



A MITEL
PRODUCT
GUIDE

Zoom with OpenScape Voice and OpenScape SBC

Bring Your Own Carrier (BYOC) and Bring Your Own PBX (BYOP) Solution Guide V11

Document Version 1.6

June 2025

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks Corporation (MITEL®)**. 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), its affiliates, parents, or subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

®,™ Trademark of Mitel Networks Corporation

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Contents

1 History of Changes.....	1
2 Introduction.....	2
2.1 Prerequisites.....	3
2.2 Additional Support Information.....	3
2.3 Related Documentation.....	4
3 Zoom Web Portal Configuration.....	5
3.1 Adding Phone Users.....	5
3.1.1 Assigning a Calling Plan to a phone user.....	7
3.2 Adding the OpenScape SBC.....	8
3.2.1 Configuring the Route Group.....	11
3.2.2 Configuring the SIP Group.....	14
3.2.3 Configuring the Routing Rule.....	16
3.3 Adding BYOC Phone numbers.....	20
3.3.1 Assigning BYOC numbers.....	21
3.4 Adding BYOP numbers.....	22
4 Provisioning Phones for Zoom Phone Users.....	25
5 Unify OpenScape Voice Configuration.....	27
5.1 Configuring Endpoints.....	28
5.1.1 Configuring the OpenScape SBC Endpoint.....	28
5.1.2 Configuring the Zoom Phone Endpoint.....	34
5.1.3 Configuring the PSTN Endpoint.....	43
5.1.4 Endpoint Overview.....	50
5.2 Destinations and Routes Configuration.....	51
5.2.1 Configuring the Zoom Destination.....	51
5.2.2 Configuring the PSTN Destination.....	55
5.2.3 Configuring the OpenScape OSV extension Destination.....	58
5.3 Translation Configuration.....	61
5.3.1 Configuring the Zoom Numbers Routing.....	62
5.3.2 Configuring the PSTN Numbers Routing.....	63
5.4 Configuring the SIP UA Forking.....	65
5.5 Configuring Display Number Modification.....	66
6 Unify OpenScape SBC Configuration.....	71
6.1 Configuring Network settings.....	75

6.2 Configuring SIP Server.....	76
6.3 Configuring Certificates.....	78
6.4 Configuring Media Profiles.....	82
6.4.1 Configuring the Codec Manipulation Options.....	82
6.4.2 Configuring the Zoom Media Profile.....	84
6.4.3 Configuring the PSTN Media Profile.....	87
6.4.4 Configuring the Unify OpenScape Voice Media Profile.....	90
6.4.5 General Media Settings.....	91
6.5 Configuring Remote Endpoints.....	92
6.5.1 Configuring the Zoom Remote Endpoints.....	93
6.5.2 Configuring the PSTN Remote Endpoint.....	100

History of Changes

1

Issue	Date	Summary
1	10/2024	The first issue of the guide.
1.1	10/2024	Updated document for Unify OpenScape SBC/OpenScape Voice configurations.
1.2	11/2024	Updated access interface and routing configurations in Configuring Network settings on page 75. Added a table of other Zone Zoom IPs in Unify OpenScape SBC Configuration on page 71 for Unify OpenScape SBC/OpenScape Voice configurations.
1.3	01/2025	Updated the entire document.
1.4	02/2025	Minor updates and enhancements. Updated the Prerequisites section.
1.5	04/2025	Updated the Prerequisites under the Unify OpenScape SBC Configuration section.
1.6	06/2025	Updated the Unify OpenScape SBC Configuration section.

This chapter contains the following sections:

- [Prerequisites](#)
- [Additional Support Information](#)
- [Related Documentation](#)

This document outlines the process of connecting the **OpenScape SBC** (OSSBC) and **OpenScape Voice** to **Zoom Phone** using Bring Your Own Carrier (BYOC)¹ and Bring Your Own PBX (BYOP)² configurations.

This hybrid integration model allows organizations to leverage Zoom's cloud platform while maintaining their existing OpenScape Voice (OSV) infrastructure for telephony features and PSTN connectivity. This solution is particularly valuable for organizations already using Zoom as their primary collaboration platform who want to preserve their investment in OSV for call management.

How it works:

The integration allows Zoom Phone to connect to the OSV system through a Generic SIP Trunk. OpenScape SBC and OpenScape Voice manage the communication between Zoom Phone and external networks, including the PSTN (Public Switched Telephone Network). OpenScape Voice handles SIP message manipulation and call routing, ensuring proper communication between Zoom Phone and external networks (like PSTN). It also sets up signaling paths to Zoom Phone data centers and the SSP (PSTN provider), ensuring smooth call flow *to* and *from* Zoom Phone and the PSTN. Zoom Phone takes care of the cloud-based communication features, while OpenScape SBC (OSSBC) links Zoom Phone and your on-premises infrastructure, ensuring smooth integration.

This solution provides secure traffic management, allowing users to retain their OSV system while benefiting from Zoom's cloud features. Proper configuration of both OpenScape Voice and OpenScape SBC within the user environment is essential for successful deployment (Chapters 5-6). Once OSV is configured, they can use the SBC to route calls, secure communication, and manage traffic between Zoom Phone and PSTN networks.

For detailed Zoom Phone settings and configuration, please refer to the official Zoom support page under the [Settings and Configuration for Zoom Phone](#) section and the following [Zoom Web Portal Configuration](#) on page 5 chapter.

Important:

For Licensing information, please refer to the [OpenScape Solution Set V11, Zoom with OpenScape Voice and OpenScape SBC Phone System Integration \(PSI\), Service Documentation](#).

¹ **Bring Your Own Carrier (BYOC):** Connecting your existing telecom provider (carrier) to Zoom Phone.

² **Bring Your Own PBX (BYOP):** Integrating your existing phone system (PBX) with Zoom Phone.

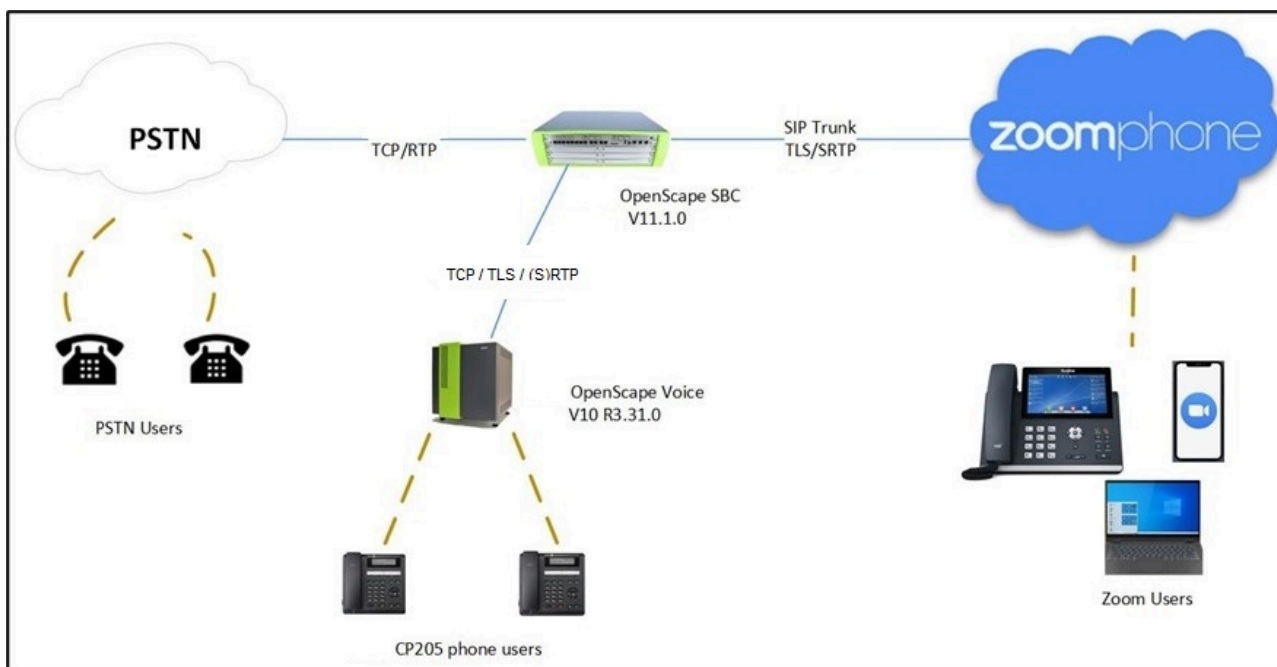


Figure 1: Network Topology Block Diagram

2.1 Prerequisites

Supported product versions

Product	SW Version (minimum)
Zoom Workplace app	6.2.0
OpenScape Voice	V10.3.31
OpenScape SBC	V11R1.0.0

2.2 Additional Support Information

In the current Mitel product software implementation:

- OpenScape SBC with Mitel OpenScape 4000 solution is supported.
- SBC standalone mode (without PBX) is currently supported.
- Domain-based Zoom multi-tenancy is supported.
- Comfort Noise generation is currently not supported by OpenScape SBC.

- The History-Info header is not currently supported by Mitel OpenScape Voice and Mitel OpenScape 4000.
- The OSEE environment with SBC-THIG and Zoom is currently not supported.

2.3 Related Documentation

For additional information on **OpenScape SBC**, refer to the following documents:

- [OpenScape SBC V11 Administration Guide](#)
- [OpenScape SBC V11 Configuration Guide, Administration Documentation](#)
- [OpenScape SBC V11 Installation Guide](#)
- [OpenScape SBC V11 Security Checklist](#)

For additional information on **OpenScape Voice**, refer to the following documents:

- [OpenScape Voice V10 Administrator Guide](#)
- [OpenScape Voice V10 Service Manual, Service Documentation](#)

For additional information on the **Zoom** Configurations, refer to the official [Zoom Support](#) page.

Zoom Web Portal Configuration

3

This chapter contains the following sections:

- [Adding Phone Users](#)
- [Adding the OpenScape SBC](#)
- [Adding BYOC Phone numbers](#)
- [Adding BYOP numbers](#)

This section guides you in preparing the environment for integrating and operating with external Bring Your Own Carrier (BYOC) DID phone numbers. It also explains how to add these numbers and map them to the corresponding endpoint devices, such as IP phones and other SIP devices.

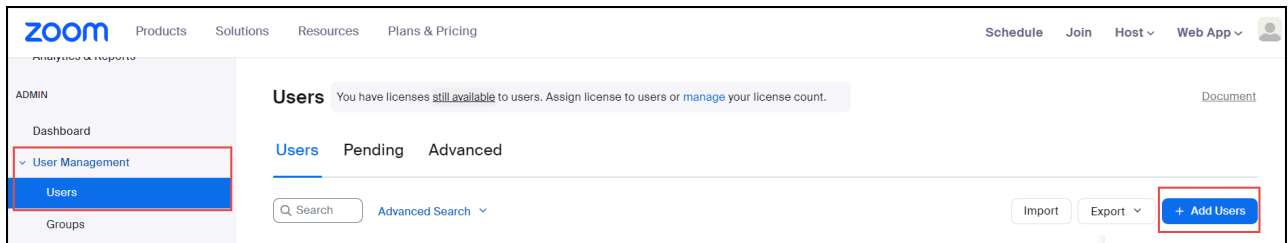
To set up users for the Zoom and OSV integration, you must first add users to your Zoom account and assign licenses to them.

3.1 Adding Phone Users

Follow the instructions below to add Zoom Phone Users. For more details, please refer to the official Zoom support page on [How to add a new user](#).

Prerequisites

1. You have a Pro, Business, or Enterprise Zoom Phone account.
 2. You are an administrator with the privilege to edit account settings.
 3. You have completed the initial Zoom Phone setup. For more information, refer to [Getting started with Zoom Phone \(admin\)](#).
1. Log in to the **Zoom web portal**.
 2. Navigate to **User Management > Users > Add Users**.



3. Configure the following in the **Add Users** pop-up:

- Enter the user's email address. To add multiple users with the same settings, enter multiple email addresses separated by commas: , .
- From the **Zoom Workplace** drop-down menu, select the available Zoom Workplace licenses to assign, such as **Zoom Meetings**.
- In the **Licenses and add-ons** section, check the **Zoom Phone Basic** checkbox.
- Click **Add**.

Add Users

Add users with their email addresses

If you enter the email address of account owners, all users on their accounts will be added to this account.


Zoom Workplace

Zoom Meetings (0 available) ▾

Licenses and add-ons

☐ Large Meeting (500 participants) (20 available)

☒ Zoom Phone Basic

 To assign Zoom Phone packages, go to [Phone System Management](#).

☐ Zoom Webinars (500 attendees) (20 available)

Department

Manager

Job Title

Location

Add

Cancel

The new user(s) will appear on the **Pending** tab of the User Management section.

Next steps

You can now assign licenses to users. After purchasing your Zoom One licenses, during the setup of Zoom Phone for your account, you can choose either to assign Zoom Phone packages automatically or manually to your Zoom One users. Before assigning a license to a phone user, ensure that automatic

phone assignment for Zoom One licenses is disabled for your account. For more information, refer to the [official Zoom support page](#).

With automatic assignment disabled, you can proceed to assign licenses to the phone user(s). For more information, refer to [How to assign Zoom licenses](#).

3.1.1 Assigning a Calling Plan to a phone user

You can assign a calling plan to phone users to enable outbound calling.

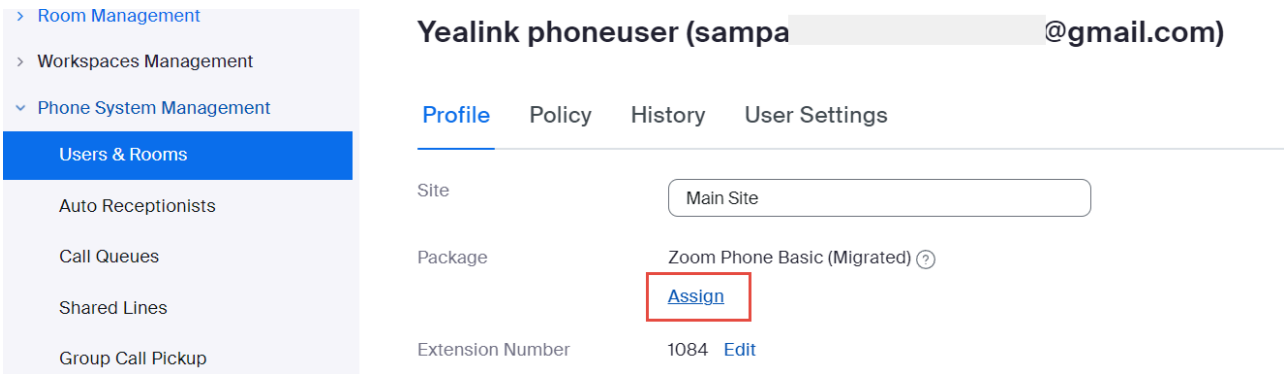
Prerequisite

- 1. You are an administrator with the privilege to edit account settings.
- 2. You have assigned licenses to the phone users. For more information, refer to [How to assign licenses](#).

- 1. Navigate to **Phone System Management > Users & Rooms**.
- 2. Select the user for whom you want to add a calling plan and click **Assign**.



- 3. Under the **Profile** tab, locate the **Package** section and click **Assign**.



4. From the **Package** drop-down menu, select **US/CA Unlimited Calling Plan**, as shown below.

The screenshot shows the Zoom Web Portal configuration interface. On the left, a sidebar menu lists various administrative functions, with 'Users & Rooms' currently selected. The main area displays the configuration for a specific user, 'Yealink phoneuser (sampa...@gmail.com)'. Under the 'Profile' tab, several fields are visible: 'Site' (Main Site), 'Package' (a dropdown menu), 'Extension Number', and 'Emergency Address'. The 'Package' dropdown is open, showing two available plans. The 'US/CA Unlimited Calling Plan (9 Available)' is highlighted with a red rectangular box, indicating the selection step described in the text. Below it, the 'Zoom Phone Power Pack (19 Available)' is also visible. The 'Emergency Address' field shows a default address in Plano, Texas.

5. Click **Confirm**.

3.2 Adding the OpenScape SBC

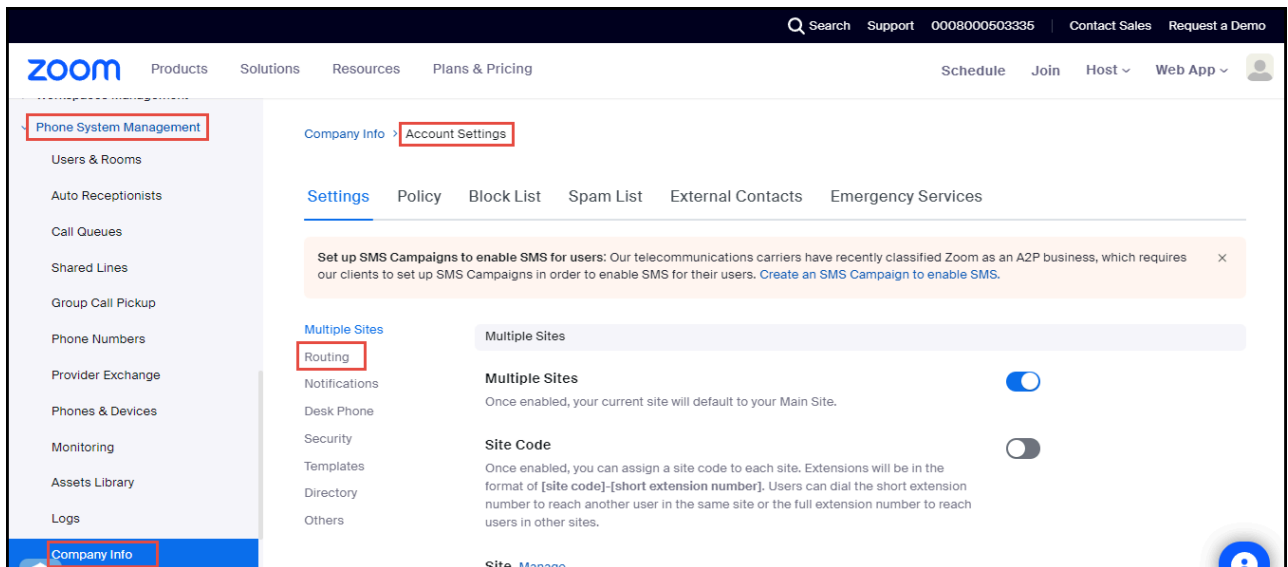
Follow the instructions below to add your OpenScape SBC in the Zoom Web Portal.

Prerequisites

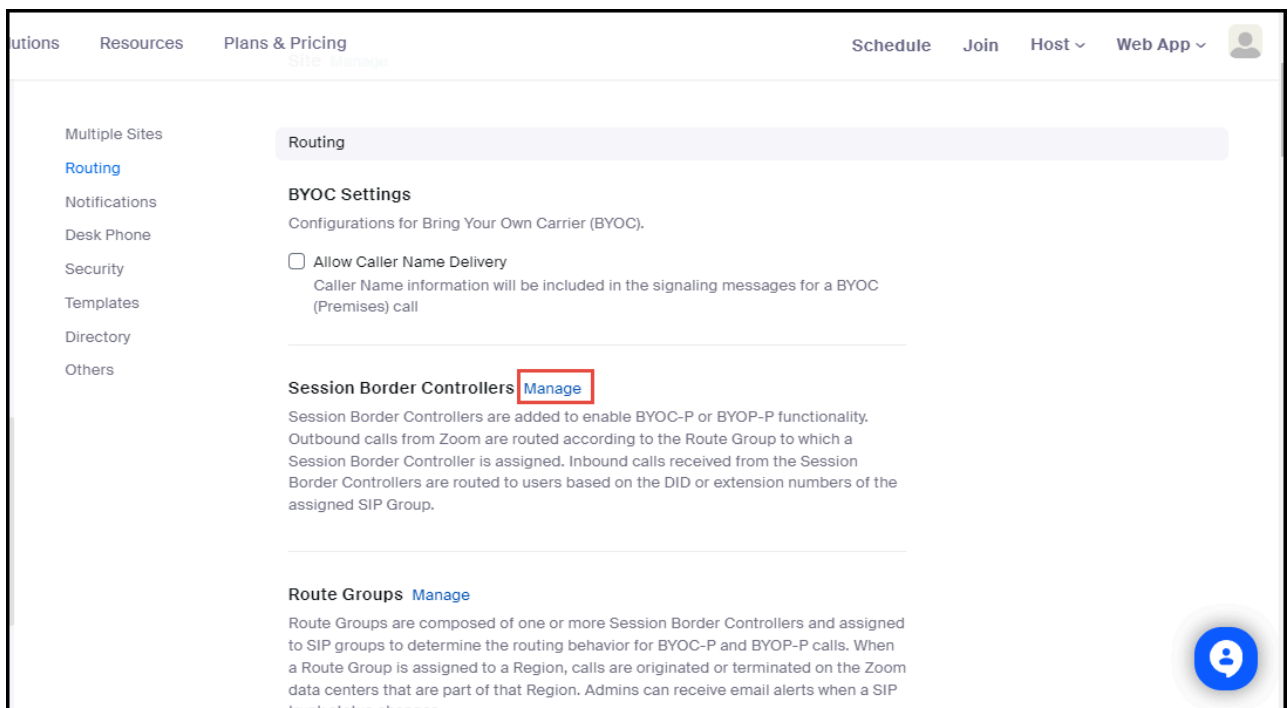
1. You are an administrator.
2. You have completed the initial Zoom Phone setup.
3. You have configured appropriate firewall rules for connectivity. For more information, refer to [Zoom network firewall or proxy server settings](#).
4. You have a public IP address for SIP trunk connectivity.

1. Log in to the **Zoom Admin Portal**.

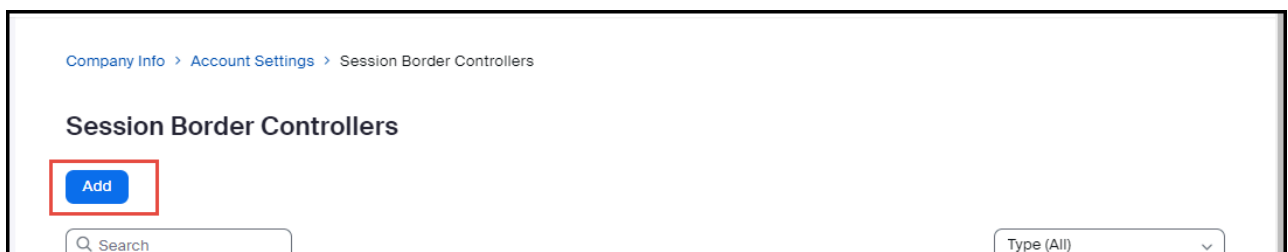
2. Navigate to **Phone System Management > Company Info > Account Settings > Routing**.



3. Locate the **Session Border Controllers** section and click **Manage**.



4. Click **Add**.



5. Configure the following:

- a. **Display Name:** Type the display name of your choice. For example, **OpenScape_SBC**.
- b. **IP Address:** Enter the IP address of the OpenScape SBC interface facing towards Zoom and configure the port number (for example, 5061).
- c. **In-Service:** Click the toggle button to enable the **In-Service** option.
- d. Under the **Settings** section, check the following checkboxes:
 - **Integrate an on-premises PBX (Bring Your Own PBX-Premises) with Zoom**
 - **Send OPTIONS ping messages to the SBC to monitor connectivity status**
 - **Include diversion headers in the sip signaling messages for forwarded calls**

Add Session Border Controllers

Display Name

Description (Optional)

Protocol

TLS

IP Address ?

Public IP Address

Port Number ?

In-Service ?
☒

Settings

☒ Integrate an on-premises PBX (Bring Your Own PBX - Premises) with Zoom
☒ Send OPTIONS ping messages to the SBC to monitor connectivity status
☒ Include diversion headers in the sip signaling messages for forwarded calls
☐ Include original calling number within the P-Asserted-Identity (PAI) header for forwarded calls
☐ Use T.38 protocol for faxing ?
☐ Allow REFER support to transfer calls BETA

Address(Optional) ?

Country/Region

Select

Email(Optional) ?

Phone Number(Optional) ?

Save

Close

6. Click **Save**.

Note:

To ensure Zoom's network allows traffic from your OSSBC, contact your **Zoom representative** to **whitelist** the SBC's **IP address** and **port** in Zoom's **Access Control Lists (ACLs)**. Once the **whitelisting** is done, you can start sending traffic (i.e., calls or data) between your system and Zoom.

Use **SIP OPTIONS** to check that the connection between your SBC and Zoom is working correctly after the transport is established.

3.2.1 Configuring the Route Group

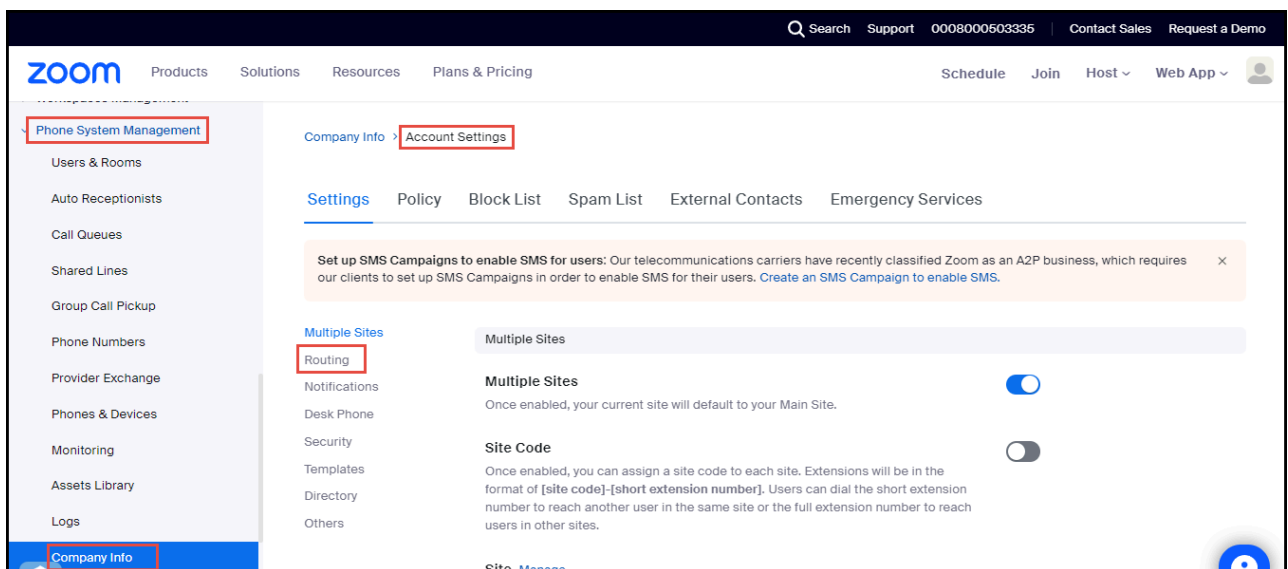
Route Groups are collections of Session Border Controllers (SBCs), which manage and route voice traffic across a network. A Route Group determines how calls are routed and handled by directing them to specific SIP endpoints. The **Region** setting ensures that calls are routed through the appropriate Zoom data centers based on their geographic location.

Note:

These configurations (Route Group, SIP Group, and Routing Rule) will take effect once phone numbers are added and assigned to the appropriate users. Until then, the routing logic will be in place, but calls will not be routed as expected.

To add a Route Group:

1. Navigate to **Phone System Management > Company Info > Account Settings > Routing**.



2. Locate the **Route Groups** section and click **Manage**.

Routing

Multiple Sites

Routing

Notifications

Desk Phone

Security

Templates

Directory

Others

BYOC Settings
Configurations for Bring Your Own Carrier (BYOC).

☐ Allow Caller Name Delivery
Caller Name information will be included in the signaling messages for a BYOC (Premises) call

Session Border Controllers [Manage](#)
Session Border Controllers are added to enable BYOC-P or BYOP-P functionality. Outbound calls from Zoom are routed according to the Route Group to which a Session Border Controller is assigned. Inbound calls received from the Session Border Controllers are routed to users based on the DID or extension numbers of the assigned SIP Group.

Route Groups [Manage](#)
Route Groups are composed of one or more Session Border Controllers and assigned to SIP groups to determine the routing behavior for BYOC-P and BYOP-P calls. When a Route Group is assigned to a Region, calls are originated or terminated on the Zoom data centers that are part of that Region. Admins can receive email alerts when a SIP trunk status changes.

3. Click **Add**.

[Company Info](#) > [Account Settings](#) > Route Group

Route Group

Last Updated Time: 07:07 AM, Apr 29, 2024 🔄

Add

4. Configure the following:

- a. **Display Name:** Type the display name of your choice. For example, **Route_group_OpenScape**.
- b. From the **Type** drop-down menu, select **BYOC-P**.
- c. From the **Region** drop-down menu, select the region code for your location. The format will be similar to: **US01-US(SJ/DV/NY)**

Note:

The format given above is an example. Choose the zone (SJ/DV/NY etc.) that is geographically closest to your SBC installation location.

- d. From the **Distribution** drop-down menu, select **Sequential** and then from the **Session Border Controllers** drop-down menu, select the OpenScape_SBC that was created in [Adding the OpenScape SBC](#) on page 8.

Add a new Route Group

Display Name

Route_group_OpenScape

Type

BYOC-P

Region

US01 - US (SJ/DV/NY)

Distribution

Sequential

Session Border Controllers

1: OpenScape_SBC (192.)

Add

Backup Route Group (Optional)

Select

Got old Route Groups?

Save

Cancel

5. Click **Save**.

A green light indicates that the trunk status is active, as shown below:

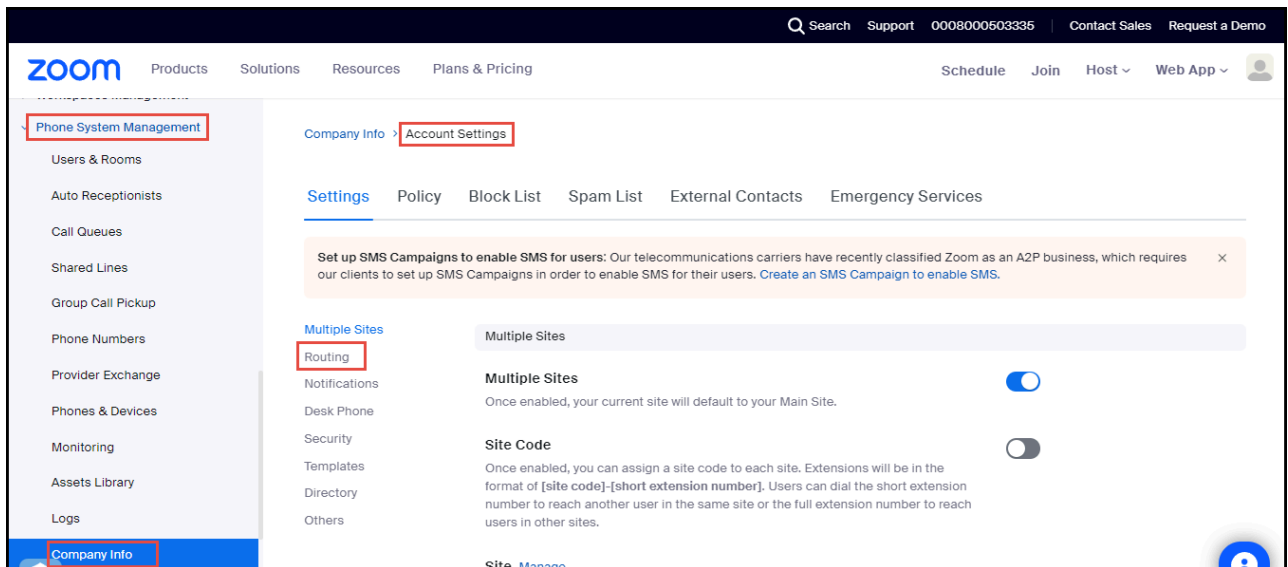
6. Optional: Hover over the green LED icon to view the trunk status, as shown below:

3.2.2 Configuring the SIP Group

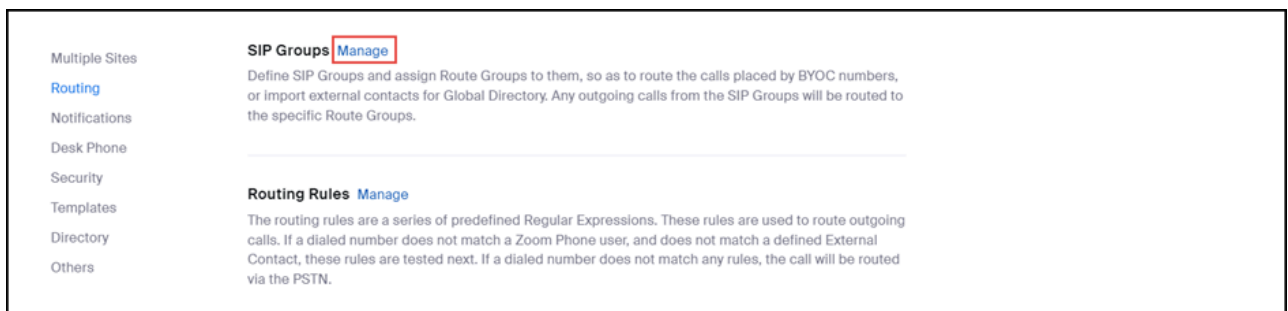
Follow the instructions below to configure SIP groups and assign Route Groups to them, in order to route calls placed by BYOC numbers. This step is mandatory for uploading the BYOC numbers.

To add a SIP Group:

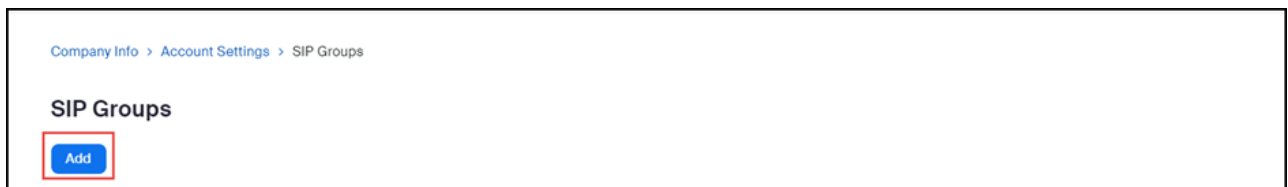
1. Navigate to **Phone System Management > Company Info > Account Settings > Routing**.



2. Locate the **SIP Groups** section and click **Manage**.



3. Click **Add**.



4. Configure the following:

- a. **Display Name:** Type the display name of your choice. For example, **sip_group_OpenScape**.
- b. From the **Route** drop-down menu, select the **Route_group_OpenScape (BYOC)** group, created in [Configuring the Route Group](#) on page 11.

Add SIP Group

Display Name

☐ Send SIP Group Name in SIP header [?](#)

Route Group

Description (Optional)

5. Click **Save**.

3.2.3 Configuring the Routing Rule

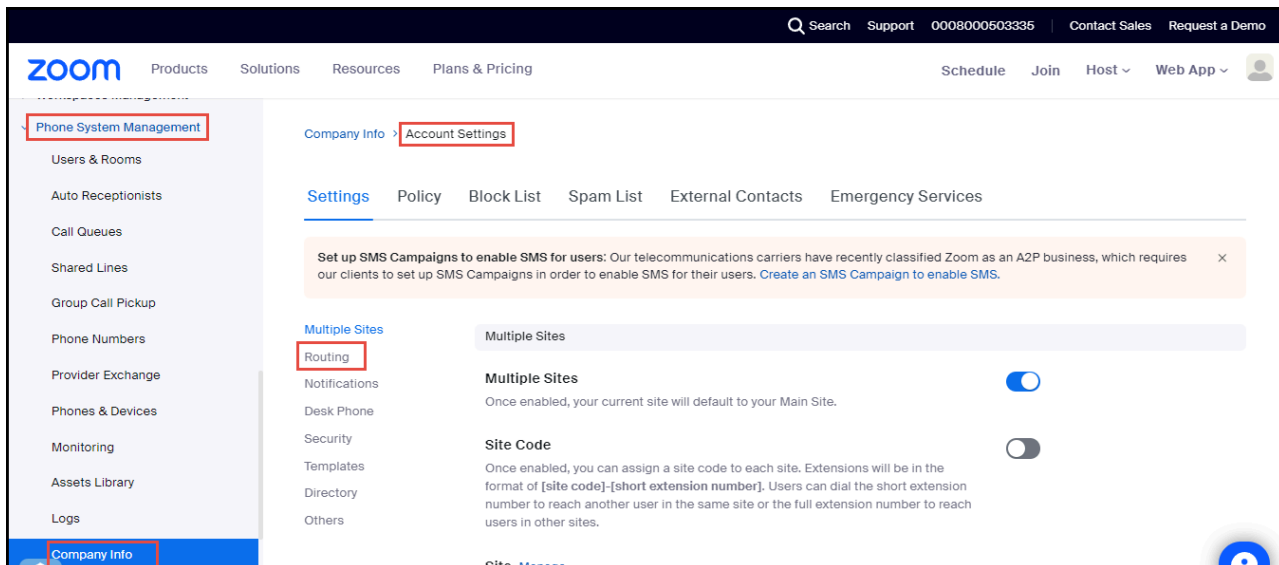
When configuring a **BYOC (Bring Your Own Carrier)** setup, you might create a routing rule to specify that calls from certain users or departments go through your OSSBC or network route. To add a Routing Rule for outbound calls:



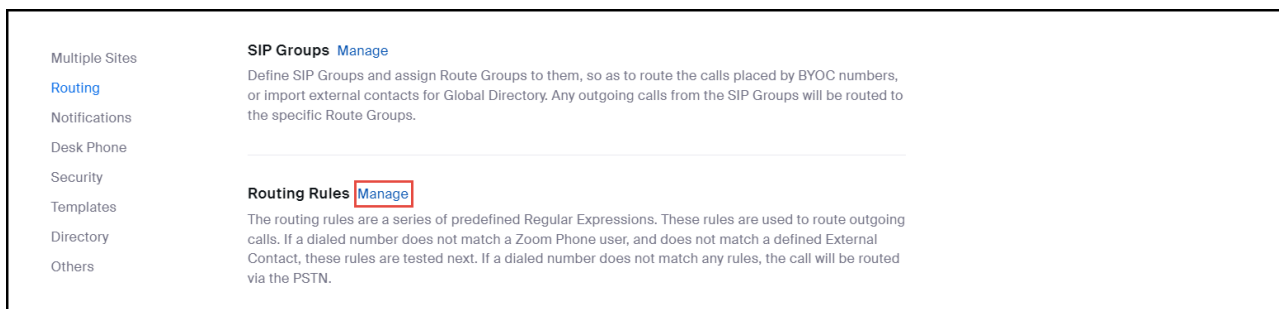
Note:

Ensure that your Session Border Controller (OSSBC) is properly configured and connected before setting up routing rules. Additionally, phone users must be provisioned and assigned to the correct phone numbers for routing rules to function correctly.

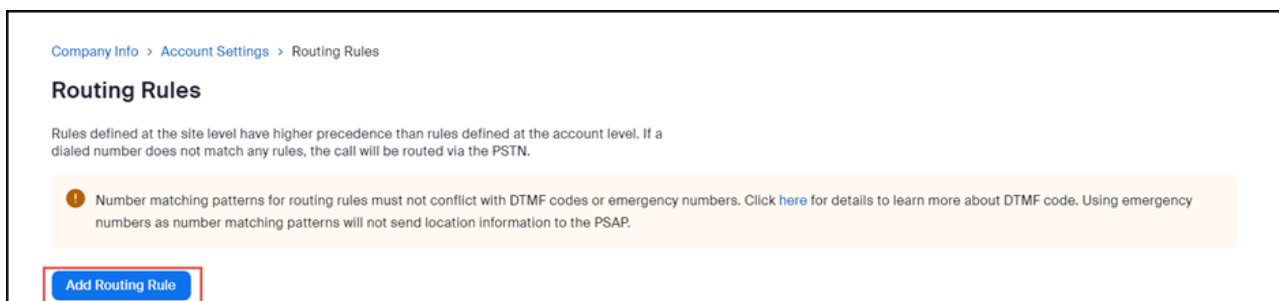
1. Navigate to **Phone System Management > Company Info > Account Settings > Routing**.



2. Locate the **Routing Rule** section and click **Manage**.



3. Click **Add Routing Rule** to add your rule.



4. Configure the following:

- a. **Rule Name:** Type the rule name of your choice. For example, **Outgoing**.
- b. **Number Matching and Translation:** Enter the `^(\d{11})$` Number Pattern (as given below)
- c. **Routing path:** Select the **sip_group_OpenScape** routing path, created in [2.3 Adding SIP Group](#).

Add Routing Rule

Level

Account

Rule Name

Outgoing

Number Matching
and Translation ?

Number Pattern

 $\wedge \backslash d \{ 11 \} \$$

Translation (Optional)

Replacement Pattern must be in E.164 format

Test ?



Number matching patterns for routing rules must not conflict with DTMF codes or emergency numbers. Click [here](#) for details to learn more about DTMF code. Using emergency numbers as number matching patterns will not send location information to the PSAP.

Routing Path

sip_group_OpenScape

Call Forwarding ?



Save

Cancel

5. Click **Save**.

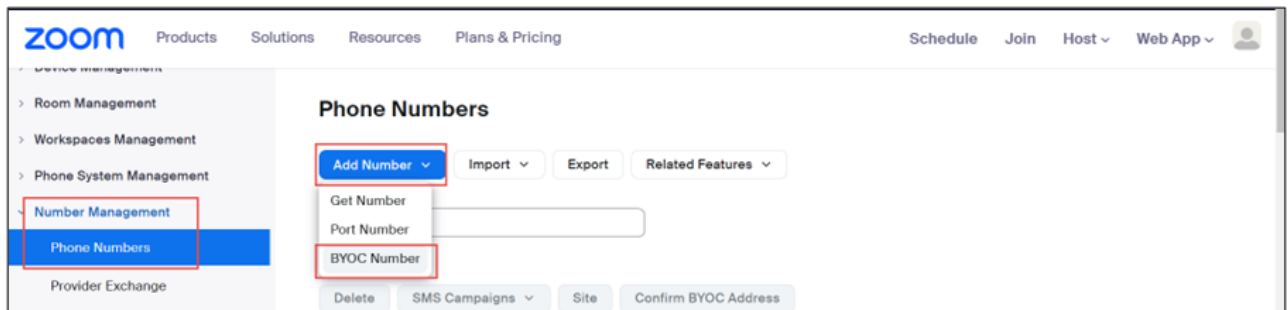
3.3 Adding BYOC Phone numbers

You can upload BYOC phone numbers.

Prerequisite

1. You are an administrator with the privilege to edit account settings.

1. Log in the **Zoom web portal**.
2. Navigate to **Number Management > Phone numbers**.
3. From the **Add Number** drop-down menu, select **BYOC Number**.



4. In the **Add BYOC Numbers** window:

- a. From the **Product** drop-down menu, select **Phone**.
- b. From the **Country/Region** drop-down menu, select the country to which the phone numbers belong. For example, United States.
- c. In the **Numbers** field, enter the phone numbers separated by ', ', as shown in the image below.
- d. From the **SIP System** drop-down menu, select **Zoom Phone**.
- e. From the **SIP Group** drop-down menu, select the SIP group created in [Configuring the SIP Group](#) on page 14.
- f. Check the acknowledgment box to consent.
- g. Click **Submit**.

Add BYOC Number

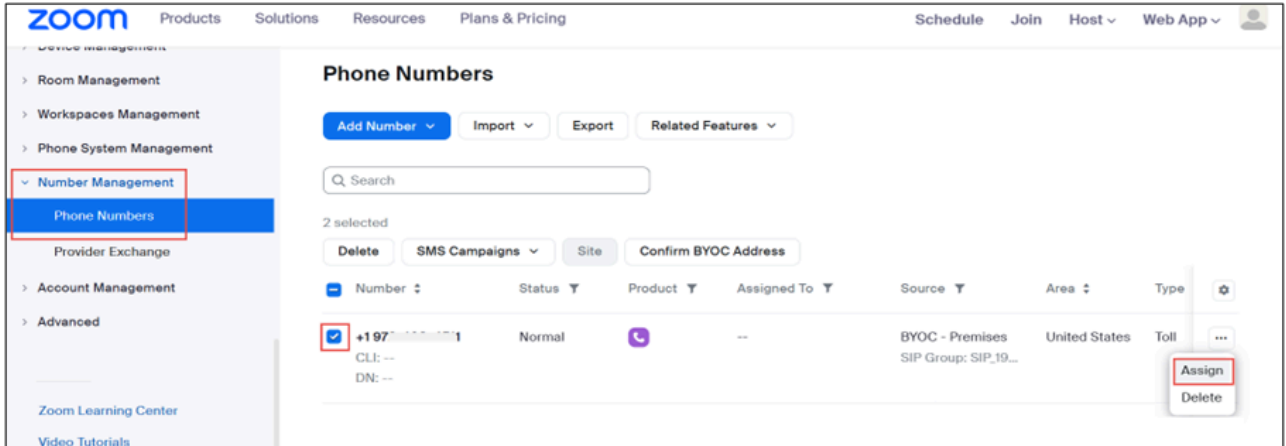
Product	Phone	▼
Site	Main Site	
Country/Region	United States	▼
Numbers	9728522000,9728522001,9728522002	
SIP System	Zoom Phone	▼
SIP Group	Choose a routing path for calls to/from the numbers sip_group_OpenScape	
<input checked="" type="checkbox"/> I acknowledge that by checking the box, I attest that the phone numbers to be imported belong to me or my organization		
<input type="button" value="Submit"/>		<input type="button" value="Cancel"/>

3.3.1 Assigning BYOC numbers

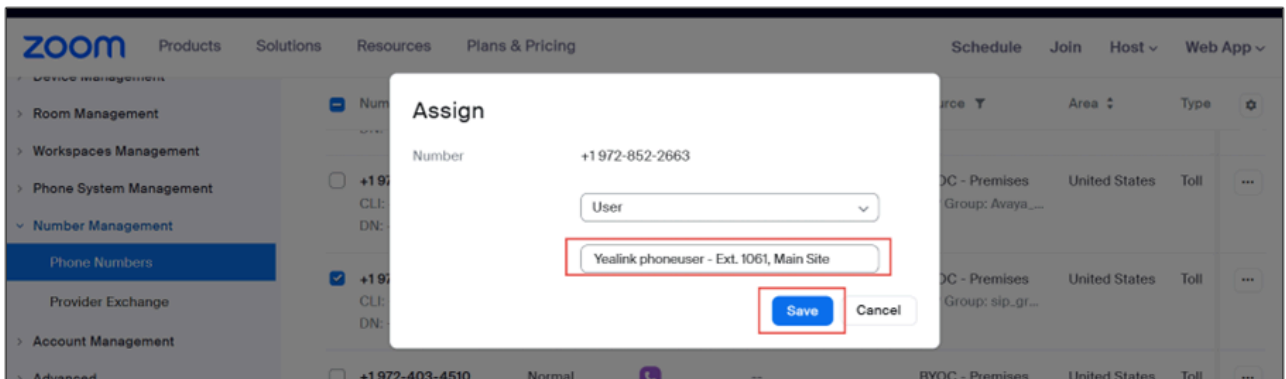
To assign Bring Your Own Carrier (BYOC) numbers to the Zoom phone users:

1. Navigate to **Number Management > Phone Numbers**.
2. Select the **phone number** that needs to be assigned to the Zoom phone user and click "...".

3. Click **Assign**.



4. From the drop-down menu, select an extensions to assign the phone number to and click **Save**.



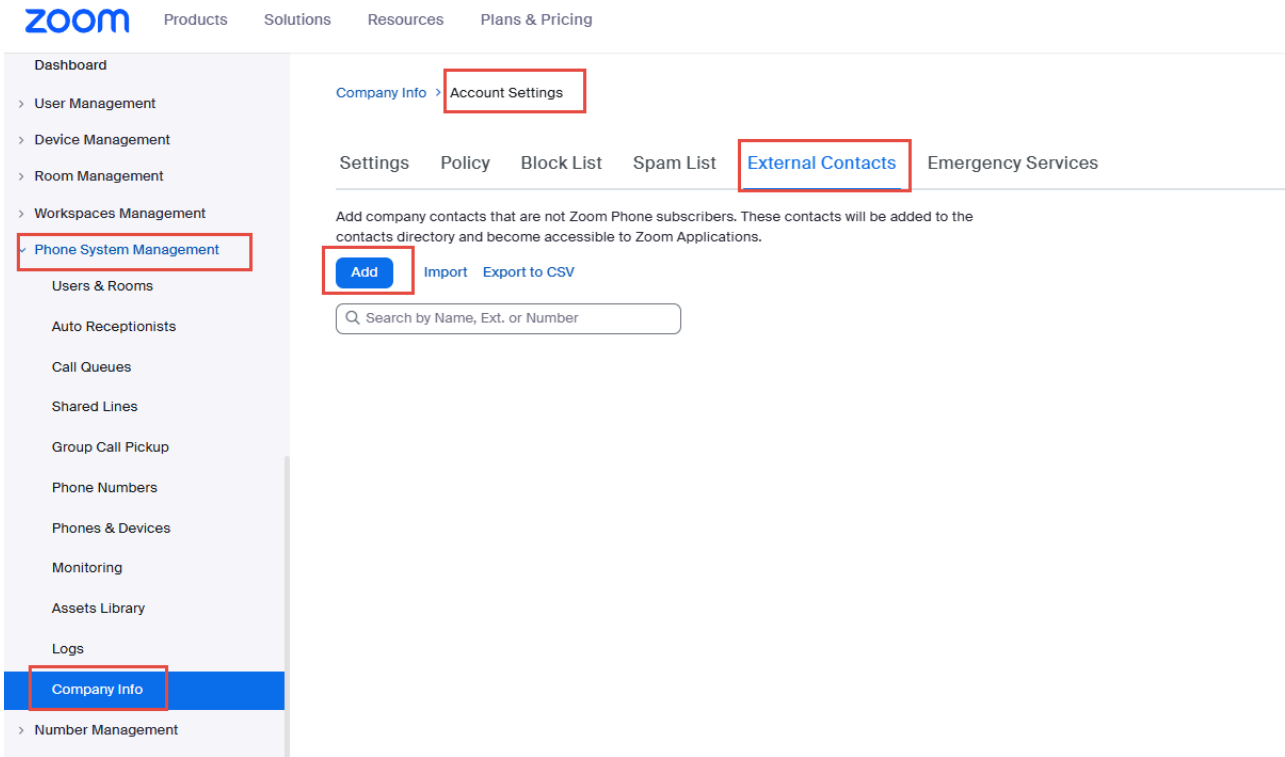
The phone number will be assigned to the selected user.

3.4 Adding BYOP numbers

Administrators can add OpenScape Voice users as external contacts, which will be added to the contacts directory and be accessible to Zoom applications. To add Bring Your Own PBX (BYOP) numbers:

1. Navigate to **Phone System Management > Company Info > Account Settings > External Contacts**.

2. Click **Add**.



3. In the **Add External contact** pop-up, configure the following:

- **Name:** Type the name of the OpenScape Voice user. For example, **OSV_user1**.
- In the **Extension Number** field, enter the extension number of the OpenScape Voice user.
- From the **Routing path** drop-down menu, select the **SIP Group** created in [Configuring the SIP Group](#) on page 14.

Add External Contact

ID (Optional) (?)

Name

Email (Optional)

Extension Number (?)

Phone Number (Optional) (?)

Description (Optional)

Routing Path (?)

Auto Call Recorded (?) ☐

Save Cancel

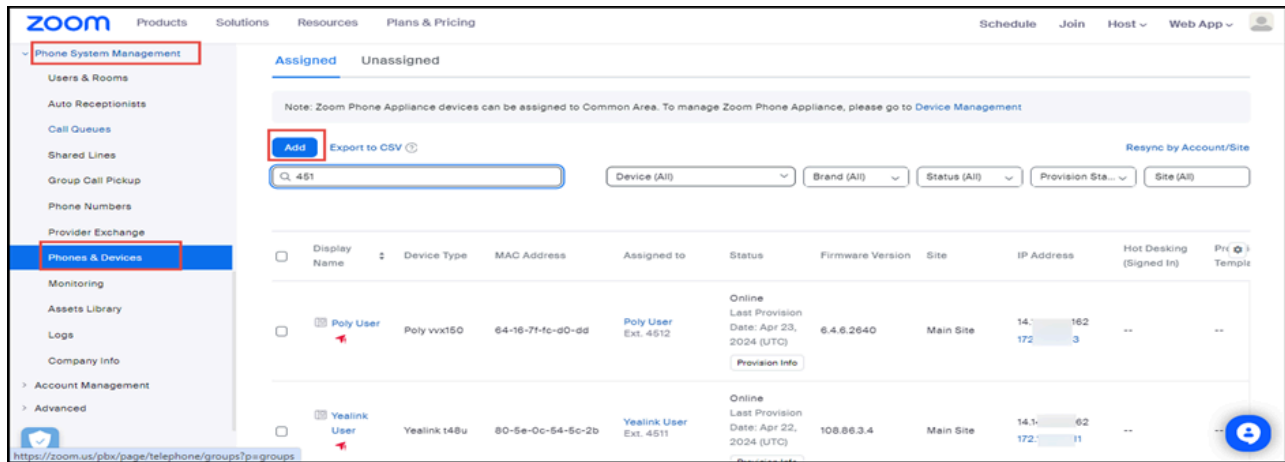
4. Click **Save**.

Provisioning Phones for Zoom Phone Users

4

Follow the instructions below to provision Desk phones for Zoom Phone users. Zoom-certified vendor phone models are used for this test and will be available after provisioning.

1. Navigate to **Phone System Management > Phones & Devices**.
2. Click **Add**.



3. In the **Add Device** pop-up, configure the following:

- a. **Display Name:** Type the display name for the phone. For example, **Yealink phoneuser**.
- b. **MAC Address:** Enter the **MAC address** of the phone.
- c. **Device Type:** Select the device type. For example, **Yealink**.
- d. From the **Assigned to** drop-down menu, select the user to whom you want to assign the phone number and click **Add**.
- e. Click **Save**.

Add Device

Display Name

Yealink phoneuser

Description
(Optional)

MAC Address

80-5e-0c-54-5c-2b

Device Type

Yealink

t48u

This device type supports up to 1 assignee.

Assigned to

User

Yealink phoneuser - Ext. 1084, Main S

Add

Cancel

Provision
Template
(Optional)

Not Set

Save

Cancel

Unify OpenScape Voice Configuration

5

This chapter contains the following sections:

- [Configuring Endpoints](#)
- [Destinations and Routes Configuration](#)
- [Translation Configuration](#)
- [Configuring the SIP UA Forking](#)
- [Configuring Display Number Modification](#)

This chapter describes the OpenScape Voice configuration for connecting to OpenScape SBC. The purpose of this connectivity is for OpenScape Voice to provide the necessary SIP message manipulation and call routing facilities to OpenScape SBC so that the latter can interconnect to Zoom Phone SBC and calls between Zoom clients and PSTN subscribers are feasible.

In OpenScape Voice, you must set up the connection to the OpenScape SBC and the signaling paths to Zoom Phone data centers and the SSP (PSTN provider).

Call routing must also be configured based on the numbering plan for Zoom users and PSTN subscribers.

As an example:

Items	Example
SBC IP	10.8.242.72 TCP 5060
Signaling path to Zoom destination 1 ³	10.8.242.72 TCP 50001
Signaling path to Zoom destination 2	10.8.242.72 TCP 50002
Signaling path to Zoom destination 3	10.8.242.72 TCP 50003
Signaling path to PSTN provider: BCOM	10.8.242.72 TCP 50010
Zoom user number ranges (reachable from PSTN)	1972598xxxxx

³ Please refer to the **Signaling Traffic** table under the **Premises Peering Firewall Requirements for Media and Signaling** section in the **Zoom Phone Bring Your Own Carrier- Premises (BYOC-P) Solution Reference Guide**.

5.1 Configuring Endpoints

An **Endpoint** is a network component, such as an originating or terminating device and in our case the 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.

5.1.1 Configuring the OpenScape SBC Endpoint

To configure the OpenScape SBC Endpoint Profile:

1. Navigate to **Unify OpenScape Common Management Platform > Configuration > Unify OpenScape Voice > Business Group > Business Group List**.
2. From the **Business Group List** drop-down menu, select your Business Group. For example, **Zoom_BG**.
3. In the selected Business Group, navigate to **Profiles > Endpoint** and click **Add**.
4. In the **Add Endpoint Profile** window, under the **General** tab, configure the following:
 - a. **Name:** Enter the name of the endpoint profile. For example, **EPP_SBC01**.
 - b. From the **SIP Privacy Support** drop-down menu, select **Full**.

The screenshot displays the 'Add Endpoint Profile' window in a web browser. The browser's address bar shows the URL: <https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/Profiles/PopUps/modif...>. The window title is '[OSV] - [ZOOM_BG] - Add Endpoint Profile'. The 'General' tab is selected, showing the following fields:

- Name:** EPP_SBC01
- Remark:** (empty text area)
- Numbering Plan:** NP_ZOOM_BG
- SIP Privacy Support:** Full

Below the 'General' tab is the 'Management Information' section, which includes fields for Class of Service, Routing Area, Calling Location, and Time Zone, each with a dropdown menu. At the bottom right of the window are 'Save' and 'Cancel' buttons.

5. In the **Services** tab, enable the following required services by selecting **Yes** from the corresponding drop-down menus:

- **Message Waiting**
- **Call Transfer**

The screenshot shows a web browser window with the URL <https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/Profiles/PopUps/modif...>. The page title is "[OSV] - [ZOOM_BG] - Add Endpoint Profile". Below the title bar, there is a message "Please enter the profile data." and three tabs: "General", "Endpoints", and "Services". The "Services" tab is selected and highlighted with a red box. Under the "Services" tab, there are several configuration options, each with a radio button and a dropdown menu. The "Message Waiting:" and "Call Transfer:" options are both set to "Yes" and are highlighted with a red box. Other options include "Call Forward Invalid Destination:" (No), "Toll and Call Restrictions:" (No), "Park to Server:" (No), and "CSTA Network Interface Device:" (No). There is also a checkbox for "Enable Name Provider and Limited Call Control" which is unchecked. Below these options, there is a section titled "What to do if Application fails to handle inbound calls:" with a dropdown menu set to "Allow call to proceed as norm". At the bottom right of the form, there are "Save" and "Cancel" buttons, with the "Save" button highlighted by a red box.

6. Click **Save**.

7. Navigate to **Unify OpenScape Common Management Platform > Configuration > Unify OpenScape Voice > Business Group > Members > Endpoints** to configure the **Endpoint**.

8. Click **Add**.

9. In the **General** tab, configure the following:

- a. **Name:** Enter the name of the SBC endpoint. For example, **EP_SBC01**.
- b. **Profile:** Select the previously created endpoint profile. For example, **EPP_SBC01**.
- c. **Endpoint Template:** Select **Central SBC** (set of pre-configured endpoint attributes).
- d. Click **Save**.

The screenshot shows the 'Add Endpoint' configuration window in the Unify OpenScape management portal. The browser address bar shows the URL: https://10.70.16.6/management/portal/_ns:YWE1NWl3ZWVhLTlVIZmItNDg2Ni0.... The page title is '[OSV] - [ZOOM_BG] - [Main Office] - Add Endpoint : EP_SBC01'. The 'General' tab is selected, and the following fields are highlighted with red boxes:

- Name:** EP_SBC01
- Profile:** EPP_SBC01
- Endpoint Template:** Central SBC
- Save** button

Other visible fields include Remark, Registered (checked), Branch Office, Associated Endpoint, Default Home DN, Location Domain, Endpoint Type (Central SBC), and Max number of users.

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

- a. Select the **SIP Trunking** option to enable it.
- b. From the **Type** drop-down menu, select **Static** (it can be enabled only if the **SIP Proxy** attribute is enabled).
- c. From the **Signaling Address Type** drop-down menu, select **IP Address or FQDN** (route the calls via proxy).
- d. **Endpoint Address**: Enter the SBC address.
- e. **Port**: Enter the port number.
- f. From the **Transport protocol** drop-down menu, select **TCP**.

The screenshot shows a web browser window with the title "[OSV] - [ZOOM_BG] - [Main Office] - Add Endpoint - Google Chrome". The address bar shows a "Not secure" warning and the URL "https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessG...". The page title is "[OSV] - [ZOOM_BG] - [Main Office] - Add Endpoint".

At the top, there are tabs for "General", "SIP", "Attributes", "Aliases", "Routes", and "Accounting". The "SIP" tab is selected.

Below the tabs, there are three radio button options:

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

Below these options is a section titled "SIP Signaling". It contains a note: "For the static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format." and a warning icon with the text: "Note that the address of the signaling interface cannot be modified unless the entry in the security section has first been removed."

Below the note is a form with the following fields:

- Type: Static (dropdown menu)
- Signaling Address Type: IP Address or FQDN (dropdown menu)
- Endpoint Address: 10.70.16.6 (text input)
- Port: 5060 (text input)
- Transport protocol: TCP (dropdown menu)

11. Locate the **Security** section, click **Edit**, and add the primary SIP port (5060) of the SBC. Click **Save**.

[grp1019] - [Zoom PSI] - [Main Office] - Edit Endpoint : SBC_Zoom_PSI

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

SRTP media mode: Enabled

ANAT Support: Enabled

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: 5060-5060 **Edit...**

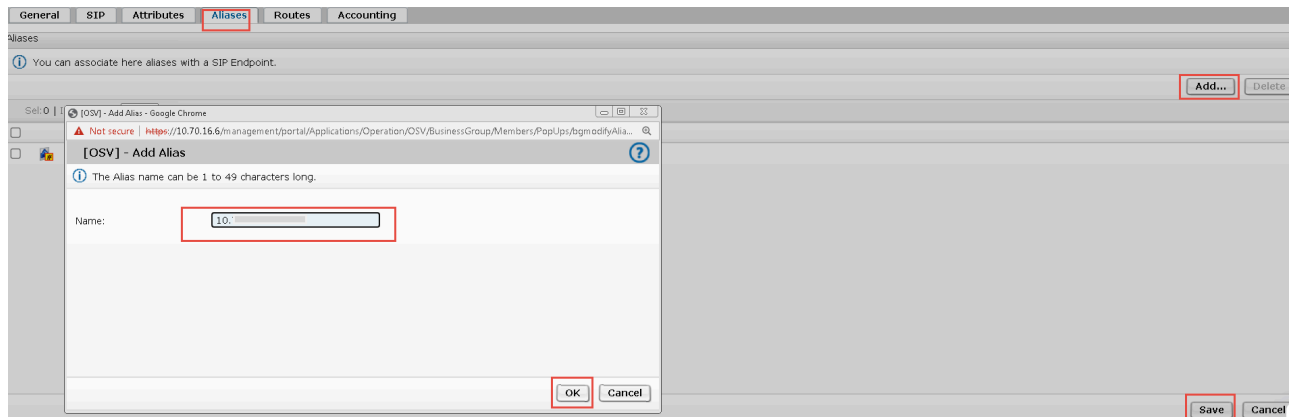
Save **Cancel**

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

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

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"/>		
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"/>		

13. Select the **Aliases** tab and click **Add** to enter the SBC LAN interface for incoming SIP traffic.



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

5.1.2 Configuring the Zoom Phone Endpoint

Prerequisite

To configure **SIP UA Forking Support** for the Zoom Phone Endpoint, you must enable the SIP UA Forking Support option. To do this, follow the instructions in [Configuring the SIP UA Forking](#) on page 65.

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

3. In the **Add Endpoint Profile** window, under the **General** tab, configure the following:

- **Name:** Enter the name of the endpoint profile. For example, **EPP_Zoom**.
- From the **SIP Privacy Support** drop-down menu, select **Full Receive**.

[OSV] - [ZOOM_BG] - Add Endpoint Profile - Google Chrome

Not secure | https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/Profiles/PopUps/modif...

[OSV] - [ZOOM_BG] - Add Endpoint Profile

Please enter the profile data.

General | Endpoints | Services

Name: EPP_Zoom

Remark:

Numbering Plan: NP_ZOOM_BG

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

Save Cancel

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

The screenshot shows a web browser window titled "[OSV] - [ZOOM_BG] - Add Endpoint Profile - Google Chrome". The address bar shows a URL starting with "https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/Profiles/PopUps/modif...". The page title is "[OSV] - [ZOOM_BG] - Add Endpoint Profile". Below the title bar, there is a message "Please enter the profile data." and three tabs: "General", "Endpoints", and "Services". The "Services" tab is selected and highlighted with a red box. Under the "Services" tab, there are several configuration options, each with a radio button and a dropdown menu. The "Call Transfer" option is selected with a radio button and its dropdown menu is set to "Yes", which is also highlighted with a red box. Other options include "Message Waiting" (set to "No"), "Call Forward Invalid Destination" (set to "No"), "Toll and Call Restrictions" (set to "No"), "Park to Server" (set to "No"), and "CSTA Network Interface Device" (set to "No"). There is also a checkbox for "Enable Name Provider and Limited Call Control" which is unchecked. At the bottom right of the form, there are "Save" and "Cancel" buttons, with the "Save" button highlighted by a red box.

5. Click **Save**.
6. In the OpenScape Common Management Platform, navigate to **Configuration > OpenScape Voice > Business Group > Members > Endpoints** and click **Add**.

7. In the **Add Endpoint** pop-up, under the **General** tab, configure the following:

- a. **Name:** Enter the name of the Zoom endpoint. For example, **EP_Zoom_SP1**.
- b. **Profile:** Select the previously created Zoom endpoint profile. For example, **EPP_Zoom**.

The screenshot shows the 'Add Endpoint' pop-up window in the Unify OpenScape management portal. The window is titled '[OSV] - [ZOOM_BG] - [Main Office] - Add Endpoint' and has tabs for 'General', 'SIP', 'Attributes', 'Aliases', 'Routes', and 'Accounting'. The 'General' tab is active. The form contains the following fields:

- Name:** EP_Zoom_SP1
- Remark:** (empty text area)
- Registered:** ☐
- Profile:** EPP_Zoom
- Branch Office:** (empty text field)
- Associated Endpoint:** (empty text field)
- Default Home DN:** (empty text field)
- Location Domain:** (empty text field)
- Endpoint Template:** (empty text field)
- Endpoint Type:** (empty text field)
- Max number of users:** (empty text field)

The 'Save' button is highlighted with a red box.

8. Click **Save**.

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

- a. Select the **SIP Trunking** option to enable it.
- b. From the **Type** drop-down menu, select **Static** (it can be enabled only if the **SIP Proxy** attribute is enabled).
- c. From the **Signaling Address Type** drop-down menu, select **IP Address or FQDN** (route the calls via proxy).
- d. **Endpoint Address:** Enter the SBC address.
- e. **Port:** Enter the port number for Zoom trunk.
- f. From the **Transport protocol** drop-down menu, select **TCP**.
- g. From the **SRTP media mode** drop-down menu, select **Disabled**.

The screenshot shows the 'Add Endpoint' configuration page in the Unify OpenScope Voice Configuration interface. The browser address bar shows the URL: <https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/Members/PopUps/modifyBGEndpoint.psmi?callPointParam=tru...>. The page has tabs for General, SIP, Attributes, Aliases, Routes, and Accounting. The SIP tab is selected. The configuration options are as follows:

- SIP Private Networking:** ☐
- SIP Trunking:** ☒ (highlighted with a red box)
- 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 (dropdown menu)
- Signaling Address Type:** IP Address or FQDN (dropdown menu)
- Endpoint Address:** 10. (text input field)
- Port:** 50001 (text input field)
- Transport protocol:** TCP (dropdown menu)
- Endpoint does not accept incoming TLS connections:** ☐
- SRTP media mode:** Disabled (dropdown menu, highlighted with a red box)
- Key Exchange:** (dropdown menu)

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

- h. From the **SIP UA Forking Support** drop-down menu, select **Full**:

Key Exchange Mechanisms Supported:	<input type="text"/>
ANAT Support:	<input type="text" value="Disabled"/>
ICE Support:	<input type="text" value="Enabled"/>
DTLS Support:	<input type="text" value="Enabled"/>
SIP UA Forking Support:	<input type="text" value="Full"/>
Use Proxy/SBC Best-Effort SRTP settings for calls to subscribers: AS-SIP Interface	<input type="checkbox"/>
Management Address:	<input type="text"/>
Red Sky E911 Manager node:	<input type="checkbox"/>

10. Locate the **Security** section, click **Edit**, and add the primary SIP port (5060) of the SBC.

11. Click **Save**.

[grp1019] - [Zoom PSI] - [Main Office] - Edit Endpoint : SBC_Zoom_PSI

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

S RTP media mode: Enabled

ANAT Support: Enabled

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: 5060-5060 **Edit...**

Save **Cancel**

12. In the **Attributes** tab, select the following parameters to activate them:

- **SIP Proxy**
- **Route via Proxy**
- **Allow sending of Insecure Referred-By Header**

General	SIP	Attributes	Aliases	Routes	Accounting
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"/>					

- **Do not send Invite without SDP**
- **Send International Numbers in Global number format (GNF)**

Send P-Preferred-Identity rather than P-Asserted-Identity	<input type="checkbox"/>
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"/>

- **Enable Session Timer**
- **Limited PRACK Support**

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"/>

- **Support Replaces Header**
- **Ignore Receipt/Do not send Privacy Header**
- **Enable REFER Notifications**

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"/>
History-Info Supported	<input type="checkbox"/>
Increment SDP o-line	<input type="checkbox"/>

13. Select the **Aliases** tab, click **Add** and enter the **SBC LAN interface** with port number for incoming SIP traffic.

The screenshot shows the 'Aliases' tab in the configuration interface. A dialog box titled '[OSV] - Add Alias' is open, prompting the user to enter an alias name. The 'Name' field contains the text '10.10.10.10'. The 'Add...' button in the top right corner of the dialog is highlighted with a red box. The 'OK' and 'Cancel' buttons are at the bottom of the dialog.

14. Click **OK** and then click **Save**.
15. Repeat the same procedure to create the endpoints for the remaining Zoom IPs, assigning the respective port numbers:
 - EP_Zoom_SP2 with port 50002
 - EP_Zoom_SP3 with port 50003

5.1.3 Configuring the PSTN Endpoint

Note:

The configuration below is an example. The actual configuration steps depend on your provider's requirements.

1. Navigate to **Unify OpenScope Common Management Platform > Configuration > Unify OpenScope Voice > Business Group > Profiles > Endpoint** to configure the PSTN Endpoint Profile.
2. Click **Add**.
3. In the **Add Endpoint Profile** pop-up, under the **General** tab, configure the following:
 - a. **Name:** Enter the name of the endpoint profile. For example, **EPP_PSTN**.
 - b. From the **SIP Privacy Support** drop-down menu, select **Full**.

[OSV] - [ZOOM_BG] - Add Endpoint Profile - Google Chrome

Not secure | <https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/Profiles/PopUps/modifyEndPointProfile.psml?callPoi...>

[OSV] - [ZOOM_BG] - Add Endpoint Profile

Please enter the profile data.

General | Endpoints | Services

Please enter a unique name to identify this profile.

Name:

Remark:

Numbering Plan: ...

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: ▼

Failed Calls Intercept Treatment: ▼

Save **Cancel**

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

The screenshot shows a web browser window with the title "[OSV] - [ZOOM_BG] - Add Endpoint Profile - Google Chrome". The address bar shows a URL starting with "https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/Profiles/PopUps/modif...". The browser tab is labeled "[OSV] - [ZOOM_BG] - Add Endpoint Profile".

Below the browser window, there is a message: "Please enter the profile data." and three tabs: "General", "Endpoints", and "Services". The "Services" tab is selected and highlighted with a red box.

Under the "Services" tab, there are several configuration options, each with a radio button and a dropdown menu:

- Message Waiting:** Set to "No".
- Call Transfer:** Set to "Yes" (highlighted with a red box).
- 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".

There is also a checkbox labeled "Enable Name Provider and Limited Call Control" which is unchecked.

Below these options, there is a section titled "What to do if Application fails to handle inbound calls:" with a dropdown menu set to "Allow call to proceed as norm" and an empty text input field.

At the bottom right of the form, there are two buttons: "Save" (highlighted with a red box) and "Cancel".

5. Click **Save**.
6. To add Endpoints: In the Unify OpenScape Common Management Platform, navigate to **Configuration > OpenScape Voice > Business Group > Members > Endpoints**
7. Click **Add**.

8. In the **Add Endpoint** pop-up, under the **General** tab, configure the following:

- a. **Name:** Enter the name of the PSTN endpoint. For example, **EP_PSTN**.
- b. **Profile:** Select the previously created PSTN endpoint profile. For example, **EPP_PSTN**.

The screenshot shows the 'Add Endpoint' pop-up window in the Unify OpenScape Voice Configuration interface. The window is titled '[OSV] - [ZOOM_BG] - [Main Office] - Add Endpoint' and is displayed in a Google Chrome browser. The 'General' tab is selected, showing fields for Name, Remark, Registered, Profile, Branch Office, Associated Endpoint, Default Home DN, Location Domain, Endpoint Template, Endpoint Type, and Max number of users. The 'Name' field is set to 'EP_PSTN' and the 'Profile' field is set to 'EPP_PSTN'. The 'Save' button is highlighted with a red box.

- c. Click **Save**.

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

- a. Select the **SIP Trunking** option to enable it.
- b. From the **Type** drop-down menu, select **Static** (it can be enabled only if the **SIP Proxy** attribute is enabled).
- c. From the **Signaling Address Type** drop-down menu, select **IP Address or FQDN** (route the calls via proxy).
- d. **Endpoint Address**: Enter the SBC address.
- e. **Port**: Enter the port number for the PSTN trunk.
- f. From the **Transport protocol** drop-down menu, select **TCP**.
- g. From the **SRTP media mode** drop-down menu, select **Disabled**.

The screenshot shows the 'Add Endpoint' configuration page for a SIP endpoint. The 'SIP' tab is active. The 'SIP Trunking' option is selected. The 'Type' is set to 'Static', 'Signaling Address Type' is 'IP Address or FQDN', 'Endpoint Address' is '10.0.0.1', 'Port' is '50015', and 'Transport protocol' is 'TCP'. The 'SRTP media mode' is set to 'Disabled'. The 'Endpoint does not accept incoming TLS connections' checkbox is unchecked. The 'Key Exchange Mechanisms Supported' dropdown is set to 'None'.

- h. From the **SIP UA Forking Support** drop-down menu, select **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:

10. Locate the **Security** section, click **Edit**, and add all the ports. Click **Save**.

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: All	Edit...
---------	---	------------	-------------------------

[Save](#) [Cancel](#)

11. In the **Attributes** tab, select the following parameters to activate them:

- **SIP Proxy**
- **Route via Proxy**
- **Allow Sending of Insecure Referred-By Header**

General	SIP	Attributes	Aliases	Routes	Accounting
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"/>					

- **Do not send Invite without SDP**
- **Send International Numbers in Global Number Format (GNF)**

Send P-Preferred-Identity rather than P-Asserted-Identity	<input type="checkbox"/>
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"/>

- **Enable Session Timer**
- **Limited PRACK Support**

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"/>

- **Support Replaces Header**
- **Enable REFER Notifications**

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 type="checkbox"/>
Enable REFER Notifications	<input checked="" type="checkbox"/>
History-Info Supported	<input type="checkbox"/>

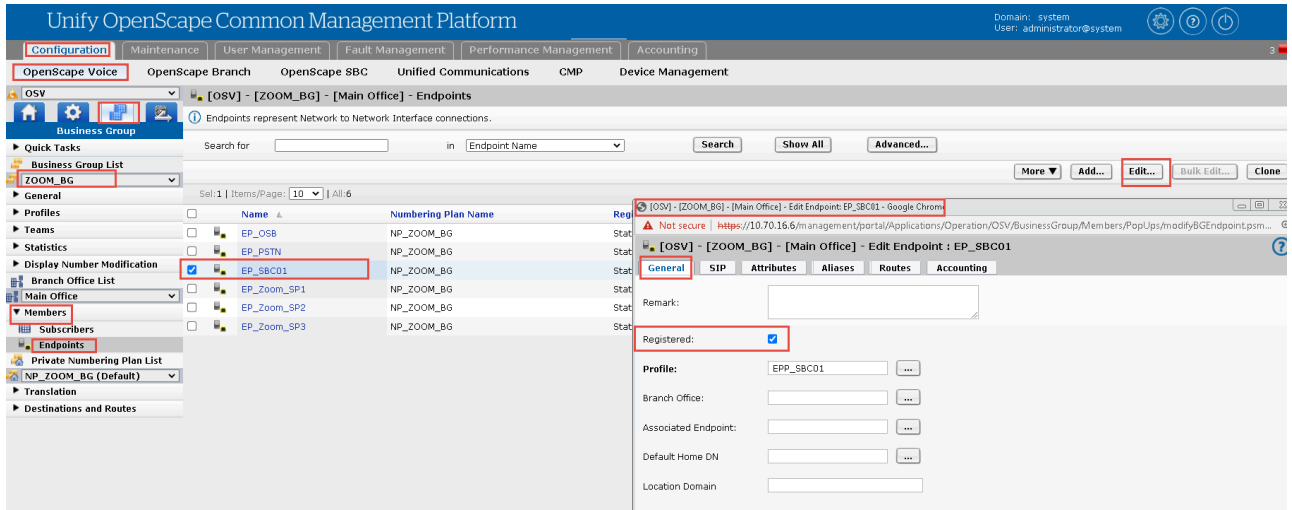
12. Select the **Aliases** tab, click **Add** and enter the **SBC LAN interface** with port number for the incoming SIP traffic.

The screenshot shows the 'Aliases' tab selected in the configuration interface. An 'Add Alias' dialog box is open, prompting the user to enter an alias name. The 'Name' field contains the text '10.'. The dialog box has 'OK' and 'Cancel' buttons at the bottom. In the background, the 'Add...' button in the Aliases list is highlighted with a red box.

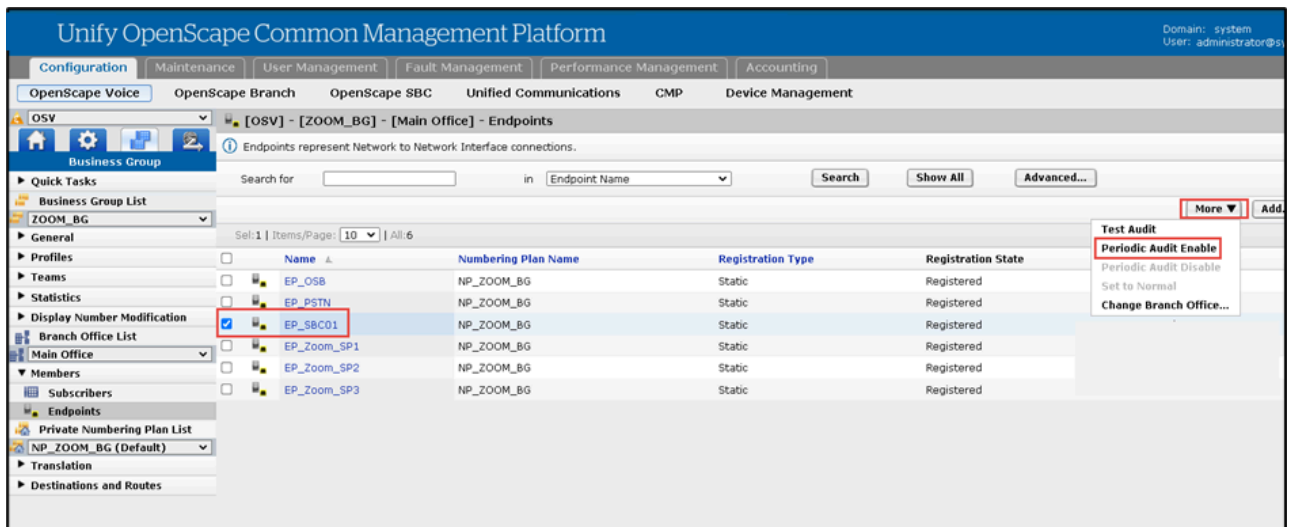
13. Click **OK** and then click **Save**.

5.1.4 Endpoint Overview

1. Navigate to the **Unify OpenScape Common Management Platform > Configuration > Unify OpenScape Voice > Business Group > Members > Endpoints** window. A list of all the configured endpoints in Unify OpenScape Voice is displayed.
2. Select an endpoint and click **Edit**.
3. In the **Edit Endpoint** pop-up, under the **General** tab, check the **Registered** checkbox.



4. Enable the **Registered** option for all the created endpoints.
5. To activate the sending of SIP OPTIONS messages for all the created endpoints, select an endpoint and click the **More** drop-down menu to expand it.



6. Select the **Periodic Audit Enable** option to enable it and route the traffic to the accessible Zoom endpoint(s).

The overview of the created endpoints on the Common Management Platform window is displayed as below:

5.2 Destinations and Routes Configuration

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

Each **Route** is a collection of groups or addresses providing a destination path.

5.2.1 Configuring the Zoom Destination

1. Navigate to **Unify OpenScape Common Management Platform > Configuration > Unify OpenScape Voice > Business Group > Destinations and Routes > Destinations**.
2. Click **Add**.
3. In the **Add Destination** pop-up, under the **General** tab, enter the name of the Zoom destination. For example, **DST_Zoom**.

[OSV] - [ZOOM_BG] - [NP_ZOOM_BG] - Add Destination - Google Chrome

Not secure | https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/DestinationAndRout...

[OSV] - [ZOOM_BG] - [NP_ZOOM_BG] - Add Destination

Destinations are used for routing a call to an endpoint.

General | Routes | Route Lists | Destination Codes

Name: DST_Zoom

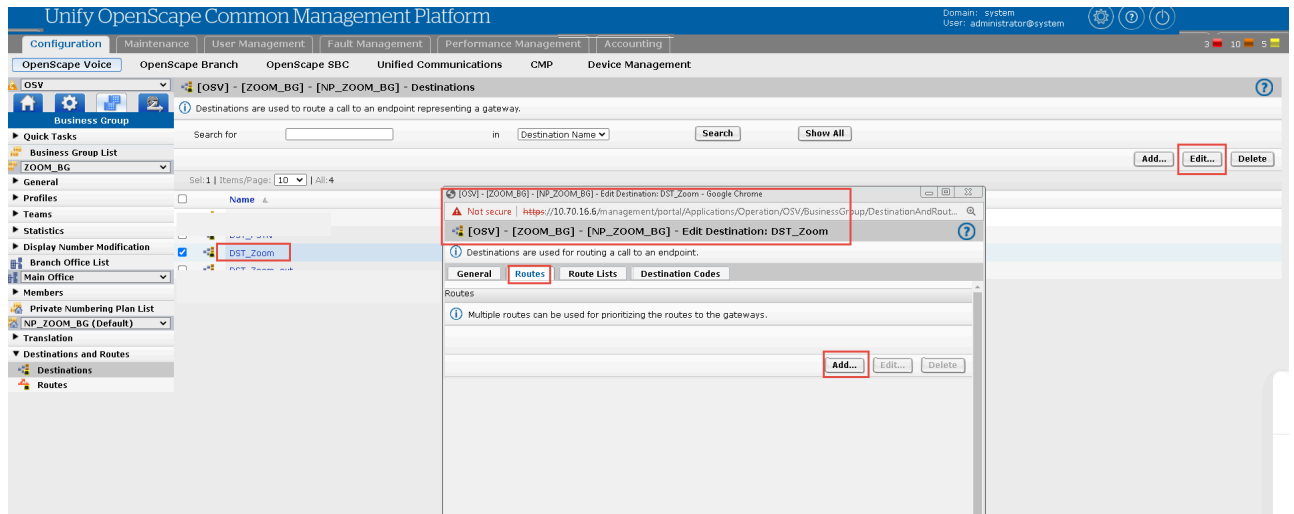
is a Media Server: ☐

is Conference Focus Server : ☐

Save Cancel

4. Click **Save**.
5. Select the destination you created in the previous step and click **Edit**.

6. In the **Edit Destination** pop-up, select the **Routes** tab and click **Add**.



7. In the **Add Route** pop-up, configure the following:

- a. **ID**: Enter the priority level of this route ID as 1 (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).
- b. From the **Type** drop-down menu, select **SIP Endpoint**.
- c. Click the three-dot icon at the right side of the **SIP Endpoint**.
- d. In the **Branch Office List** pop-up, select **Main Office** and click **Next**.

[OSV] - [ZOOM_BG] - [NP_ZOOM_BG] - Add Route

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

ID

The Route ID indicates the priority level.

ID: 1

Type: SIP Endpoint

SIP Endpoint: [] ...

Originator Attributes

Restricts the traffic according to specified settings. Routes with the same

Signaling Type: Undefined

Bearer Capability: Unassigned

Destination Directory Number

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

Modification Type: None

Branch Office List

Branch Office List

Business Group: ZOOM_BG

Items/Page: 10 | All: 1

Branch Office Name

Main Office

Next Cancel

8. In the **Endpoint list** pop-up, select the **Zoom endpoint** and click **OK**, which applies in the SIP endpoint field. Configure the destination directory number settings as below:

- From the **Modification Type** drop-down menu, select **Number Manipulation**.
- From the **Number of digits to delete** drop-down menu, select the number of digits to cut off from the directory number.
- From the **Digits to insert** drop-down menu, enter the digit string which gets added to the beginning of the remaining digits.
- From the **Nature of Address** drop-down menu, select **International**.
- Click **Save**.

The screenshot shows two overlapping windows from the Unify OpenScape Voice Configuration interface. The background window is titled '[OSV] - Endpoint List - Google Chrome' and shows a list of endpoints under the 'Business Group' 'ZOOM_BG'. The 'EP_Zoom_SP1' endpoint is selected. The foreground window is titled '[OSV] - [ZOOM_BG] - [NP_ZOOM_BG] - Add Route'. It shows the configuration for a route with ID '1' and Type 'SIP Endpoint'. The 'SIP Endpoint' field is set to 'EP_Zoom_SP1'. Under 'Originator Attributes', the 'Modification Type' is set to 'Number Manipulation', 'Number of digits to delete' is '0', 'Digits to insert' is '1', and 'Nature of Address' is 'International'. The 'Save' button is highlighted.

9. Repeat the same procedure for the remaining Zoom endpoints, assigning a different ID and priority level per endpoint, as shown in the example below:

General Routes Route Lists Destination Codes						
Routes						
Multiple routes can be used for prioritizing the routes to the gateways.						
Sel: 0 Items/Page: 10 All: 3						
ID	Endpoint	Route Type	Delete	Insert	Nature of Address	
1	EP_Zoom_SP1	SIP-Endpoint	0	1	International	
2	EP_Zoom_SP2	SIP-Endpoint	0	1	International	
3	EP_Zoom_SP3	SIP-Endpoint	0	1	International	

10. In the **Route Lists** tab, select the **Prioritized** flag to enable the Zoom route prioritization, as shown below:

The screenshot shows the 'Route Lists' configuration window. At the top, there are four tabs: 'General', 'Routes', 'Route Lists' (which is selected and highlighted with a red box), and 'Destination Codes'. Below the tabs, there is a description: 'This list provides an overview of all routes with the same originating signaling type and bearer capability. Prioritization is possible.' Below this, there is a table with the following columns: 'Originating Signaling Type', 'Originating Bearer Capability', 'Prioritized', and 'Fallback to Local Numbering Plan'. The 'Prioritized' column has a checkbox that is checked and highlighted with a red box. The 'Fallback to Local Numbering Plan' column has two sub-columns: 'w Dialed Number' and 'w Modified Number', both with unchecked checkboxes. At the bottom right of the window, there are 'Save' and 'Cancel' buttons, with the 'Save' button highlighted by a red box.

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"/>

11. Click **Save**.

5.2.2 Configuring the PSTN Destination

Note:

The configuration below is an example. The actual configuration steps depend on your provider's requirements.

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

3. In the **Add Destination** pop-up, under the **General** tab, enter the name of the Zoom destination. For example, DST_PSTN.

[OSV] - [ZOOM_BG] - [NP_ZOOM_BG] - Add Destination - Google Chrome

Not secure | https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/DestinationAndRout...

[OSV] - [ZOOM_BG] - [NP_ZOOM_BG] - Add Destination

Destinations are used for routing a call to an endpoint.

General Routes Route Lists Destination Codes

Name: DST_PSTN

is a Media Server: ☐

is Conference Focus Server : ☐

Save Cancel

4. Click **Save**.
5. Select the destination you created in the previous step and click **Edit**.
6. In the **Edit Destination** window, select the **Routes** tab and click **Add**.

[OSV] - [ZOOM_BG] - [NP_ZOOM_BG] - Edit Destination: DST_PSTN - Google Chrome

Not secure | https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/DestinationAndRout...

[OSV] - [ZOOM_BG] - [NP_ZOOM_BG] - Edit Destination: DST_PSTN

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

7. In the **Add Route** pop-up, configure the following:

- a. **ID**: Enter the priority level of this route ID as 1 (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).
- b. From the **Type** drop-down menu, select **SIP Endpoint**.
- c. In the **SIP Endpoint** field, enter the **PSTN endpoint**. For example, **EP_PSTN**.

[OSV] - [ZOOM_BG] - [NP_ZOOM_BG] - Add Route - Google Chrome

Not secure | https://10.70.16.6/management/portal/Applications/Operation/OSV/Bu...

[OSV] - [ZOOM_BG] - [NP_ZOOM_BG] - Add Route

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

ID

The Route ID indicates the priority level.

ID: 1

Type: SIP Endpoint

SIP Endpoint: EP_PSTN

Originator Attributes

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

Signaling Type: Undefined

Bearer Capability: Unassigned

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: None

Save Cancel

8. Click **Save**.

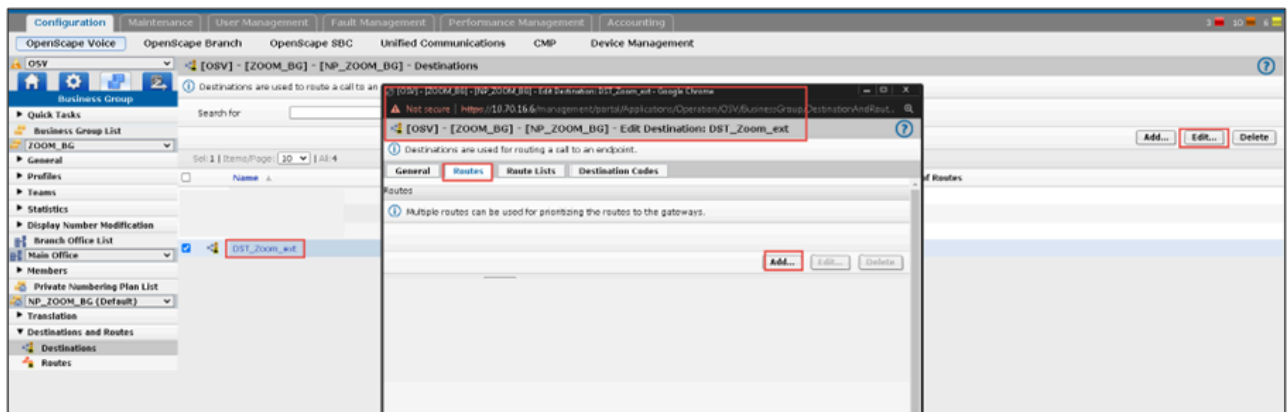
5.2.3 Configuring the OpenScape OSV extension Destination

1. Navigate to **Unify OpenScape Common Management Platform > Configuration > Unify OpenScape Voice > Business Group > Destinations and Routes > Destinations**.
2. Click **Add**.
3. In the **Add Destination** pop-up, under the **General** tab, enter the name of the Zoom destination. For example, **DST_Zoom_ext**.

The screenshot shows a web browser window with the title "[OSV] - [ZOOM_BG] - [NP_ZOOM_BG] - Add Destination - Google Chrome". The address bar displays "https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/DestinationAndRoute...". The page content includes a header with the same title and a sub-header "Destinations are used for routing a call to an endpoint." Below this, there are four tabs: "General", "Routes", "Route Lists", and "Destination Codes". The "General" tab is active, showing a form with a "Name:" label and a text input field containing "DST_Zoom_ext". Below the name field, there are two checkboxes: "is a Media Server:" and "is Conference Focus Server :", both of which are unchecked. At the bottom right of the form, there are "Save" and "Cancel" buttons.

4. Click **Save**.
5. Select the destination you created in the previous step and click **Edit**.

6. In the **Edit Destination** window, select the **Routes** tab and click **Add**.



7. In the **Add Route** pop-up, configure the following:

- a. **ID**: Enter the priority level of this route ID as 1 (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).
- b. From the **Type** drop-down menu, select **SIP Endpoint**.
- c. In the **SIP Endpoint** field, enter the **Zoom endpoint**. For example, **EP_Zoom_SP1**.
- d. Configure the destination directory number settings as below:
 - i. From the **Modification Type** drop-down menu, select **Number Manipulation**.
 - ii. In the **Number of digits to delete** field, enter the number of digits to cut off from the directory number.
 - iii. From the **Number of Address** drop-down menu, select **Unknown**.
- e. Click **Save**.

ID

The Route ID indicates the priority level.

ID: 1

Type: SIP Endpoint

SIP Endpoint: EP_Zoom_SP1

Originator Attributes

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

Signaling Type: Undefined

Bearer Capability: Unassigned

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 Manipulation

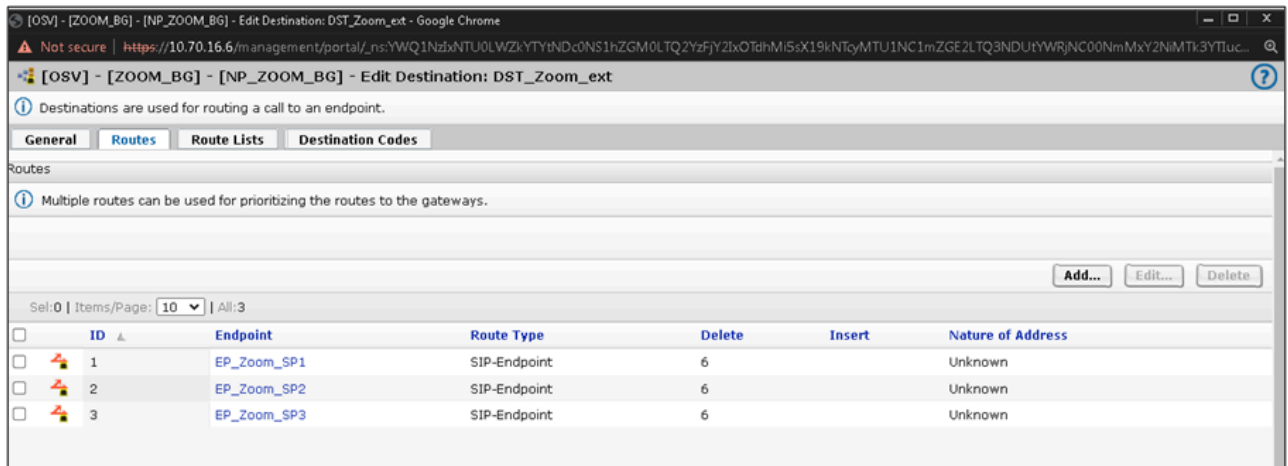
Number of digits to delete: 6

Digits to insert:

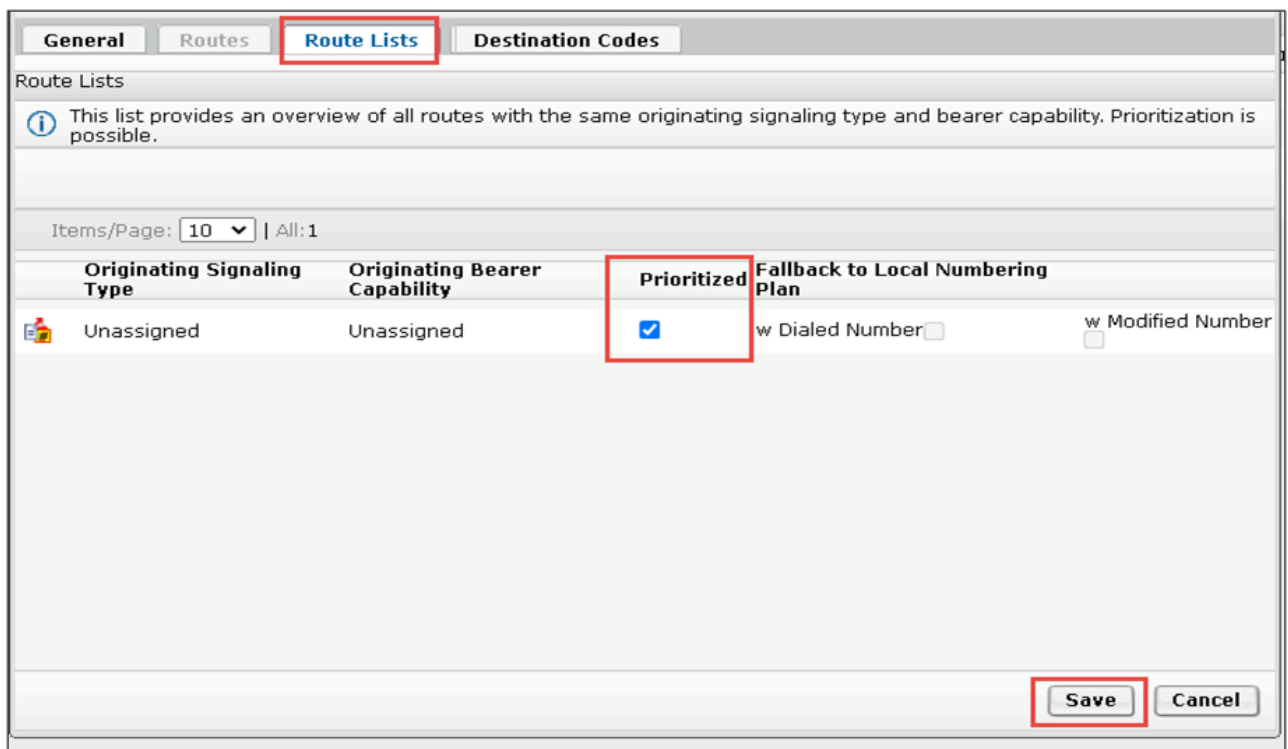
Nature of Address: Unknown

Save Cancel

8. Repeat the same procedure for the remaining Zoom Endpoints, assigning a different ID and priority level per endpoint, as shown in the example below:



9. In the **Route Lists** tab, enable the **Prioritized** flag and click **Save**.



5.3 Translation Configuration

With **Translation**, the administrator configures the routing of outgoing calls based on the dialed digits from OS Voice subscribers. 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 will be applied to a call if the dialed or modified (via PAC) digits and the nature of the address match.

5.3.1 Configuring the Zoom Numbers Routing

1. Navigate to **OpenScape Common Management Platform > Configuration > OpenScape Voice > Business Group > Translation > Prefix Access Codes**.
2. Click **Add**.
3. In the **Add Prefix Access Code** pop-up, configure the following parameters:
 - a. **Prefix Access Code**: Enter the starting digits of Zoom users.
 - b. **Minimum Length**: Enter the minimum expected length of Zoom numbers.
 - c. **Maximum Length**: Enter the maximum expected length of Zoom numbers.
 - d. **Digit Position**: Configure as 0, which implies not removing any digits from the dialed number before sending it to the destination.
 - e. **Prefix Type**: Configure the off-net access to permit access to remote destinations.
 - f. From the **Nature of Address** drop-down menu, select **International**.
 - g. From the **Destination Type** drop-down menu, select **None**. The resulting digits will be processed in the user's numbering plans destination codes table.
 - h. Click **Save**.
4. Navigate to **OpenScape Common Management Platform > Configuration > Unify OpenScape Voice > Business Group > Translation > Destination Codes**.
5. Click **Add**.

6. In the **Add Destination Code** pop-up, configure the following:

- a. **Destination Code:** Select the previously created Prefix Access Code (PAC).
- b. From the **Nature of Address** drop-down menu, select **International**.
- c. From the **Destination Type** drop-down menu, select **Destination**.
- d. **Destination:** Select the destination of Zoom. For example, DST_Zoom.
- e. Click **Save**.

Add Destination Code

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: 972852

Remark:

Nature Of Address: International

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_Zoom

DN Office Code:

Save **Cancel**

5.3.2 Configuring the PSTN Numbers Routing

Note:

The configuration below is an example. The actual configuration steps depend on your provider's requirements.

1. Navigate to **OpenScape Common Management Platform > Configuration > OpenScape Voice > Business Group > Translation > Prefix Access Codes**.
2. Click **Add**.
3. In the **Add Prefix Access Code** pop-up, configure the following:
 - a. **Prefix Access Code:** Enter the starting digits of the PSTN users.
 - b. **Minimum Length:** Enter the minimum expected length of the PSTN numbers.
 - c. **Maximum Length:** Enter the maximum expected length of the PSTN numbers.
 - d. **Digit Position:** Configured as 0, which implies not removing any digits from the dialed number before sending it to the destination.
 - e. From the **Prefix Type** drop-down menu, select **Off-net access** to permit access to remote destinations.
 - f. From the **Nature of Address** drop-down menu, select **International**.
 - g. From the **Destination Type** drop-down menu, select **None** so that the resulting digits are processed in the user's numbering plan destination codes table.
4. Click **Save**.

Identification

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

Prefix Access Code:

Remark:

Minimum Length:

Maximum Length:

Digit Position:

Digits to insert:

Settings

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

Prefix Type:

Nature of Address:

Destination Type:

Destination: ...

Save **Cancel**

5. Navigate to **OpenScape Common Management Platform > Configuration > Unify OpenScape Voice > Business Group > Translation > Destination Codes**.
6. Click **Add**.

7. In the **Add Destination Code** pop-up, configure the following:

- a. **Destination Code:** Select the previously created Prefix access code.
- b. From the **Nature of Address** drop-down menu, select **International**.
- c. From the **Destination Type** drop-down menu, select **Destination**.
- d. **Destination:** Select the destination of PSTN.

8. Click **Save**.

5.4 Configuring the SIP UA Forking

OSV Passive Forking (UAC) provides an interworking function that merges multiple Zoom downstream early dialogs into a single upstream SIP dialog. This functionality shields upstream SIP clients (SIP UAC) establishing sessions with the Zoom network from being exposed to the full RFC 3261/RFC3264 forking SIP Proxy server behavior of the Zoom Phone System. The SIP UA Forking tab enables the feature and lists all devices configured with their respective SIP forking capabilities.

To activate the OSV Passive Forking feature:

1. Navigate to **OpenScape Common Management Platform > Configuration > OSV > Administration > Signaling Management > SIP**.

2. In the **SIP UA Forking** tab, from the **OSV Passive Forking** drop-down menu, select **Enabled** and click **Save**.

[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

5.5 Configuring Display Number Modification

In case the FROM of an INVITE message needs to be manipulated from, for example, the SBC to the SSP, the header manipulation occurs in the OpenScape Voice **Display Number Modification** configuration.

Prerequisite

1. You have created an Office Code to OpenScape Voice. For example:

- Country Code: 1
- Area Code: 972
- Local Office Code: 598
- Directory Number Start:xxx (starting extension)

To configure the Display Number Modification, follow the instructions below:



Note:

The number modification configuration below is an example. The actual configuration steps are dependent on the requirements of your provider.

1. Navigate to **OpenScape Common Management Platform > Configuration > OSV > Business Group > Display Number Modification > Modifications.**
2. Click **Add.**

3. Add the office code by entering the following:

- **Endpoint:** EP_Zoom_SP1
- **Input Type Of Number:** International
- **Priority:** 1 (highest priority)
- **Output Type Of Number:** Extension
- **Number Source:**

Input Number (defines the input format of the "presenter number" when it comes into the OpenScape Voice.

[mgmttest42] - Display Number Modification - Google Chrome

Not secure https://10.14.254.6/management/portal/Applications/Operation/OSV/Busi...

[MgmtTest42]-Display Number Modification

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

Originating Context Setting

Select a business group and/or numbering plan from the list.

Business Group Zoom_BG ...

Numbering Plan NP_Zoom_BG ...

Terminating Context Setting

Select a numbering plan and/or endpoint from the list.

Business Group Zoom_BG

Numbering Plan NP_Zoom_BG ...

Endpoint EP_Zoom_SP1 ...

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: Extension ▾

Number Source: Input Number ▾

Presentation Restricted: ☐

Prefix Required: ☐

Optimize Type Of Number: None ▾

Save **Cancel**

4. Repeat the steps for the remaining Zoom endpoints.
5. Click **Save**.

Unify OpenScape SBC Configuration

6

This chapter contains the following sections:

- [Configuring Network settings](#)
- [Configuring SIP Server](#)
- [Configuring Certificates](#)
- [Configuring Media Profiles](#)
- [Configuring Remote Endpoints](#)

This chapter outlines the configuration of OpenScape SBC for interworking with Zoom Direct Routing. Once OSV is configured, you can use the SBC to route calls, secure communication, and manage traffic to Zoom Phone and PSTN networks.

Prerequisite

1. You have obtained a public certificate issued by one of the Zoom-supported CAs. Refer to the [Configuring Certifications](#) section.

The OpenScape Session Border Controller is a highly scalable SBC solution supporting broad SIP interoperability, advanced media handling and robust security. OpenScape SBC enables enterprises to deliver voice services like SIP trunking and unified communications. OpenScape SBC performs interoperability, security, management, and control capabilities to support SIP trunking applications. OpenScape SBC incorporates a B2BUA in the standalone mode with internal SIP stack and has limited SIP message manipulation and routing capabilities. In the other modes the ICPs i.e OpenScape Voice IP-PBX provides call routing and more sophisticated SIP message manipulation. Thus, the SIP signaling for incoming and outgoing calls to Zoom clients will always pass through the OS Voice.

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

As an example:

Table 1: Zoom IPs Table

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

Items	Example
OS Voice node 2 (SIP Signaling) IP	10.8.242.26 TCP 5060
Zoom IP 1 SIP trunk	162.12.233.59 (see the important note below) TLS 5061 (LAN port for OS Voice trunk 50001)
Zoom IP 2 SIP trunk	162.12.232.59 (see the important note below) TLS 5061 (LAN port for OS Voice trunk 50002)
Zoom IP 3 SIP trunk	162.12.235.59 (see the important note below) TLS 5061 (LAN port for OS Voice trunk 50003)
SSP (BCOM) SIP trunk	Remote URL: sip.bcom.nl Default Home DN: 31850080990 (LAN port for OS Voice trunk 50010)

**Important:**

The Zoom IP address example is valid for the North America region. Please check the [Zoom site](#) for the current IP Addresses.

Whether routine or not, Zoom Phone Direct Routing's specific OSSBC configuration will be omitted. Unify OpenScape SBC installation and administration documentation can be found on the [Unify customer documentation site](#).

Table 2: Signaling Traffic IPs

Traffic Type	Protocol	Source	Destination Ports	Destination IPs	Region
				162.12.233.59	North America
				162.12.232.59	
				162.12.235.85	

Traffic Type	Protocol	Source	Destination Ports	Destination IPs	Region
				64.211.144.247	LATAM
				149.137.69.247	
				213.19.144.198	EMEA
				213.244.140.198	
Signaling	TLS	Customer SBC	5061	103.122.166.248 103.122.167.248	Australia
				149.137.41.246	APAC
				207.226.132.198	
				209.9.211.198	HK
				101.36.167.237	HK2
				149.137.25.246	Japan
				207.226.132.198	

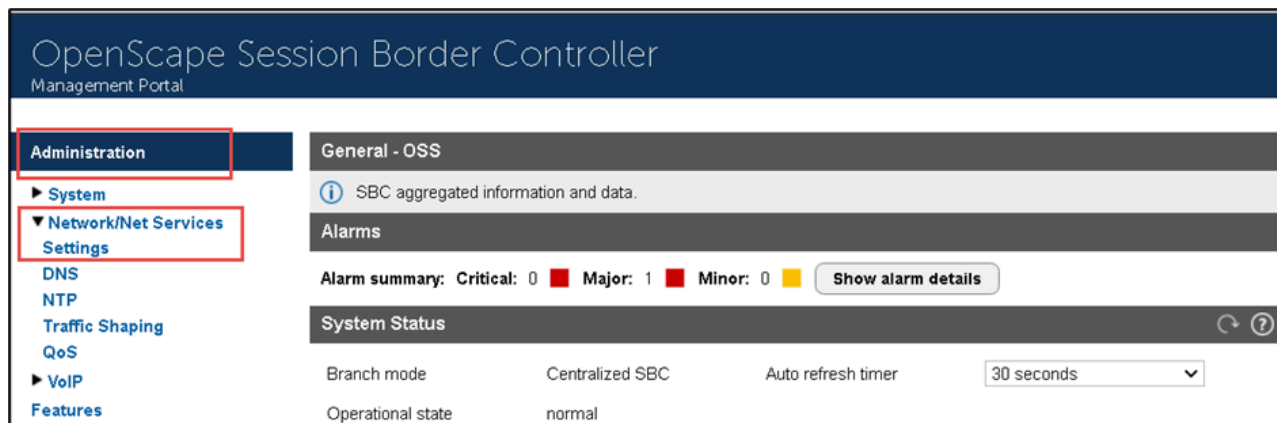
Table 3: Media Traffic IPs

Traffic Type	Protocol	Source	Destination Ports	Destination IPs	Region
				162.12.232.0/24	North America
				162.12.233.0/24	
				162.12.235.0/24	

Traffic Type	Protocol	Source	Destination Ports	Destination IPs	Region
				64.211.144.0/24	LATAM
				149.137.69.0/24	
				213.19.144.128/25	EMEA
				213.244.140.0/24	
Media	UDP/SRTP	Customer SBC	20000-64000	103.122.166.0/24 103.122.167.0/24	Australia
				149.137.41.0/24	APAC
				207.226.132.0/24	
				209.9.211.192/26	HK
				101.36.167.0/24	
				207.226.132.0/24	Japan
				149.137.25.0/24	

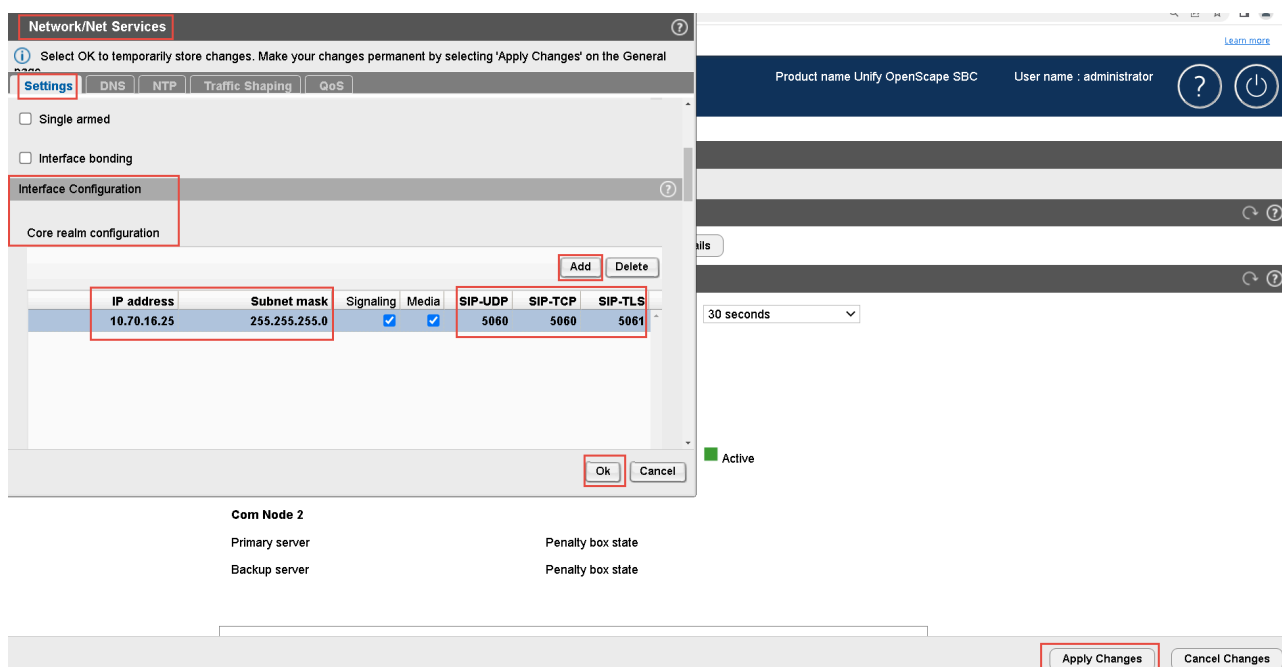
6.1 Configuring Network settings

1. Navigate to **Administration > Network/Net Services > Settings**.

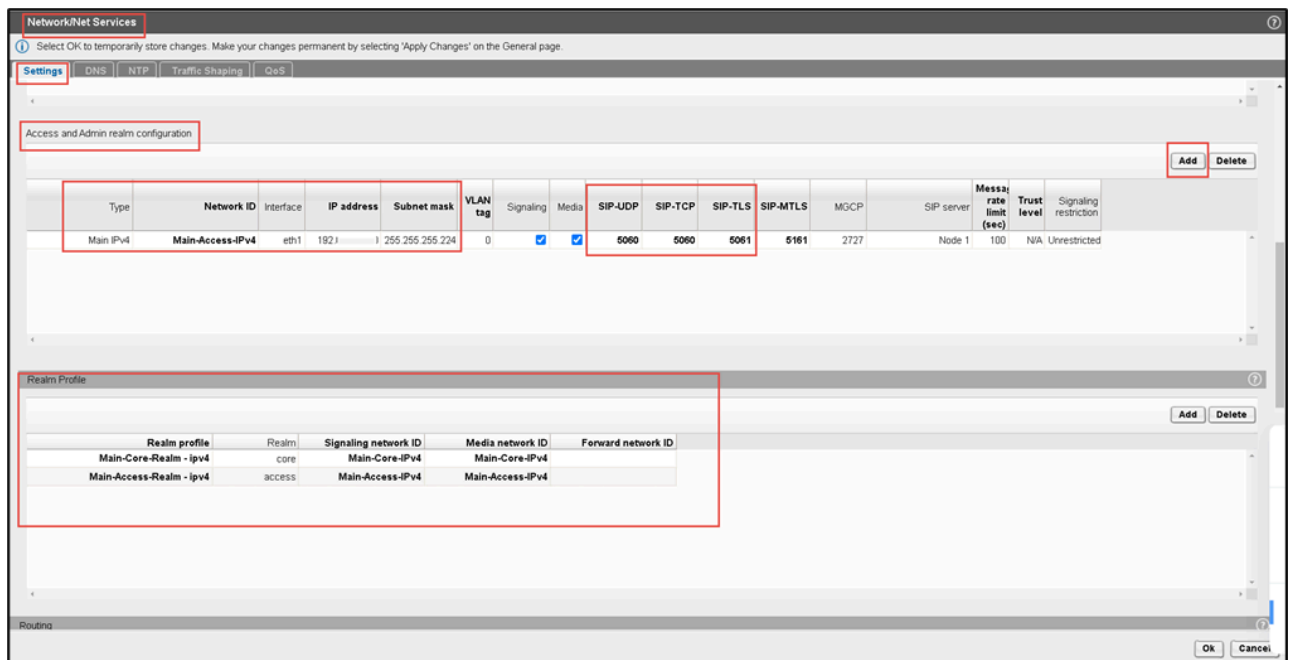


2. In the **Network/Net Services** window, under the **Settings** tab, locate the **Interface Configuration > Core Realm Configuration** area and click **Add**. Configure the following:

- a. **IP address**: Enter the SBC IP address.
- b. **Subnet mask**: Enter the subnet mask value.
- c. Select the appropriate interface for core Realm (for example, **eth0**).
- d. **SIP-UDP**: Configure port number as 5060.
- e. **SIP-TCP**: Configure port number as 5060.
- f. **SIP-TLS**: Configure port number as 5061.
- g. Click **Ok**, then click **Apply Changes** on the SBC Main page.



3. In the **Network/Net Services** window, under the **Settings** tab, locate the **Access and Admin realm configuration** area and click **Add**.
4. In the **Network/Net Services** pop-up, configure the following:
 - a. **Type:** Select Type as Main IPV4.
 - b. **Network-ID:** Configure network ID as Main-Access-IPv4.
 - c. Select the appropriate Interface for core Realm (for example, **eth1**).
 - d. **IP address:** Enter the SBC IP address associated with the public side of the network.
 - e. **Subnet mask:** Enter the subnet mask value.
 - f. **SIP-UDP:** Configure port number as 5060.
 - g. **SIP-TCP:** Configure port number as 5060.
 - h. **SIP-TLS:** Configure port number as 5061.
 - i. Map the **realm profile** for **core** and **access** interface as shown in the below screenshot.
 - j. Click **Ok**.
 - k. Click **Apply Changes** on the SBC Main page.

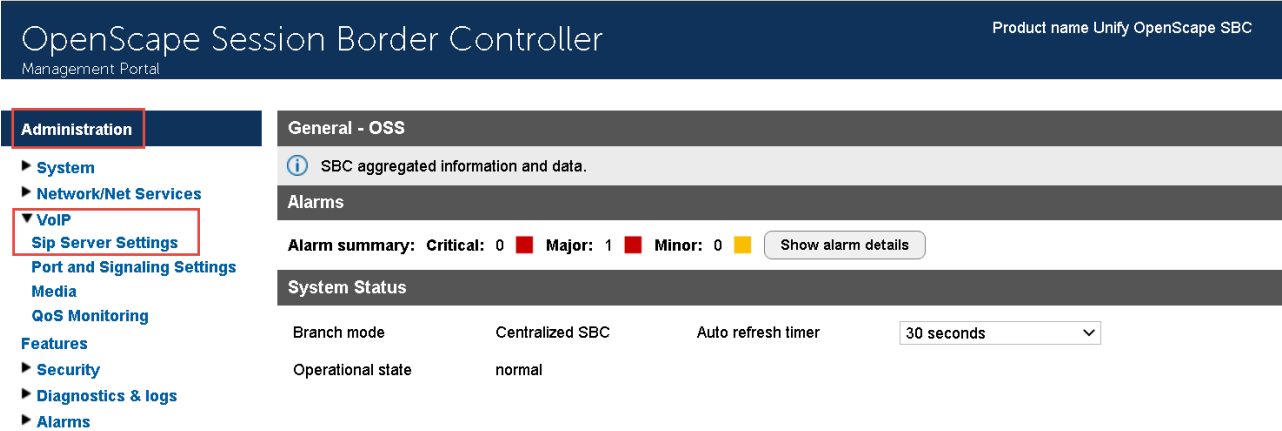


5. In the **Network/Net Services** pop-up, under the **Settings** tab, locate the **Routing** area to configure the default gateway address.
6. In the **Routing Configuration** section, click **Add** and add the static routes for core and access interface.
7. Click **Ok**.
8. Click **Apply Changes**.

6.2 Configuring SIP Server

The SIP connectivity to OpenScape Voice is configured in the **OSSBC Management Portal > VOIP** window.

1. Navigate to **Administration > VoIP > SIP Server Settings**.



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

- a. Under **General**, from the **Comm System Type** drop-down menu, select **Simplex**.

Note:

The **Simplex** option is available for OSV deployed as a Single Server . If your OpenScape Voice is deployed as a Dual-Node (Redundant), select one of the other options based on the OSV deployment: Collocated, Active-Standby, or Clustered.

b. Under the **Node 1** section:

- From the **Target type** drop-down menu, select **Binding**.
- **Primary Server:** Enter the OpenScape Voice **SIP Signaling IP address**.
- **Transport:** **TCP** (for both OS Voice Node 1 and Node 2)
- **Port:** **5060** (listening port for both **OS Voice Node 1** and **Node 2**).

3. Click **OK**.

4. Click **Apply Changes**.

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 /etc/hq8000 folder (parameters "sipsm1_vip" for **OS Voice Node1** and "sipsm2_vip" for **OS Voice**). Alternatively, the OS Voice SIPSM IP addresses can be found from CMP.

6.3 Configuring Certificates

Zoom Phone System allows only TLS connections for SIP traffic from SBCs with a certificate signed by one of the Zoom-supported Certification Authorities.

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

Important:

The list of trusted root authorities for Zoom services is maintained by Zoom and may change over time. Including static information from internal documents is not recommended due to potential changes without notice. Always rely on official Zoom documentation or support channels. For the most accurate and up-to-date information, users must contact Zoom Support directly.

To contact Zoom Support, visit the [Zoom Support Contact Page](#) or reach out to your Zoom account representative.

For the OpenScape SBC TLS interconnection to the Zoom Phone System, three files in 'pem' format are required from the Certification Authority:

- A certificate authority or certification authority (CA) certificate (for example, "ca_chain.pem"). The CA certificate contains a public key and the owner's identity, ensuring an entity can be trusted.
- Server certificate for OSSBC (for example, "certificate.pem").
- OSSBC server certificate private key used for the CSR to CA (for example, "privatekey.pem").

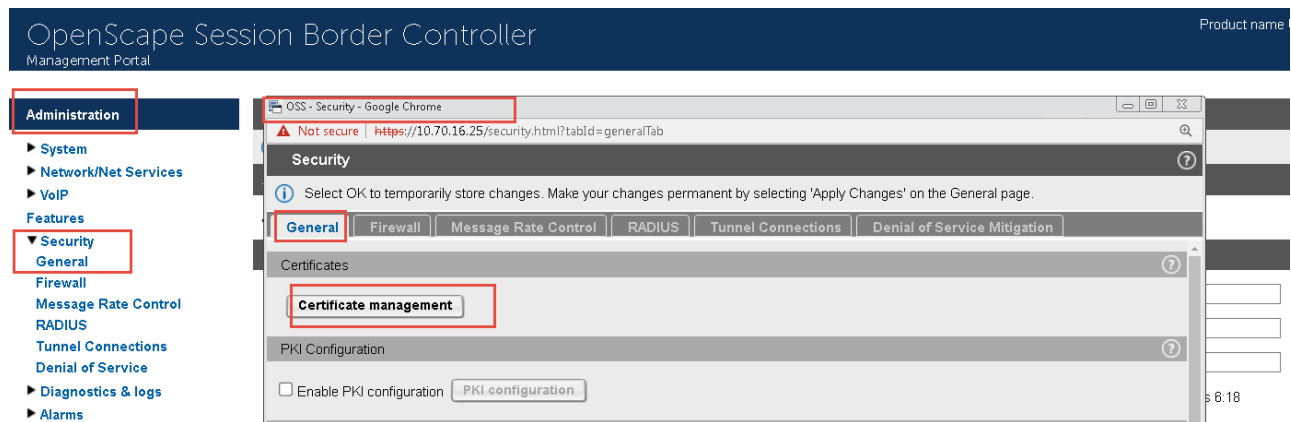
The files mentioned above must be uploaded to OpenScape SBC for the TLS connection with the Zoom Phone System interface.

Prerequisite

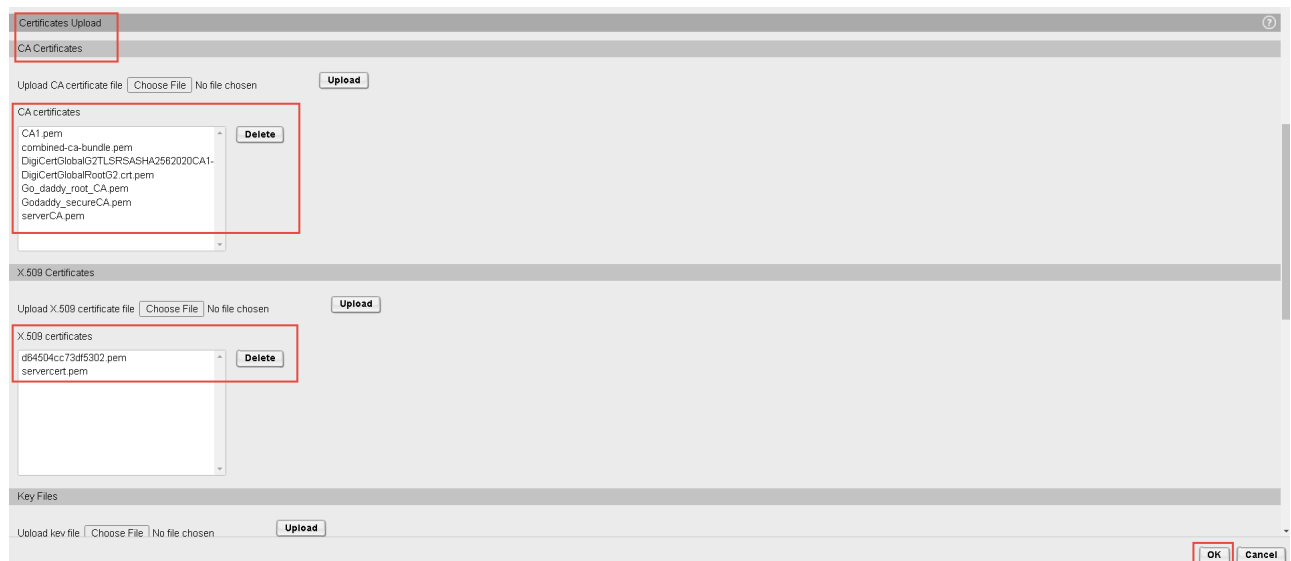
1. Adequate administrative permissions.
 2. Adequate knowledge of TLS certificate handling.
 3. At least one OpenScape SBC is configured and in operation.
 4. The connection to the OpenScape Voice system is up.
-
1. Navigate to OpenScape SBC **Management Portal** > **Security** > **General**.

2. In the **Security** pop-up, under the **Certificates** section, click **Certificate Management**.

The **Certificate Management** window appears with the **General Configuration** tab displayed as default.



3. Under the **CA Certificate** area, click **Choose File** and browse to select the **CA certificates**. Click **Upload**.
4. Under the **X.509 Certificate** area, click **Choose File** and browse to select the **X.509** certificates. Click **Upload**.



5. Under the **Key Files** section, click **Choose File** and browse to select the OSSBC server certificate private key. Click **Upload**.

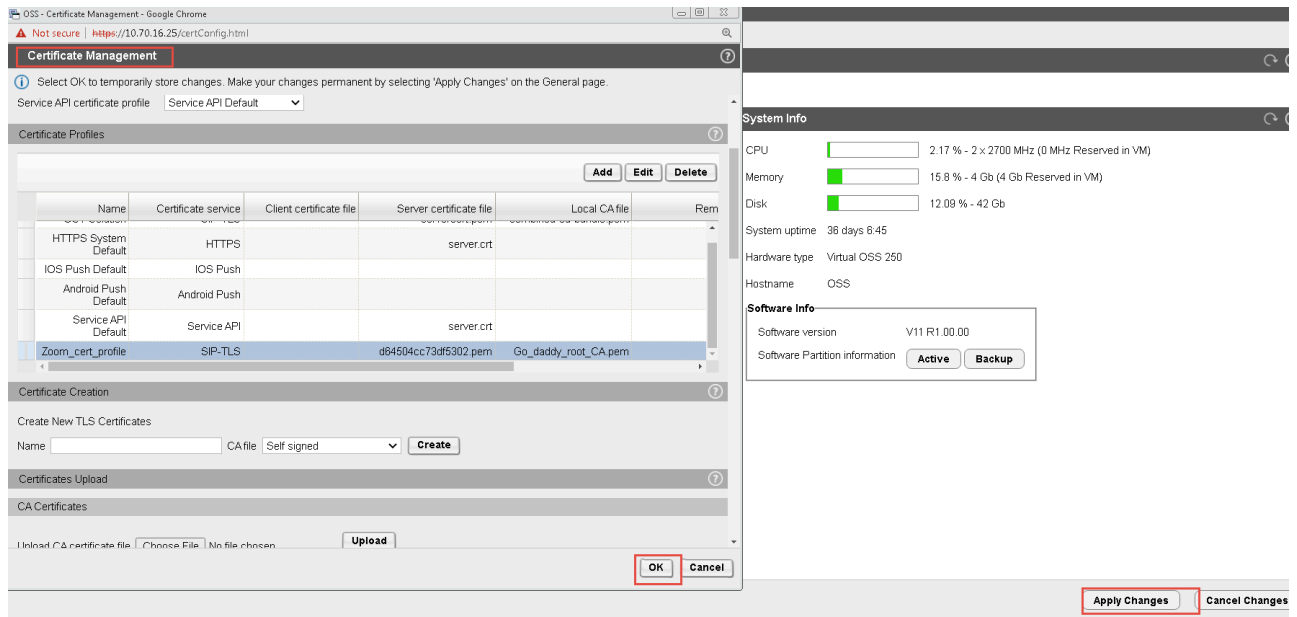
6. To create the Zoom certificate profile: In the **Certificate Management** pop-up, under the **Certificate profiles** area, click **Add**.

7. Configure the following parameters:

- a. **Certificate profile name:** Enter the name of the Zoom certificate profile.
- b. From the **Certificate Service** drop-down menu, select **SIP-TLS**.
- c. From the **Local server certificate file** drop-down menu, select the certificate to be used when establishing a TLS connection as a server.
- d. From the **Local CA file** drop-down menu, select the CA certificate.
- e. From the **Local key file** drop-down menu, select the key file that contains the private key.
- f. From the **TLS version** drop-down menu, select **TLS1.2**.

8. Click **OK**.
9. Click **OK** in the **Certificate Management** window and in the **Security** window.

10. Click **Apply Changes** on the OpenScape SBC main page.



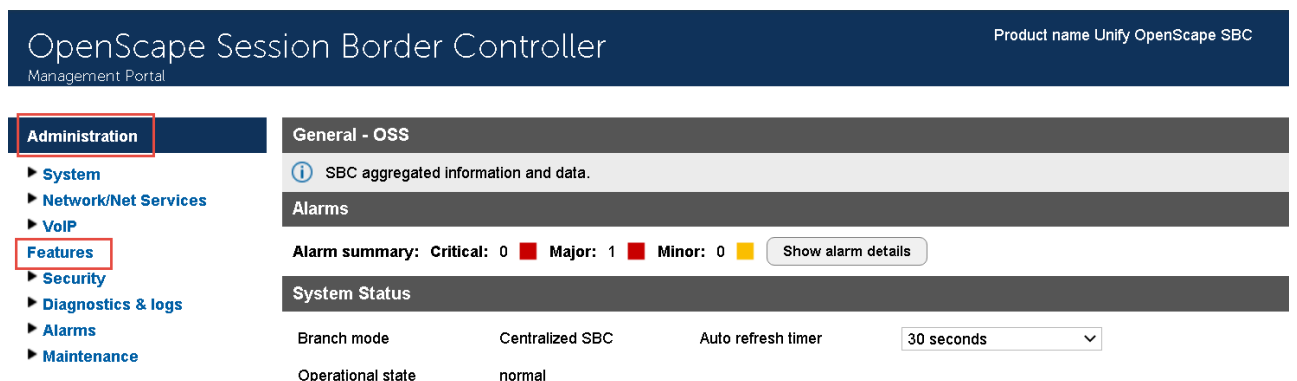
6.4 Configuring Media Profiles

In the **Media Profiles** settings, various SDP messages and audio (RTP) traffic parameters can be configured for the OpenScape SBC SIP endpoints to Zoom Phone System, SSP (PSTN provider), and Unify OpenScape Voice.

6.4.1 Configuring the Codec Manipulation Options

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

1. Navigate to the **OpenScape SBC Management Portal > Features** window.



2. Check 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 ⓘ

- ☐ Enable Remote Subscribers Configure
- ☐ Enable Remote Endpoints Configure
- ☒ Enable Codec Support for transcoding Configure
- ☐ Enable TURN Server Configure
- ☐ Enable Circuit Telephony Connector Configure
- ☐ Enable Sip Load Balancer Configure
- ☐ Enable Push Notification Service Configure
- ☐ Enable Ganglia Monitoring Daemon
- ☐ Enable Circuit Zookeeper Client
- ☐ Enable THIG
- ☐ Enable Standalone

OK Cancel

3. In the **Features** pop-up, check the **Enable Codec Support for transcoding** checkbox and click **Configure**.

Features ⓘ

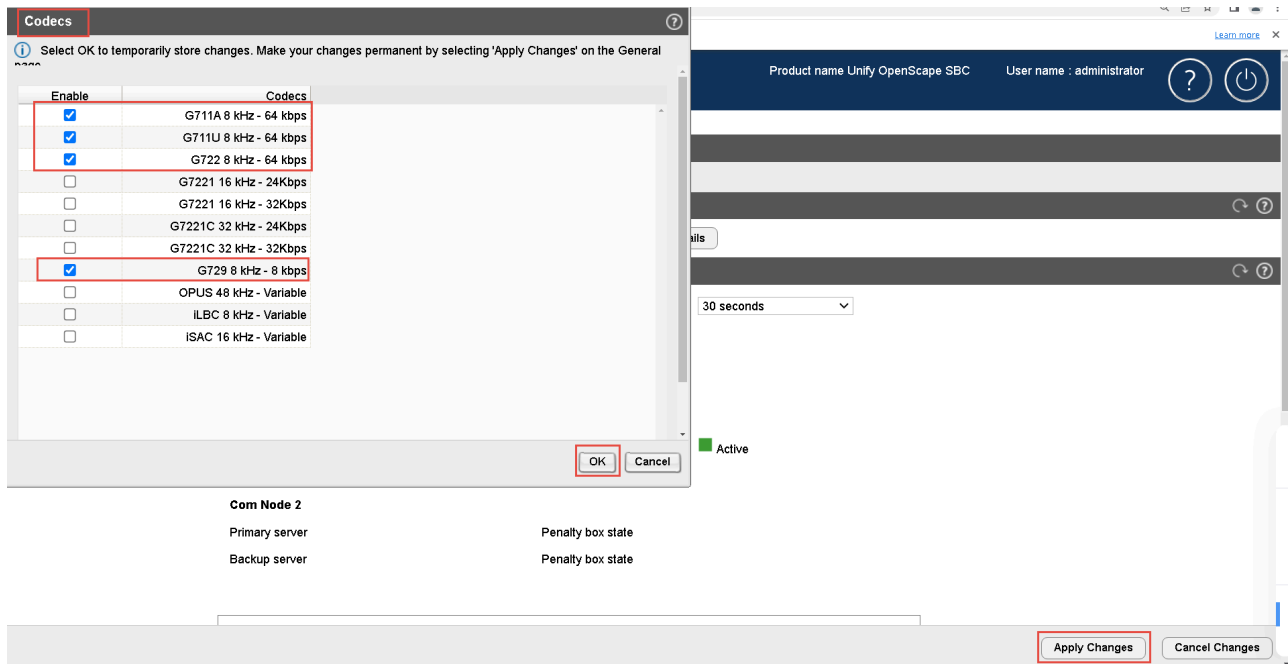
ⓘ Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Features configuration ⓘ

- ☐ Enable Remote Subscribers Configure
- ☐ Enable Remote Endpoints Configure
- ☒ Enable Codec Support for transcoding Configure
- ☐ Enable Sip Load Balancer Configure
- ☐ Enable Push Notification Service Configure
- ☐ Enable THIG
- ☐ Enable Standalone

4. In the **Codecs** window, you can enable the codecs to be available for the media profiles (for example, transcoding and prioritization). Select the following checkboxes:

- a. G711A 8 kHz - 64 kbps
- b. G711U 8 kHz - 64 kbps
- c. G722 8 kHz - 64 kbps
- d. G729 8 kHz - 64 kbps



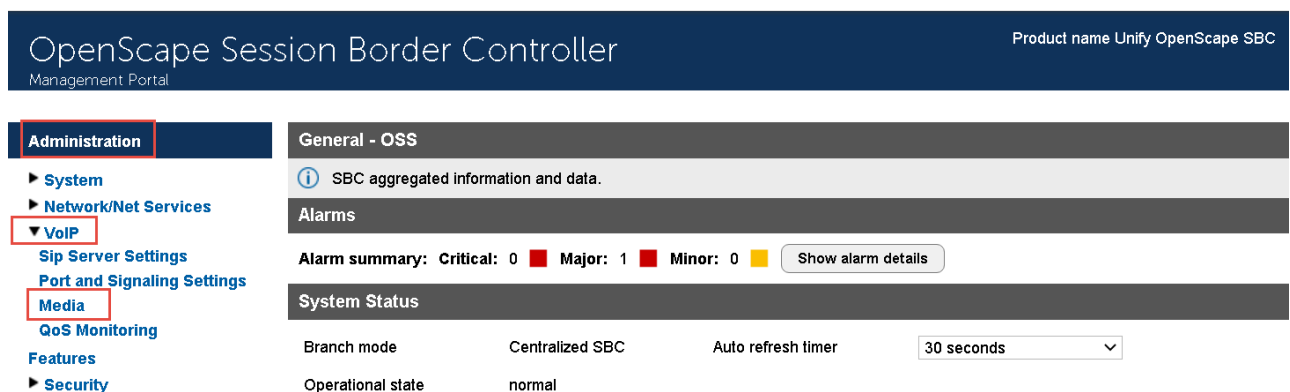
1. Click **OK**.
2. Click **Apply Changes**.

6.4.2 Configuring the Zoom Media Profile

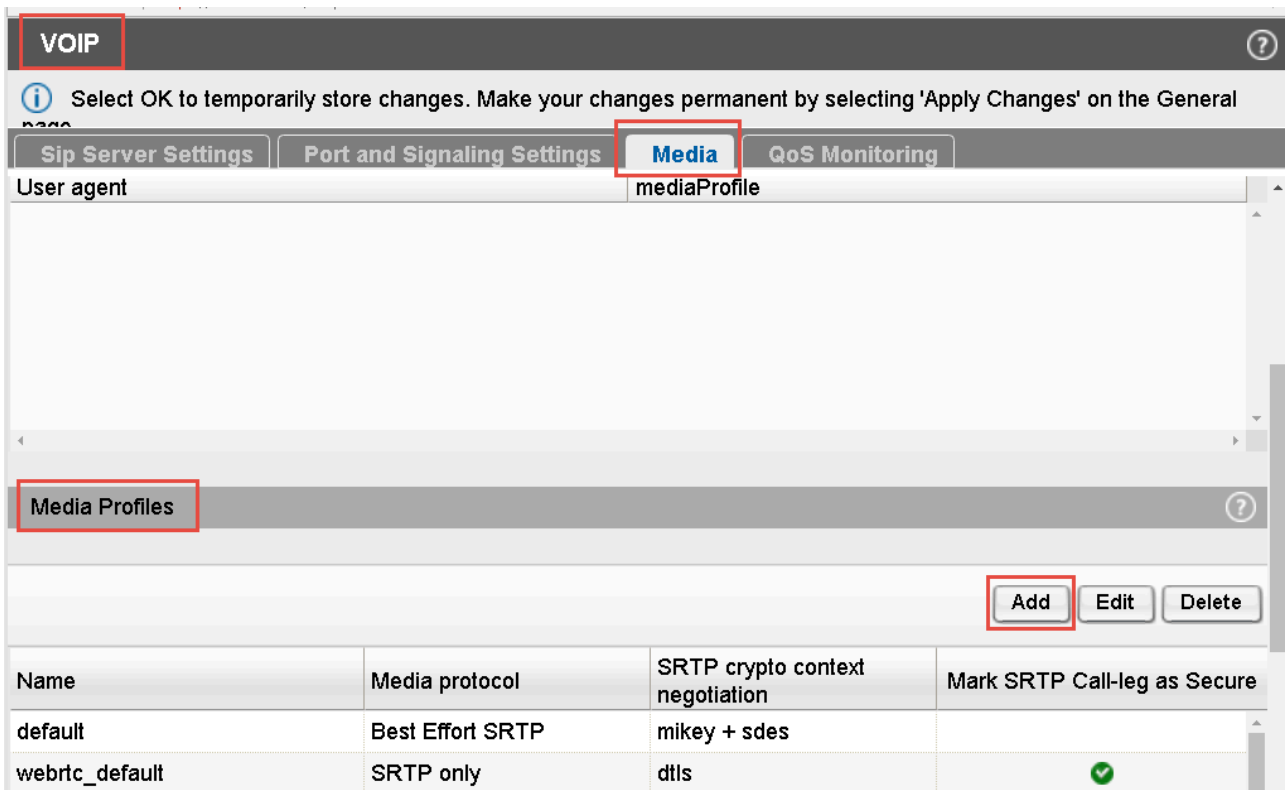
The communication between the OSSBC and the Zoom Phone System is secured with SRTP.

In the example presented in the current sub-section, the PSTN is supposed to not support G.711, and transcoding to G.711 is required for calls between PSTN subscribers and Zoom clients on OSSBC —Zoom Phone System SIP trunks.

1. **Navigate to OSSBC Management Portal > VOIP > Media.**



2. In the **VOIP** pop-up, go to the **Media** tab.



3. Locate the **Media Profiles** area and click **Add**.

The **Media Profile window** pops up.

4. Under the **General** area, create the media profile for OSSBC - Zoom connections by entering the following:

- **Name:** Type the media profile name. For example, Zoom_MP.
- From the **Media protocol** drop-down menu, select **SRTP only**.
- Check the **RTP/RTCP Multiplex in offer** checkbox.
- Under the **SRTP configuration** area, check the following checkboxes:
 - **SDES**
 - **MIKEY**
 - **Mark SRTP Call-leg as Secure**

The screenshot shows the 'Media Profile' configuration window. The 'General' tab is active, showing the 'Name' field set to 'Zoom_MP' and the 'Media protocol' dropdown set to 'SRTP only'. The 'RTP/RTCP Multiplex in offer' checkbox is checked. The 'SRTP configuration' tab is also visible, showing 'SRTP crypto context negotiation' with 'MIKEY' and 'SDES' selected, and 'Mark SRTP Call-leg as Secure' checked. Red boxes highlight the 'Name' field, 'Media protocol' dropdown, 'RTP/RTCP Multiplex in offer' checkbox, and the 'SRTP configuration' section.

Media Profile

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

General

Name Zoom_MP

Media protocol SRTP only ☐ Direct Media Support

☐ Support ICE Full

☐ Support NGTC Trickle ICE

☐ Enable NGTC WebRTC Compatibility

☐ 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

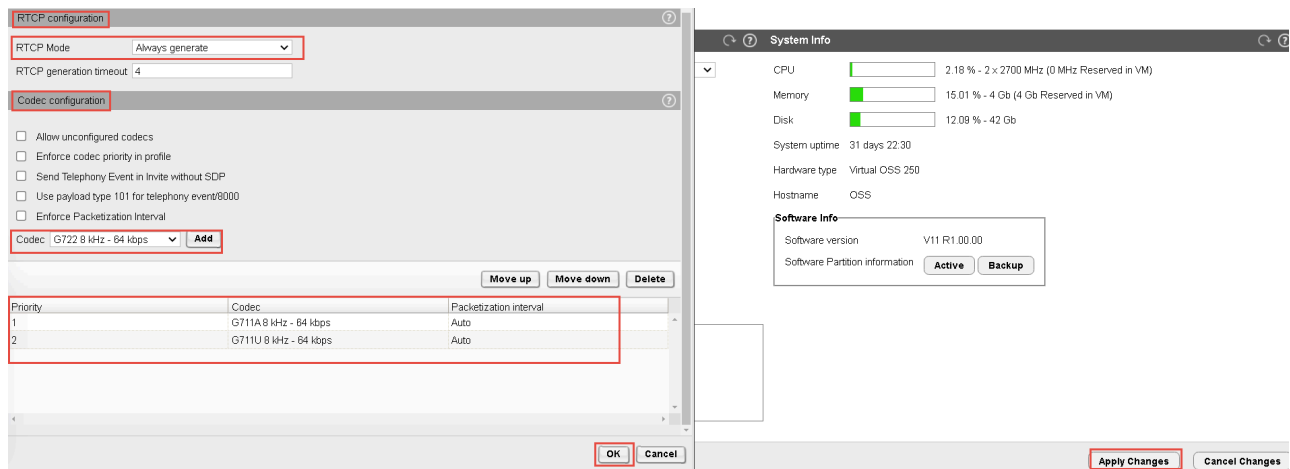
SRTP configuration

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

☒ Mark SRTP Call-leg as Secure

5. Under the **RTCP configuration** area, from the **RTCP Mode** drop-down menu, select **Generate Always**.

- Under the **Codec Configuration** area, select the required codecs and click **Add** to add them for transcoding (with priority). For example G711A, and G711U, as shown below:



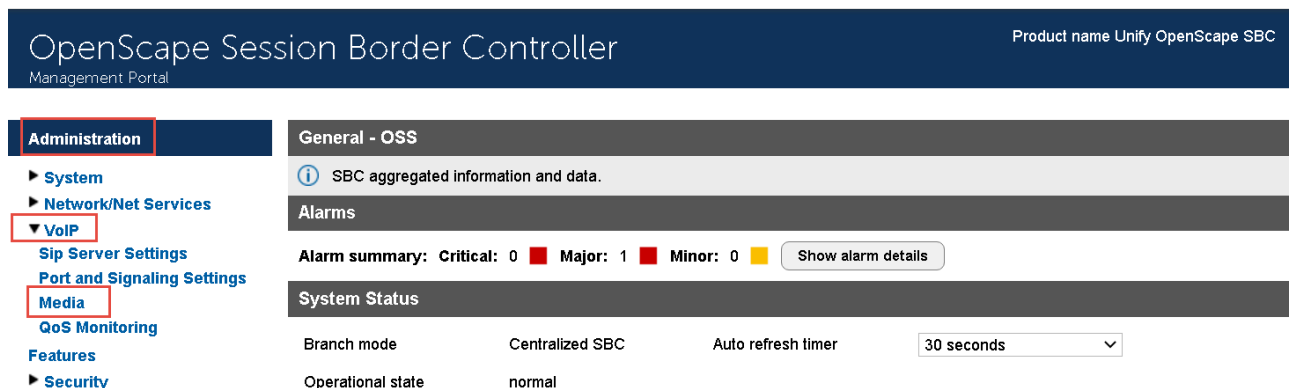
- Click **OK** to return to the **Media** window.
- Click **OK** on the **VoIP** window.
- Click **Apply Changes**.

6.4.3 Configuring the PSTN Media Profile

Note:
The configuration below is an example. The actual configuration steps depend on your provider's requirements.

In the current sub-section, as an example, it is supposed that for calls between Zoom clients and PSTN subscribers, certain codecs need to be prioritized on OSSBC – SSP (BCOM) SIP trunk.

- Navigate to the **Unify OpenScape SBC Management Portal > VOIP > Media** window.



- In the **VOIP** pop-up, go to the **Media** tab.

3. Locate the **Media Profiles** area and click **Add** to create the media profile for OSSBC to PSTN service provider trunk.

The screenshot shows the configuration interface for the Unify OpenScape SBC. At the top, the 'VOIP' tab is selected. Below it, a message states: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page'. The 'Media' tab is highlighted in the sub-menu. The 'User agent' field is set to 'mediaProfile'. Below this, the 'Media Profiles' section is visible, containing an 'Add' button, 'Edit', and 'Delete' buttons. A table lists the existing media profiles:

Name	Media protocol	SRTP crypto context negotiation	Mark SRTP Call-leg as Secure
default	Best Effort SRTP	mikey + sdes	
webrtc_default	SRTP only	dtls	

4. In the **Media profile** pop-up, locate the **General** section and configure the following:

- **Name:** Enter the name of the media profile.
- From the **Media protocol** drop-down menu, select **RTP only**.
- Check the **RTP/RTCP Multiplex in offer** checkbox.
- Under the RTCP configuration area, from the **RTCP Mode** drop-down menu, select **Bypass**.

Media Profile

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

General

Name PSTN_Media_profile

Media protocol RTP only ☐ Direct Media Support

☐ Support ICE Full

☐ Support NGTC Trickle ICE

☐ Enable NGTC WebRTC Compatibility

☐ 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 Bypass

RTCP generation timeout 4

5. In the **Codec configuration**, select the **Allow unconfigured codecs** option, then select the required codecs from the drop-down menu. Click **Add** to add them.

6. Click **OK**.

7. Click **Apply Changes** on the SBC main page.

Codec configuration

☒ Allow unconfigured codecs

☐ Enforce codec priority in profile

☐ Send Telephony Event in Invite without SDP

☐ Use payload type 101 for telephony event/9000

☐ 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**

Apply Changes **Cancel Changes**

System Info

Memory 10.10 TB - 4 GB (4 GB reserved for VM)

Disk 12.08 % - 42 GB

System uptime 31 days 22:48

Hardware type Virtual OSS 250

Hostname OSS

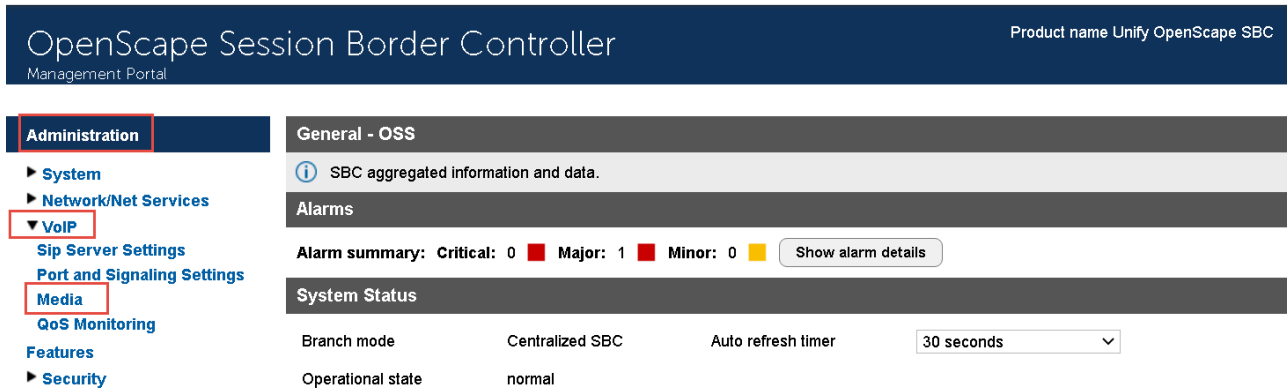
Software Info

Software version V11 R1.00.00

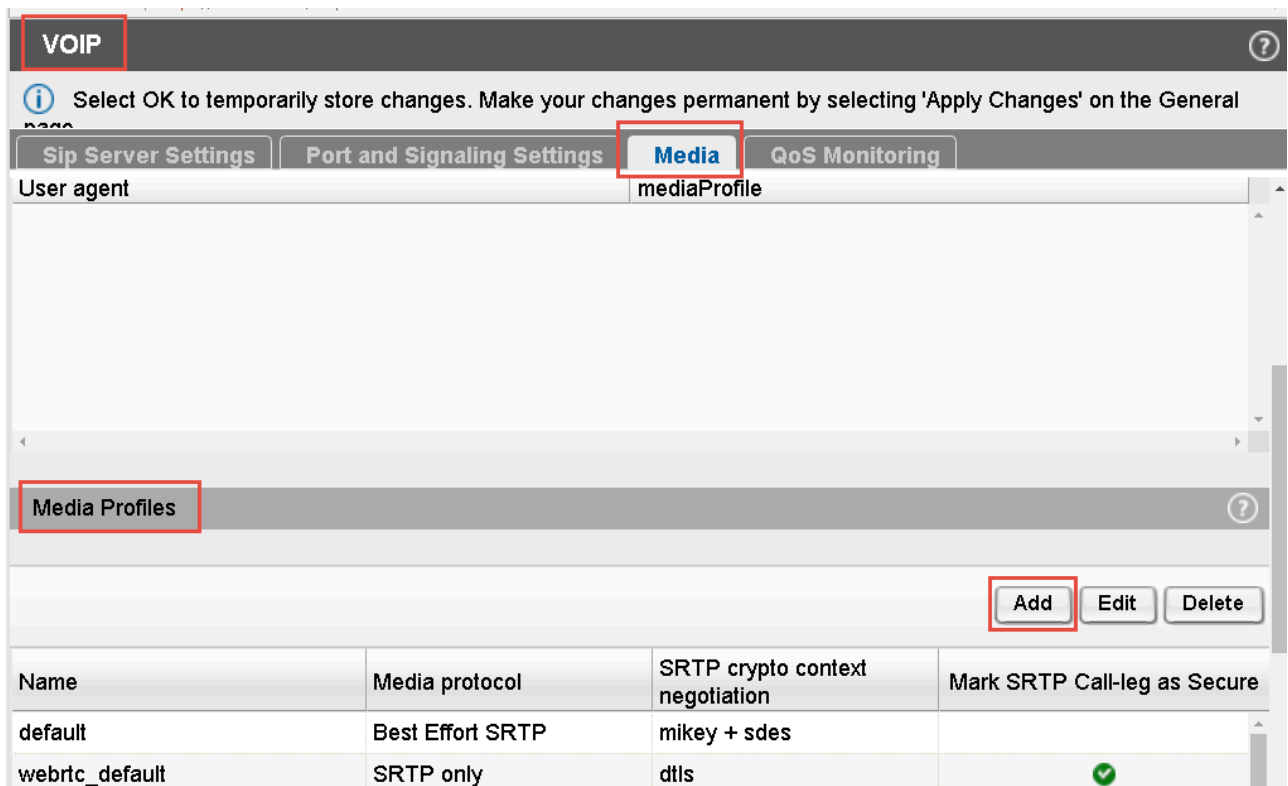
Software Partition information **Active** **Backup**

6.4.4 Configuring the Unify OpenScape Voice Media Profile

1. Navigate to the **OSSBC Management Portal > VOIP > Media** window.

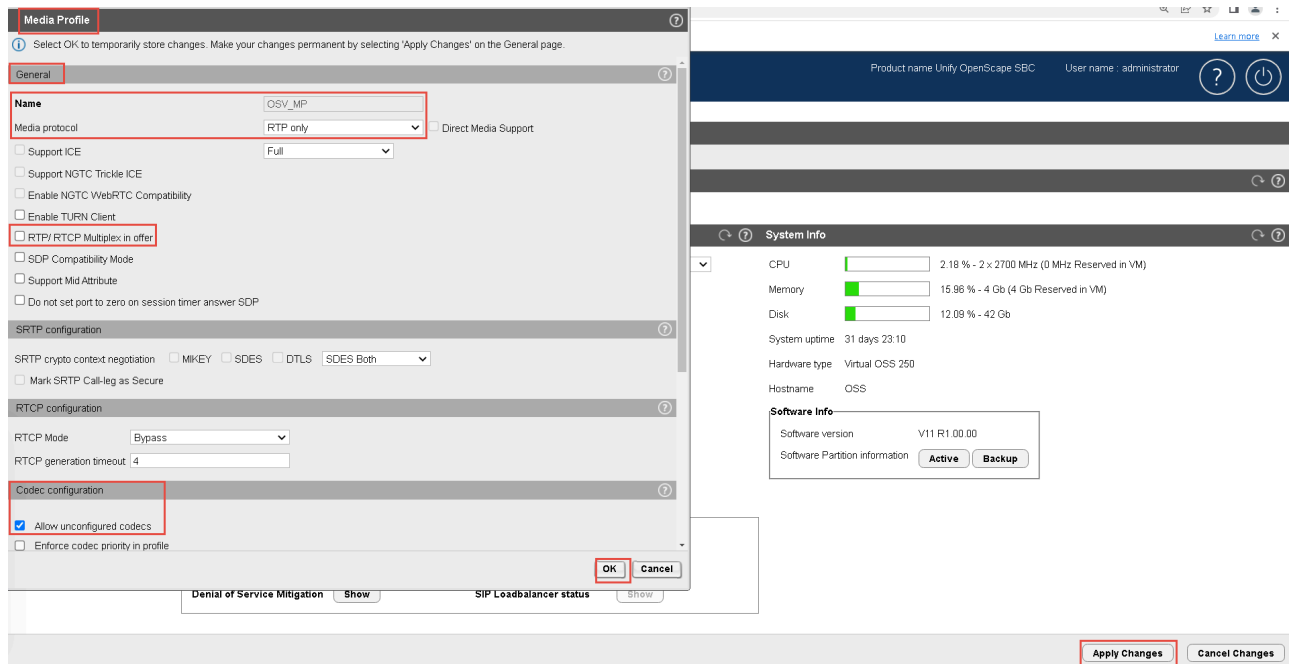


2. In the **VOIP** pop-up, go to the **Media** tab.
3. In the **Media Profiles** area, click **Add** to create the media profile for OSSBC – OS Voice connection.



4. In the **Media profile** pop-up, locate the **General** section and configure the following:
 - **Name:** Enter the name of the media profile.
 - From the **Media protocol** drop-down menu, select **RTP only**.
 - Check the **RTP/RTCP Multiplex in offer** checkbox.

5. In the **Codec Configuration**, select the **Allow unconfigured codecs** option, then select the required codecs from the drop-down menu. Click **Add** to add them.

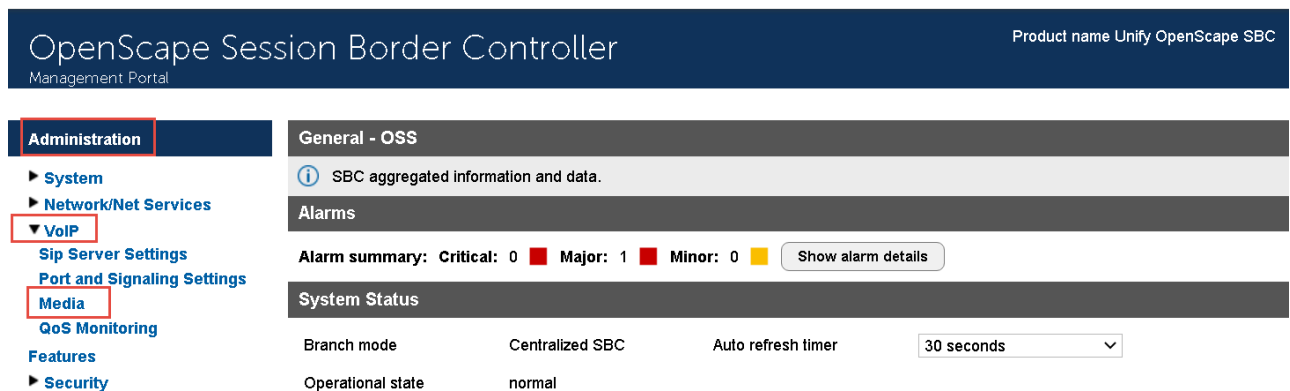


6. Click **OK**.
7. Click **Apply Changes** on the SBC main page.

6.4.5 General Media Settings

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

1. Navigate to the **OSSBC Management Portal > VOIP > Media** window.



2. In the **VOIP** pop-up, go to the **Media** tab.
3. Locate the **Core Side Media Configuration** area and select the previously created OpenScape Voice media profile from the **Media Profile** drop-down menu, used for the OSSBC – OS Voice SIP trunk.

4. Check the **Support OpenScape Cloud** checkbox to enable this option.

The screenshot displays the 'Media' configuration tab in the Unify OpenScape SBC interface. The 'Core Side Media Configuration' section shows the 'Media profile' set to 'OSV_MP'. Below this, there is a table of 'Media Profiles' with columns for Name, Codecs, Media protocol, SRTP crypto context negotiation, and Mark-SRTP Call-leg as Secure. The 'Cloud Support' section at the bottom has the 'Support OpenScape Cloud' checkbox checked. The 'System Info' panel on the right shows system details like CPU, Memory, Disk, and Software version (V11 R1.00.00).

Name	Codecs	Media protocol	SRTP crypto context negotiation	Mark-SRTP Call-leg as Secure
WE_Phone_default		Best Effort SRTP	mikey + sdes	
VodafoneMP	G711A,G729	RTP only	none	
AmazonChimeVC_MP	G711U,G711A	RTP only	none	
Unify_OSV_PBX_Media_Profile	G711U,G711A,G729	RTP only	none	
PSTN_Media_profile	G711A,G711U,G722,C	RTP only	none	

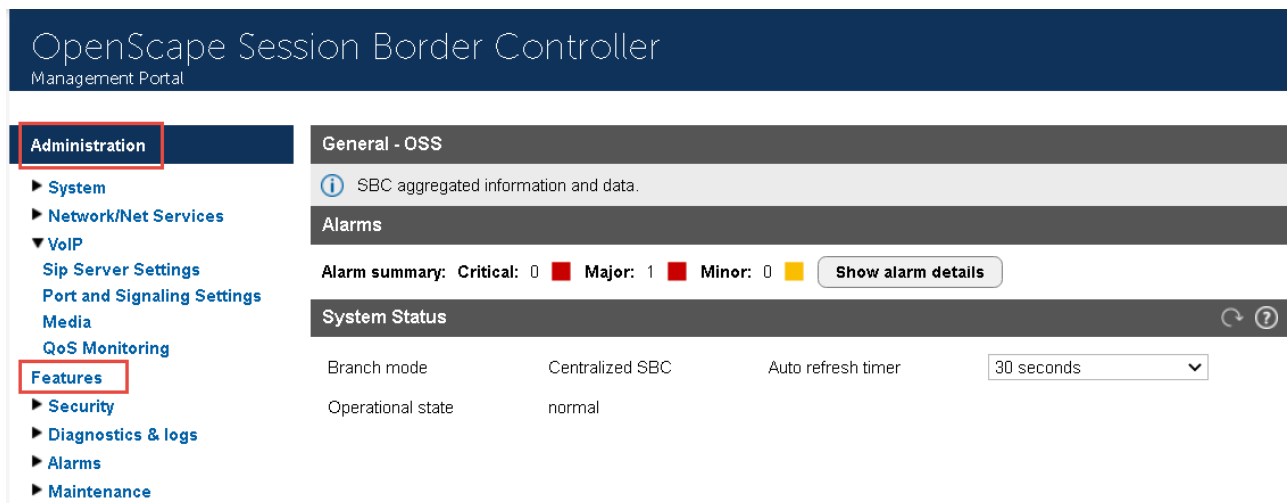
5. Click **OK** and then click **Apply Changes** on the SBC main page.
 6. Click **OK**.
 7. Click **Apply Changes**.

6.5 Configuring Remote Endpoints

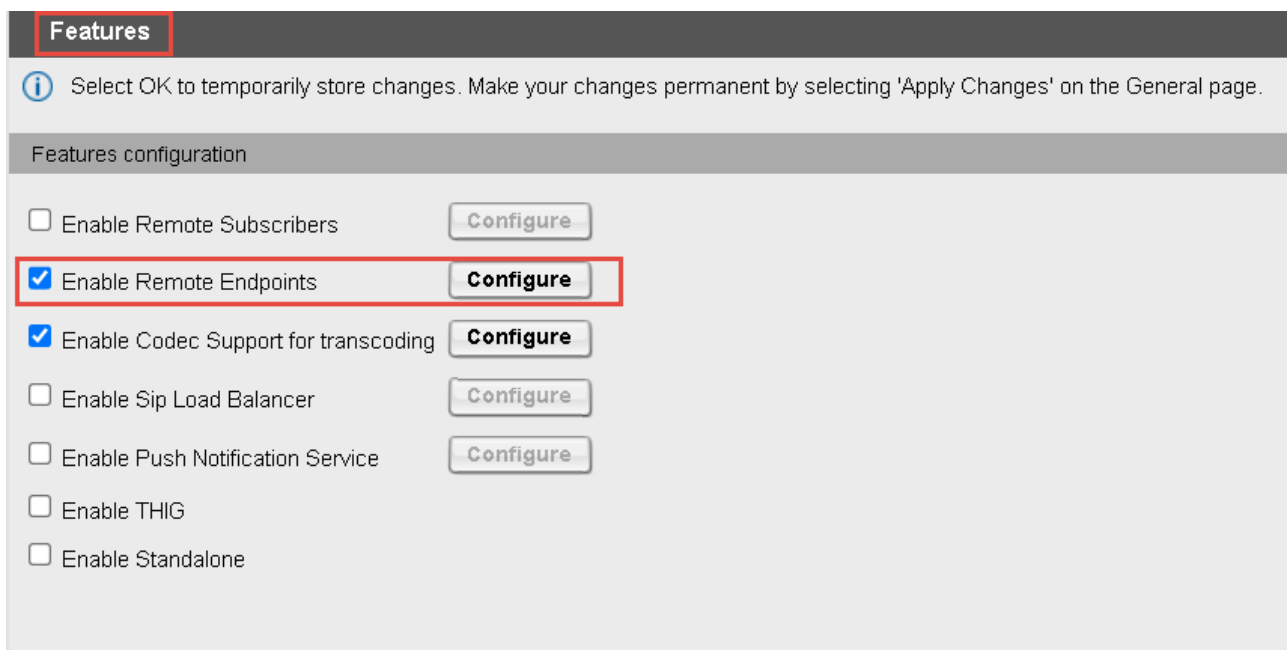
In the **Remote Endpoint** configuration, you can set up the OpenScape SBC with Zoom Phone System and the PSTN (BCOM SSP) SIP trunks.

6.5.1 Configuring the Zoom Remote Endpoints

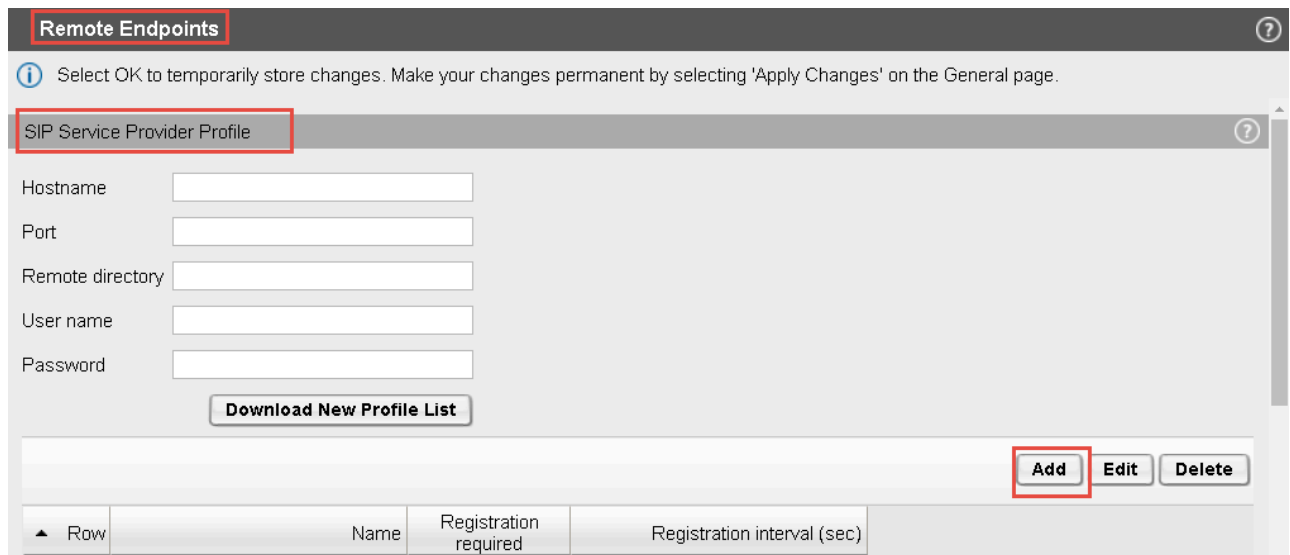
1. Navigate to the **Administration > Features** window.



2. In the **Features** pop-up, check the **Enable Remote Endpoints** checkbox and click **Configure**.



3. In the **Remote Endpoints** pop-up, locate the **SIP Service Provider Profile** area and click **Add** to add the endpoint profile for the OSSBC – Zoom Phone System endpoint.



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

Port

Remote directory

User name

Password

[Download New Profile List](#)

[Add](#) [Edit](#) [Delete](#)

▲ Row	Name	Registration required	Registration interval (sec)
-------	------	-----------------------	-----------------------------

4. In the **SIP Service Provider** pop-up, configure the following:

- a. **Name:** Enter the name of the SIP Service Provider profile. For example, **Zoom**.
- b. From the **Default SSP Profile** drop-down menu, select **Unify Office**.
- c. **SIP service address:** Enter the SBC's public FQDN and click **OK** to return to the **Remote endpoints** window.

SIP Service Provider Profile

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

General

Name Zoom

Default SSP profile Unify Office

☐ Allow sending of insecure Referred-By header

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

☐ Do not send Diversion header

☐ Send URI in telephone-subscriber format

☐ Send authentication number in Diversion header

☐ Send authentication number in P-Asserted-Identity header

☐ Send authentication number in From header

☐ Include restricted numbers in From header

SIP Privacy

Privacy support Full

SIP Service Address

☒ Use SIP Service Address for identity headers

SIP service address sbc3.tekvizionlabs.com

☐ Use SIP Service Address in Request-URI header

☐ Use SIP Service Address in To header

☒ Use SIP Service Address in Diversion header

☒ Use SIP Service Address in Via header

☒ Use SIP Service Address in From header

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

☒ Use SIP Service Address in Contact header

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

SIP User Agent

OK **Cancel**

5. In the **Remote Endpoints** window, locate the **Remote endpoint configuration** area and click **Add**.

Remote Endpoints

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

User name

Password

Download New Profile List

AddEditDelete

Row	Name	Registration required	Registration interval (sec)
1	PSTN1	<input type="checkbox"/>	3600
2	UnigySSP	<input type="checkbox"/>	60
3	UnifySPP	<input type="checkbox"/>	3600
4	Zoom	<input type="checkbox"/>	3600

Remote endpoint configuration

AddEditDeleteExport Logical IDs

6. In the **Remote endpoint configuration** pop-up, configure the following:

- a. **Name:** Enter the name of the remote endpoint. For example, ZoomSP1.
- b. From the **Type** drop-down menu, select **SSP**.
- c. From the **Profile** drop-down menu, select **Zoom**.
- d. From the **Signaling address type** drop-down menu, select **IP address or FQDN**.

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 ZoomSP1 **Edit**

Type SSP

Profile Zoom

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 IP address or FQDN

7. Locate the **Remote Location domain** area and click **Add** to add the IP address.

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

- a. **Remote URL:** Enter the Zoom IP address (see the Zoom IPs Table under Chapter 3 [Unify OpenScape SBC Configuration](#) on page 71).
- b. **Remote port:** Enter the port number (**5061**).
- c. Locate the **TLS** area, and from the **TLS mode** drop-down menu, select **Server authentication**.
(or Mutual authentication in case MTLS is required)
- d. From the **Remote transport** drop-down menu, select TLS.
- e. From the **Certificate profile** drop-down menu, select **Zoom_Cert_Profile**.
- f. Locate the **Media Configuration** area, and select the **Zoom** media profile from the **Media profile** drop-down menu.

Remote Location Domain

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

General

Remote URL: 162.12.233.59 ☐ Shared domain

Remote port: 5061

Remote transport: TLS

Signaling

INVITE No Answer timeout (msec): 360000

INVITE No Reply timeout (msec): 3000

TLS

TLS mode: Server authentication

Certificate profile: Zoom_cert_profile

☐ TLS keep-alive

Keep-alive interval (seconds): 120

Keep-Alive timeout (sec): 10

Media Configuration

Media profile: Zoom_MP

OK Cancel

9. Click **OK**.

10. In the **Remote endpoint configuration** window, locate the **Remote Location Identification Routing** area.

11. In the **Core realm port** field, enter the core realm value as **50001**.

!

Important:

The value for each Endpoint of Zoom should be unique. Add **50002** for the second Zoom endpoint, **50003** for the third, and so on.

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

Default home DN

☐ 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

OK

Cancel

Product name Unify OpenScape SBC

User name : administrator

System Info

CPU

Memory

Disk

System uptime

Hardware type

Hostname

Software Info

Software version

Software Partition information

Active

Backup

Apply Changes

Cancel Changes

12. Repeat the configurations in the **Remote endpoint configuration** window for the remaining Zoom IPs.
13. Click **OK**.
14. Click **Apply changes**.

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.

2	UnigySSP	<input type="checkbox"/>	80
3	UnifySPP	<input type="checkbox"/>	3600
4	Zoom	<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	Associated Endpoint	Link
2	ZoomSP1	Main-Access-Realm - ipv4	SSP	Zoom	162.12.233.59	5061	TLS		
3	ZoomSP2	Main-Access-Realm - ipv4	SSP	Zoom	162.12.232.59	5061	TLS		
4	ZoomSP3	Main-Access-Realm - ipv4	SSP	Zoom	162.12.235.85	5061	TLS		

**Note:**

See the Tables in [Unify OpenScape SBC Configuration](#) on page 71

**Note:**

Please refer to the Signaling Traffic table under the Premises Peering Firewall Requirements for Media and Signaling section in the **Zoom Phone Bring Your Own Carrier- Premises (BYOC-P) Solution Reference Guide**.

6.5.2 Configuring the PSTN Remote Endpoint

**Note:**

The configuration below is an example. The actual configuration steps depend on your provider's requirements.

1. Navigate to the **Administration > Features** window.

The screenshot displays the OpenScape Session Border Controller Management Portal. The left sidebar shows the navigation menu with 'Administration' and 'Features' highlighted. The main content area shows the 'General - OSS' section, which includes an 'Alarms' summary and a 'System Status' table.

General - OSS			
SBC aggregated information and data.			
Alarms			
Alarm summary: Critical: 0 Major: 1 Minor: 0 Show alarm details			
System Status			
Branch mode	Centralized SBC	Auto refresh timer	30 seconds
Operational state	normal		

2. In the **Features** pop-up, check the **Enable Remote Endpoints** checkbox and click **Configure**.

Features

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

Features configuration

☐ Enable Remote Subscribers Configure

☒ **Enable Remote Endpoints** **Configure**

☒ Enable Codec Support for transcoding Configure

☐ Enable Sip Load Balancer Configure

☐ Enable Push Notification Service Configure

☐ Enable THIG

☐ Enable Standalone

3. In the **Remote Endpoints** window, click **Add** in the **SIP Service Provider Profile** area to add the endpoint profile for the OSSBC – SSP (BCOM) endpoint.

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

Port

Remote directory

User name

Password

Download New Profile List

Add Edit Delete

Row	Name	Registration required	Registration interval (sec)

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

- **Name:** Enter the name of the profile. For example, **PSTN1**.
- Click **OK** to return to the **Remote endpoints** window.

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**

☐ Allow sending of insecure Referred-By header ☐ Send authentication number in Diversion header

☐ Send P-Preferred-Identity rather than P-Asserted-Identity ☐ Send authentication number in P-Asserted-Identity header

☐ Do not send Diversion header ☐ Send authentication number in From header

☐ Send URI in telephone-subscriber format ☐ Include restricted numbers in From header

SIP Privacy

Privacy support

SIP Service Address

☐ 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

OK **Cancel**

5. Locate the Remote endpoint configuration area and click Add.

Remote Endpoints

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

Port

Remote directory

User name

Password

Download New Profile List

Add **Edit** **Delete**

▲ Row	Name	Registration required	Registration interval (sec)
1	PSTN1	<input type="checkbox"/>	3600
2	UnigySSP	<input type="checkbox"/>	60
3	UnifySPP	<input type="checkbox"/>	3600
4	Zoom	<input type="checkbox"/>	3600

Remote endpoint configuration

Add **Edit** **Delete** **Export Logical IDs**

6. In the **Remote Endpoint configuration** window, configure the following parameters:

- **Name:** Enter the name of the remote endpoint. For example, PSTN.
- From the **Type** drop-down menu, select **SSP**.
- From the **Profile** drop-down menu, select the PSTN SIP service provider profile. For example, PSTN1.
- From the **Signaling address type** drop-down menu, select **IP address or FQDN**.

Remote endpoint configuration

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

Remote Endpoint Settings

Name
Type
Profile

Edit

Access realm profile
Core realm profile
Associated Endpoint
☐ Enable Call Limits
Maximum Permitted Calls
Reserved Calls

Remote Location Information

☐ Support Peer Domains
☐ Support Foreign Peer Domains
☐ Enable access control

Signaling address type

7. Locate the **Remote Location domain** area and click **Add** to add the Zoom IP address.

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

- a. **Remote URL:** Enter the PSTN IP address
- b. **Remote port:** Enter the port number provided by the PSTN provider (for example, **5061**)
- c. From the **Remote transport** drop-down menu, select the transport protocol provided by the PSTN provider. For example **TCP**.
- d. Locate the **Media Configuration** area, and from the **Media profile** drop-down menu, select the **PSTN** media profile.
- e. Click **OK**.

Remote Location Domain

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

General

Remote URL: 10.64.1.72 ☐ Shared domain

Remote port: 5060

Remote transport: TCP

Signaling

INVITE No Answer timeout (msec): 360000

INVITE No Reply timeout (msec): 3000

TLS

TLS mode: Server authentication

Certificate profile: OSV Solution

☐ TLS keep-alive

Keep-alive interval (seconds): 120

Keep-Alive timeout (sec): 10

Media Configuration

Media profile: PSTN_Media_profile

OK Cancel

9. In the **Remote endpoint configuration** window, locate the **Remote Location Identification Routing** area.

10. In the **Core realm port** field, enter the core realm value as **50015**.

The screenshot displays the 'Remote endpoint configuration' window. The 'Remote Location Identification/Routing' tab is active. The 'Core realm port' field is highlighted with a red box and contains the value '50015'. Other fields include 'Core FQDN', 'Default core realm location domain name', 'Default home DN', 'Enable routing based on domain' (unchecked), 'FQDN', and 'Incoming Routing prefix'. The 'Digest Authentication' tab is also visible. The 'OK' button is highlighted with a red box. In the background, the 'System info' window shows system details like CPU, Memory, Disk, System uptime, Hardware type, Hostname, and Software version. The 'Apply Changes' button is highlighted with a red box at the bottom right of the main window.

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

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

13. Click **Apply Changes**.

