ?

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Remote Location Identification/Routing ? ^

Core FQDN

Core realm port

Default core realm location domain name

☐ Enable routing based on domain

FQDN

Incoming Routing prefix **Add**

Delete

Digest Authentication ?

☐ Digest authentication supported

Digest authentication realm

Digest authentication user ID

Digest authentication password

Access Side Firewall Settings ?

☐ Enable Firewall Settings **Firewall Settings**

OK **Cancel**

7. Click on **[Add]** in the **Remote Location domain list** area.

9. In the **Remote Location Domain** window, enter the following:

- **Remote URL:** sip.pstnhub.microsoft.com (Teams FQDN 1)
- **Remote port:** 5061
- **Remote transport:** TLS
- **TLS mode:** Server authentication
(or Mutual authentication in case MTLS is required – refer to section 3.2)
- **Certificate profile:** Teams_Cert_Profile (refer to section 3.2)
- **Media profile:** Teams (refer to sub-section 3.3.2)

The screenshot shows the 'Remote Location Domain' configuration window. At the top, a message states: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' The window is divided into several sections: 'General' with fields for Remote URL (sip.pstnhub.microsoft.com), Remote port (5061), Remote transport (TLS), and a 'Shared domain' checkbox; 'Signaling' with INVITE No Answer timeout (360000) and INVITE No Reply timeout (3000); 'TLS' with TLS mode (Server authentication), Certificate profile (Teams_Cert_Profile), a checkbox for TLS keep-alive, and Keep-alive interval (120) and timeout (10); 'Media Configuration' with Media profile (Teams) and Media realm subnet IP address; 'Outbound Proxy Configuration' with Outbound Proxy and Outbound Proxy Port; and 'Registrar Server Configuration' with Registrar Server and Registrar Server Port. The bottom right corner has 'OK' and 'Cancel' buttons.

10. Click **OK** to return to the **Remote endpoint configuration** window.

11. Repeat the procedure **Remote endpoint configuration** for the rest MS Teams FQDNs (i.e., sip2.pstnhub.microsoft.com, sip3.pstnhub.microsoft.com and sip-all.pstnhub.microsoft.com - refer to chapter 3).

12. Click **OK** to return to the **Remote Endpoints** window.

The **"Remote Endpoints"** window should look like the figure below:

Remote Endpoints

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

SIP Service Provider Profile

Hostname

Remote directory

User name

Password

Row	Name	Registration required	Registration interval (sec)
1	TeamsCloud	<input type="checkbox"/>	3600

Remote endpoint configuration

Row	Name	Access realm profile	Type	Profile / Circuit ID	Remote IP address / Logical-Endpoint-ID / Circuit URL	Remote port	Remote transport	Associ.
1	TeamsSP1	Main-Access-Realm - ipv4	SSP	TeamsCloud	sip.pstnhub.microsoft.com	5061	TLS	
2	TeamsSP2	Main-Access-Realm - ipv4	SSP	TeamsCloud	sip2.pstnhub.microsoft.com	5061	TLS	
3	TeamsSP3	Main-Access-Realm - ipv4	SSP	TeamsCloud	sip3.pstnhub.microsoft.com	5061	TLS	
4	TeamsSP_ALL	Main-Access-Realm - ipv4	SSP	TeamsCloud	sip-all.pstnhub.microsoft.com	5061	TLS	

13. Click **OK** on all open windows.
14. Click **Apply Changes** on OS SBC main page.

3.6.2 PSTN Remote Endpoint Configuration

1. Go to **OS SBC Management Portal > Features > Enable Remote Endpoints**.
2. Click **Configure**.
The **Remote Endpoints** window opens.
3. Click **Add** in the **SIP Service Provider Profile** area to add the endpoint profile for the OS SBC – SSP (BCOM) endpoint.

SIP Service Provider Profile ⓘ

ⓘ Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General ⓘ

Name **Default SSP profile**

☒ Use SIP Service Address for identity headers

SIP service address

☒ Use SIP Service Address in Request-URI header

☒ Use SIP Service Address in From header

☒ Use SIP Service Address in To header

☒ Use SIP Service Address in P-Asserted-Identity header

☒ Use SIP Service Address in Diversion header

☐ Use SIP Service Address in Contact header

☐ Use SIP Service Address in Via header

☐ Use SIP Service Address in P-Preferred-Identity header

SIP User Agent ⓘ

SIP User Agent towards SSP **SIP User Agent**

Registration ⓘ

☒ Registration required

Registration interval (sec)

Business Identity ⓘ

☐ Business identity required

Business identity DN

OK **Cancel**

SIP Service Provider Profile ⓘ

ⓘ Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Outgoing SIP manipulation ⓘ

☐ Insert anonymous caller ID for blocked Caller-ID

Manipulation

Incoming SIP manipulation ⓘ

Calling Party Number

Flags ⓘ

☐ FQDN in TO header to SSP

☐ Use To DN to populate the RURI

☐ Send Default Home DN in Contact for Call messages

☐ Allow SDP changes from SSP without session version update

☐ Do not send INVITE with sendonly media attribute

☐ Do not send INVITE with inactive media attribute

☐ Do not send INVITE with video media line

☐ Do not send Invite without SDP

☐ Do not send Re-Invite when no media type change

☐ Do not send Re-Invite

☐ Remove Silence Suppression parameter from SDP

☐ Enable pass-through of Optional parameters

☐ Force direction attribute to sendrcv

☐ Send default Home DN in PAI

☐ Send default Home DN in PPI

☐ Preserve To and From headers per RFC2543

OK **Cancel**

SIP Service Provider Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

- ☐ Do not send INVITE with video media line
- ☐ Do not send Invite without SDP
- ☐ Do not send Re-Invite when no media type change
- ☐ Do not send Re-Invite
- ☐ Remove Silence Suppression parameter from SDP
- ☐ Enable pass-through of Optional parameters
- ☐ Force direction attribute to sendrcv
- ☐ Send default Home DN in PAI
- ☐ Send default Home DN in PPI
- ☐ Preserve To and From headers per RFC2543
- ☐ Disable FQDN pass-through in FROM header
- ☐ Keep Digest Authentication Header
- ☐ Send Contact header in OPTIONS
- ☐ Do not send Privacy header in response messages
- ☐ Remove bandwidth (b) lines from SDP
- ☐ Keep P-Asserted-Identity from access side

TLS

TLS Signaling: Endpoint Config

Sip Connect

- ☐ Use tel URI
- ☐ Send user=phone in SIP URI
- ☐ Registration mode
- ☐ 1TR118

OK Cancel

4. In the **SIP Service Provider** window, configure the following:

- **Name:** BCOM
(friendly name)
- **Default SSP Profile:** BCOM

Note: Selecting the "Bcom" profile automatically enables all required flags. If the provider is not available in the drop-down list, leave this field blank and manually configure the required flags for the SSP in use.

- **Use SIP Service Address for identity headers:** BCOM
- **Use SIP Service Address in Request-URI header:** Activated
- **Use SIP Service Address in From header:** Activated
- **Use SIP Service Address in To header:** Activated
- **Use SIP Service Address in P-Asserted-Identity header:** Activated
- **Use SIP Service Address in Diversion header:** Activated

5. Click **OK** to return to the **Remote Endpoints** window.

6. In the **Remote endpoint configuration** area, click **Add**.

Remote endpoint configuration ?

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Remote Endpoint Settings ?

Name BCOM

Type SSP

Profile BCOM

Access realm profile Main-Access-Realm - ipv4

Core realm profile Main-Core-Realm - ipv4

Associated Endpoint

☐ Enable Call Limits

Maximum Permitted Calls 0

Reserved Calls 0

Remote Location Information ?

☐ Support Peer Domains

☐ Support Foreign Peer Domains White list

☐ Enable access control

Signaling address type DNS SRV

Remote Location domain list ?

Add Edit Delete

Row	Remote URL	Remote port	Remote transport	Media IP	Media profile	TLS mode	Certificate profile	TLS keep-all

OK Cancel

Remote endpoint configuration ?

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Remote Location Identification/Routing ?

Core FQDN

Core realm port 50010

Default core realm location domain name

Default home DN 31850080990

☐ Enable routing based on domain

FQDN

Incoming Routing prefix Add

Delete

Digest Authentication ?

☒ Digest authentication supported

Digest authentication realm sip.bcom.nl

Digest authentication user ID 31850080990

Digest authentication password

OK Cancel

Remote endpoint configuration ?

Access Side Firewall Settings ?

☐ Enable Firewall Settings **Firewall Settings**

Emergency configuration ?

Emergency numbers **Add**

Delete

Emergency call routing

MSRP Data Configuration ?

☐ Enable MSRP Relay Support

☒ use IP address in MSRP-path ☐ use FQDN in MSRP-path FQDN

☒ Authentication required Realm Password **Show**

☐ Access side only Qop Expire time/sec

Miscellaneous ?

☒ Open external firewall pinhole

OK Cancel

7. In the **Remote endpoint configuration** window, configure the following:

- **Name:** BCOM (friendly name)
- **Type:** SSP
- **Profile:** BCOM
- **Signaling address type:** DNS SRV
- **Core realm port:** 50010 (refer to sub-section 2.1.3)
- **Default home DN:** 31850080990
- **Digest authentication supported:** Activated
- **Digest authentication realm:** sip.bcom.nl (data provided by the BCOM SSP)
- **Digest authentication user ID:** 31850080990 (data provided by the BCOM SSP)
- **Digest authentication password:** <password> (data provided by the BCOM SSP)
- **Open external firewall pinhole:** Activated

8. Click **Add** in the **Remote Location domain list** area.

Remote Location Domain ⓘ

ⓘ Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General ⓘ

Remote URL: ☐ Shared domain

Remote port:

Remote transport:

Signaling ⓘ

INVITE No Answer timeout (msec):

INVITE No Reply timeout (msec):

TLS ⓘ

TLS mode:

Certificate profile:

☐ TLS keep-alive

Keep-alive interval (seconds):

Keep-Alive timeout (sec):

Media Configuration ⓘ

Media profile:

Media realm subnet IP address:

Outbound Proxy Configuration ⓘ

Outbound Proxy:

Outbound Proxy Port:

8. In the **Remote Location Domain** window, enter the following:

- **Remote URL:** sip.bcom.nl (BCOM)
- **Remote transport:** UDP
- **Media profile:** BCOM (refer to sub-section 3.3.4)

9. Click **OK** to return to the **Remote endpoint configuration** window.

10. Click **OK** to return to the **Remote Endpoints** window.

The **"Remote Endpoints"** window should look like the figure below:

Remote Endpoints

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

SIP Service Provider Profile

Hostname

Remote directory

User name

Password

Download New Profile List

AddEditDelete

Row	Name	Registration required	Registration interval (sec)
1	TeamsCloud	<input type="checkbox"/>	3600
2	BCOM	<input checked="" type="checkbox"/>	60

Remote endpoint configuration

AddEditDelete

Row	Name	Access realm profile	Type	Profile / Circuit ID	Remote IP address / Logical-Endpoint-ID / Circuit URL	Remote port	Remote transport	Associ
1	TeamsSP1	Main-Access-Realm - ipv4	SSP	TeamsCloud	sip.pstnhub.microsoft.com	5061	TLS	
2	TeamsSP2	Main-Access-Realm - ipv4	SSP	TeamsCloud	sip2.pstnhub.microsoft.com	5061	TLS	
3	TeamsSP3	Main-Access-Realm - ipv4	SSP	TeamsCloud	sip3.pstnhub.microsoft.com	5061	TLS	
4	BCOM	Main-Access-Realm - ipv4	SSP	BCOM	sip.bcom.nl	0	UDP	
5	TeamsSP_ALL	Main-Access-Realm - ipv4	SSP	TeamsCloud	sip-all.pstnhub.microsoft.com	5061	TLS	

OKCancel

11. Click **OK** on all open windows.

12. Click **Apply Changes**.

