

A MITEL PRODUCT GUIDE

OpenScape Solution Set V11

Zoom Phone with OpenScape SBC and OpenScape Voice (Bring Your Own Carrier -BYOC)

Document Version 1.3

January 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 Additional Support Information	
2.2 Network Topology	
2.3 Related Documentation	4

3 Zoom Web Portal Configuration	5
3.1 Adding Phone Users	
3.1.1 Assigning a Calling Plan to a phone user	
3.2 Adding the OpenScape SBC	
3.2.1 Configuring the Route Group	11
3.2.2 Configuring the SIP Group	
3.2.3 Configuring the Routing Rule	
3.3 Adding BYOC Phone numbers	
3.3.1 Assigning BYOC numbers	
3.4 Adding BYOP numbers	

4 Provisioning Phones for Zoom Phone Users......25

5 Unify OpenScape Voice Configuration	27
5.1 Configuring Endpoints	
5.1.1 Configuring the OpenScape SBC Endpoint	28
5.1.2 Configuring the Zoom Phone Endpoint	
5.1.3 Configuring the PSTN Endpoint	43
5.1.4 Endpoint Overview	
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	60
5.3.1 Configuring the Zoom Numbers Routing	61
5.3.2 Configuring the PSTN Numbers Routing	62
5.4 Configuring the SIP UA Forking	64
5.5 Configuring Display Number Modification	65

6 Unify OpenScape SBC (Configuration70
6.1 Configuring Network settings.	

6.2 Configuring SIP Server	75
6.3 Configuring Certificates	77
6.4 Configuring Media Profiles	81
6.4.1 Configuring the Codec Manipulation Options	
6.4.2 Configuring the Zoom Media Profile	83
6.4.3 Configuring the PSTN Media Profile	86
6.4.4 Configuring the Unify OpenScape Voice Media Profile	
6.4.5 General Media Settings	
6.5 Configuring Remote Endpoints	91
6.5.1 Configuring the Zoom Remote Endpoints	
6.5.2 Configuring the PSTN Remote Endpoint	

History of Changes

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 74. Added a table of other Zone Zoom IPs in Unify OpenScape SBC Configuration on page 70 for Unify OpenScape SBC/OpenScape Voice configurations.	
1.3	01/2025	Updated entire document.	

Introduction

This chapter contains the following sections:

- Additional Support Information
- Network Topology
- Related Documentation

This document outlines the process of connecting the **Unify 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 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 (OSV) for telephony features. It is ideal for organizations that are currently using Zoom as a main collaboration tool and want to continue using their OSV system for call management and PSTN connectivity.

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. To support this integration, users must have OpenScape Voice and OpenScape SBC properly configured within their environment. 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:

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 BYOC/BYOP licenses will NOT BE NEEDED as part of the Zoom subscription.

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.

Product	Software Version
Unify OpenScape Voice	V10.3.31
OpenScape SBC	V11R1.0.0
Unify OpenScape Apps	V10 R3.10.1

2.1 Additional Support Information

In the current Unify product software implementation:

- OpenScape SBC with Unify 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 <u>not</u> supported by OpenScape SBC.
- The History-Info header is <u>not</u> currently supported by Unify OpenScape Voice

and Unify OpenScape 4000.

• The OSEE environment with SBC-THIG and Zoom is currently <u>not</u> supported.

2.2 Network Topology

The block diagram below shows the Zoom Phone connection topology.



Figure 1: Network Topology Block Diagram

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

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.



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 BYOC/BYOP licenses will NOT BE NEEDED as part of the Zoom subscription.

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.

ZOOM Products Sol	utions Resources Plans & Pricing	Schedule Join Host - Web App -
ADMIN	Users You have licenses still available to users. Assign license to users or manage your license count.	Document
Dashboard V User Management	Users Pending Advanced	
Users Groups	Q Search V	Import Export × + 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.

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.

sampa @gm	nail.com
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	e.g. Product
Manager	Enter manager's name or email
Job Title	e.g. Product Manager
Location	e.g. San Jose
	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

Document Version 1.3

Zoom Phone with OpenScape SBC and OpenScape Voice (Bring Your Own Carrier - BYOC)

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.

> User Management			
> User Management			
> Device Management			
> Room Management			
> Workspaces Management			
 Phone System Management 			
Users & Rooms			
Auto Receptionists			
Call Queues	Yealink phoneuser sampathindhu0804+ac 1@gmail.com	Online Active Main Site	

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

Room Management	Yealink phoneuser (sampa		@gmail.com)
> Workspaces Management			0 /
 Phone System Management 	Profile Policy	History User Settings	
Users & Rooms			
Auto Receptionists	Site	Main Site	
Call Queues	Package	Zoom Phone Basic (Migrated) 🧿	
Shared Lines		Assign	
Group Call Pickup	Extension Number	1084 Edit	

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

	Analytics & Reports	Yealink phoneus	ser (sampa	@gmail.com)
	ADMIN	Profile Policy H	listory User Settings	
	Dashboard			
	> User Management	Site	Main Site	
	> Device Management	Package	Select Package	^
	> Room Management		US/CA Unlimited Calling Plan (Q Availa	able)
	> Workspaces Management		Pro Features · Unlimited Domestic	
	 Phone System Management 	Extension Number	Zoom Phone Power Pack (19 Available) Power Pack Features)
	Users & Rooms	E		
	Auto Receptionists	Emergency Address (?)	Default: 3701 W PLANO PKWY, STE 300 STE 3	300, PLANO, Texas 75075, United States
	Call Queues		Personal Emergency Address	
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.

utions	Resources	Plans & Pricing Site Manage	Schedule	Join	Host ~	Web App ~	
r	Multiple Sites	Routing					
	Notifications Desk Phone Security Templates	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 (Premises) call	BYOC				
	Directory	Session Border Controllers Manage Session Border Controllers are added to enable BYOC-P or BYOP-P function Outbound calls from Zoom are routed according to the Route Group to which Session Border Controller is assigned. Inbound calls received from the Sess Border Controllers are routed to users based on the DID or extension number assigned SIP Group.	nality. h a sion ers of the				
		Route Groups Manage Route Groups are composed of one or more Session Border Controllers and to SIP groups to determine the routing behavior for BYOC-P and BYOP-P cal a Route Group is assigned to a Region, calls are originated or terminated on data centers that are part of that Region. Admins can receive email alerts whit to the scheme of	l assigned Is. When the Zoom nen a SIP				9

4. Click Add.

Company Info > Account Settings > Session Border Controllers		
Session Border Controllers		
Add		
Q Search	Type (All)	7

- 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 Tour 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

	Openscape_SBQ
Description (Optional)	Enter
Protocol	TLS
IP Address 곗	Public IP Address Port Number ⑦ 192. 5061
In-Service ⑦	
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 v
Email(Optional) 💮	Enter Email
Phone Number(Optional) 🧿	Enter Phone Number
Save	



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.



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.

Multiple Sites	BYOC Settings
Routing	Configurations for Bring Your Own Carrier (DVOC)
Notifications	
Desk Phone	Allow Caller Name Delivery Caller Name information will be included in the signaling messages for a RYOC (Premises) call
Security	
Templates	
Directory	Session Border Controllers Manage
Others	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.



- 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	
Туре	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 Gro	Save	Cancel

5. Click Save.

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

ZOOM Products Solu	utions Resources Plans & Pri	cing		
Device Management Room Management	Company Info > Account Settings	> Route Group		
Workspaces Management	Route Group			
 Phone System Management 	Last Updated Time: 03:13 PM, Nov	06, 2024 C		
Users & Rooms	Add			
Auto Receptionists	Q Search by Name			
Call Queues				
Shared Lines	Display Name 🍦	Session Border Controllers	Туре 🧿	Backup Route Group
Group Call Pickup	Route_group_OpenScape			
Phone Numbers	Region (?):	Sequential (?):		
Phones & Devices	US01 - US (SJ/DV/NY)			
Monitoring	- US Central (Colorado) 🕧	OpenScape_SBC (192.(1)	BYOC-P	
Assets Library	- US West (N. California) 🕧	OpenScape_SBC		
Logs	- US East (New York)	(192.) 1)		
Company Info		(192.)		
> Number Management				

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

Route_group_O	penScane			
Pogion ()	Normal: We sen	t Options Ping mess	ages	
Region ().	to the SBC and i	received successful		
US01 - US (SJ/[responses			
	responses			
- US Central (Co	oloradoj (j	OpenScape_	SBC	
		(192.	I)	BYOC-P
		0	CRO	
- US West (N. C	alifornia) ()	OpenScape_	SBC	
		(192.	1)	
UC Fast (Naw)	Varia O	0	600	
- US East (New	YOFK)	openscape_	SBC	
		(192.()	

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.

Multiple Sites	SIP Groups Manage
Routing	Define SIP Groups and assign Route Groups to them, so as to route the calls placed by BYOC numbers,
Notifications	or import external contacts for Global Directory. Any outgoing calls from the SIP Groups will be routed to
Desk Phone	the specific Route Groups.
Security Templates Directory Others	Routing Rules Manage The routing rules are a series of predefined Regular Expressions. These rules are used to route outgoing calls. If a dialed number does not match a Zoom Phone user, and does not match a defined External Contact, these rules are tested next. If a dialed number does not match any rules, the call will be routed via the PSTN.

3. Click Add.

Company Info > Account Settings > SIP Groups		
SIP Groups		

- 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 G	aroup
Display Name	sip_group_OpenScape
	Send SIP Group Name in SIP header ?
Route Group	Route_group_OpenScape (BYOC)
Description (Optional)	Enter

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:



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.

Multiple Sites	SIP Groups Manage
Routing	Define SIP Groups and assign Route Groups to them, so as to route the calls placed by BYOC numbers, or import external contacts for Global Directory. Any outgoing calls from the SIP Groups will be routed to
Notifications	the specific Route Groups.
Desk Phone	
Security	urity Routing Rules Manage plates The centre rules are a partice of prodefined Decular Expressions. These rules are used to route outgoing.
Templates	
Directory	calls. If a dialed number does not match a Zoom Phone user, and does not match a defined External
Others	Contact, these rules are tested next. If a dialed number does not match any rules, the call will be routed via the PSTN.

3. Click Add Routing Rule to add your rule.

Compa	any Info > Account Settings > Routing Rules
Rou	ting Rules
Rules d dialed	defined at the site level have higher precedence than rules defined at the account level. If a number does not match any rules, the call will be routed via the PSTN.
0	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.
Add	Routing 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.

	Account
Level	Account
Rule Name	Outgoing
Number Matching and Translation (?)	Number Pattern (^(\d{11})\$
	Translation (Optional)
	Replacement Pattern must be in E.164 format
Number mai	tching patterns for routing rules must not conflict with DTMI nergency numbers. Click here for details to learn more about
DTME code	Using emergency numbers as number matching patterns
DTMF code. will not send	Using emergency numbers as number matching patterns I location information to the PSAP.
DTMF code. will not send	Using emergency numbers as number matching patterns d location information to the PSAP.
Call Forwarding ?	Using emergency numbers as number matching patterns d location information to the PSAP. sip_group_OpenScape

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.

ZOOM Products Solution	s Resources Plans & Pricing	Schedule	Join	Host ~	Web App ~	0
> Room Management	Phone Numbers					
Phone System Management	Add Number V Export Related Features V					
 Number Management 	Get Number Port Number					
Phone Numbers	BYOC Number					
Provider Exchange	Delete SMS Campaigns v Site Confirm BYOC Address					

- 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						
		10					
SIP System	Zoom Phone	~					
SIP Group	Choose a routing path for calls to/from the numbers						
	sip_group_OpenScape						
I acknowledg imported belo	e that by checking the box, I attest that the phone numb ong to me or my organization	ers to be					
	Submit	Cancel					

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.

ZOOM Products Solution	ns Resources Plans & Pricing	Schedule Jo	in Host v	Web App 🗸 🚨
> Room Management	Phone Numbers			
> Workspaces Management	Add Number v Import v Export Related Features v			
Phone System Management Number Management	Q Search			
Phone Numbers	2 selected			
Provider Exchange	Delete SMS Campaigns V Site Confirm BYOC Address			
> Account Management	Number Status Product Assigned To	Source T	Area ‡	Туре
> Advanced	CLI: DN:	BYOC - Premises SIP Group: SIP_19	United States	Toll Assign Delete
Zoom Learning Center				Donote

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

ZOOM Products S	Solutions Resources Plans & I	Pricing	Schedule	Join Host ~	Web App ~
Room Management	Assign		arce T	Area 🗘	Туре
> Workspaces Management	Number	+1972-852-2663			
> Phone System Management	+195 CLI:	User	C - Premises Group: Avaya	United States	Toll
V Number Management	DN: -				
Phone Numbers	✓ +197	Yealink phoneuser - Ext. 1061, Main Site	DC - Premises	United States	Toll
Provider Exchange	CLI:	Save Cancel	Group: sip_gr		
> Account Management					
Advanced	+1972-403-4510	Normal 🗖 E	BYOC - Premises	United States	Toll

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.

ZOOM Products Solu	tions Resources Plans & Pricing
Dashboard > User Management	Company Info > Account Settings
 > Device Management > Room Management 	Settings Policy Block List Spam List External Contacts Emergency Services
Workspaces Management Phone System Management Users & Rooms	Add company contacts that are not Zoom Phone subscribers. These contacts will be added to the contacts directory and become accessible to Zoom Applications.
Auto Receptionists	Q Search by Name, Ext. or Number
Call Queues	
Shared Lines	
Group Call Pickup	
Phone Numbers	
Phones & Devices	
Monitoring	
Assets Library	
Logs	
Company Info	
> Number Management	

- 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) ⑦	Auto generation for default.						
Name	OSV_user1						
Email (Optional)							
Extension Number ⑦ (Optional)	2078						
Phone Number (?) (Optional)	Enter in the E.164 format. Separated by commas.						
Description (Optional)							
Routing Path (?) (Optional)	sip_group_OpenScape	8~					
Auto Call Recorded ?							
	Save	Cancel					

4. Click Save.

Provisioning Phones for Zoom Phone Users

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.

ZOOM Products Sole	lutions I	Resources	Plans & Pricing					S	chedule Join	Host ~ Web	App -
 Phone System Management Users & Rooms 	Ass	igned Una	ssigned								
Auto Receptionists	Not	e: Zoom Phone A	Appliance devices	can be assigned to Con	nmon Area. To manaj	ge Zoom Phone Ap	pliance, please go to	Device Manag	ement		
Call Queues		_									
Shared Lines	Ade	Export to C	sv 💿							Resync by Ac	count/Site
Group Call Pickup	Q 4	61			Device (All)	~ (Brand (All) 🗸 🧹	Status (All)	V Provision St	ta 🗸 Site (All)	
Phone Numbers											
Provider Exchange											
Phones & Devices	0	Display Name	Device Type	MAC Address	Assigned to	Status	Firmware Version	Site	IP Address	Hot Desking (Signed In)	Pr () Templa
Monitoring											
Assets Library		-				Last Provision					
Logs	0	Poly User	Poly vvx150	64-16-7f-fc-d0-dd	Ext. 4612	Date: Apr 23, 2024 (UTC)	6.4.6.2640	Main Site	14. 162 172 3		
Company Info						Provision Info					
> Account Management						Opliga					
> Advanced		III Yealink			Maniah Hang	Last Provision					
	0	User	Yealink t48u	80-5e-0c-54-5c-2b	Ext. 4511	Date: Apr 22, 2024 (UTC)	108.86.3.4	Main Site	172. 11		- (3)
https://zoom.us/pbx/page/telephone/group	s?p=groups					and the second second					

- 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. From the Route drop-down menu, select the Route_group_OpenScape (BYOC) group, created in Configuring the Route Group on page 11.
 - f. Click Save.

Δ

Add Device	2
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 Vealink phoneuser - Ext. 1084, Main S
	Add Cancel
Provision Template (Optional)	Not Set
	Save Cancel

Unify OpenScape Voice Configuration

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 Unify OpenScape Voice configuration for connecting to OpenScape SBC. The purpose of this connectivity is for Unify 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 Unify 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:	10.8.242.72 TCP 50010
ВСОМ	
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.**

Zoom Phone with OpenScape SBC and OpenScape Voice (Bring Your Own Carrier - BYOC)

5

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.

😒 [OSV] - [ZOOM_BG] - Add Endpoint	t Profile - Google Chrome	
A Not secure https://10.70.1	6.6/management/portal/Applicatio	or s/Operation/OSV/BusinessGroup/Profiles/PopUps/modif @
🥞 [OSV] - [ZOOM_BG] -	Add Endpoint Profile	()
() Please enter the profile dat	a.	
General Endpoints	Services	
Enapoint Profile		
 Please enter a unique name 	e to identify this profile.	
Name:	EPP_SBC01	
Remark:		
Numbering Plan:	NP_ZOOM_BG	
Management Information		
(i) Please enter the data for the	ne following fields in the correspor	onding screens.
Class of Service:		
Deuting Areas		
Routing Area:		
Calling Location:		
Time Zone:		
SIP Privacy Support:	Full	
		Save Cancel

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

3	🕙 [OSV] - [ZOOM_BG] - Add Endpoint Profile - Google Chrome										
▲ Not secure https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/Profiles/PopUps/modif ④											
	😂 [OSV] - [ZOOM_BG] - Add Endpoint Profile 🛛 👔										
(i	() Please enter the profile data.										
General Endpoints Services											
	•	Message Waiting:	Yes	$\overline{}$							
	٠	Call Transfer:	Yes	~							
	•	Call Forward Invalid Destination:	No	~							
	•	Toll and Call Restrictions:	No	~							
	•	Park to Server:	No	~							
	•	CSTA Network Interface Device:	No	~	Enable Name Provider and Limited Call Control						
					What to do if Application fails to handle inbound calls:						
					Allow call to proceed as norm 💙						
					•						
					Save						

- 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.

📀 [OSV] - [ZOOM_BG] - [Main Of	ffice] - Add Endpoint - Google Chrome 📃 👘 🔀									
A Not secure https://10.70.16.6/management/portal/_ns:YWE1NWIzZWVkLTVIZmItNDg2Ni0 @										
🖣 [osv] - [zoom_ве	3] - [Main Office] - Add Endpoint : EP_SBC01 🛛 👔 🕜									
General SIP Att	ributes Aliases Routes Accounting									
Endpoint										
Define the connection data of an endpoint, e.g. you may use this to add a gateway to a switch.										
Name:	EP_SBC01									
Remark:										
Registered:										
Profile:	EPP_SBC01									
Branch Office:										
Associated Endpoint:										
Default Home DN										
Location Domain										
Endpoint Template:	Central SBC									
Endpoint Type:	Central SBC									
Max number of users:										
1 11										
	Save Cancel									

- **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.

🕙 [(<mark>)</mark> SV] - [ZOOM_BG] - [Main Office] -	- Add Endpoint - Google Chrome								
▲ Not secure https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessG ④									
🖣 [OSV] - [ZOOM_BG] - [Main Office] - Add Endpoint 🛛 👔									
General SIP Attr	ributes Aliases	Routes Acco	unting						
			^						
SIP Private Networking:	0								
SIP Trunking:	۲								
SIP-Q Signaling:	0								
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. 									
Туре:	Static 🗸								
Signaling Address Type:	IP Address or FQDN	~							
Endpoint Address:	10.7 :								
Port:	5060								
Transport protocol:	TCP 🗸								

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

Image: spin start structure Image: spin									
General SIP Att	ributes Aliases Ro	utes 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:				I					
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	el					
- **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 Rout	tes Accounting
Attributes	
() Attributes available for this SIP endpoint	
Supports SIP UPDATE Method for Display Updates	
UPDATE for Confirmed Dialogs Supported	
Survivable Endpoint	
SIP Proxy	2
Central SBC	<
Route via Proxy	2
Allow Proxy Bypass	
Public/Offnet Traffic	
Accept Billing Number	
Enable Session Timer	
Ignore Answer for Announcement	
Enable TLS RFC5626 Ping	

Enable TLS Dual Path Method	
Ignore Receipt of 181 Call is Being Forwarded	
Use extended max, count for loop prevention	
Do Not Audit Endpoint	

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

General	d ATD Mellodar Alexan Davise Languilla	
General	II SIP AUTOULES Aldees Roules Accounting	
Aliases		
(i) You d	can associate here aliases with a SIP Endpoint.	
		Add Delete
Sel:0	I O (03/) - Add Alias - Geogle Chrome	
	▲ Not secure Https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/Members/Populos/bgmodifyAlia @	
0 🖍	[OSV] - Add Alias	
	(1) The Alias name can be 1 to 49 characters long.	
	Name: 10.	
	OK Cancel	
		Save Cance

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 64.

- 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	23
A Not secure https://10.70.16.6/mai	agement/portal/Applications/Operation/OSV/BusinessGroup/Profiles/PopUps/modif	Ð
🧶 [OSV] - [ZOOM_BG] - Add E	ndpoint Profile	2
() Please enter the profile data.		
General Endpoints Service	s	
Name:	EPP_Zoom	^
Remark:		
		I
Numbering Plan:	NP_ZOOM_BG	
Management Information		
() Please enter the data for the follow	ving fields in the corresponding screens.	
Class of Service:		
Routing Area:		
Calling Location:		J
Time Zone:		
SIP Privacy Support:	Full Receive	Ŧ
	Save Cance	

- 🕙 [OSV] [ZOOM_BG] Add Endpoint Profile Google Chrome A Not secure https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/Profiles/PopUps/modif... Ð 🥂 [OSV] - [ZOOM_BG] - Add Endpoint Profile (?) Please enter the profile data. General Endpoints Services Message Waiting: No ¥ ~ Yes Call Transfer: ٠ Call Forward Invalid Destination: No. ¥ No. ~ Toll and Call Restrictions: Park to Server: No ~ ~ CSTA Network Interface Device: No Enable Name Provider and Limited Call Control What to do if Application fails to handle inbound calls: Allow call to proceed as norm 🗸 4 II Cancel Save
- 4. In the Services tab, enable the Call Transfer option, by selecting Yes from the drop-down menu.

- 5. Click Save.
- 6. In the Unify OpenScape Common Management Platform, navigate to Configuration > OpenScape Voice > BusinessGroup > 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**.

🖻 [OSV] - [ZOOM_BG] - [Main Of	fice] - Add Endpoint - Google Chrome	
A Not secure https://10.3	70.16.6/management/portal/Applications/Oper	tion/OSV/BusinessGroup/Members/PopUps/modifyBGEndpoint.psml?callPointParam = tru \mathbf{Q}
	i] - [Main Office] - Add Endpoint	(?)
General SIP Att	ributes Aliases Routes Accour	- ting
Indpoint		
() Define the connection d	ata of an endpoint, e.g. you may use this to a	dd a gateway to a switch.
Name:	EP_Zoom_SP1	
Remark:		
Registered:		
Profile:	EPP_Zoom	
Branch Office:		
Associated Endpoint:		
Default Home DN		
Location Domain		
Endpoint Template:		
Endpoint Type:		
Max number of users:		
		Save

- 8. 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.

Not secure https://10.70.16.6/management/partal/Applications/Ob ration/OSV/BusinessGroup/Members/PopUps/modifyBGEndpoint.psml?calPointParametru	🔇 [OSV] - [ZOOM_BG] - [Main Off	fice] - Add Endpoint - Google Chrome	
OSV] - [ZOOM_BG] - [Main Office] - Add Endpoint General SIP Attributes Aliases Routes Accounting SIP Private Networking: SIP Trunking: SIP-Q Signaling PSignaling PSignaling Porthe stable Address of the SIP signaling interface can be specified in IP or FQQN format. Yore the stable Address of the SIP signaling interface can be specified in IP or FQQN format. Type: Stable Address or FQQN Port: S0001 Tansport protocol: SCOULT COUNT OF COUNT O	A Not secure https://10.7	70.16.6/management/portal/Applications/Op	Dperation/OSV/BusinessGroup/Members/PopUps/modifyBGEndpoint.psml?callPointParam=tru 🔍
General SIP Attributes Aliases Routes Accounting SIP Private Networking: SIP Trunking: SIP-Q Signaling: IP Signaling: IP Signaling: IP Signaling: IP Signaling: IP To the static Endopoints the address of the SIP signaling interface can be specified in IP or FQDN format. IP Note that the address of the SIP signaling interface can be specified in IP or FQDN format. IP Note that the address or FQDN IP net: S001 Tansport protocol: ICP <	🖣 [osv] - [zoom_bg	i] - [Main Office] - Add Endpoint	(?)
SIP Private Networking: SIP Private Networking: SIP Trunking: SIP-Q Signaling: For the static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format. The static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format. The static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format. The static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format. The static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format. The static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format. The static Interface can be specified in IP or FQDN format. The static Interface can be specified in IP or FQDN format. The static Interface can be specified in IP or FQDN format. The static Interface can be specified in IP or FQDN format. The static Interface can be specified in IP or FQDN format. The static Interface can be specified in IP or FQDN format. The static Interface can be specified in IP or FQDN format. The static Interface can be specified in IP or FQDN format. The static Interface can be specified in IP or FQDN format. The static Interface can be specified in IP or FQDN format. The static Interface can be specified in IP or FQDN format. The static Interface can be specified in IP or FQDN format. The static Interface can be specified in IP or FQDN format. The static Interface can be specified in IP or FQDN format. The static Interface can be specified in IP or FQDN format. Static Interface can be specified in IP or FQDN format. Static Interface can be specified in IP or FQDN format. Static Interface can be specified in IP or FQDN format. Static Interface can be specified in IP or FQDN format. Static Interface can be specified in IP or FQDN format. Static Interface can be specified in IP or FQDN format. Static Interface can be specified in IP or FQDN format. Static Interface can be specified in IP or FQDN f	General SIP Attr	ributes Aliases Routes Acco	counting
SIP Private Networking: SIP Private Networking: SIP Trunking: SIP-Q Signaling: To the static Endpoints the address of the SIP signaling interface can be specified in IP or FQON format. The static Endpoints the address of the SIP signaling interface can be specified unless the entry in the security section has first been removed. Type: Static Type: Static Type: Static S			
SIP Funking: SIP-Q Signaling: SIP-Q Signaling: For the stable Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format. Note that the address of the signaling interface cannot be modified unless the entry in the security section has first been removed. Type: Static Signaling Address: ID. Port: S0001 Tansport protocol: TCP Endpoint does not accept incoming TLS connections: SRTP media mode: Disabled Key Exchange Cancel	SIP Private Networking:	0	
SIP Trunking: SIP-Q Signaling: IP Signaling: Tor the static Endopoints the address of the SIP signaling interface can be specified in IP or FODN 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 Type: Static Signaling Address Type: IP Address or FQDN IO. Port: South address: IO. Port: South address: South address: Signaling Ts connections: SRTP media mode: Disabled Key Exchange Save			
SIP-Q signaling: IP Signaling: IP For the static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format. Note that the address of the signaling interface cannot be modified unless the entry in the security section has first been removed. Type: Signaling Address Type: IP Address or FQDN Signaling Address: 10. Port: 50001 Transport protocol: TCP Endpoint does not accept incoming TLS connections: SRTP media mode: Disabled Save Cancel	SIP Trunking:	۲	
SIP Signaling Image: Signaling interface cannot be modified unless the entry in the security section has first been removed. Type: Static Signaling Address Type: IP Address or FQDN Endpoint Address: 10. Port: 50001 Tansport protocol: TCP SRTP media mode: Disabled Save Cancel	SIP-Q Signaling:	0	
IP Signaling IP For the static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format. Note that the address of the signaling interface cannot be modified unless the entry in the security section has first been removed. Type: Static Signaling Address Type: IP Address or FQDN Endpoint Address: 10. Port: 50001 Transport protocol: TCP Endpoint does not accept incoming TLS connections: SRTP media mode: Disabled Save Cancel			
Note that the address of the signaling interface cannot be modified unless the entry in the security section has first been removed. Type: Static Signaling Address Type: IP Address or FQDN Endpoint Address: 10. Port: 50001 Transport protocol: TCP Endpoint does not accept incoming TLS connections: SRTP media mode: Disabled Save Cancel	For the static Endnoints	the address of the SIP signaling interface (e can be specified in IP or FODN format.
Type: Static Signaling Address Type: IP Address or FQDN Endpoint Address: 10. Port: 50001 Transport protocol: TCP Transport protocol: TCP SRTP media mode: Disabled Key Exchange Key Exchange Save	 Note that the address o has first been removed. 	f the signaling interface cannot be modified	ed unless the entry in the security section
Signaling Address Type: IP Address or FQDN Endpoint Address: 10. Port: 50001 Tansport protocol: TCP TCP Cancel SRTP media mode: Disabled Save Save Cancel	Туре:	Static 🗸	
Signaling Address ivpe: IP Address of FQUN Endpoint Address: 10. Port: 50001 Transport protocol: TCP Endpoint does not accept incoming TLS connections: SRTP media mode: Disabled Key Exchange Save Cancel	Cianalian Adduces Tours		
Endpoint Address: 10. Port: 50001 Transport protocol: TCP <	Signaling Address type:	IP Address of PQDN	
Port: 5001 Transport protocol: TCP Endpoint does not accept - SRTP media mode: Disabled Disabled - Key Exchange Save Cancel	Endpoint Address:	10.	
Transport protocol: TCP Endpoint does not accept incoming TLS connections: SRTP media mode: Disabled Key Exchange Image:	Port:	50001	
Iransport protocol: ICP Endpoint does not accept incoming TLS connections: SRTP media mode: Disabled Key Exchange Key Exchange Save Cancel		TCD	
Endpoint does not accept incoming TLS connections: SRTP media mode: Disabled Key Exchange Save Cancel	iransport protocoi:		
SRTP media mode: Disabled Key Exchange Save Cancel	Endpoint does not accept incoming TLS connections:		
SRTP media mode: Disabled Key Exchange Save Cancel			
Key Exchange	SRTP media mode:	Disabled	
Save Cancel	Key Exchange	~	
			Save Cancel

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

Unify OpenScape Voice Configuration

Key Exchange Mechanisms Supported:	▼
ANAT Support:	Disabled V
ICE Support:	Enabled V
DTLS Support:	Enabled V
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	
noae:	

9. 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 : SI	BC_Zoom_PSI	?
General SIP Att	ributes Aliases	Routes Accounting	9	
SRTP media mode:	Enabled	~		•
ANAT Support:	Enabled V			
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				-1
 Set the Realm, Usernam one. 	e and Password for digest	authentication or configure	e the signaling address as a truste	d
Trusted	Ports: 5060-5060	Edit		ļ
			Save	ncel

Unify OpenScape Voice Configuration

- **10.** 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	
Central SBC	
Route via Proxy	
Allow Proxy Bypass	
Public/Offnet Traffic	
Accept Billing Number	
Use Billing Number for Display Purposes	
Allow Sending of Insecure Referred-By Header	~
Override IRM Codec Restriction	
Transfer HandOff	

Do not send Invite without SDP

• Send International Numbers in Global number format (GNF)

Send Authentication Number in P-Asserted-Identity header	
Automatic Collect Call Blocking supported	
Enhanced Subscriber Rerouting	
Rerouting Forwarded Calls	
Rerouting Direct Incoming Calls	
Send International Numbers in Global Number Format (GNF)	
Do not Send Invite without SDP	
Do not send Diversion header	
Send Redirect Number instead of calling number for redirected calls	
Send domain name in From and P-Preferred-Identity headers	
Send P-Preferred-Identity rather than P-Asserted-Identity	

- Enable session timer
- Limited PRACK support

Enable Session Timer	
Ignore Answer for Announcement	
Enable TLS RFC5626 Ping	
Enable TLS Dual Path Method	
Ignore Receipt of 181 Call is Being Forwarded	
Use extended max, count for loop prevention	
Do Not Audit Endpoint	
Use Proxy/SBC ANAT settings for calls to subscribers	
Support for Callback Path Reservation	
Send Progress to Stop Call Proceeding Supervision Timer	
Limited PRACK Support	Z
Support Media Redirection	

- Support Replaces Header
- · Ignore Receipt/Do not send privacy header
- Enable REFER Notifications

Do not send Conference Indication (Hide isFocus)	
Do Not Allow Geolocation Info	
Ignore Location by Value on SIP INVITE/REINVITE	
Support Foreign Peer Domain	
Suppress Alert Info Auto Answer	
Support Replaces Header	
Ignore Receipt/Do not send Privacy Header	
Enable REFER Notifications	
History-Info Supported	
Increment SDP o-line	

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

Conoral	RID Attributes Alizzar Doutes Accounting	
General	SIP AUDULES Audes Accounting	
Allases		
 You ca 	n associate here aliases with a SIP Endpoint.	
		Add
Sel:0 I	🕲 [OSV] - Add Alias - Google Chrome	
	A Not secure https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/Members/PopUps/bgmodifyAlia @	
D 🏂	[OSV] - Add Alias	
	() The Alias name can be 1 to 49 characters long.	
	Name: [10.1	
	OK Cancel	
		Save Cancel

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

Document Version 1.3

5.1.3 Configuring the PSTN Endpoint



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 > 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				
A Not secure https://10.70.16.6/ma	inagement/portal/App	lications/Operation/OSV,	/BusinessGroup/Profiles/	PopUps/modifyEndPointProt	file.psml?callPoi 🔍
🥞 [OSV] - [ZOOM_BG] - Add	Endpoint Profile				?
() Please enter the profile data.					
General Endpoints Service	es				
() Please enter a unique name to ide	entify this profile.				ŕ
Name:	EPP_PSTN				
Remark:					
Numbering Plan:	NP_ZOOM_BG				
Management Information					
() Please enter the data for the follo	wing fields in the corr	esponding screens.			
Class of Service:					
Develop Anne.					
Routing Area:					
Calling Location:					
Time Zone:					
	(=				
SIP Privacy Support:	Full	V			
Failed Calls Intercent Treatment	Disabled	~			
					Save Cancel

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

S [0SV] -	[ZOOM_BG] - Add Endpoint Profile - Google	Chrome				
A	Not	secure https://10.70.16.6/manageme	nt/portal/Applica	tions/Op	eration/C	OSV/BusinessGroup/Profiles/PopUps/modif	⊕.
۲	[09	SV] - [ZOOM_BG] - Add Endpoi	int Profile				?
()	Plea	se enter the profile data.					
G	ienera	al Endpoints Services					
	•	Message Waiting:	No	~			
	٠	Call Transfer:	Yes	$\overline{}$			
	٠	Call Forward Invalid Destination:	No	•			
	٠	Toll and Call Restrictions:	No	•			
	٠	Park to Server:	No	•			
	•	CSTA Network Interface Device:	No	•		Enable Name Provider and Limited Cal	l Control
					What t	to do if Application fails to handle inboun	d calls:
					Allow o	call to proceed as norm 🗸	
(osV) - [ZOOM_BG] - Add Endpoint Profile Please enter the profile data. General Endpoints Services • Message Waiting: No V • Call Transfer: Yes V • Call Forward Invalid Destination: No V • Call Restrictions: No V • Toll and Call Restrictions: No V • Park to Server: No V • CSTA Network Interface Device: No V • Enable Name Provider and Limited Call Control What to do if Application fails to handle inbound calls: Allow call to proceed as norm V • Save Cancel							
•						Save Ca	ncel
(

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.

🌀 [OSV] - [ZOOM_BG] - [Main O	ffice] - Add Endpoint - Google Chrome	- 0 X
A Not secure https://10.	.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/Members/PopUps/modifyBGE	ndpoi 🔍
🖳 [OSV] - [ZOOM_ВО	G] - [Main Office] - Add Endpoint	?
General SIP Att	tributes Aliases Routes Accounting	
Endpoint		
() Define the connection of	data of an endpoint, e.g. you may use this to add a gateway to a switch.	_
Name:	EP_PSTN	
Remark:		
Registered:		
Profile:	EPP_PSTN	
Branch Office:		
Associated Endpoint:		
Default Home DN		
Location Domain		
Endpoint Template:		
Endpoint Type:		
Max number of users:		
- 1k]J.k	Save	Cancel

- 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 PSTN trunk.
 - f. From the Transport protocol drop-down menu, select TCP.
 - g. From the SRTP media mode drop-down menu, select Disabled.

🚱 [OSV] - [ZOOM_BG] - [Main Off	ïce] - Add Endpoint - Google Chrome			
A Not secure https://10.7	'0.16.6/management/portal/Applicat	ions/Operation	/OSV/BusinessGroup/Member	rs/PopUps/modifyBGEndpoi 🤅
■ <mark>.</mark> [OSV] - [ZOOM_BG] - [Main Office] - Add Endp	oint		?
General SIP Attr	ibutes Aliases Routes	Accounting		_
SIP Private Networking:	0			
SIP Trunking:	۲			
SIP-Q Signaling:	0			
SIP Signaling				
For the static Endpoints Note that the address of has first been removed.	the address of the SIP signaling int f the signaling interface cannot be r	cerface can be modified unless	specified in IP or FQDN forma the entry in the security sec	t. xion
Туре:	Static 🗸			
Signaling Address Type:	IP Address or FQDN	•		
Endpoint Address:	10			
Port:	50015			
Transport protocol:	TCP 🗸			
Endpoint does not accept incoming TLS connections:				
SRTP media mode:	Disabled 🗸			
Key Exchange Mechanisms Supported:	~			
				Save Cancel

h. From the SIP UA Forking Support drop-down menu, select None.

Unify OpenScape Voice Configuration

ANAT Support:	Disabled 🗸
ICE Support:	Enabled 🗸
DTLS Support:	Enabled 🗸
SIP VA 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	e and Password for digest authentication or configure the signaling address as a trusted one.
Trusted	Ports: All Edit
	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		
Control SBC		
Route via Proxy		
Allow Proxy Bypass		
Public/Offnet Traffic		
Accept Billing Number		
Une Dilling Muselson for Directory Durange		
Use Bliling Number for Display Purposes		
Allow Sending of Insecure Referred-By Header		
Override IRM Codec Restriction		
Transfer HandOff		

Do not send Invite without SDP

• Send International Numbers in Global number format (GNF)

Send P-Preferred-Identity rather than P-Asserted-Identity	
Send domain name in From and P-Preferred-Identity headers	
Send Redirect Number instead of calling number for redirected calls	
Do not send Diversion header	
Do not Send Invite without SDP	
Send International Numbers in Global Number Format (GNF)	
Rerouting Direct Incoming Calls	
Rerouting Direct Incoming Calls Rerouting Forwarded Calls	
Rerouting Direct Incoming Calls Rerouting Forwarded Calls Enhanced Subscriber Rerouting	
Rerouting Direct Incoming Calls Rerouting Forwarded Calls Enhanced Subscriber Rerouting Automatic Collect Call Blocking supported	

Enable session timer

Limited PRACK support

Unify OpenScape Voice Configuration

Enable Session Timer	
Ignore Answer for Announcement	
Enable TLS RFC5626 Ping	
Enable TLS Dual Path Method	
Ignore Receipt of 181 Call is Being Forwarded	
Use extended max. count for loop prevention	
Do Not Audit Endpoint	
Use Proxy/SBC ANAT settings for calls to subscribers	
Support for Callback Path Reservation	
Send Progress to Stop Call Proceeding Supervision Timer	
Limited PRACK Support	
Support Media Redirection	

Support Replaces Header

Enable REFER Notifications

Ignore Location by Value on SIP INVITE/REINVITE	
Support Foreign Peer Domain	
Suppress Alert Info Auto Answer	
Support Replaces Header	
Ignore Receipt/Do not send Privacy Header	
Enable REFER Notifications	
History-Info Supported	

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

General	SIP Attributes Aliases Routes Accounting			
Viases				
(i) You ca	an associate here aliases with a SIP Endpoint.			
				Add
Sel:0]	1 @ 1090 - Add Aliar - Google Chrome			
n	Not secure https://10.70.16.6/management/portal/Applications/Operation/OSV/	BusinessGroup/Members/PopUps/bgmodifyAlia @		
	[OSV] - Add Alias	(?)		
	(i) The Alias name can be 1 to 49 characters long.	Ű		
	Name: [10."			
	-	OK Cancel		
				Save

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.

Unify Ope	enScape C	lommon Manag	ement Platform						Domain: system User: administrator@system	
Configuration	1aintenance U	Jser Management Fault	Management Performance	Managemen	t Accounting					3
OpenScape Voice	OpenScape Bra	anch OpenScape SBC	Unified Communications	CMP	Device Management					
🔥 OSV	🗸 🚽 Los	V] - [ZOOM_BG] - [Main 0	ffice] - Endpoints							
Business Group	🖄 🛈 Endp	oints represent Network to Netw	ork Interface connections.							
Quick Tasks	Searc	ch for	in Endpoint Name		✓ Searce	h Show All	Advanced	l		
Business Group List	~								More ▼ Add	Edit Bulk Edit Clone
▶ General	Sel:1	Items/Page: 10 🗸 All:6			0001 - 1700M RG1	(Main Office) - Edit Endnointe	ED SPC01 - Google (hrom		
Profiles		Name 🔺	Numbering Plan Name		Reg A Not secure bt	tas: //10.70.16.6/manariem	ent/nortal/Applica	tions/Oneration/	SV/BusinessGroup/Members	/Popl Ins/modify/BGEndpoint.nsm
Teams	•	EP_OSB	NP_ZOOM_BG		Stat	OM BCI - EMain Offi	ool - Edit Endr	alot I ED CD	••••	G
 Statistics Display Number Modifica 	ation	EP_PSTN	NP_ZOOM_BG		Stat	OW_BO] - [Walli Offic	ce] - Eair Enap	Joint : EP_SBC	.01	C.
Branch Office List	addin 🔽 📲	EP_SBC01	NP_ZOOM_BG		Stat General SIP	Attributes Alia:	ses Routes	Accounting		
Main Office		EP_Zoom_SP1	NP_ZOOM_BG		Stat					
▼ Members	•	EP_Zoom_SP2	NP_ZOOM_BG		Stat Remark:			11		
III Subscribers	O 4.	EP_Zoom_SP3	NP_ZOOM_BG		Stat					
Endpoints					Registered.					
NR ZOOM BC (Default)	n List				Profile:	EPP_SBC01)		
Translation	, .									
Destinations and Routes					Branch Office:			ļ		
					Associated Endpoir	t:				
					Default Home DN					
					Location Domain					

- 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.

Unify OpenScape Common Management Platform Domain: system User administrat						tem strator@sy				
Configuration Maintenar	Configuration Maintenance User Management Fault Management Performance Management Accounting									
OpenScape Voice OpenS	cape Bra	anch OpenScape SBC	Unified Con	nmunications CMP	Device Mar	nagement				
	H LOS	V] - [700M BC] - [Main 0	ffice] - Endpoir	ate						
	· [05	v] - [200M_B6] - [main 0]	mce] - Enaboli	105						
	(i) Endp	oints represent Network to Netwo	ork Interface conne	ections.						
Ouick Tasks	Seard	h for	in	Endpoint Name	~	Search	Show All	Advanced	1	
Business Group List										-
ZOOM_BG V									More V	Add.
▶ General	Sel:1	Items/Page: 10 🗸 All:6							Test Audit	
► Profiles		Name 🔺	Numbering Pla	n Name	Registration T	Type	Registration S	tate	Periodic Audit Enable	
► Teams	o 🖡	EP_OS8	NP_ZOOM_BG		Static		Registered		Set to Normal	
Statistics	- ×.	EP_PSTN	NP_ZOOM_BG		Static		Registered		Change Branch Office	
Display Number Modification	Z .	EP_SBC01	NP ZOOM BG		Static		Registered			-
Branch Office List		EP Zoom SP1	NP ZOOM BG		Static		Registered			
Main Office V	0 P	EP Zoom SP2	NP ZOOM BG		Static		Registered			
Members	n #.	EP Zoom SP3	NP ZOOM BG		Static		Registered			
Endpoints		C. CroomCo. o					ring store of			
A Private Numbering Plan List										
NP_ZOOM_BG (Default) V										
Translation										
Destinations and Routes										

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:

Document Version 1.3

Zoom Phone with OpenScape SBC and OpenScape Voice (Bring Your Own Carrier - BYOC)

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.

S [05V] - [ZOOM_BG] - [NP_ZOOM_B	G] - Add Destination - Google	e Chrome		
A Not secure https://10.70.10	5.6/management/portal/A	Applications/Operation	/OSV/BusinessGroup/DestinationAndRout 🖻	2
🔩 [OSV] - [ZOOM_BG] -	[NP_ZOOM_BG] - A	dd Destination	(?)
() Destinations are used for ro	uting a call to an endpoi	nt.		
General Routes Rou	te Lists Destination	n Codes		
Name:	DST_Zoom			
is a Media Server:				
is Conference Focus Server :				
			Save)

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.

Unify OpenScape Common Management	Platform	Domain: system User: administrator@system	(O)(O)(O)
Configuration Maintenance User Management Fault Managemen	nt Performance Management Accounting		3 🖬 10 📕 5 🗮
OpenScape Voice OpenScape Branch OpenScape SBC Unified	Communications CMP Device Management		
05V Y 4 [OSV] - [ZOOM BG] - [NP ZOOM BG] - [estinations		0
Business Group	representing a gateway.		
Quick Tasks Search for	in Destination Name Search Show All		
🖑 Business Group List			Add Edit Delete
ZOOM_BG V			
► General Sel:1 Items/Page: 10 ▼ All:4	Ca (OSU - 1700M BG) - INP 700M BG) - Edit Destination: DST 7nom - Google Chrome		
Profiles Name 4	Not secure https://10.70.16.6/management/nortal/Annications/Operation/OSV/BusinessGroup/DestinationAnd	Rout @	
P Teams			
Statistics Dicplay Number Medification	- [USV] - [ZOOM_BG] - [NP_ZOOM_BG] - Edit Destination: DST_Zoom		
Branch Office List	(j) Destinations are used for routing a call to an endpoint.		
Main Office	General Routes Route Lists Destination Codes		
▶ Members	Routes	-	
🚜 Private Numbering Plan List	Multiple routes can be used for prioritizing the routes to the gateways		
🛣 NP_ZOOM_BG (Default) 🗸			
► Translation			
Destinations and Routes		alata)	
Destinations			
Routes			

- 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 	e destination with an endpoint representing a gate	eway.	
ID			
(i) The Route ID indicat	tes the priority level.		
ID:	1		
		🚱 [OSV] - Branch Office List - Google Chrome 📃 🖾	
Type:	SIP Endpoint 🗸	A Not secure https://10.70.16.6/management/portal/Applicati 🔍	
		🔡 Branch Office List 🕜	
SIP Endpoint:	· · · · · · · · · · · · · · · · · · ·	() Branch Office List	
		Business Group	
Restricts the traffic a	according to specified settings. Routes with the sa	Business Group: ZOOM_BG	
Signaling Type	Undefined 🗸	Branch Office List	
Bearer Capability:	Unassigned 🗸	Items/Page: 10 V All:1	
Destination Directory Num	hber	Branch Office Name	
Number of digits to (delete: Leading digits are cut off from the Director	v t Main Office	
 Digits to insert: the 	digit string is added to the beginning of the remai	nır	
Modification Type:	None 🗸		
		-	
		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:
 - a. From the Modification Type drop-down menu, select Number Manipulation.
 - **b.** From the **Number of digits to delete drop-down menu**, select the number of digits to cut off from the directory number.
 - **c.** From the **Digits to insert** drop-down menu, enter the digit string which gets added to the beginning of the remaining digits.
 - d. From the Nature of Address drop-down menu, select International.
 - e. Click Save.

S [OSV] - Endpoint List - Google Chrome				
Not secure https://10.70.16.6/management/portal/_ns:VTFi	() A route connects the destination with an endpoint representing a gateway.			
Select a Endpoint cut of the list	ID:	1		
Business Groun	Type:	SIP Endpoint		
, Business Group: ZOOM_BG V	SIP Endpoint:	EP_Zoom_SP1		
Endpoint List	Originator Attributes			
Items/Page: 10 V All:6	() Restricts the traffic acc	ording to specified settings. Routes with the same restrictions can be prioritized.		
Endpoint	Signaling Type	Undefined V		
	Bearer Capability:	Unassigned •		
O EP_SBC01	Destination Directory Numbe	er		
EP_Zoom_SP1	Number of digits to del Digits to insert: the dig	lete: Leading digits are cut off from the Directory Number. jit string is added to the beginning of the remaining digits.		
	Modification Type:	Number Manipulation 🗸		
	Number of digits to delete:	0		
	Digits to insert:	1		
	Nature of Address:	International V		
OK Cancel		Save		

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	General Routes Route Lists Destination Codes					
Routes						
(i) Multip	e routes can be used for priori	tizing the routes to the gateways.				
Sel:0 I	tems/Page: 10 🗸 All:3					
	ID 🛦	Endpoint	Route Type	Delete	Insert	Nature of Address
0 🐴	1	EP_Zoom_SP1	SIP-Endpoint	0	1	International
0 🐴	2	EP_Zoom_SP2	SIP-Endpoint	0	1	International
0 🐴	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:

General Routes Route Lists Destination Codes						
Route	Lists					
1	This list provides an overview of all routes with the same originating signaling type and bearer capability. Prioritization is possible.					
Ite	ems/Page: 10 👻 All:1					
	Originating Signaling Type	Originating Bearer Capability	Prioritized	Fallback to Local Numbe Plan	ering	
6	Unassigned	Unassigned		w Dialed Number	w Modified Number	
					Save Cancel	

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.

Document Version 1.3

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

S [OSV] - [ZOOM_BG] - [NP_ZOOM_BG] - Add Destination - Google Chrome		8				
A Not secure https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/Destination	AndRout	Ð				
📲 [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_RSIN						
is a Media Server:						
is Conference Focus Server :						
Save	2) Canc	cel				

- 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.

S [OSV] - [ZOOM_BG] - [NP_ZOOM_BG] - Edit Destination: DST_PSTN - Google Chrome					
A Not secure https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGro	ıp/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	A				
(i) 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.

S [OSV] - [ZOOM_BG] - [NP_ZOOM_BG] - Add Route - Google Chrome 📃 🖂					
A Not secure https://10.7	0.16.6/management/porta	l/Applications/Ope	ation/OSV/Bu 🔍		
🐴 [osv] - [zoom_вg] - [NP_ZOOM_BG] -	Add Route	?		
() A route connects the destination with an endpoint representing a gateway.					
ID					
() The Route ID indicates t	he priority level.				
ID:	1]			
Туре:	SIP Endpoint 🗸]			
SIP Endpoint:	EP_PSTN				
Originator Attributes					
 Restricts the traffic acco can be prioritized. 	rding to specified settings	. Routes with the s	ame restrictions		
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 🗸				
		L	Save Cancel		

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.

🔄 [OSV] - [ZOOM_BG] - [NP_ZOOM_E	3G] - Add Destination - Google Chrome	
A Not secure https://10.70.1	.6.6 /management/portal/Applications/Operatio	1/OSV/BusinessGroup/DestinationAndRout 🍳
📲 [osv] - [zоом_вG] -	[NP_ZOOM_BG] - Add Destination	0
(i) Destinations are used for ro	outing a call to an endpoint.	
General Routes Rou	ite Lists Destination Codes	
Name:	DST_Zoom_ext	
is a Media Server:		
is Conference Focus Server :		
		Save

- 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.

Configuration Maintenance User Management Fault Man	agement Performance Management Accounting	3 🗰 30 🗰 6 🚍
OpenScape Voice OpenScape Branch OpenScape SBC	Unified Communications CMP Device Management	
	.BG] - Destinations	0
Outinations are used to route a call to an Business Group Quick Tasks Search for	(2) 1094 - 1000K-1994 - 1994 - 2000K-1991 - Fair Strationation 1517, Zonew, xet - Gangle Chrome. (- O X A Net secure Https://10.70.15.6/management/partal/kgalcations/Operations/OPV/ScoressOPmot/Pattons/ScoressOPmot/Pattons/OPV/ScoressOPmot/Pattons/OPV/ScoressO	
Sections: Comp List ZOOM, BG Comp List Command Section Section		Edit Delete d Routes
Members Monitors M	Lift. [jaketa	

Document Version 1.3

- 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.

 A route connects the destination with an endpoint representing a gateway. 				
ID				
(i) The Route ID indicates t	the priority level.			
ID:	1			
Type:	SIP Endpoint 🗸			
SIP Endpoint:	EP_Zoom_SP1			
Originator Attributes				
 Restricts the traffic according be prioritized. 	ording to specified settings. Route:	s with the same restrictions can		
Signaling Type:	Undefined 🗸			
Bearer Capability:	Unassigned 🗸			
Destination Directory Number	-			
Number of digits to dele Digits to insert: the digits	ete: Leading digits are cut off from t string is added to the beginning	the Directory Number. of the remaining digits.		
Modification Type:	Number Manipulation 🗸			
Number of digits to delete:	6			
Digits to insert:				
Nature of Address:	Unknown 🗸			
		Save		

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:

()	🖉 (OSV) - [ZOOM_B6] - [NP_ZOOM_B6] - Edit Destination: DST_Zoom_ext - Google Chrome 📃 🔍						I X	
A	A Not secure Https://10.70.16.6/management/portal/_ns:YWQ1NzJxNTU0LWZkYTYtNDc0NS1hZGM0LTQ2YzFjY2JxOTdhMi5sX19kNTcyMTU1NC1mZGE2LTQ3NDUtYWRjNC00NmMxY2NiMTk3YTIuc						c Q	
-4	[osv] - [ZOOM_BG]	- [NP_ZOOM_BG] - Edit Destinat	tion: DST_Zoom_ext				?
1	Destin	ations are used for r	outing a call to an endpoint.					
Ge	neral	Routes Ro	ute Lists Destination Codes					
Route	s							-
1	Multipl	e routes can be use	d for prioritizing the routes to the gatev	ways.				
	Add Edit Delete					te		
S	el:0 D	ems/Page: 10 🗙	All:3					
		ID 🔺	Endpoint	Route Type	Delete	Insert	Nature of Address	
	4	1	EP_Zoom_SP1	SIP-Endpoint	6		Unknown	
	4	2	EP_Zoom_SP2	SIP-Endpoint	6		Unknown	
	4	3	EP_Zoom_SP3	SIP-Endpoint	6		Unknown	_

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

Ge	neral Routes Ro	oute Lists Destination (Codes		
Route	Lists				
()	This list provides an overv possible.	iew of all routes with the sa	me originating	signaling type and bearer	capability. Prioritization is
It	ems/Page: 10 🗸 All:1				
	Originating Signaling Type	Originating Bearer Capability	Prioritized	Fallback to Local Numbe Plan	ring
6	Unassigned	Unassigned		w Dialed Number	w Modified Number
					Save Cancel

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.

Remark:				
		1		
Nature Of Address:	International			
nator Attributes				
Optionally, an additiona	al match is required if the ori	iginator of the call belongs to t	e specified Class of Service and Routin	g Area.
Class Of Service:				
Routing Area:				
с Туре				
Specify the traffic type '	for this destination code.			
ine	۲			
e Local Toll Table	0			
lect Traffic Type	0			
ination				
Specify additional para	neters to determine how th	e call will be routed.		
Destination Type:	Destination	~		
Destination:	DST_Zoom			
DN Office Code:				

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 m	natch this code, the specified modification to these dialed digits is executed.
Prefix Access Code:	1214
Remark:	
Minimum Length:	10
Maximum Length:	20
Digit Position:	0
Digits to insert:	
Settings	
() Specify additional pa	arameters to determine how the call will be routed.
Prefix Type:	Off-net Access 🗸
Nature of Address:	International V
Destination Type:	None v
Destination:	
	Save

- 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.

🔩 [osv] - [zoom_bg]] - [NP_ZOOM_BG] - Edit Destination Code: 1214	?
() This destination code will	l be used for a call if the dialed or modified (in PAC) digits and the Nature of Address are matching.	
Destination Code:	1214	
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 fo	r this destination code.	
None (
Use Local Toll Table (0	
Select Traffic Type (0	
Destination		
(j) Specify additional parame	eters to determine how the call will be routed.	
Destination Type:	Destination	
Destination:	DST_PSTN	
DN Office Code:	· · · · · · · · · · · · · · · · · · ·	
		Save Cancel

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 Setting	s				(?)
(j) SIP Settings					
General Rerouting Audi	t SIP Timers	DTLS Interwo	orking SRTP Inte	erworking	
ICE Support AEI Support	FQDN ANAT	Interworking	Responsible Doma	ains SIP UA Fo	rking
(j) SIP UA Forking Configuration					
ninger start	_				
OSV Passive Forking: Enabled	~				
SIP UA Forking Devices					with the ore
UA Proxy Capability setting.	n present in the UA	header will cause t	he registering device b	e accounted as comp	atible with the SIP
				Add	Edit Delete
Sel:0 Items/Page: 10 🗸 All:0	ļ.				
Device Identifier		SIP UA For	king 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.

Document Version 1.3

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:



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.

🕑 [IVIgmtTest42] - Display I	Number Modification - Google Chrome — 🛛 🗙
Not secure https://	10.14.254.6/management/portal/Applications/Operation/OSV/Busi
😫 [MgmtTest42]-D	isplay Number Modification 📀
i Create/Edit the "calling	g party display number" to a specific format
Originating Context Setting	
(j) Select a business grou	ip and/or numbering plan from the list.
Business Group	Zoom_BG
Numbering Plan	NP_Zoom_BG
Terminating Context Setting	
(j) Select a numbering pl	an 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 N Source), what the form needs to be added and	umber, Priority and define which number needs to be put out (Number nat is (Output TON), how to optimize it (Optimize TON) and whether a prefix d 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

Document Version 1.3
- **4**. Repeat the steps for the remaining Zoom endpoints.
- 5. ClickSave.

Unify OpenScape SBC Configuration

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.

B 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 BYOC/BYOP licenses will NOT BE NEEDED as part of the Zoom subscription.

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. The OpenScape SBC is not a B2BUA and has limited SIP message manipulation capabilities. The OpenScape Voice IP-PBX provides call routing, enhanced SIP message manipulation, and number modification facilities. 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

Zoom Phone with OpenScape SBC and OpenScape Voice (Bring Your Own Carrier - BYOC)

6

Unify OpenScape SBC Configuration

Items	Example
SBC Public FQDN	sbc01.athdrlabs.xyz
OS Voice node 1 (SIP Signaling) IP	10.8.242.16 TCP 5060
OS Voice node 2 (SIP Signaling) IP	10.8.242.26 TCP 5060
Zoom IP 1 SIP trunk	162.12.233.59 (see note)
	TLS 5061 (LAN port for OS Voice trunk 50001)
Zoom IP 2 SIP trunk	162.12.232.59 (see note)
	TLS 5061 (LAN port for OS Voice trunk 50002)
Zoom IP 3 SIP trunk	162.12.235.59 (see note)
	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 T ype	Protocol	Source	Destination Ports	Destination IPs	Region
				162.12.233.59	

Traffic T ype	Protocol	Source	Destination Ports	Destination IPs	Region
				162.12.232.59	North America
				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	5061	103.122.166.248	Australia
		SBC		103.122.167.248	
				149.137.41.246	APAC
				207.226.132.198	
				209.9.211.198	нк
				101.36.167.237	HK2
				149.137.25.246	Japan
				207.226.132.198	

Table 3: Media Traffic IPs

Traffic T ype	Protocol	Source	Destination Ports	Destination IPs	Region
				162.12.232.0/24	

Document Version 1.3

Zoom Phone with OpenScape SBC and OpenScape Voice (Bring Your Own Carrier - BYOC)

Traffic T ype	Protocol	Source	Destination Ports	Destination IPs	Region
				162.12.233.0/24	North America
				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	20000-64000	103.122.166.0/24	Australia
		SBC		103.122.167.0/24	
				149.137.41.0/24	APAC
				207.226.132.0/24	
				209.9.211.192/26	нк
				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.

OpenScape Se Management Portal	ession Border (Controller						
Administration	General - OSS							
► System	SBC aggregated information and data.							
▼ Network/Net Services Settings	Alarms							
DNS	Alarm summary: Critic	al: 0 📕 Major: 1 📕 Mi	nor: 0 📕 Show alarm det	ails				
Traffic Shaping	System Status				େ 🕐			
QoS	Denote the	0		20				
► VoIP	Branch mode	Centralized SBC	Auto refresh timer	30 seconds	~			
Features	Operational state	normal						

- 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.

Network/Net Services					?					~ E # U • 3
Select OK to temporarily store of	hanges. Make your cha	anges permanent by s	electing 'App	ly Changes' on the Genera	al					Learn more ×
	raffic Shaping Qo	s		, j en ange		P	roduct name Unify Ope	nScape SBC	User name : administrator	(?)
Single armed					^					\odot
□ Interface bonding										
Interface Configuration					?					
										ে 🖓
Core realm configuration						ails				
				Add Delete						ୁ ଜ ଜ
IP address	Subnet mask	Signaling Media	SIP-UDP	SIP-TCP SIP-TLS						
10.70.16.25	255.255.255.0	2 2	5060	5060 5061 ^		30 seconds	~			
				Ok Can	icel	Active				
	Com Node 2									
	Primary server			Penalty box state						
	Backup server			Penalty box state						
								_		
									Apply Changes	Cancel Changes

- 3. In the Network/Net Services window, under the Settings tab, locate the Access and Admin realm configuration area.
- 4. Click Add. 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.

Network	/Net Services																		0
() Select (OK to temporarily store	e changes. Make your	changes pe	rmanent by sele	cting 'Apply Chang	es' on the	General pa	ige.											
Settings	DNS NTP	Traffic Shaping	QoS																
Access ar	nd Admin realm configu	uration																	
																		Add De	lete
1						VLAN									Messa	Trust	Signaling		
	Type	Network ID	Interface	IP address	Subnet mask	tag	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	SIP-MTLS	MGCP	SIP serv	er limit (sec)	level	restriction		
	Main IPv4	Main-Access-IPv4	eth1	192.1	255 255 255 224	0	2	~	5060	5060	5061	5161	2727	Node	1 100	N/A	Unrestricted		
Realm Pr	ofile																		0
_																		() (.	
_																		Add	lete
	Rea Main-Core-Re	ilm profile	Realm	Signaling ne	etwork ID	Media	network ID	F	Forward netw	vork ID									
	Main-Access-Re	alm - ipv4	access	Main-Acc	ess-IPv4	Main-A	ccess-IPv4												
			_			_	_	_							_	_			
Routing			-	-		-	-	-	_	_	_	_	_	_	-	-	_		
																		Ok	Cancel

- 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.

OpenScape Session Border Controller Product name Unify OpenScape SBC Management Portal										
Administration	General - OSS									
► System	 SBC aggregated inf 	ormation and data.								
Network/Net Services	Alarms									
▼ VolP Sip Server Settings	P Server Settings Alarm summary: Critical: 0 Major: 1 Minor: 0 Show alarm details									
Media	System Status									
QoS Monitoring Features	Branch mode	Centralized SBC	Auto refresh timer	30 seconds V						
Security	Operational state	normal								
Diagnostics & logs										
Alarms										

- 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 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).

VOIP	0			ч E н Ш .
Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' c	on the General			Learn more
Sip Server Settings Port and Signaling Settings Media QoS Monitoring		Product name Unify OpenScape SBC	User name : administrator	(?) ()
General	0			$\bigcirc \bigcirc$
Comm System Type Simplex				
Allow Register from SERVER				C ()
Other trusted servers		ails		
Node 1	?			Q ()
Target type Binding		30 seconds		
Primary 10.70.16.12 Transport TCP V Port 5060				
Backup server Transport TCP V Port				
SRV Transport TCP				
		Active		
NODE 2	()			
Target Rinding				
le la	OK Cancel			
		,		

- 3. Click OK.
- 4. Click Apply Changes.



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/hiq8000 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 Zoom's trusted Certification Authorities.

Document Version 1.3

Apply Changes

Cancel Changes

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.

OpenScape Sessi Management Portal	on Border Controller	Ρ	roduct name
Administration	OSS - Security - Google Chrome A Not secure https://10.70.16.25/security.html?tabId=generalTab	<u> </u>	
 System Network/Net Services VolP 	Security Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.	0	
Features ▼ Security	General Firewall Message Rate Control RADIUS Tunnel Connections Denial of Service Mitigation		
General Firewall	Certificates	?	
Message Rate Control RADIUS Tunnel Connections	Ecriticate management	0	
Denial of Service ▶ Diagnostics & logs	Enable PKI configuration PKI configuration		s 6:18
Alarms			

- 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.

Petriteses Island	0
Upload CA certificate file Choose File No file chosen Upload	
CA certificates	
CA1 pem ^ Delete combined-a-bundle pem	
DigGertSideal371.SF8ASH4258200CA1- DigGertSideal6712.SF8ASH4258200CA1-	
Gol addy_root_CAgem Gradady_senueCAgem	
serverCApem	
X 509 Certificates	
Upload X 509 certificate file Choose File No file chosen Upload	
X 509 certificates	
d#4504c=72df302 gem * Delete serverent pem	
Key Files	
Lichard Kar / Be Choose Edia No Kie choose Upload	
	OK Cancel

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.

Certificate Profile	0
 Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page. 	
Certificate Profile configuration	?
Certificate profile name iZoom_cert_profile	
Certificate service SIP-TLS V	
Local clert certificate file Show.	
Local server certificate file db450/4c73df5002 perm 👻 Show	
Local CAfile Go_dady_root_CAperr V Show	
Remote CAfile Show	
Local key file zoomcert key 🗸	
EC param secp256r1	
Attach to Config file	
Validation	0
Certificate Verification None	
Revocation status	
ldentity Check	
Renegotation	0
Enforce TLS session renegotation	
TLS session renegotation interval (minutes) 60	
TLS version	0
Minimum TLS version TLS V12	
DLS version	(\mathbf{r})
Opner Suites	U U
	OK Cancel

- 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.

🖭 OSS - Certificate Management	- Google Chrome					00	8					
A Not secure https://10.	70.16.25/certConfig.html						Q					
Certificate Managem	ent					(?					େ (
() Select OK to tempora	rily store changes. Make	e your changes permane	ent by selecting 'Apply Change	s' on the General page.								
Service API certificate prof	file Service API Defau	ult 🗸					*					
								System Info				୦ (
Certificate Profiles						U	2	CPU		2.17 % - 2 × 2700 MH	Iz (0 MHz Reserved in VM)	
				Add	Edit	Delete		Memory		15.8% - 4 Gb (4 Gb	Reserved in VM)	
											(000110011111)	
Name	Certificate service	Client certificate file	Server certificate file	Local CA file	е	Rem		Disk		12.09 % - 42 Gb		
HTTPS System	HTTPS		server.ort					System uptime	36 days 6:45			
IOS Push Default	IOS Push							Hardware type	Virtual OSS 250			
Android Push Default	Android Push							Hostname	OSS			
Service API Default	Service API		server.crt					Software Info-	sion	V11 R1.00.00		
Zoom_cert_profile	SIP-TLS		d64504cc73df5302.pem	Go_daddy_root_CA.pen	n	•		Software Par	tition information	Active Backup		
•				_		•						
Certificate Creation						0						
Create New TLS Certificat	tes											
Name	CAfi	le Self signed	✓ Create									
Contification Lipland					_	0						
Continuates opioad					_	\odot						
CA Certificates							1					
Linioad CA certificate file	Choose File No file ch	usen U	oload				¥					
					ОК	Cancel						
								,			Apply Changes	Cancel Changes

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.

OpenScape Ses Management Portal	ssion Border (Controller		Product name Unify OpenScape SBC		
Administration	General - OSS					
System	(i) SBC aggregated inf	ormation and data.				
Network/Net Services Alarms						
Features	Alarm summary: Criti	cal: 0 📕 Major: 1 📕	Minor: 0 <mark> Show alarm</mark>	details		
 Security Diagnostics & logs 	System Status					
Alarms	Branch mode	Centralized SBC	Auto refresh timer	30 seconds 🗸		
r wantenance	Operational state	normal				

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

2. Check the Enable Codec Support for transcoding checkbox.

Features		?
(i) Select OK to temporarily store changes	s. Make your changes permanent by selecting 'Apply Changes' on the General page.	
Features configuration		0
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 C	ancel

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	
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 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

decs			ຈ			« 8 8 1
	un antication alegan a Malagoria					Learn mo
Select OK to ten	nporarily store changes, make your	manges permanent by selecting Apply changes on the General	^	Product name Unify OpenScape SBC	User name : administrator	(?) (()
Enable	Codecs					
	G711A 8 kHz - 64 kbps	*				
	G711U 8 kHz - 64 kbps					
✓	G722 8 kHz - 64 kbps					
	G7221 16 kHz - 24Kbps					
	G7221 16 kHz - 32Kbps					<u></u>
	G7221C 32 kHz - 24Kbps		jile			
	G7221C 32 kHz - 32Kbps					
Z	G729 8 kHz - 8 kbps					୯
	OPUS 48 kHz - Variable					
	iLBC 8 kHz - Variable		30 seconds	÷		
	iSAC 16 kHz - Variable					
		OK Cancel	Active			
	Com Node 2					
	Primary server	Penalty box state				
	Backup server	Penalty box state				
					Annhy Charges	Canaal Charge
					Apply Changes	Cancel Chang

- 1. Click OK.
- 2. Click Apply Changes.

6.4.2 Configuring the Zoom Media Profile

The communication between the SBC 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.

OpenScape Sess	sion Border Co	ontroller		Product name Unify OpenScape SBC		
Administration	General - OSS					
► System	(i) SBC aggregated information and data.					
Network/Net Services	Alarms					
Sip Server Settings	Alarm summary: Critical	: 0 📕 Major: 1 📕	Minor: 0 Show alarm det	ails		
Media	System Status					
QoS Monitoring Features	Branch mode	Centralized SBC	Auto refresh timer	30 seconds V		
Security	Operational state	normal				

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

VOIP								
i Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General								
Sip Server Settings	Port and Signaling Settings	Media QoS Monitorii	ng					
User agent		mediaProfile						
			A					
			•					
4			+					
Madia Profiles			0					
Media Fromes			\bigcirc					
			Add Edit Delete					
		SRTP crypto context						
Name	Media protocol	negotiation	Mark SRTP Call-leg as Secure					
default	Best Effort SRTP	mikey + sdes						
webrtc_default	SRTP only	dtls	ø					

3. Locate the Media Profiles area and click Add.

- **4.** In the **Media Profile** pop-up, 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

Media Profile				0
 Select OK to temporarily store changes. Make you 	r changes permanent	by selecting 'Appl	y Changes' on the General p	lage.
General				0
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 SD	Р			
SRTP configuration				0
SRTP crypto context negotiation 🛛 MIKEY 🗹 SDB	es 🗆 dtls 🛛 sde	S Both 🔹	 Image: A set of the set of the	
Mark SRTP Call-leg as Secure				

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

6. 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:

RTCP configuration		(2	
RTCP Mode Alway	s generate 🗸		ে ি) System Info C 🕐 🕐
RTCP generation timeout 4			~	CPU 2.18 % - 2 × 2700 MHz (0 MHz Reserved in VM)
Codec configuration		(2	Memory 15.01 % - 4 Gb (4 Gb Reserved in VM)
				Disk 12.09 % - 42 Gb
Allow unconfigured codecs				System uptime 31 days 22:30
 Enforce codec priority in prof 	ile			
Send Telephony Event in Invit	te without SDP			Hardware type - Virtual OSS 250
 Use payload type 101 for tele 	phony event/8000			Hostname OSS
 Enforce Packetization Interva 	al			Software Info
Codec G722 8 kHz - 64 kbps	✓ Add			Software version V11 R1.00.00
				Software Partition information
		Move up Move down Delete		ACUVE
Priority	Codec	Packetization interval		
1	G711A8 kHz - 64 kbps	Auto	*	
2	G711U 8 kHz - 64 kbps	Auto		
			-	
4		,		
			_	
		OK Can	el	Apply Changes Cancel Changes

- 7. Click OK to return to the Media window.
- 8. Click OK on the VoIP window.
- 9. 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.

1. Navigate to the Unify OpenSape SBC Management Portal > VOIP > Media window.

OpenScape Ses Management Portal	Product name Unify OpenScape SBC			
Administration System Network/Net Services VoIP Sip Server Settings Port and Signaling Settings	General - OSS SBC aggregated infor Alarms Alarm summary: Critica	mation and data. al: 0 <mark>–</mark> Major: 1 <mark>–</mark>	Minor: 0 🧧 Show alarm de	tails
Media	System Status			
QoS Monitoring Features	Branch mode	Centralized SBC	Auto refresh timer	30 seconds V
Security	Operational state	normal		

2. 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.

VOIP			0
(i) Select OK to tempora	rily store changes. Make your cl	nanges permanent by selecting	g 'Apply Changes' on the General
Sip Server Settings	Port and Signaling Settings	Media QoS Monitori	ing
User agent		mediaProfile	A
			*
			*
4			. →
Madia Drofilaa			
Media Promes			\bigcirc
			Add Edit Delete
		SRTP crypto context	
Name	Media protocol	negotiation	Mark SRTP Call-leg as Secure
default	Best Effort SRTP	mikey + sdes	
webrtc_default	SRTP only	dtis	2

- 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 of	changes permanent by selecting 'Apply Changes' on the General page.	
General		?
Name	PSTN_Media_profile	
Media protocol	RTP only	
Support ICE	Full V	
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 V	
Mark SRTP Call-leg as Secure		
RTCP configuration		?
DTCD Made		
DTOD execution times at 1		
RICP 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.

I Allow unconfigured codes Enforce codes priority in profile Enforce codes priority in profile Send Tiephony Event in Note without SDP Use payload type 101 for telephony event/8000 Enforce Packetization Interval Codec Move up Move down Deletete Priority Codec Priority Codec Priority Codec Packetization Interval Code Priority Code Packetization Interval Code Code Priority Code Packetization Interval Code Priority Code Packetization Interval Code Code Priority Code Packetization Interval Code Code Code Code Code Code Code Code <t< th=""><th>Lodec contiduration</th><th></th></t<>	Lodec contiduration	
Import Allow unconfigured codec Import Allow unconfigured codec Import Allow unconfigured codec Send Telephony Event Instru without SDP Use payload type 101 for telephony event/8000 Import Allow unconfigured codec Import Allow		Disk 12.09 % - 42 Gb
Enforce codec protify in profile Enforce Codec protify in profile Use payload type 101 for telephony event08000 Enforce Packetization interval Codec Add Software land Software version V11 R1 00 00 Software version V11 R1 00 00 Software Virtual OSS 250 Hourse of Codec Hourse of Codec Profile Profile For Codec Packetization interval Codec Codec Codec Packetization interval Codec Codec Codec Packetization interval Codec	Allow unconfigured codecs	System uptime 31 days 22:49
Send Telephony Event in Invite without SDP De payload type 101 for telephony event@000 Enforce Packetzation Interval Codec Move up Move down Delete Priority Codec Payload type 101 In 814z - 64 kops Auto 3 G7120 814z - 64 kops 4 O728 814z - 64 kops 4 O728 814z - 64 kops 4 O728 814z - 64 kops Auto 4 O728 814z - 64 kops 4 O728 814z - 64 kops <th>Enforce codec priority in profile</th> <th></th>	Enforce codec priority in profile	
Use payload type 101 for telephony event@000 Codec Codec Move up Move down Deletete Priority Codec Priority <th>Send Telephony Event in Invite without SDP</th> <th>Hardware type - Virtual USS 250</th>	Send Telephony Event in Invite without SDP	Hardware type - Virtual USS 250
Enforce Packetization Interval Codec Move up Move down Delete Priorithy Codec 1 G711A 8147z-64 kbps 2 G711U 8147z-64 kbps 3 G722 8147z-64 kbps 4 G728 8147z-84 kbps 4 G728 8147z-84 kbps 4 G728 8147z-84 kbps	Use payload type 101 for telephony event/8000	Hostname OSS
Codec Nove up Nove down Delete Priority Codec Pecketzani interval 1 G711A 81Hz - 64 kbps Auto 2 G7110 8Hz - 64 kbps Auto 3 G722 81Hz - 64 kbps Auto 4 G723 81Hz - 84 kbps Auto	Enforce Packetization Interval	Software Info
Move up Move down Delete Priority Codec Pecketzation interval 1 G711A B14z - 64 kbps Auto 2 G711U 814z - 64 kbps Auto 3 G722 814z - 64 kbps Auto 4 G729 814z - 84 kbps Auto	Contec V Add	Software version V11 R1.00.00
Move up Move down Delete Priority Codec Packetization interval 1 G711A8 lkHz. 64 kbps Auto 2 G711U 8 kHz 64 kbps Auto 3 G7122 8 kHz. 64 kbps Auto 4 G728 8 kHz. 64 kbps Auto		Software Partition information
Priority Codec Packetization interval 1 GT11A 8/47z - 64 kbps Auto 2 GT11U 8/47z - 64 kbps Auto 3 GT22 8 /47z - 64 kbps Auto 4 G729 8 /47z - 8 kbps Auto 4 G729 8 /47z - 8 kbps Auto		Active
Priority Codec Pscelutzation interval 1 OT1A B14764 ktops Auto 2 G7110 B147_e 64 ktops Auto 3 G7122 B147_e 64 ktops Auto 4 O728 B147_e 76 ktops Auto		
1 G7110 8 H/z - 64 kbps Auto 2 G7110 8 H/z - 64 kbps Auto 3 G722 8 H/z - 64 kbps Auto 4 G729 8 H/z - 8 kbps Auto	Priority Codec Packetization interval	
2 G7110 8 Hz - 6 Hxbps Auto 3 G722 8 Hz - 6 Hxbps Auto 4 G728 8 Hz - 8 Hxbps Auto 	1 G711A8 kHz - 64 kbps Auto]
3 G722 814tz - 64 kbps Auto 4 G728 814tz - 8 kbps Auto 	2 G711U 8 kHz - 84 kbps Auto	
4 G729 8 KHz - 8 Kbps Auto	3 G722 8 kHz - 64 kbps Auto	
	4 G729 8 kHz - 8 kbps Auto	
	· · · · · · · · · · · · · · · · · · ·	
	OK Cancel	Annhy Changes Connert Changes
Apply changes Cancel changes		Apply changes

6.4.4 Configuring the Unify OpenScape Voice Media Profile

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

OpenScape Ses Management Portal	Product name Unify OpenScape SBC			
Administration	General - OSS			
► System	(i) SBC aggregated inform	nation and data.		
Network/Net Services VoIP Sip Server Settings	Alarms			
	Alarm summary: Critical	I: 0 📕 Major: 1 📕	Minor: 0 <mark> Show alarm de</mark>	tails
Media	System Status			
QoS Monitoring Features	Branch mode	Centralized SBC	Auto refresh timer	30 seconds V
Security	Operational state	normal		

- 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.

VOIP			0
i Select OK to temporarily sto	re changes. Make your chan	ges permanent by selecting 'A	opply Changes' on the General
Sip Server Settings Port	and Signaling Settings	Media QoS Monitoring	
User agent		mediaProfile	
			*
4			- F
Media Profiles			(?)
			Add Edit Delete
Name	Media protocol	SRTP crypto context negotiation	Mark SRTP Call-leg as Secure
default	Best Effort SRTP	mikey + sdes	
webrtc_default	SRTP only	dtis	۷

- 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.

Media Profile			\bigcirc	чых п ■ :
 Select OK to temporarily store char 	nges. Make your changes permanent by selecting 'A	pply Changes' on the General page.		Learn more X
General		Q	n	Product name Unify OpenScape SBC User name : administrator () (()
Name	OSV_MP			\odot
Media protocol	RTP only	 Direct Media Support 		
Support ICE	Full 🗸	_		
Support NGTC Trickle ICE				ତ ହ
Enable NGTC WebRTC Compatibilit	Y			
Enable TURN Client			l	
RTP/ RTCP Multiplex in offer			C ()	System Info 🖓 🖓
SDP Compatibility Mode			~	CPU 2.18 % - 2 × 2700 MHz (0 MHz Reserved in VM)
Support Mid Attribute				Memory 15.96 % - 4 Gb (4 Gb Reserved in VM)
Do not set port to zero on session tir	mer answer SDP			Disk 12.09 % - 42.Gb
SRTP configuration		0		Sustam untime 31 days 32:10
SRTP crypto context neoptiation	WKEY SDES DTLS SDES Both	*		System upon el si bays 20.10
Mark SRTP Call-leg as Secure				Hardware type – Virtual USS 250
				Hostname OSS
RTCP configuration		(r	2	Software Info
RTCP Mode Bypass	~			Software version V11 R1.00.00
RTCP generation timeout 4				Software Partition information Active Backup
Codec configuration		(7		
Allow unconfigured codecs				
Enforce codec priority in profile			*	
		OK Cance	н	
	Denial of Service Mitigation Show	SIP Loadbalancer status Show		
L L				
				Apply Changes Cancel Changes

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.

OpenScape Ses Management Portal	Product name Unify OpenScape SBC				
Administration	General - OSS				
► System	 SBC aggregated information and data. 				
Network/Net Services	Alarms				
Sip Server Settings	Alarm summary: Criti	cal: 0 📕 Major: 1 📕	Minor: 0 🧧 Show alarm det	ails	
Port and Signaling Settings Media	System Status				
QoS Monitoring Features	Branch mode	Centralized SBC	Auto refresh timer	30 seconds V	
Security	Operational state	normal			

- 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.

VOIP					0	ч Ш н) Ш н :
 Select OK to temporarily sto 	re changes. Make vour	changes permanent by se	electing 'Apply Changes' on the	General page.		Leam more ×
Sip Server Settings Por	and Signaling Setting	IS Media QoS M	Ionitoring	1.5		Product name Unify OpenScape SBC User name : administrator
Care Ride Media Configuration				0	· ·	
Core Side Media Corniguration				(
Media profile OSV_MP	~					
				Add Delete		େ ପ୍
User agent		media	Profile			
					î с	System Info
					~	CPU 2.18 % - 2 × 2700 MHz (0 MHz Reserved in VM)
						Memory 14.97 % - 4 Gb (4 Gb Reserved in VM)
4) - F		Disk 12.09 % - 42 Gb
Media Profiles				(?		System uptime 31 days 23:20
						Hardware type Virtual OSS 250
				Add Edit Delete	2	Hostname OSS
Name	Codecs	Media protocol	SRTP crypto context negotiation	Mark SRTP Call-leg as Secure		Software Info
WE_Phone_default		Best Effort SRTP	mikey + sdes		•	Software version V11 R1.00.00
VodafoneMP	G711A,G729	RTP only	none			Software Partition information Active Backup
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	÷	•	
Claud Support				0		
Cloud Support	_			C.		
Support OpenScape Cloud						
Media Realm Groups				(
				OK Cance		Apply Changes Cancel Changes

- 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.

OpenScape Ses Management Portal	sion Border (Controller			
Administration	General - OSS				
▶ System	 SBC aggregated inf 	ormation and data.			
Network/Net Services	Alarms				
▼ voiP Sip Server Settings Port and Signaling Settings	Alarm summary: Critic	al: 0 📕 Major: 1 📕 M	nor: 0 <mark> Show alarm def</mark>	tails	
Media	System Status				୍ ଚ
QoS Monitoring Features	Branch mode	Centralized SBC	Auto refresh timer	30 seconds	~
Security	Operational state	normal			
Diagnostics & logs					
Alarms					
Maintenance					

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

Features	
() Select OK to temporarily store changes	s. 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" 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			0
() Select OK to temporarily store chang	es. Make your changes p	permanent by selecting 'Apply Change	es' on the General page.
SIP Service Provider Profile			0
Hostname			
Port			
Remote directory			
User name			
Password			
Download New	Profile List		
			Add Edit Delete
A Row N	ame 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 cha	anges 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 authentication number in Diversion header	
Send P-Preferred-Identity rather than P-Asserted-Identit	y 🛛 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 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 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		? -
	OKCar	icel

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

er name				
	Download New Profile	List		
				Add Edit Delete
Row	Name	Registration required	Registration interval (sec)	
1	PSTN1		3600	· · · · · · · · · · · · · · · · · · ·
2	UnigySSP		60	
3	UnifySPP		3600	
4	Zoom		3600	
				•

- 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 co	nfiguration					?
() Select OK to tempora	rily store changes. Make your c	hanges perm	anent by selecting 'App	oly Changes' on the Ge	neral page.	
Remote Endpoint Settings	;					?
Name	ZoomSP1	Edi	t			
Туре	SSP 🗸					
Profile	Zoom 🗸					
Access realm profile	Main-Access-Realm - ipv 🗸					
Core realm profile	Main-Core-Realm - ipv4 🗸					
Associated Endpoint	~					
Enable Call Limits						
Maximum Permitted Calls	0					
Reserved Calls	0					
Remote Location Informat	ion					?
Support Peer Domains	s					
Support Foreign Peer	Domains White list					
Enable access control						
Signaling address type	IP address or FQDI	1 ~				

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 70).
 - 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 from the Media profile drop-down menu, select the Zoom media profile.

Remote Location Domain		?
() Select OK to temporarily stor	e changes. Make your changes permanent by selecting 'Apply Changes' on the General page.	
General		2
Remote URL 162.12.233.59	C Shared domain	
Remote port 5061		
Remote transport TLS	~	
Signaling		2
INVITE No Answer timeout (msec) 360000	
INVITE No Reply timeout (msec)	3000	
TLS		?
TLS mode	Server authentication	
Certificate profile	Zoom_cert_profile	J.
TLS keep-alive		
Keep-alive interval (seconds)	120	
Keep-Alive timeout (sec)	10	
Media Configuration		?
Media profile	Zoom_MP	
	OK	;el

- 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. 		Learn more X
	^	Product name Unify OpenScape SBC User name : administrator ?
4 · · · · · · · · · · · · · · · · · · ·		<u>^</u>
Remote Location Identification/Routing		
Core FQDN		
Core realm port 50001	00	ව System Info (ි ලි
Default core realm location domain name	~	CPU 2.19 % - 2 × 2700 MHz (0 MHz Reserved in VM)
Default home DN		Memory 15.92 % - 4 Gb (4 Gb Reserved in VM)
Enable routing based on domain		Disk 12.09 % - 42 Gb
FQDN		System uptime 32 days 1:47
Incoming Routing prefix Add		Hardware type Virtual OSS 250
^ Delete		Hostname OSS
		Software Info
		Software version V11 R1.00.00
· · ·		Software Partition information Active Backup
Digest Authentication (2)		
Digest authentication supported	<u> </u>	
Digest authentication realm		
Digest authentication user ID		
Digest authentication password		
Access Side Firewall Settings		
	•	
OK Cancel)	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:

2	Unig	ySSP 🗌		60					
3	Unif	ySPP		3600					
4		Zoom 🗌		3600					
e endpoint co	onfiguration								
te endpoint co	onfiguration								
te endpoint co	onfiguration	-		-	-	-	-	_	
te endpoint co	onfiguration	_			Remote IP address /				
te endpoint co Row	nfiguration	Access realm pro	ile Type	Profile / Circuit ID	Remote IP address / Logical-Endpoint-ID / Circuit URL	Remote port	Remote transport	Associated Endpoint	
te endpoint co Row	nfiguration Name ZoomSP1	Access realm pro Main-Access-Realm - ip	ile Type v4 SSP	Profile / Circuit ID Zoom	Remote IP address / Logical-Endpoint-ID / Circuit URL 162.12.233.59	Remote port	Remote transport TLS	Associated Endpoint	
te endpoint co tow	Name ZoomSP1 ZoomSP2	Access realm pro Main-Access-Realm - ir Main-Access-Realm - ir	ile Type v4 SSP v4 SSP	Profile / Circuit ID Zoom Zoom	Remote IP address / Logical-Endpoint-ID / Circuit URL 162.12.233.59 162.12.232.59	Remote port 5061 5061	Remote transport TLS TLS	Associated Endpoint	

 Note: See the Tables in Unify OpenScape SBC Configuration on page 70

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.

OpenScape Ses Management Portal	sion Border (Controller			
Administration	General - OSS				
▶ System	 SBC aggregated inf 	ormation and data.			
Network/Net Services	Alarms				
▼ VoIP					
Sip Server Settings	Alarm summary: Critic	al: 0 📕 Major: 1 📕 Mi	nor: 0 📒 🛛 Show alarm de	etails	
Port and Signaling Settings Media	System Status				C ()
QoS Monitoring		Controlling of ORC	Austa unformela timo en	20	
Features	Branch mode	Centralized SBC	Auto retresh timer	30 seconds	V
Security	Operational state	normal			
Diagnostics & logs					
▶ Alarms					
Maintenance					

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
Configure
Enable Codec Support for transcoding Configure
Enable Sip Load Balancer Configure
Enable Push Notification Service Configure
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			0
() Select OK to temporarily store changes. M	ake your changes p	ermanent by selecting 'Apply Change	es' on the General page.
SIP Service Provider Profile			0
Hostname			
Port			
Remote directory			
User name			
Password			
Download New Profil	e 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 cha	nges permanent by selecting 'Apply Changes' on the General page.
General	0
Name PSTN1	Default SSP profile
Allow sending of insecure Referred-By header	Send authentication number in Diversion header
Send P-Preferred-Identity rather than P-Asserted-Identit	y
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	0
Privacy support Full	
SIP Service Address	0
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.

emote directory	orarily store changes. Mal	ke your changes pe	manent by selecting 'Apply Changes'	on the General page.
ser name				
(Download New Profile	List		
				Add Edit Delete
- Row	Name	Registration required	Registration interval (sec)	
1	PSTN1		3600	•
2	UnigySSP		60	
3	UnifySPP		3600	
4	Zoom		3600	
	guration			(7
emote endpoint config				

- 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 co	nfiguration
 Select OK to temporal 	rily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.
Remote Endpoint Settings	
Name	PSTN
Туре	SSP V
Profile	PSTN1 V
Access realm profile	Main-Access-Realm - ipv 🗸
Core realm profile	Main-Core-Realm - ipv4 🗸
Associated Endpoint	✓
Enable Call Limits	
Maximum Permitted Calls	0
Reserved Calls	0
Remote Location Informat	ion
Support Peer Domains	S .
Support Foreign Peer I	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 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 	e 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 V	
TLS keep-alive		
Keep-alive interval (seconds)	120	
Keep-Alive timeout (sec)	10	
Media Configuration		?
Media profile F	2STN_Media_profile	
	OK C:	ancel

9. In the Remote endpoint configuration window, locate the Remote Location IdentificationRouting area.
10. In the Core realm port field, enter the core realm value as 50015.

Remote endpoint confi	iguration			0		Learn more X
Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.						
				-		Product name Unify OpenScape SBC User name : administrator (?)(())
					-	$\bigcirc \bigcirc \bigcirc$
4				•		
Remote Location Identification	on/Routing			?		
Core FQDN						୦ ମ
Core realm port	50015					
Default core realm location domain name						
Default home DN					· (7)) System into
Enable routing based on domain						CPU 2.19 % - 2 × 2700 MHz (0 MHz Reserved in VM)
FQDN						Memory 15.62 % - 4 Gb (4 Gb Reserved in VM)
Incoming Routing prefix			Add			Disk 12.09 % - 42 Gb
		4	Delete			System uptime 32 days 2:19
						Hardiware type Virtual OSS 250
						Hostname OSS
						Software Info
Digest Authentication 📀						Software version V11 R1.00.00
						Software Partition information Active Backup
				OK Cancer	J	
	Services status	Show	Registered subscribers	Show		
	SSP status	Show	Dynamic port mapping	Show		
	Denial of Service Mitigation	Show	SIP Loadbalancer status	Show		
	Denna of Service Integration	51104		SHOW		
						Apply Changes Cancel Changes

- 11. Click **OK** to return to the Remote Endpoints window.
- 12. Click OK on all open windows.
- 13. Click Apply Changes.



Copyright 2025, Mitel Networks Corporation. All Rights Reserved. The Mitel word and logo are trademarks of Mitel Networks Corporation, including itself and subsidiaries and authorized entities. Any reference to third party trademarks are for reference only and Mitel makes no representation of ownership of these marks.