A MITEL
PRODUCT
GUIDE

OpenScape Solution Set V11

Zoom Phone System with Mitel OpenScape 4000 and Mitel OpenScape SBC (Bring Your Own Carrier, Bring Your Own PBX)

Solution Guide

07/2025

A31003-S1100-M129-02-76A9

Mitel

Notices

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

Trademarks

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

Contents

1 History of Changes

Issue	Date	Summary
1	03/2025	The first issue of the guide.
2	07/2025	Updates throughout the document.

2 Introduction

This document outlines the process of connecting the **OpenScape 4000** (OS4K) to **Zoom Phone** using Bring Your Own Carrier (BYOC)[1] and Bring Your Own PBX (BYOP)[2] configurations.

This integration provides a unified hybrid model that enables users to optimize the benefits of Zoom's cloud platform while maintaining connectivity with their on-premises telecom system (OS4K) for telephony features. It is ideal for organizations that are currently using Zoom as a main collaboration tool and want to continue using their OS4K system for call management and PSTN connectivity.

How it works:

The integration allows Zoom Phone to connect to the OS4K system through a Generic SIP Trunk.

OpenScape SBC and OpenScape 4000 manage the communication between Zoom Phone and external networks, including the PSTN (Public Switched Telephone Network).

OpenScape 4000 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.

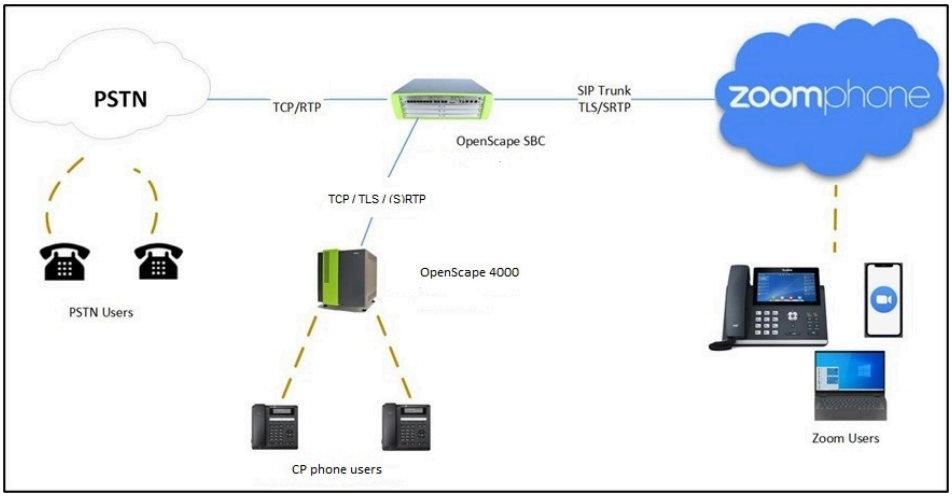
This solution provides secure traffic management, allowing users to retain their OS4K system while benefiting from Zoom's cloud features. Once OS4K is configured, they can use the SBC to route calls, secure communication, and manage traffic between Zoom Phone and PSTN networks.

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 8 chapter.

Product	Software Version
OpenScape 4000	V11R0.22
OpenScape SBC	V11 R2.1.0

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.



2.1 Prerequisites

Supported product versions

Product	**SW Version** (minimum)
Zoom Workplace app	6.3.0
OpenScape 4000	V11R0.22
OpenScape SBC	V11R2.0.0

2.2 Additional Support Information

In the current Mitel product software implementation:

- OpenScape SBC with 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 OSEE environment with SBC-THIG and Zoom is currently not supported.

2.3 Related Documentation

Zoom

- For additional information on the Zoom configuration, refer to the official Zoom Support page.

OpenScape 4000

- OpenScape 4000 V11, Installation Guide
- OpenScape 4000 V11, Ip Solutions, Service Documentation

OpenScape SBC

- OpenScape SBC V11 Administration Guide
- OpenScape SBC V11 Configuration Guide, Administration Documentation
- OpenScape SBC V11 Installation Guide
- OpenScape SBC V11 Security Checklist

3 Zoom Web Portal Configuration

This section guides you in preparing the environment for integrating and operating with external Bring Your Own Carrier (BYOC) DID phone numbers.

IMPORTANT: Initial releases of OpenScape SBC for Zoom DO NOT require a Zoom BYOC/BYOP license. However, this license will be required for future releases. During this transition, Open Scape SBC Zoom licenses will NOT BE NEEDED as part of the Zoom subscription.

To set up users for the Zoom and OS4K integration, you must first add users to your Zoom account and assign licenses to them.

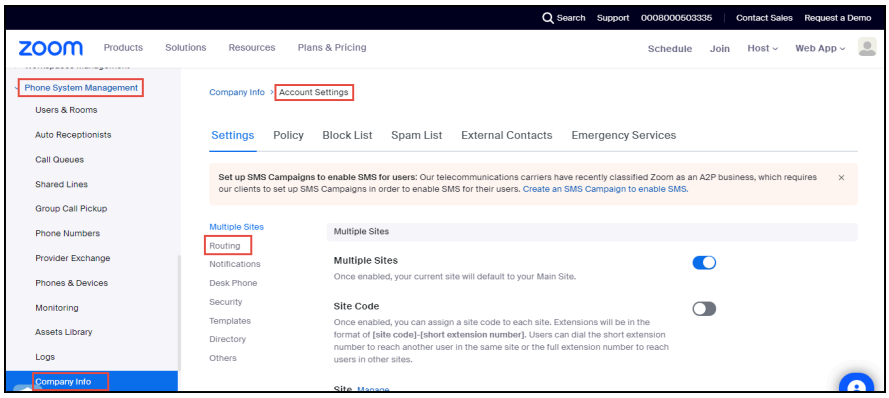
3.1 Adding the OpenScape SBC

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

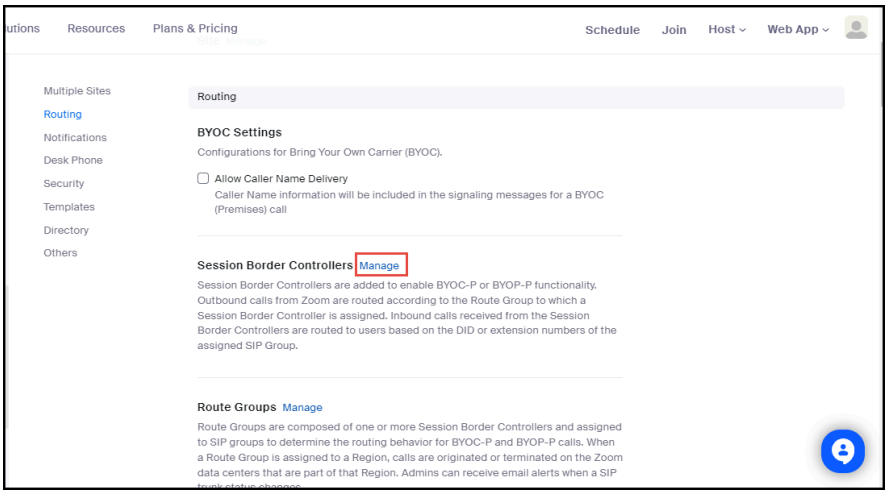
Prerequisites

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**.

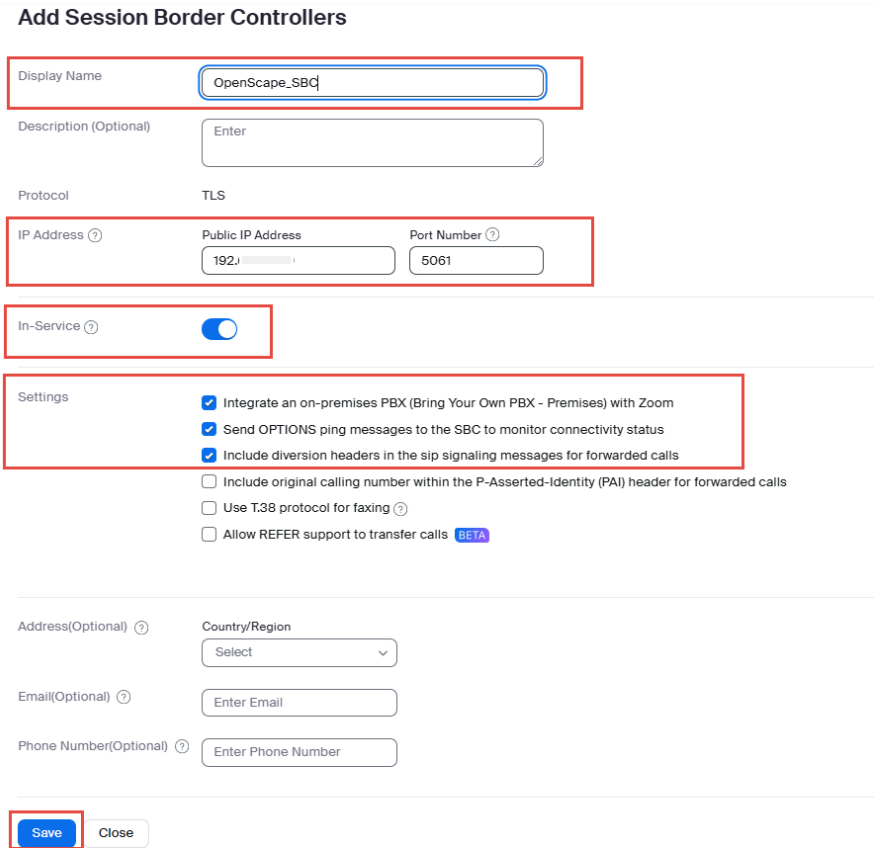
b) **IP Address:** Enter the IP address of the OpenScape SBC interface facing towards Zoom and configure the port number (for example, 5061).

c) **In-Service:** Click the toggle button to enable the **In-Service option**.

d) Under the **Settings** section, check the following checkboxes**:**

NOTICE: The first two settings are mandatory, while the remaining settings depend on the PSTN provider.

- **Integrate an on-premises PBX (Bring Tour OWN PBX-Premises) with Zoom**
- **Send OPTIONS ping messages to the SBC to monitor connectivity status**



6) Click **Save**.

NOTICE:

To ensure Zoom's network allows traffic from your OpenScape SBC, 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.

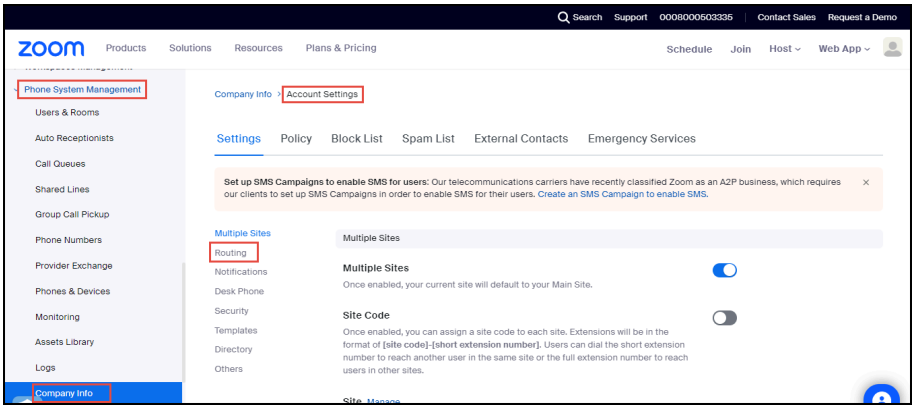
3.1.1 Configuring the Route Group

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.

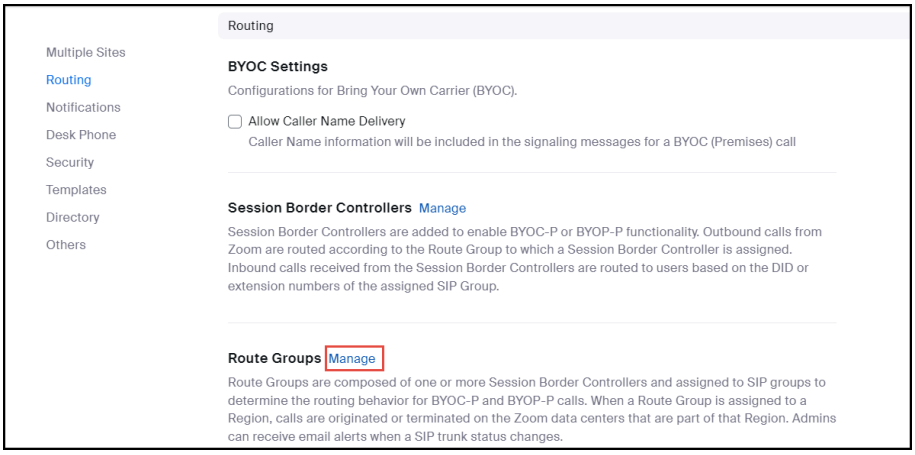
NOTICE: These configurations (Route Group, SIP Group, and Routing Rule) will take effect once phone numbers are added and assigned to the appropriate users. Until then, the routing logic will be in place, but calls will not be routed as expected.

To add a Route Group:

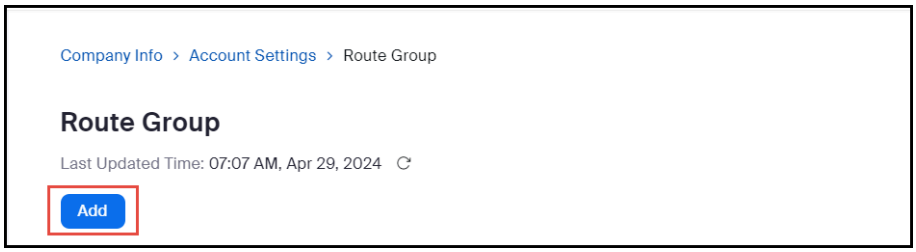
1) Navigate to **Phone System Management** > **Company Info** > **Account Settings** > **Routing**.



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



3) Click **Add.**

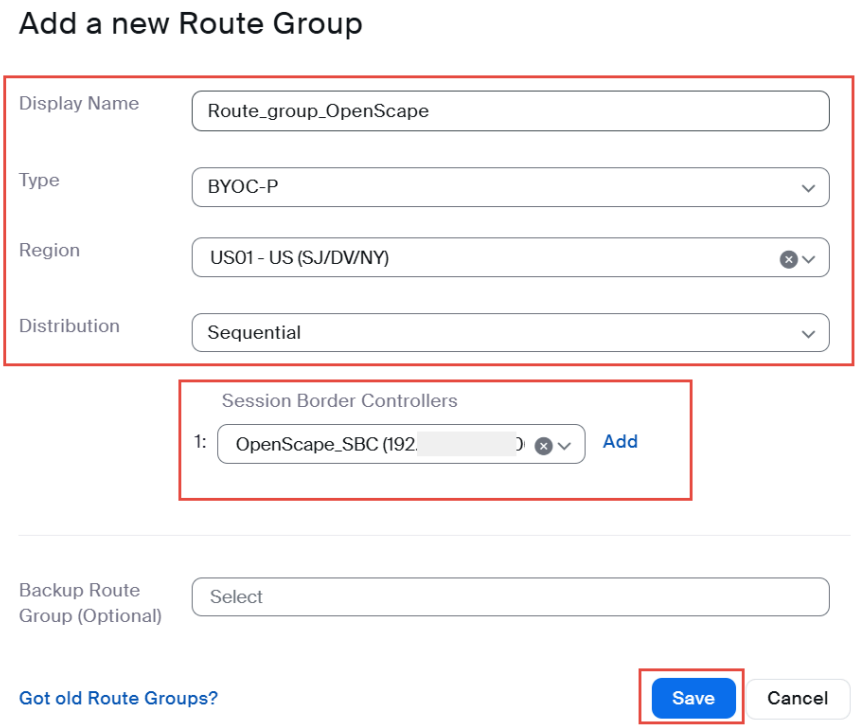


4) Configure the following:

   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)**

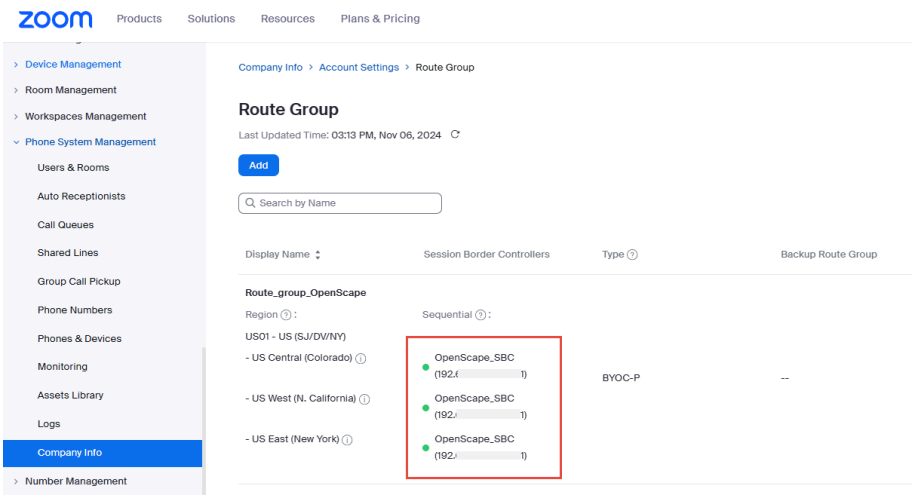
> **NOTICE:** The format given above is an example.Choose the zone (SJ/DV/NY etc.) that is geographically closest to your SBC installation location.

   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.

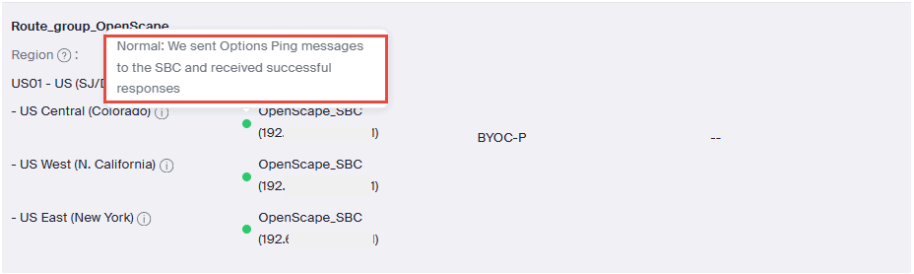


5) Click **Save**.

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:

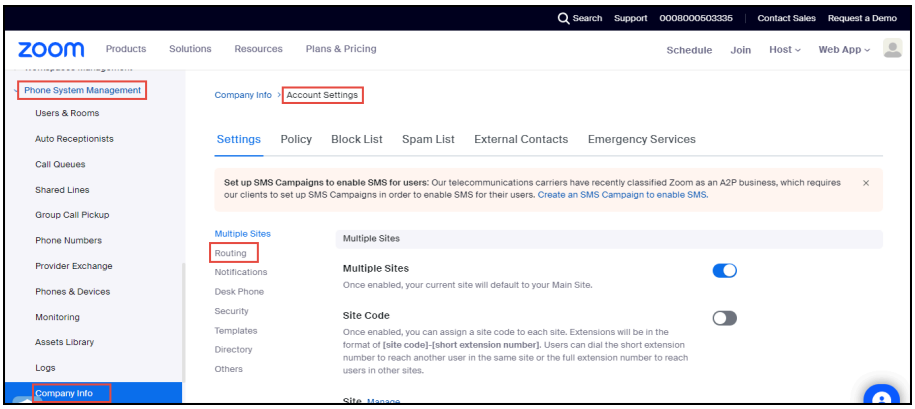


3.1.2 Configuring the SIP Group

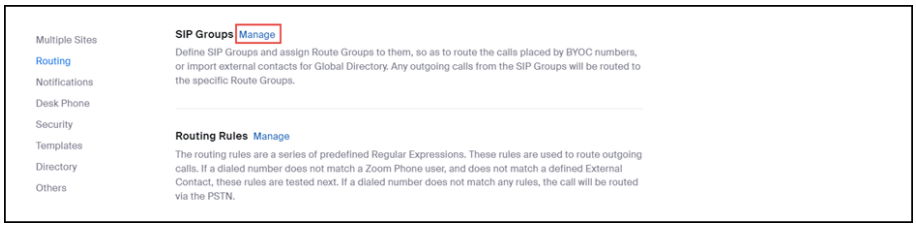
Follow the instructions below to configure SIP groups and assign Route Groups to them, in order to route calls placed by BYOC numbers. This step is mandatory for uploading the BYOC numbers.

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.**

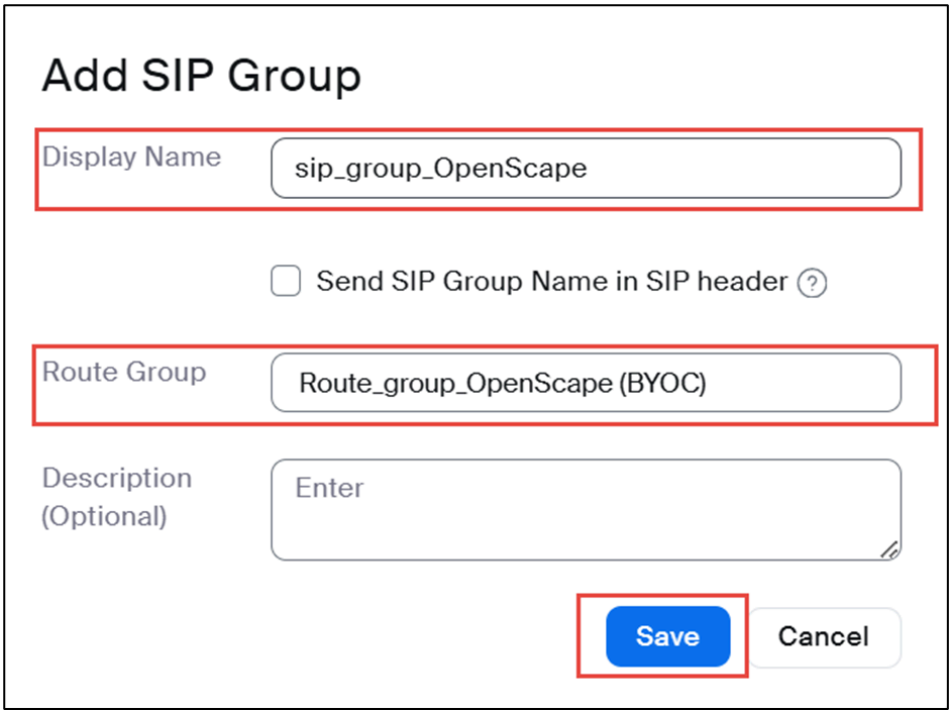


3) Click **Add.**

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.



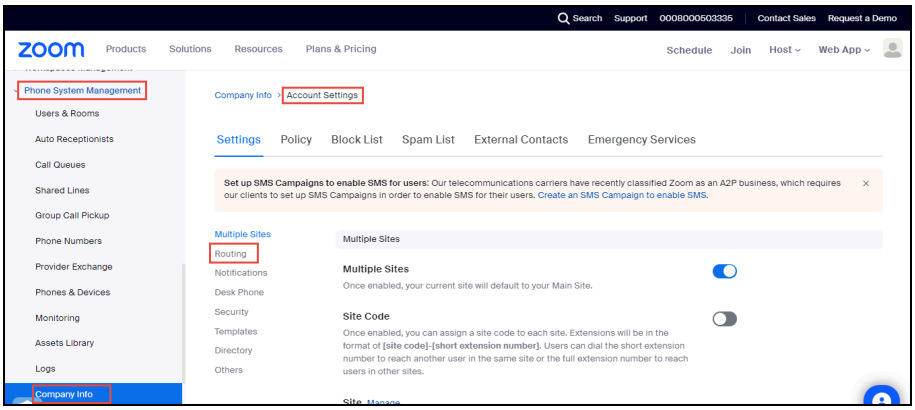
5. Click **Save.**

3.1.3 Configuring the Routing Rule

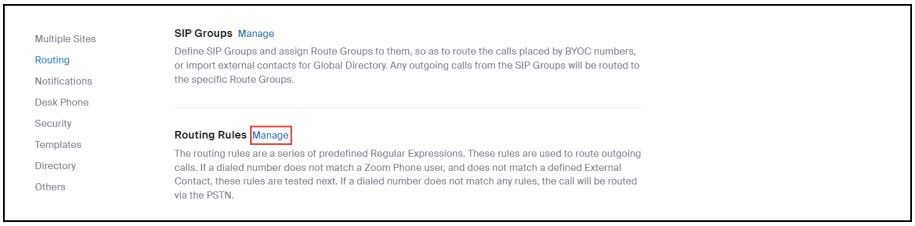
When configuring a **BYOC (Bring Your Own Carrier)** setup, you might create a routing rule to specify that calls from certain users or departments go through your OpenScape SBC or network route.To add a Routing Rule for outbound calls:

NOTICE: Ensure that your Session Border Controller (OpenScape SBC) 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.

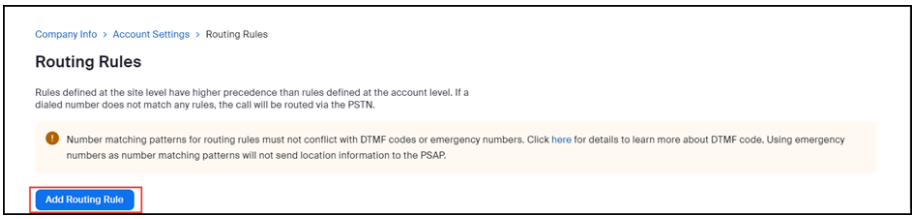
1) Navigate to **Phone System Management** > **Company Info** > **Account Settings** > **Routing**.



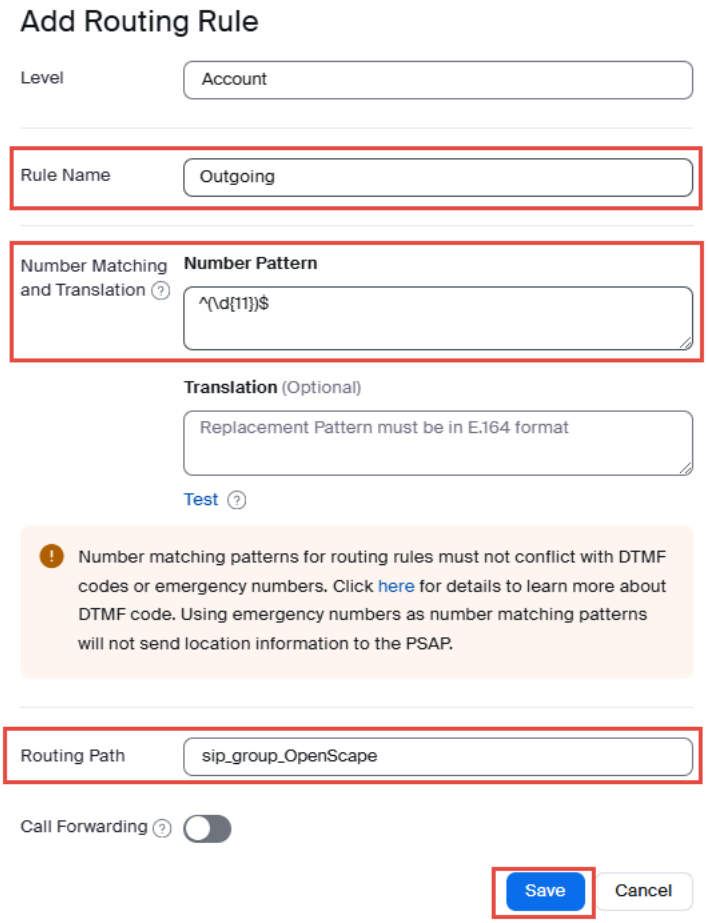
2) Locate the **Routing Rule** section and click **Manage.**



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.



5) Click **Save**.

3.2 Adding Phone Users

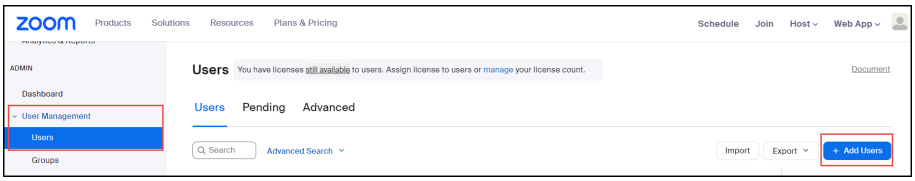
Follow the instructions below to add Zoom Phone Users. For more details, please refer to the official Zoom support page on How to add a new user.

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.**



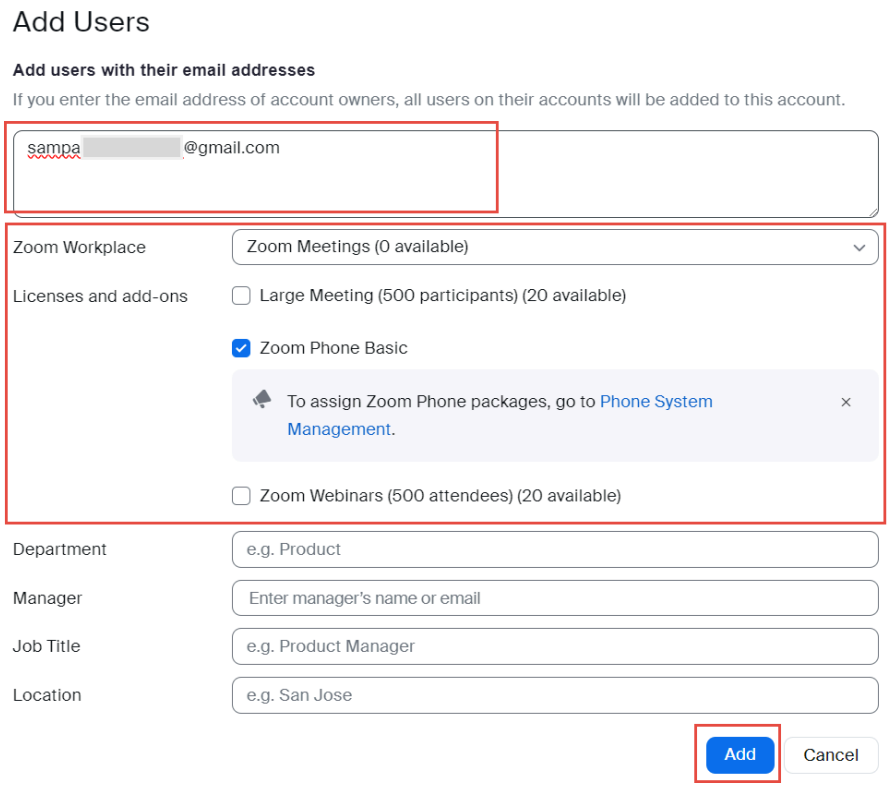
3) Configure the following in the **Add Users** pop-up:

   a) Enter the user's email address**.** To add multiple users with the same settings, enter multiple email addresses separated by commas: **,** .

   b) From the **Zoom Workplace** drop-down menu, select the available Zoom Workplace licenses to assign, such as **Zoom Meetings**.

   c) In the **Licenses and add-ons** section, check the **Zoom Phone Basic** checkbox.

   d) Click **Add**.



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.

3.2.1 Assigning a Calling Plan to a phone user

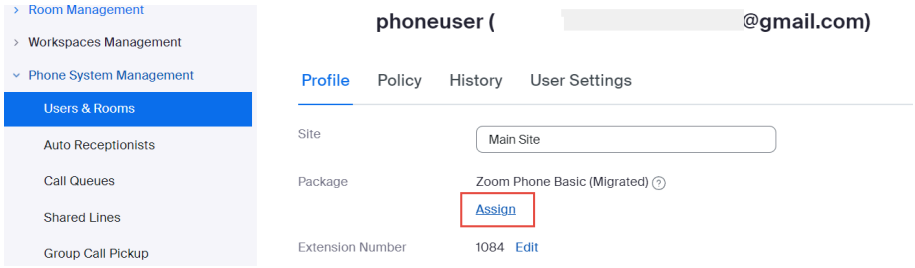
You can assign a calling plan to phone users to enable outbound calling.

Prerequisite

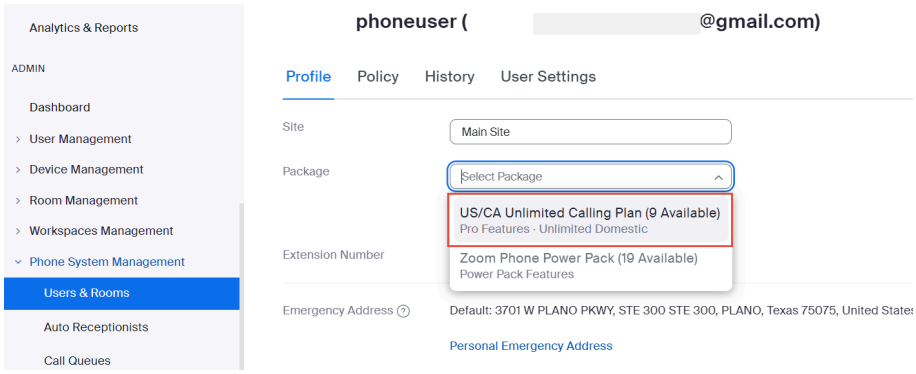
1) You are an administrator with the privilege to edit account settings.
2) You have assigned licenses to the phone users. For more information, refer to How to assign licenses.

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.



5) Click **Confirm**.

3.3 Adding BYOC Phone numbers

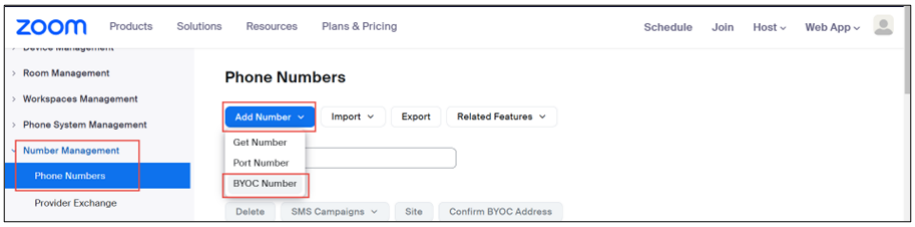
You can upload BYOC phone numbers.

Prerequisite

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

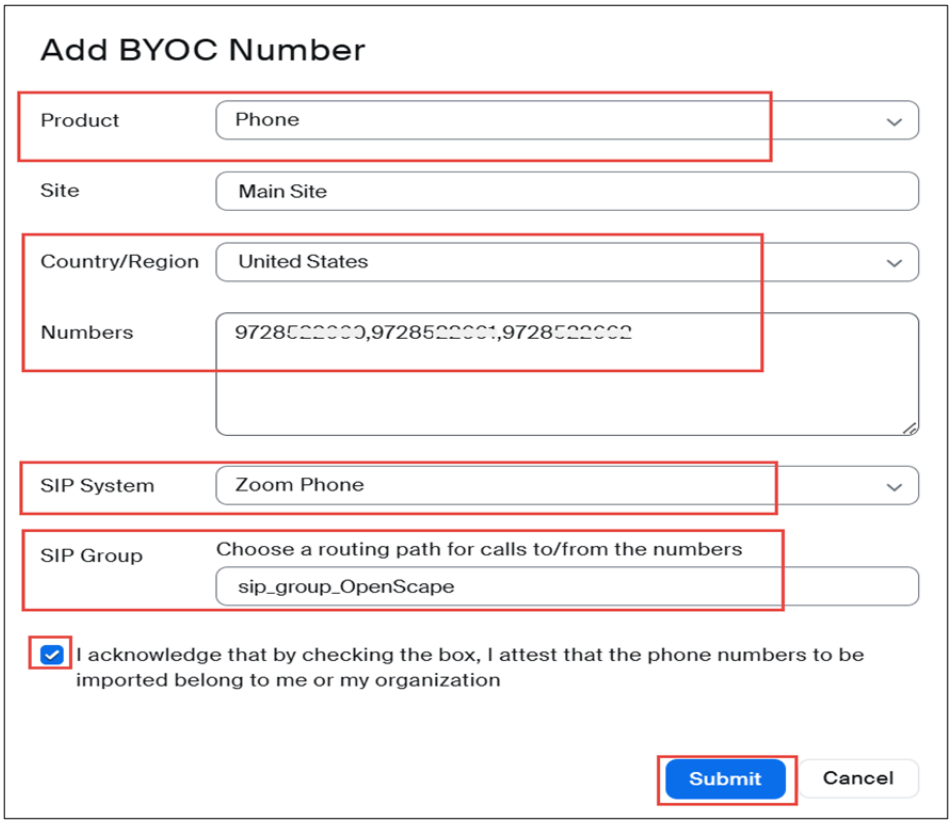
1) Log in the **Zoom web portal**.

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 13.
   f) Check the acknowledgment box to consent.
   g) Click **Submit**.

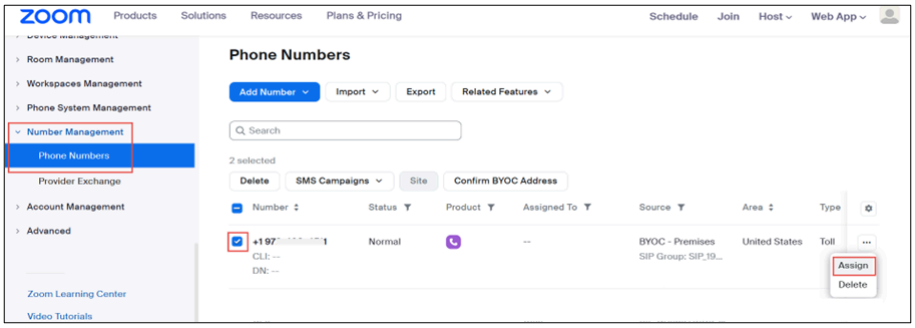


3.3.1 Assigning BYOC numbers

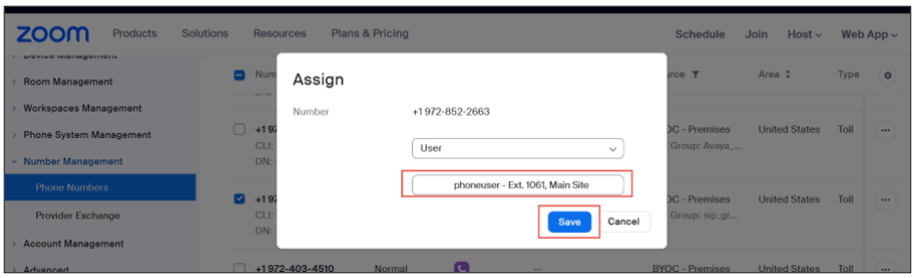
To assign Bring Your Own Carrier (BYOC) numbers to the Zoom phone users:

1) Navigate to **Phone System 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**.

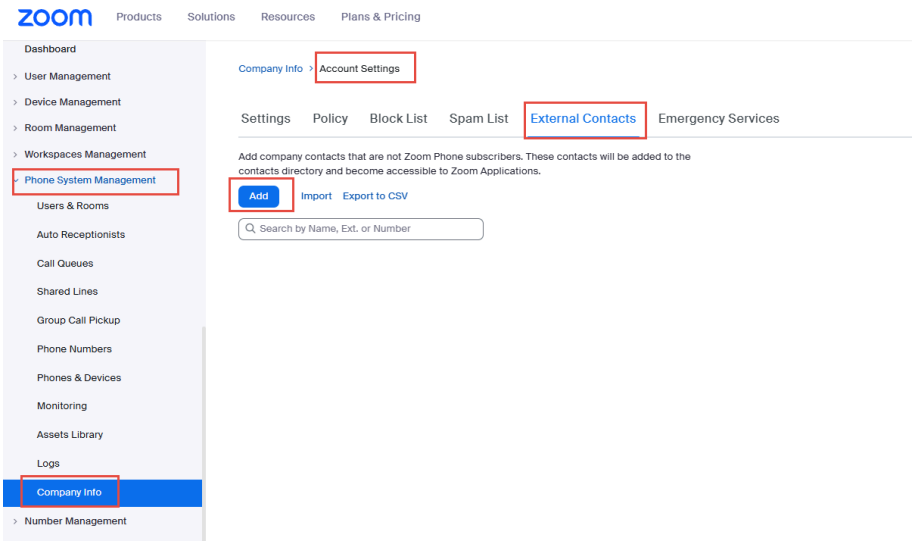


The phone number will be assigned to the selected user.

3.4 Adding BYOP numbers

Administrators can add OpenScape 4000 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 4000 user. For example, **OS4K_user1**.
   - In the **Extension Number** field, enter the extension number of the OpenScape 4000 user.
   - From the **Routing path** drop-down menu**,** select the **SIP Group** created in Configuring the SIP Group **on page 13.**
4) Click **Save**.

4 Configuring OpenScape SBC

This chapter outlines the configuration of OpenScape SBC for interworking with Zoom Direct Routing. Once OS4K is configured, you can use the SBC to route calls, secure communication, and manage traffic to Zoom Phone and PSTN networks.

IMPORTANT: Initial releases of Open Scape SBC for Zoom DO NOT require a Zoom BYOC/BYOP license. However, this license will be required for future releases. During this transition, Open Scape SBC Zoom licenses will NOT BE NEEDED as part of the Zoom subscription.

Prerequisite

1) You have obtained a public certificate issued by one of the Zoom-supported CAs. You will need it for the Configuring Certifications section.

The OpenScape SBC will be configured with the connection to OpenScape 4000, SSP and Zoom Phone System (remote) endpoints.

Whether routine or not, Zoom Phone Direct Routing's specific OpenScape SBC configuration will be omitted. Mitel OpenScape SBC installation and administration documentation can be found on the Customer documentation site.

INFO: Please check the Zoom site for the current IP Addresses.

Table 1: Zoom 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	
				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

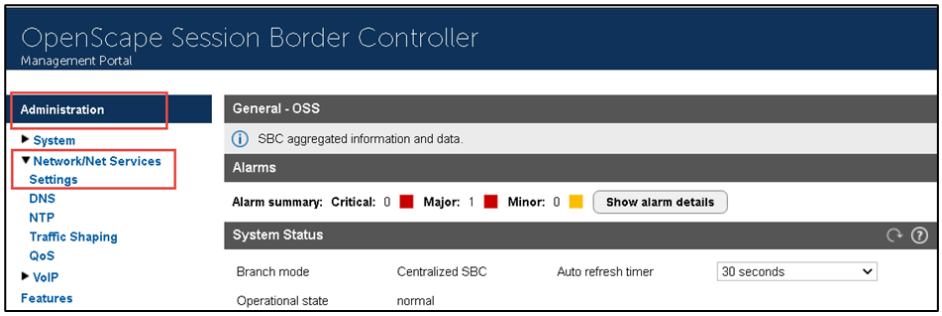
Traffic Type	Protocol	Source	Destination Ports	Destination IPs	Region
				101.36.167.237	HK2
				149.137.25.246	Japan
				207.226.132.198	

Table 2: Zoom 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	
				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	

4.1 Configuring Network settings

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

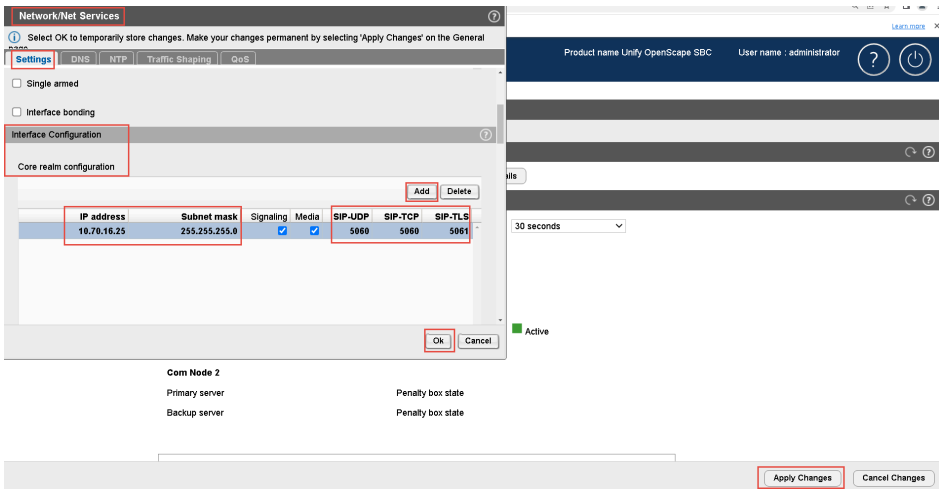


The **Network/Net Services** window pops up. By default, the **Settings** tab is displayed.

2) Locate the **Interface Configuration** > **Core Realm Configuration** area and click **Add**.

   a) Configure the following:

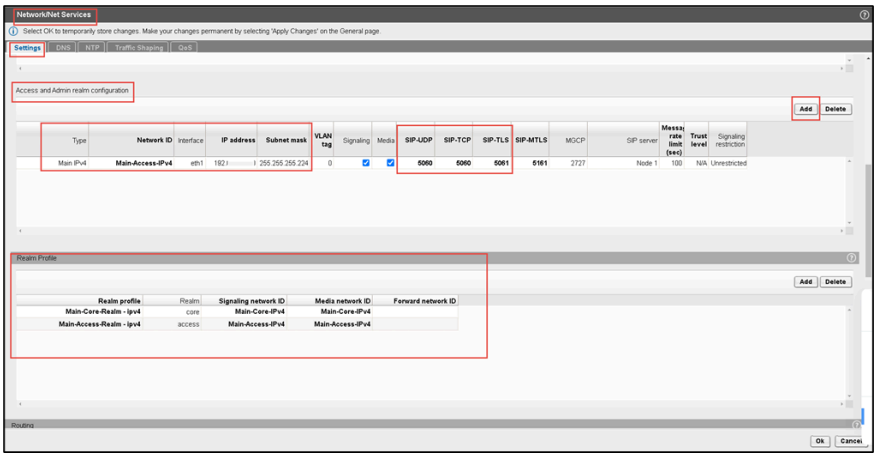
      a) **IP address**: Enter the SBC IP address associated with the core (private) side of the network.
      b) **Subnet mask:** Enter the subnet mask value.
      c) **SIP-UDP:** Configure port number as 5060.
      d) **SIP-TCP:** Configure port number as 5060.
      e) **SIP-TLS:** Configure port number as 5061.
      f) Click **Ok.**



   g) Click **Apply Changes** on the SBC Main page.

3) 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) **IP address**: Enter the SBC IP address associated with the public side of the network.
   d) **Subnet mask:** Enter the subnet mask value.
   e) **SIP-UDP:** Configure port number as 5060.
   f) **SIP-TCP:** Configure port number as 5060.
   g) **SIP-TLS:** Configure port number as 5061.
   h) Map the **realm profile** for **core** and **access** interface as shown in the below screenshot.
   i) Click **Ok.**
   j) Click **Apply Changes** on the SBC Main page.

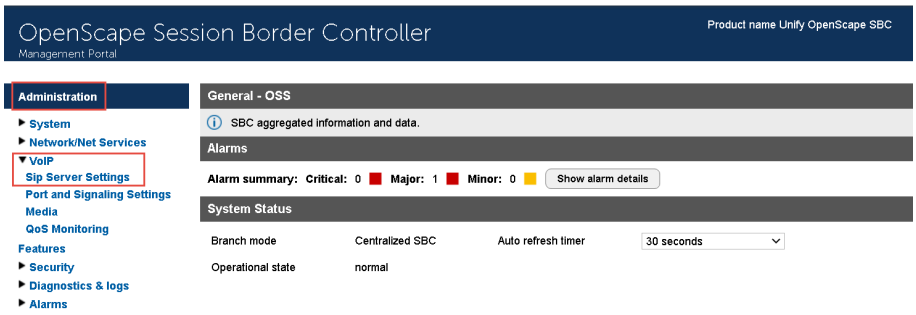


   You are redirected back to the **Network/Net Services** window.
5) Locate the **Routing** area to configure the default gateway address.
6) In the **Routing Configuration** section, click **Add** and add the static routes for core and access interface.
7) Click **OK**.
8) Click **Apply Changes**.

4.2 Configuring SIP Server

The SIP connectivity to OpenScape 4000 is configured in the **OpenScape SBC Management Portal** > **VOIP** window.

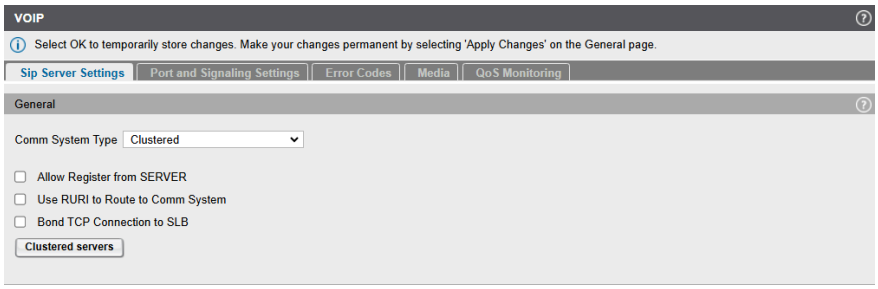
1) Navigate to **Administration** > **VoIP** > **Sip Server Settings**.



The **VOIP** window pops up.

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

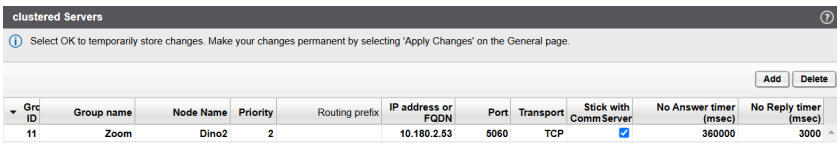
   a) Under **General**, from the **Comm System Type** drop-down menu, select **Clustered**.



> **NOTICE:** If there is only one OS4K gateway configured, then Common System Type can also be set to **Simplex**.

   b) Access the **Clustered Node Servers** section, then click **Add** :

   - Add the **Group name**
   - Add the **Node name**
   - Set the **Priority**
   - **IP Address or FQDN**: Enter the OpenScape 4000 gateway IP address.
   - **Stick with CommServer**: enabled
   - From the **Transport** drop-down menu, select **TCP/TLS**.
   - **Port**: Enter **5060/5061**.



3) Once the above parameters are set, click the **OK** button.
4) In the OS SBC main page, click the **Apply Changes** button.

4.3 Configuring Certificates

For secure communication with Zoom, a Trusted Certificate must be installed in OpenScape SBC. 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 common name (CN) in the subject field. Certificates with a wildcard in the certificate Subject Alternate Name field conforming to RFC2818 are also supported.

For more information about the certificate and current Zoom-supported Certification Authorities, refer to the official Zoom site.

NOTICE: 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 OpenScape SBC (e.g., "certificate.pem")
- OpenScape SBC server certificate private key used for the CSR to CA (e.g., "privatekey.pem")

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

Prerequisites

Adequate administrative permissions.

Adequate knowledge of TLS certificate handling.

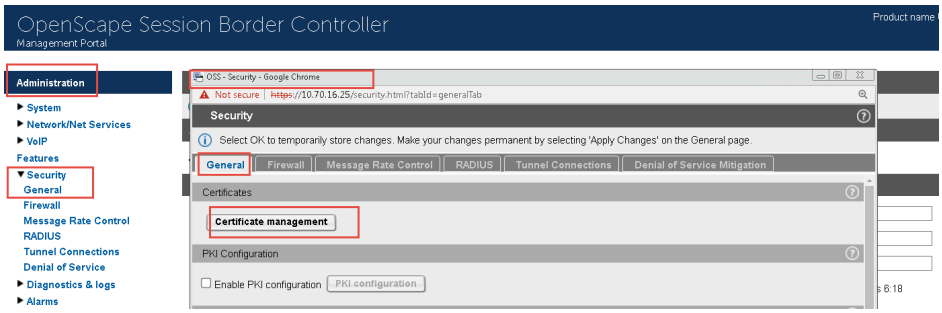
At least one OpenScape SBC is configured and in operation.

To configure Certificates:

1) Navigate to OpenScape SBC **Management Portal** > **Security** > **Denial of Service**.
2) In the **Security** pop-up, under the **Dynamic Black List** section, check the **Process initial registration** flag to enable it.
3) Click **Ok**.
4) Navigate to OpenScape SBC **Management Portal** > **Security** > **General.**

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

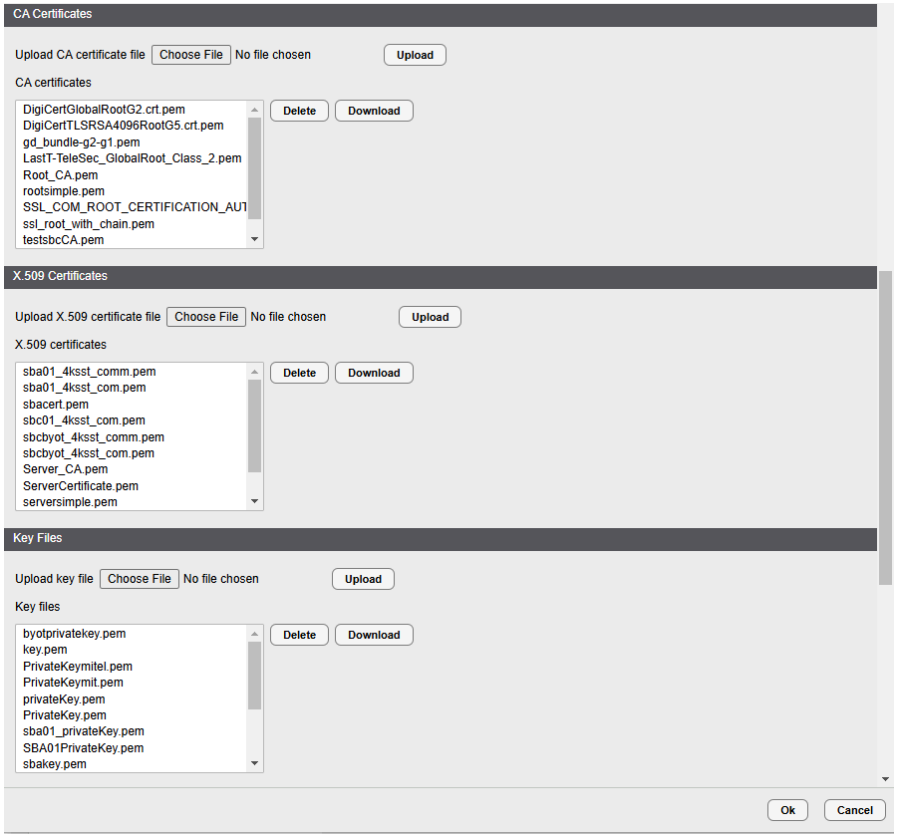
The **Certificate Management** window appears with the **General Configuration** tab displayed as default.



6) Under the **CA Certificate** area, click **Choose File** and browse to select the CA certificates. Click **Upload**.

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

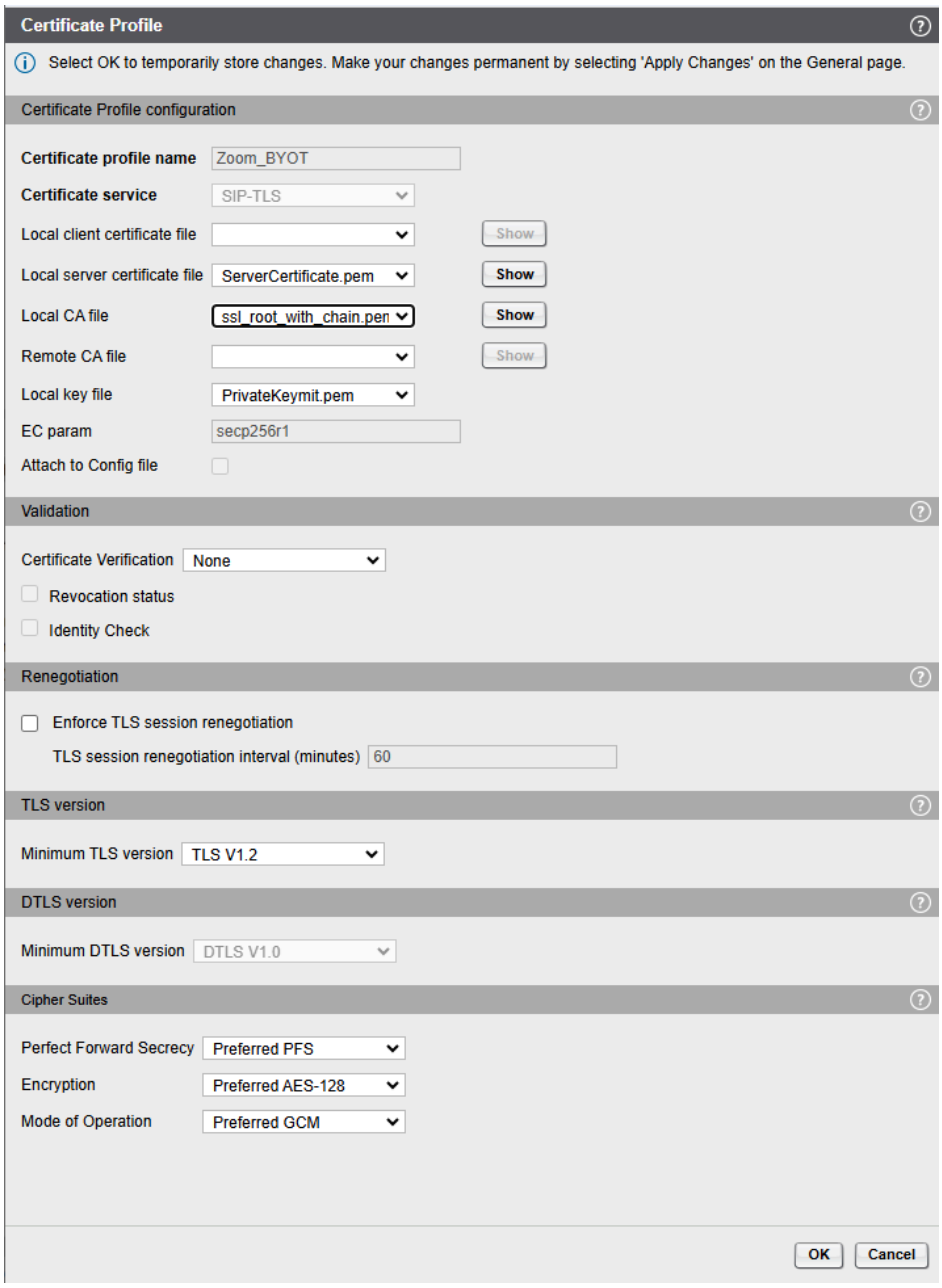
Under the **Key Files** section, click **Choose File** and browse to select the OpenScape SBC server certificate private key. Click **Upload**.



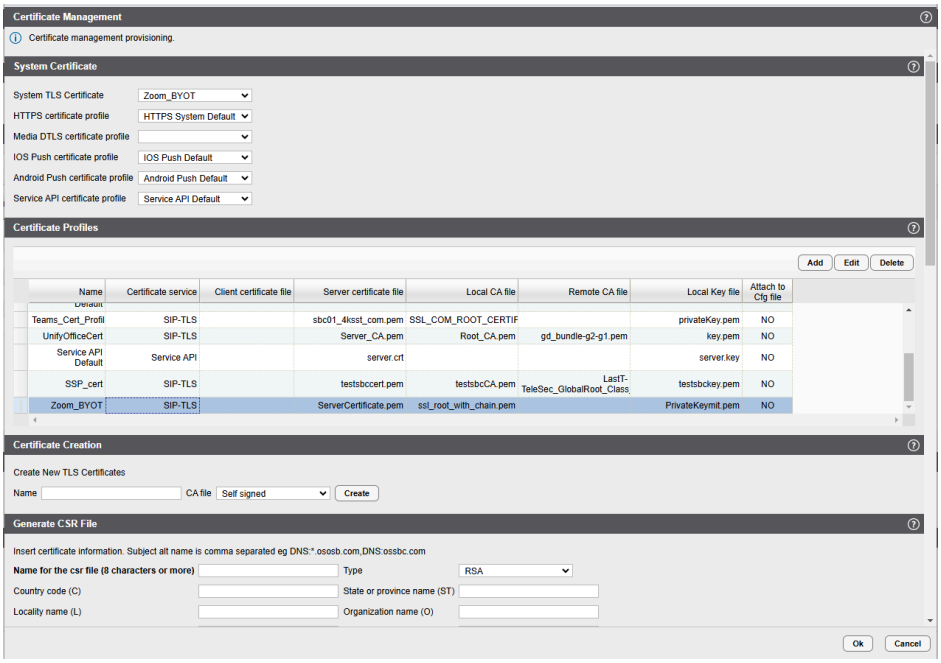
7) To create the Zoom certificate profile: In the **Certificate Management** pop-up, under the Certificate profiles area, click **Add**.

8) 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 file.
d) From the **Local CA file** drop-down menu, select the CA certificate.
e) From the **Local key file** drop-down menu, select the private key file.
f) From the **Certificate Verification** drop-down menu, select **None**.
g) From the **Minimum TLS version** drop-down menu, select **TLS1.2**.



9) Click **OK**.



10) Click **OK** in the **Certificate Management** window and in the **Security** window.

11) Click **Apply Changes** on the OpenScape SBC main page.

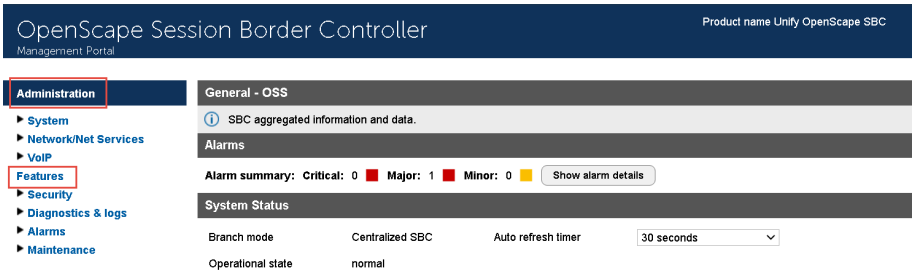
4.4 Configuring Media Profiles

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 OpenScape 4000.

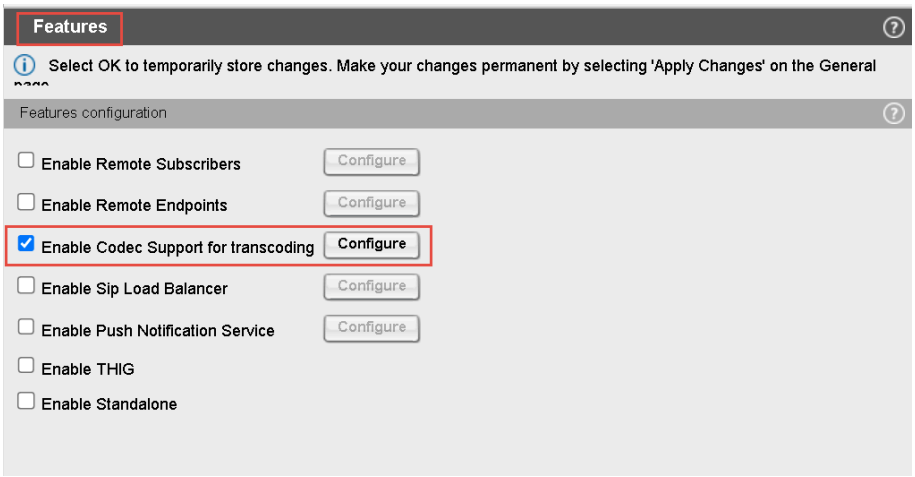
4.4.1 Configuring the Codec Manipulation Options

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

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



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

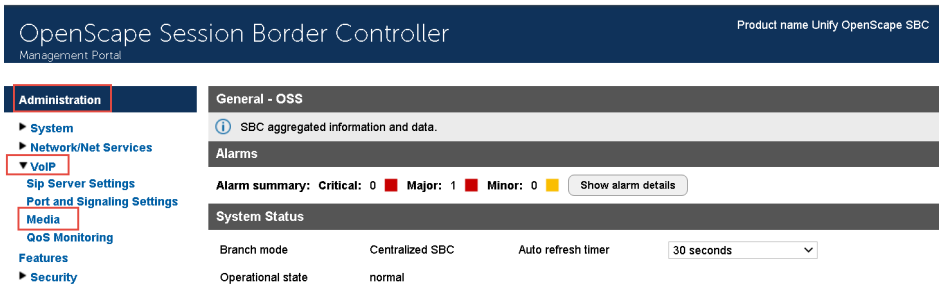


3) In the **Codecs** window, select the codecs to be available for the media profiles (for example, transcoding, prioritization).
4) Click **OK.**
5) Click **Apply Changes**.

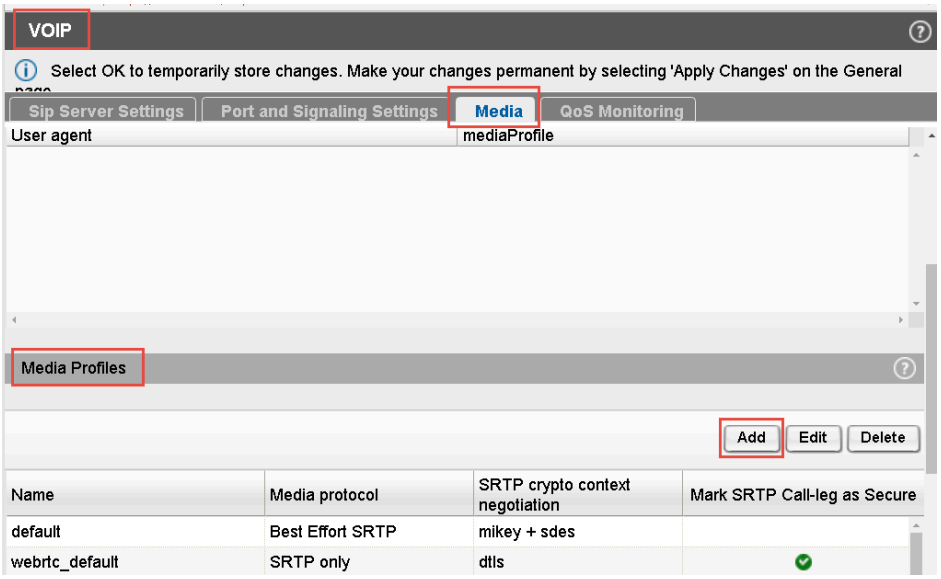
4.4.2 Configuring the Zoom Media Profile

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

1) **Navigate** to **OpenScape SBC Management Portal** > **VOIP** > **Media**.



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



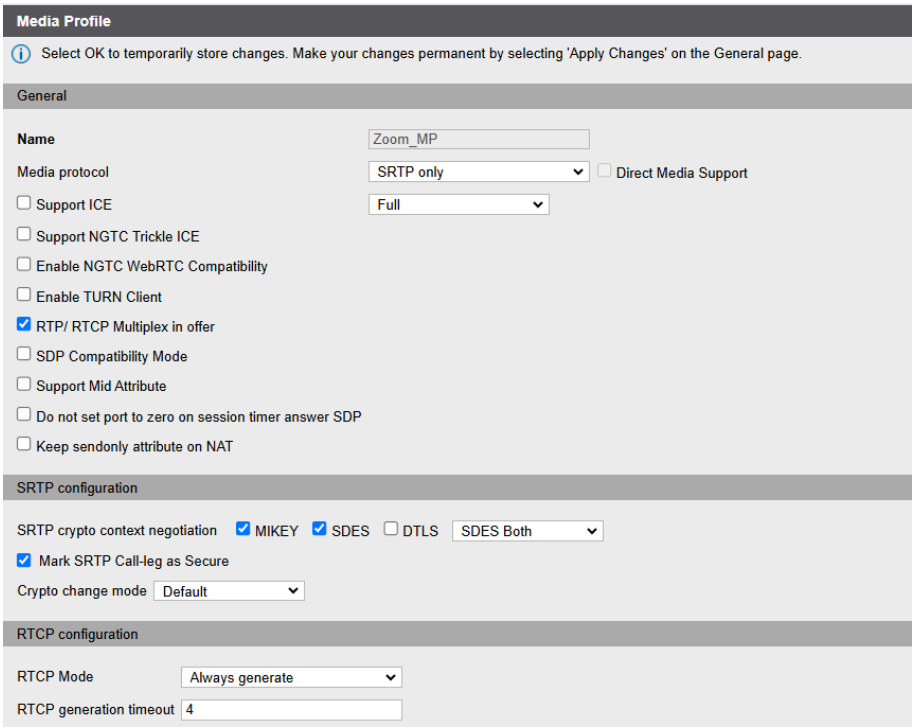
3) Locate the **Media Profiles** area and click **Add.**

The **Media profile** window pops up.

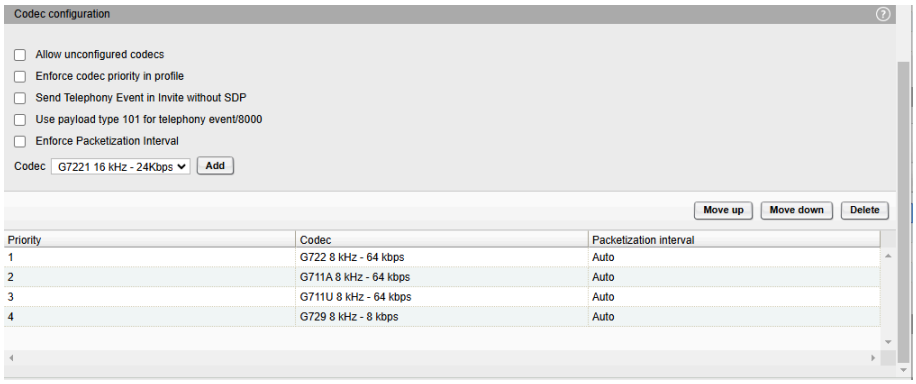
4) Under the **General** area, create the media profile for OpenScape SBC - Zoom connections by entering the following:

- **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 **MIKEY SDES** following checkbox.

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



6) Under the **Codec configuration** area, select the required codec(s).



7) Click **OK** to return to the **Media** window.
8) Click **OK** on the **VoIP** window.
9) Click **Apply Changes.**

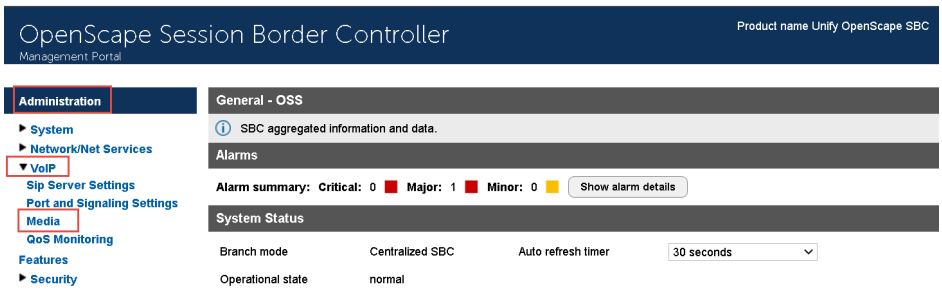
4.4.3 Configuring the PSTN Media Profile

The PSTN Media profile parameters depend on the provider's requirements.

For the configuration steps, please see: Configuring the Zoom Media Profile on page 32.

4.4.4 Configuring the OpenScape 4000 Media Profile

1) Navigate to the **OpenScape SBC Management Portal** > **VoIP** > **Media** window.



2) In the **VoIP** pop-up, go to the **Media** tab.
3) In case TCP connectivity is used between SBC and OpenScape 4000, the default profile can be used (use as media protocol **RTP only**).

If **TLS** connectivity is used, then the following configuration is needed:

1) In the **Media Profiles** area, click **Add** to create the media profile for OpenScape SBC – OS4K connection.
2) 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 **SRTP only**.
3) Under the **SRTP configuration** area, check the **SDES** checkbox.
4) In **RTCP configuration**, section, in the **RTCP Mode**select **Bypass** option.

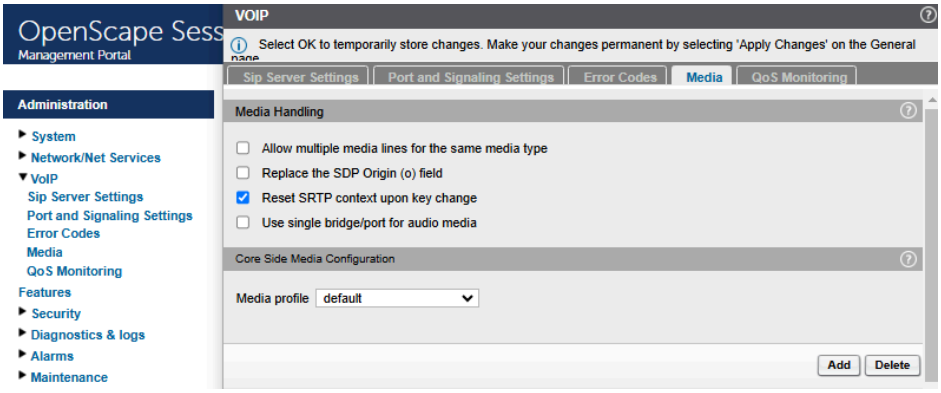
5) Locate the **Core Side Media Configuration** area and from the **Media Profile** drop-down menu and select the media profile used for the OS4K media connection which can be either the profile created for OS4K Configuring the OpenScape 4000 Media Profile on page 34 or the **default**.

   This is used for OS4K media connection.
6) Click **OK** in all open windows.
7) Click **Apply Changes** on the SBC main page.

4.4.5 General Media Settings

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

1) Navigate to the **OpenScape SBC Management Portal** > **VoIP** > **Media** window.
2) In the **VoIP** pop-up, go to the **Media** tab.
3) Under the **Media Handling** area, check the **Reset SRTP context upon key change** checkbox.



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

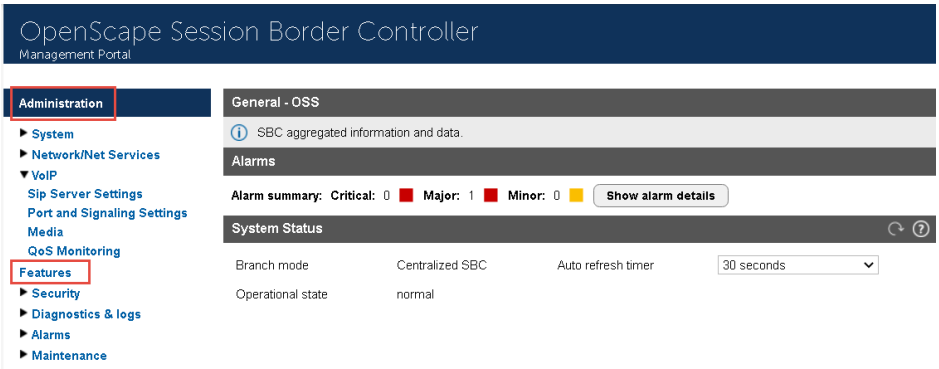
5) Click **OK** and then click **Apply Changes** on the SBC main page.

4.5 Configuring Remote Endpoints

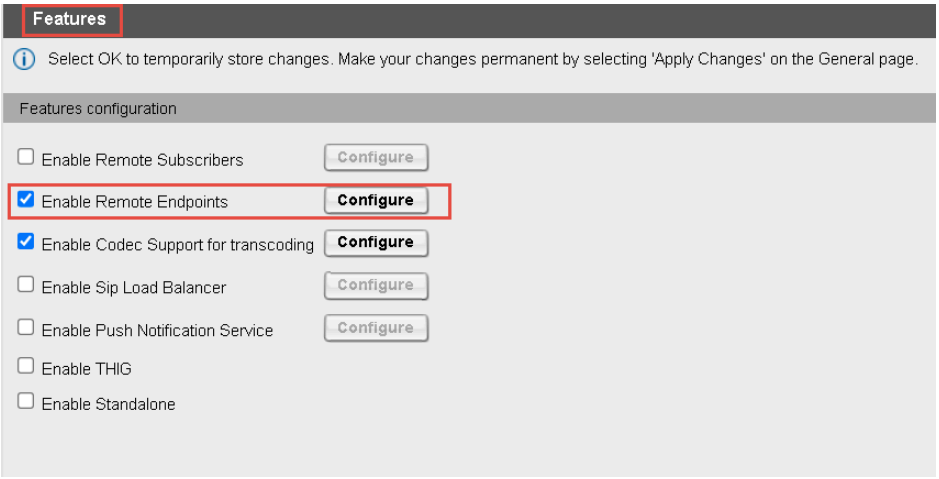
In the **Remote Endpoint** configuration, you can set up the OpenScape SBC with Zoom Phone System and the PSTN (SSP) SIP trunks.

4.5.1 Configuring the Zoom Remote Endpoints

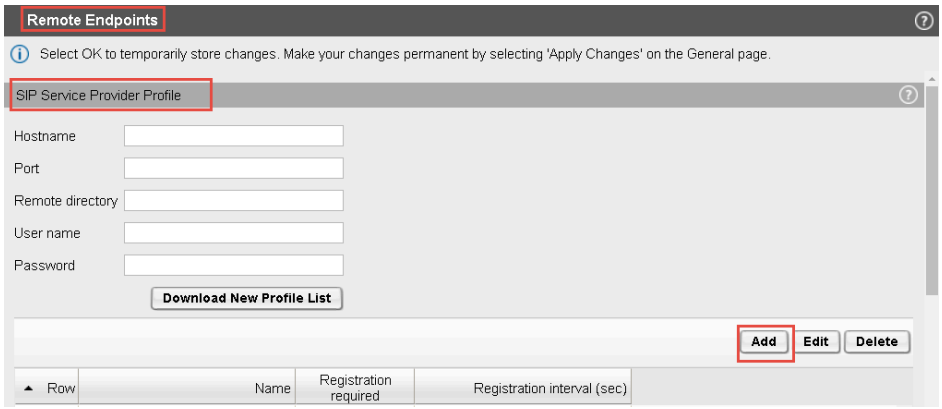
1) Navigate to the **Administration > Features** window.



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 OpenScape SBC – Zoom Phone System endpoint.

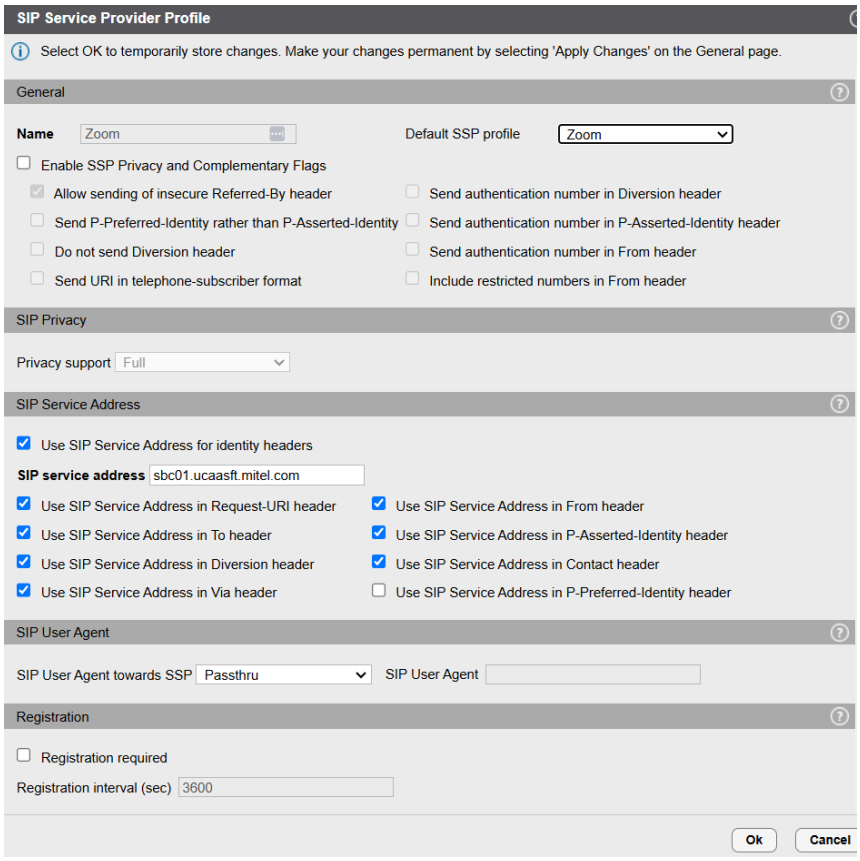


4) In the **SIP Service Provider** pop-up, configure the following:

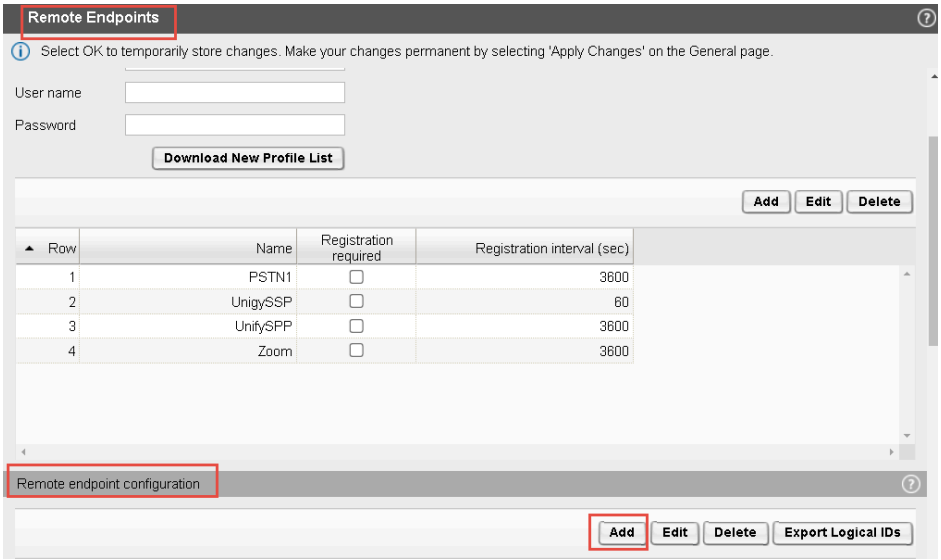
   a) **Name**: Enter the name of the SIP Service Provider profile. For example, Zoom.

   b) From the **Default SSP Profile drop-down** menu**,** select **Zoom**.

   c) **SIP service address**: Enter the SBC's public FQDN and click **OK** to return to the **Remote endpoints** window.

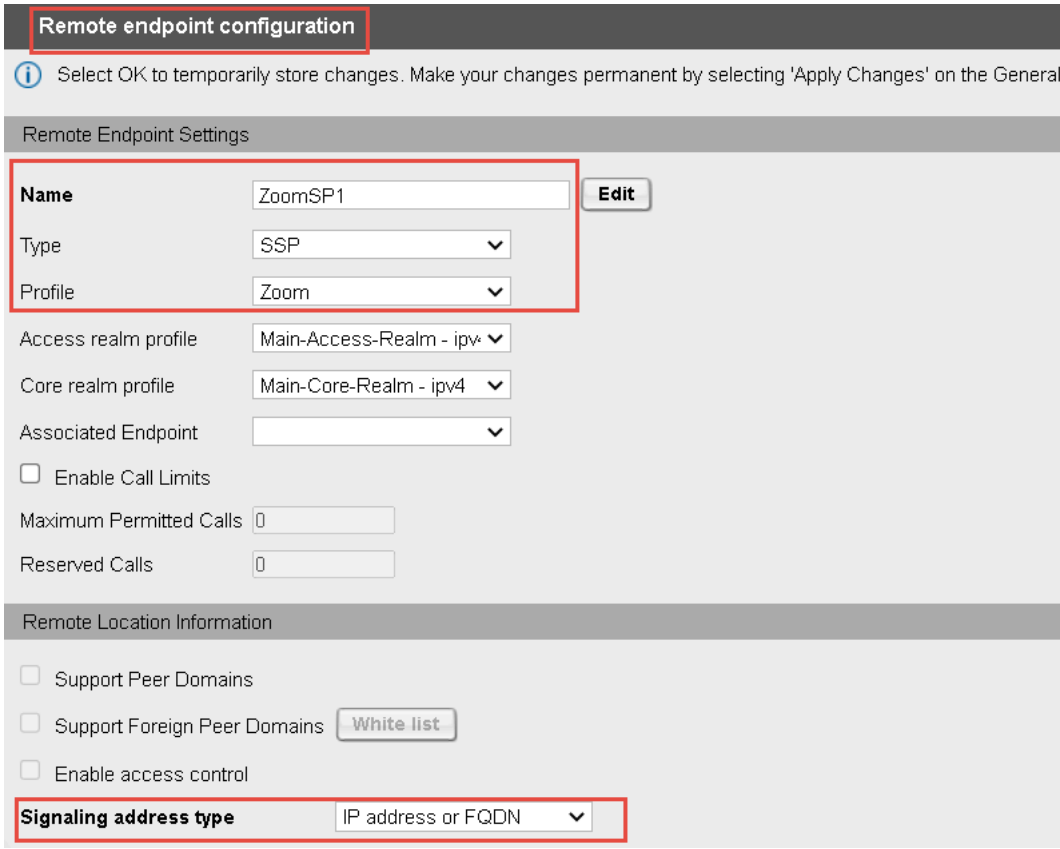


5) In the **Remote endpoints** window, locate the **Remote endpoint configuration** area, and click **Add.**



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** type drop-down menu, select **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 Configuring OpenScape SBC on page 22).

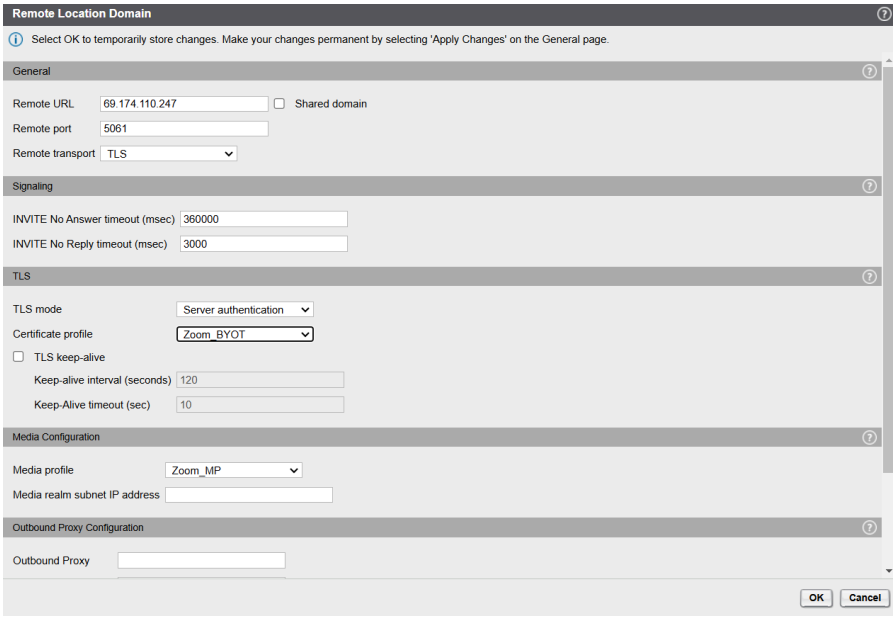
   b) Locate the **TLS** area, and from the **TLS mode** drop-down menu**,** select **Server authentication.**

   (or Mutual authentication in case MTLS is required)

   c) From the **Remote transport** drop-down menu, select TLS.

   d) From the **Certificate profile** drop-down menu, select **Zoom_BYOT.**

   e) Locate the **Media Configuration** area, and from the **Media profile** drop-down menu, select the **Zoom_MP**media profile.



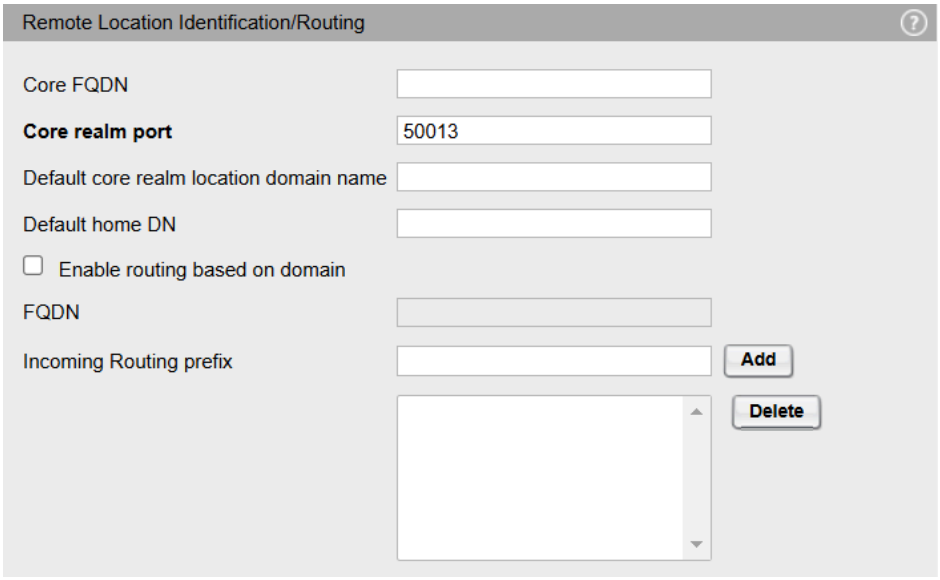
9) Click **OK**.

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 50013.

NOTICE: This value must match the port value configured in the OS4K SIP Trunk Profile. Please see: OpenScape

4000 Configuration with Zoom Phone System on page 41.



12) For each Zoom trunk a different remote endpoint must be created. Repeat the configurations in the **Remote endpoint configuration** window.

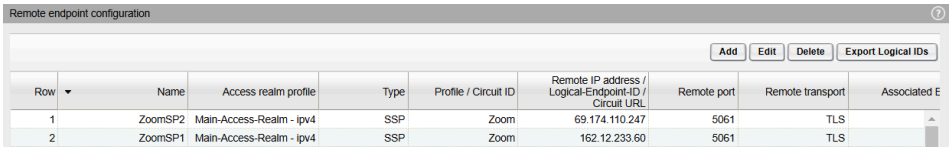
NOTICE:

The value of the core realm port for each remote endpoint must be unique.

Click **OK**.

13) Click **Apply changes**.

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



NOTICE: For the Zoom IPs, please see the Tables in Configuring OpenScape SBC on page 22.

4.5.2 Configuring the PSTN Remote Endpoint

The PSTN Remote Endpoint configuration depends on the provider's requirements.

For the configuration steps, please see: Configuring the Zoom Remote Endpoints on page 36.

5 OpenScape 4000 Configuration with Zoom Phone System

This chapter describes the OpenScape 4000 configuration to interconnect to Zoom Phone System.

Native SIP Trunking is used o connect 3rd party SIP products like Zoom.

The recommended profile for 3rd Party SIP applications is “**NatTrkEnterprise**”, which includes support for SIP Refer.

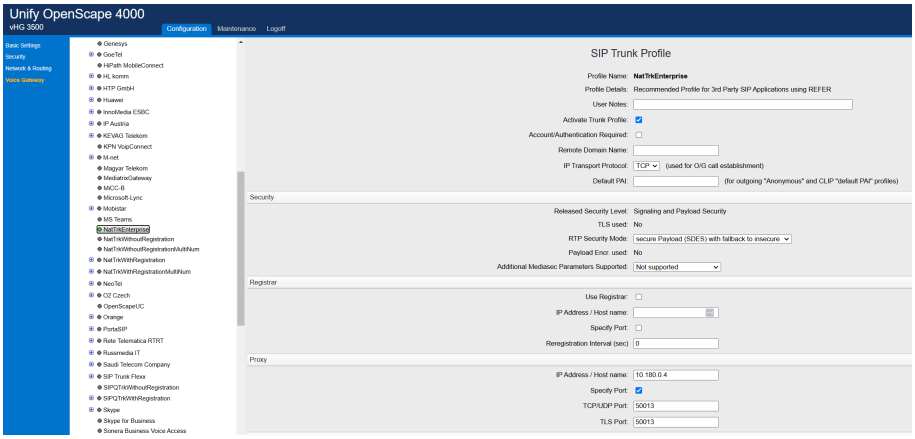
The connection to Zoom Phone system is done via OpenScape SBC.

Gateway Configuration in WBM

1) Navigate to **HG 3500 WBM.**
2) Under **Configuration > Voice Gateway**, select **SIP Trunk Profile**.

   The following settings are configured under the **NatTrkEnterprise** profile:

   - **IP address**- SBC IP address associated with the core side
   - **Port number**- Core real port that was configured in SBC Remote Endpoint for Zoom, please see Configuring the Zoom Remote Endpoints on page 36.
   - Check **Activate Trunk Profile** and click **Apply changes**.



NOTICE:

An unique SIP trunk is needed for each Zoom remote endpoint configured in SBC.

For further information regarding the SIP trunk profiles, please see Related Documentation on page 6.

5.1 OpenScape 4000 Routing

For full DN dialing

PSTN routing between Zappa tenant and PSTN is done via SBC and OS4K.

For this reason, on the OS4K there must be 2 routes configured, one to Zoom and the other to PSTN. Each route is assigned to the corresponding SIP trunk.

For extension dialing

For internal routing between Mitel PBX and Zappa Users, a route must be configured on the OS4K and assigned to the corresponding SIP trunk.

For further information, please see the Related Documentation on page 6.

6 Restrictions

In **Forward scenarios**, the information on users' display may not be correctly updated or may not contain the redirection information.

In **Transfer scenarios**, the information on users' display may not be correctly updated.

In **Conference scenarios**, the information on users' display may not be correctly updated.