

A MITEL PRODUCT GUIDE

OpenScape Solution Set V11

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

Solution Guide 07/2025

🕅 Mitel

A31003-S1100-M129-02-76A9

Notices

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

Trademarks

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

© Copyright 2025, Mitel Networks Corporation

All rights reserved

1 History of Changes	4
2 Introduction	5
2.1 Prerequisites	6
2.2 Additional Support Information	6
2.3 Related Documentation	6
3 Zoom Web Portal Configuration	8
3.1 Adding the OpenScape SBC	8
3.1.1 Configuring the Route Group	11
3.1.2 Configuring the SIP Group	13
3.1.3 Configuring the Routing Rule	14
3.2 Adding Phone Users	16
3.2.1 Assigning a Calling Plan to a phone user	
3.3 Adding BYOC Phone numbers	
3.3.1 Assigning BYOC numbers	
3.4 Adding BYOP numbers.	
4 Configuring OpenScape SBC	22
4.1 Configuring Network settings	24
4.2 Configuring SIP Server	25
4.3 Configuring Certificates	
4.4 Configuring Media Profiles	
4.4.1 Configuring the Codec Manipulation Options	
4.4.2 Configuring the Zoom Media Profile	
4.4.3 Configuring the Open Seens 4000 Media Profile	
4.4.4 Conliguring the OpenScape 4000 Media Prolite	
4.4.5 General Media Settings	
4.5 Configuring Renote Endpoints	
4.5.2 Configuring the PSTN Remote Endpoints	
5 OpenScape 4000 Configuration with Zoom Phone System	41
5.1 OpenScape 4000 Routing	41
6 Restrictions	43

1 History of Changes

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

2 Introduction

This document outlines the process of connecting the **OpenScape 4000**

(OS4K) to **Zoom Phone** using Bring Your Own Carrier (BYOC)¹ and Bring Your Own PBX (BYOP)² configurations.

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

How it works:

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

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

OpenScape 4000 handles SIP message manipulation and call routing, ensuring proper communication between Zoom Phone and external networks (like PSTN). It also sets up signaling paths to Zoom Phone data centers and the SSP (PSTN provider), ensuring smooth call flow *to* and *from* Zoom Phone and the PSTN.

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

For detailed Zoom Phone settings and configuration, please refer to the official Zoom support page under the Settings and Configuration for Zoom Phone section and the following Zoom Web Portal Configuration on page 8 chapter.

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

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

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



2.1 Prerequisites

Supported product versions

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

2.2 Additional Support Information

In the current Mitel product software implementation:

- OpenScape SBC with OpenScape 4000 solution is supported.
- SBC standalone mode (without PBX) is currently supported.
- Domain-based Zoom multi-tenancy is supported.
- Comfort Noise generation is currently not supported by OpenScape SBC.
- The OSEE environment with SBC-THIG and Zoom is currently <u>not</u> supported.

2.3 Related Documentation

Zoom

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

OpenScape 4000

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

OpenScape SBC

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

3 Zoom Web Portal Configuration

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

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

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

3.1 Adding the OpenScape SBC

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

Prerequisites

- 1) You are an administrator.
- 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.
- Navigate to Phone System Management > Company Info > Account Settings > Routing.



- tions Resources Plans & Pricing Schedule Join Host - Web App -Multiple Sites Routing Routing BYOC Settings Notifications Configurations for Bring Your Own Carrier (BYOC). Desk Phone Allow Caller Name Delivery
 Caller Name information will be included in the signaling messages for a BYOC
 (Premises) call Security Templates Directory Others Session Border Controllers Manage Session Border Controllers are added to enable BYOC-P or BYOP-P functionality. Outbound calls from Zoom are routed according to the Route Group to which a Session Border Controller is assigned, Inbound calls received from the Session Border Controllers are routed to users based on the DID or extension numbers of the assigned SIP Group. Route Groups Manage Route Groups are composed of one or more Session Border Controllers and assigned to SIP groups to determine the routing behavior for BVOC-P and BVOP-P calls. When a Route Group is assigned to a Region, calls are originated or therminated on the Zoom data centers that are part of that Region. Admins can receive email alerts when a SIP 9
- 3) Locate the Session Border Controllers section and click Manage.

4) Click Add.

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

- 5) Configure the following:
 - a) Display Name: Type the display name of your choice. For example, OpenScape_SBC.
 - **b) IP Address:** Enter the IP address of the OpenScape SBC interface facing towards Zoom and configure the port number (for example, 5061).
 - c) In-Service: Click the toggle button to enable the In-Service option.
 - d) Under the Settings section, check the following checkboxes:

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

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

Add Session Border Controllers

Display Name	OpenScape_SBQ
Description (Optional)	Enter
Protocol	TLS
IP Address	Public IP Address Port Number ⑦ 192.1 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 ③ Allow REFER support to transfer calls
Address(Optional) 🧿	Country/Region Select v
Email(Optional) 💿	Enter Email
Phone Number(Optional) (?)	Enter Phone Number
Save	

NOTICE:

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

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

3.1.1 Configuring the Route Group

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

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

To add a Route Group:

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

			Q	Gearch Support 00	08000503335	Contact Sale	s Request a Den	no
ZOOM Products Sc	lutions Resources Plan	ns & Pricing		s	chedule Jo	in Host ~	Web App ~	
Phone System Management Users & Rooms	Company Info > Account	Settings						
Auto Receptionists	Settings Policy	Block List Spam List	External Contacts	Emergency Serv	ices			
Call Queues								
Shared Lines	Set up SMS Campaigns our clients to set up SM	to enable SMS for users: Our tele S Campaigns in order to enable Si	ecommunications carriers h MS for their users. Create ar	ave recently classified Z SMS Campaign to ena	oom as an A2P t	ousiness, which r	equires ×	
Group Call Pickup								
Phone Numbers	Multiple Sites	Multiple Sites						
Provider Exchange	Routing	Multiple Sites						
Phones & Devices	Desk Phone	Once enabled, your current s	ite will default to your Main !	Site.				
Monitoring	Security	Site Code						
Assets Library	Templates	Once enabled, you can assig format of (site code)-(short of	n a site code to each site. E	xtensions will be in the	ion			
Logs	Directory Others	number to reach another use users in other sites.	r in the same site or the full	extension number to re	ach			
Company Info		Site Manage					6	





3) Click Add.



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

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

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

Add a new Route Group

Display Name	Route_group_OpenScape	
Туре	BYOC-P	~
Region	US01 - US (SJ/DV/NY)	8~
Distribution	Sequential	~
	Session Border Controllers 1: OpenScape_SBC (192.) &	
Backup Route Group (Optional)	Select	
Got old Route Gro	ups?	Cancel

5) Click Save.

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



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

Route_group_O	penScane		
Region (?):	Normal: We sent O	ptions Ping me	ssages
US01 - US (SJ/[to the SBC and rec	eived successf	ul
- US Central (Co	ioradoj (i)	Openscap	e_SBC
		• (192.	I)
- US West (N. California) (j) Oper		OpenScap	e_SBC
		(192.	1)
- US East (New York) (i) OpenScape_SBC		e_SBC	
		(192.€)

3.1.2 Configuring the SIP Group

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

To add a SIP Group:

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

		Q Search Support 0008000503335 Contact Sales Request a Demo	þ
ZOOM Products Sol	utions Resources Pla	ans & Pricing Schedule Join Host - Web App -	
Phone System Management Users & Rooms	Company Info > Account	x Settings	
Auto Receptionists	Settings Policy	Block List Spam List External Contacts Emergency Services	
Call Queues			
Shared Lines	Set up SMS Campaign our clients to set up SN	ns to enable SMS for users: Our telecommunications carriers have recently classified Zoom as an A2P business, which requires x MS Campaigns in order to enable SMS for their users. Create an SMS Campaign to enable SMS.	
Group Call Pickup			
Phone Numbers	Multiple Sites	Multiple Sites	
Provider Exchange	Routing	Muttiple Sites	
Phones & Devices	Desk Phone	Once enabled, your current site will default to your Main Site.	
Monitoring	Security	Site Code	
Assets Library	Templates	Once enabled, you can assign a site code to each site. Extensions will be in the format of feite code. Short extension number! Users can dial the short extension	
Logs	Directory Others	number to reach another user in the same site or the full extension number to reach users in other sites.	
Company Info		Site Manana	

2) Locate the SIP Groups section and click Manage.



3) Click Add.

Company Info > Account Settings > SIP G	iroups		
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 0	Group
Display Name	sip_group_OpenScape
	Send SIP Group Name in SIP header ?
Route Group	Route_group_OpenScape (BYOC)
Description (Optional)	Enter
	Save Cancel

5. Click Save.

3.1.3 Configuring the Routing Rule

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

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

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

		Q Search Support 0008000503335 Contact Sales Request a Dem	no
ZOOM Products So	olutions Resources Pla	Plans & Pricing Schedule Join Host ~ Web App ~	
Phone System Management Users & Rooms	Company Info > Accour	unt Settings	
Auto Receptionists	Settings Policy	y Block List Spam List External Contacts Emergency Services	
Call Queues			
Shared Lines	Set up SMS Campaigr our clients to set up SI	gns to enable SMS for users: Our telecommunications carriers have recently classified Zoom as an A2P business, which requires × SMS Campaigns in order to enable SMS for their users. Create an SMS Campaign to enable SMS.	
Group Call Pickup			
Phone Numbers	Multiple Sites	Multiple Sites	
Provider Exchange	Routing	Multiple Sites	
Phones & Devices	Desk Phone	Once enabled, your current site will default to your Main Site.	
Monitoring	Security	Site Code	
Assets Library	Templates	Once enabled, you can assign a site code to each site. Extensions will be in the	
Loge	Directory	number to reach another user in the same site or the full extension number to reach	
Logo	Others	users in other sites.	
Company Info		Site Manage	

2) Locate the Routing Rule section and click Manage.

Multiple Sites Routing Notifications	SIP Groups Manage 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 the specific Route Groups.
Desk Phone	
Security	Provident Parks III
Templates	The routing rules are a series of predefined Regular Expressions. These rules are used to route outgoing
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.

Company Info	> Account Settings > Routing Rules
Routing	Rules
Rules defined dialed number	at the site level have higher precedence than rules defined at the account level. If a does not match any rules, the call will be routed via the PSTN.
Number number	r 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 is as number matching patterns will not send location information to the PSAP.
Add Routing	Rulo

- 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.

		j Kule
	Level	Account
	Rule Name	Outgoing
	Number Matching and Translation ?	Number Pattern
		[[[[[[]]]]
		Translation (Optional)
		Replacement Pattern must be in E.164 format
		Test (?)
	Number mat codes or em DTMF code. will not send	ching patterns for routing rules must not conflict with DTMF ergency numbers. Click here for details to learn more about Using emergency numbers as number matching patterns location information to the PSAP.
	Routing Path	sip_group_OpenScape
	Call Forwarding ?	
		Save Cancel
5) Click Save		

Add Routing Rule

3.2 Adding Phone Users

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

Prerequisites

- 1) You have a Pro, Business, or Enterprise Zoom Phone account.
- 2) You are an administrator with the privilege to edit account settings.
- **3)** You have completed the initial Zoom Phone setup. For more information, refer to Getting started with Zoom Phone (admin).
- 1) Log in to the Zoom web portal.

2) Navigate to User Management > Users > Add Users.

ZOOM Products Solu	tions Resources Plans & Pricing	Schedule	Join	Host v	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 Advanced Search V	Impor	t Exp	oort ~	+ 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.

<u>sampa</u> @gm	ail.com	
Zoom Workplace	Zoom Meetings (0 available)	2
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 $\ensuremath{\textbf{Pending}}$ tab of the User Management section.

Next steps

You can now assign licenses to users. After purchasing your Zoom One licenses, during the setup of Zoom Phone for your account, you can choose either to assign Zoom Phone packages automatically or manually to your Zoom One users. Before assigning a license to a phone user, ensure that automatic phone assignment for Zoom One licenses is disabled for your account. For more information, refer to the official Zoom support page.

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

3.2.1 Assigning a Calling Plan to a phone user

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

Prerequisite

- 1) You are an administrator with the privilege to edit account settings.
- 2) You have assigned licenses to the phone users. For more information, refer to How to assign licenses.
- 1) Navigate to Phone System Management > Users & Rooms.
- 2) Select the user for whom you want to add a calling plan and click Assign.

> User Management	_							
> Device Management								
> Room Management								
> Workspaces Management								
 Phone System Management 								
Users & Rooms								
Auto Receptionists		nhonausar	1					
Call Queues	0	pronouaci	1084		Online	Active	Main Site	

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

 Room Management 	phoneus	er (@gmail.com)
> Workspaces Management			- 3,
 Phone System Management 	Profile Policy Hi	story 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	phoneus	ser (@gmail.co	m)
ADMIN	Profile Policy H	History User Settin	ngs	
Dashboard				
> User Management	Site	Main Site)	
> Device Management	Package	Select Package	^	
> Room Management		US/CA Unlimited (Calling Plan (9 Available)	
> Workspaces Management		Pro Features · Unlimi	ited Domestic	
 Phone System Management 	Extension Number	Zoom Phone Powe	er Pack (19 Available)	
Users & Rooms				
Auto Receptionists	Emergency Address (?)	Default: 3701 W PLANC) PKWY, STE 300 STE 300, PLANO, Texas	75075, United States
Call Queues		Personal Emergency A	ddress	

5) Click Confirm.

3.3 Adding BYOC Phone numbers

You can upload BYOC phone numbers.

Prerequisite

- 1. You are an administrator with the privilege to edit account settings.
- 1) Log in the Zoom web portal.

- 2) Navigate to Number Management > Phone numbers.
- 3) From the Add Number drop-down menu, select BYOC Number.

ZOOM Products Solutions	Resources Plans & Pricing	Schedule	Join	Host ~	Web App ~	
Room Management Workspaces Management	Phone Numbers					
Workspaces Management Phone System Management	Add Number v Import v Export Related Features v					
Number Management	Port Number					
Provider Exchange	BYOC Number Delete SMS Campaigns × 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 13.
 - f) Check the acknowledgment box to consent.
 - g) Click Submit.

Add BYOC	Number	
Product	Phone	~
Site	Main Site	•
Country/Region	United States	~
Numbers	9728522000,9728522001,9728522002	
SIP System	Zoom Phone	~
SIP Group	Choose a routing path for calls to/from the numbers	1
	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	pers 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 Sol	utions Resources Plans & Pricing	Schedule Jo	oin Host ~	Web App \sim
Device management				
Room Management	Phone Numbers			
Workspaces Management	Add Number > Import > Export Related Features >			
Phone System Management				
Number Management	O Search			
in an agenteric				
Phone Numbers	2 selected			
Phone Numbers Provider Exchange	2 selected Delete SMS Campaigns v Site Confirm BYOC Address			
Phone Numbers Provider Exchange Account Management	2 selected Delete SMS Campaigns V Site Confirm BYOC Address Number : Status Y Product Y Assigned To Y	Source T	Area ¢	Туре
Phone Numbers Provider Exchange Account Management Advanced	2 selected Delete SMS Campaigns v Site Confirm BYOC Address Number : Status Y Product Y Assigned To Y +197	Source ¥ BYOC - Premises	Area \$	Type 0
Phone Numbers Provider Exchange Account Management Advenced	2 belete Delete Number : Status Y Product Y Assigned To Y end to y and the status Y Product Y Assigned To Y end to y and the status Y Product Y Assigned To Y end to y and the status Y Product Y Assigned To Y end to y and the status Y Product Y Assigned To Y end to y and the status Y Product Y Assigned To Y	Source T BYOC - Premises SIP Group: SIP_19	Area 💲 United States	Type Ø Toll

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

ZOOM Products S	olutions Resources Plans 8	Pricing	Schedule	Join Host ~	Web App ~
Room Management	Assign		rce T	Area 🗘	Туре
> Workspaces Management	Number	+1972-852-2663			
> Phone System Management	+19; CLI:	liser	C - Premises Group: Avaya	United States	Toll
V Number Management	DN: -				
Phone Numbers	+197	phoneuser - Ext. 1061, Main Site	C - Premises	United States	Toll
Provider Exchange	CLI:	Save Cancel	Group: sip_gr		
> Account Management	DN:				
> Advanced	+1 972-403-4510	Normal C	BYOC - Premises	United States	Toll

The phone number will be assigned to the selected user.

3.4 Adding BYOP numbers

Administrators can add OpenScape 4000 users as external contacts, which will be added to the contacts directory and be accessible to Zoom applications. To add Bring Your Own PBX (BYOP) numbers:

- 1) Navigate to Phone System Management > Company Info > Account Settings > External Contacts.
- 2) Click Add.



- 3) In the Add External contact pop-up, configure the following:
 - Name: Type the name of the OpenScape 4000 user. For example, OS4K_user1.
 - In the **Extension Number** field, enter the extension number of the OpenScape 4000 user.
 - From the **Routing path** drop-down menu, select the **SIP Group** created in Configuring the SIP Group on page 13.
- 4) Click Save.

4 Configuring OpenScape SBC

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

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

Prerequisite

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

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

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

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

Traffic Type	Protocol	Source	Destination Ports	Destination IPs	Region
				162.12.233.59	North
				162.12.232.59	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 SBC	5061	103.122.166.248 103.122.167.248	Australia
				149.137.41.246	APAC
				207.226.132.198	
				209.9.211.198	нк

Table 1: Zoom Signaling Traffic IPs

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

Table 2: Zoom Media Traffic IPs

Traffic Type	Protocol	Source	Destination Ports	Destination IPs	Region
				162.12.232.0/24	North
				162.12.233.0/24	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 SBC	20000-64000	103.122.166.0/24 103.122.167.0/24	Australia
				149.137.41.0/24	APAC
				207.226.132.0/24	
				209.9.211.192/26	нк
				101.36.167.0/24	
				207.226.132.0/24	Japan
				149.137.25.0/24	

4.1 Configuring Network settings

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

OpenScape Ses Management Portal	sion Border C	Controller						
Administration	General - OSS							
► System	SBC aggregated information and data.							
Network/Net Services Settings	Alarms							
DNS	Alarm summary: Critical	: 0 📕 Major: 1 📕 Min	or: 0 <mark> Show alarm deta</mark>	ils				
NTP			_					
Traffic Shaping	System Status				C 🔿			
QoS								
► VoIP	Branch mode	Centralized SBC	Auto refresh timer	30 seconds	~			
Features	Operational state	normal						

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

- 2) Locate the Interface Configuration > Core Realm Configuration area and click Add.
 - a) Configure the following:
 - a) IP address: Enter the SBC IP address associated with the core (private) side of the network.
 - b) Subnet mask: Enter the subnet mask value.
 - c) SIP-UDP: Configure port number as 5060.
 - d) SIP-TCP: Configure port number as 5060.
 - e) SIP-TLS: Configure port number as 5061.
 - f) Click Ok.

nges. Make your chang					0						м Ш н		
nges. Make your chang													
	es permanent by se	ecting 'Apph	y Changes' o	n the Genera	al						100	more	
Tic Shaping QoS							Product nar	ne Unify OpenScap	beSBC L	lser name : administral	or (?)	(2)	
					^						···	J	
					14								
	_	_				_	_					_	
_				_								0.6	
												0.0	
			Add	Delete		IS						0.6	
Subnet mask	Signaling Media	SIP-UDP	SIP-TCP	SIP-TLS									
255.255.255.0	v v	5060	5060	5061	-	30 seconds		~					
						_							
			E	Ok Can	icel	Active							
Com Nada 2													
Com Node 2													
Primary server			Penalty t	oox state									
Backup server			Penalty t	oox state									
	Subnet mask S 255.255.255.0 S Com Node 2 Primary server Backup server	Subnet mask Z55,255,255,0 Com Node 2 Primary server Backup server	Subnet mask Subnet mask 255,255,255,0 Com Node 2 Primary server Backup server	Subnet mask Signaling Media SiP-JUP SiP-TCP 255,255,255.0 C C 960 5660 Com Node 2 Primary server Penalty Backup server Penalty	Add Delete Subnet mask Signaling Media SIF-UDP SIP-TCP SIP-TLS 255,255,255.0 C C Socie Socie Socie Com Node 2 Primary server Penalty box state Backup server Penalty box state	Subnet mask Signaling Media SIP-UDP SIP-TCP SIP-TLS 255,255.255.0 C C G SIGN C Cancel Com Node 2 Primary server Penalty box state Backup server Penalty box state	Subnet mask Signaling Media SIP-UDP SIP-TOP SIP-TO 255,255,255.0 T T 5989 5969 5969 Com Node 2 Primary server Penalty box state Backup server Penalty box state	Subnet mask Signaling Media SIP-UDP SIP-TCP SIP-TCP 255,255,255,0 Signaling Media SIP-UDP SIP-TCP SIP-TCP Seeonds Com Node 2 Primary server Penalty box state Backup server Penalty box state	Add Deter Subnet mask Signaling Media SIP-UDP SIP-TLS 255,255,255,0 Signaling Media SIP-UDP SIP-TLS Seconds	Submet mask Signaling Media SIP-UDP SIP-TCP SIP-TCP SIP-TCP SIP-TCP SIP-TCP Careel Com Node 2 Primary server Penalty box state Backup server Penalty box state	Submet mask Signaling Media SIP-UDP SIP-TCP SIP-TCP 255,255,255,0 Signaling Media SIP-UDP SIP-TCP SIP-TCP 255,255,255,0 Signaling Media SIP-UDP SIP-TCP Signaling Media Sip-TCP Signal Signaling Media Sip-TCP Signaling Medi	Add_Deter Subnet mask Subnet mask Signaling Media Subnet mask Signaling Media Signaling Media Signaling Signaling Media Media Signaling Media Signaling Media Media Signaling Media Media Signaling Media Signaling Media Signaling Media Media Media Media Media Media Media S	

- g) Click Apply Changes on the SBC Main page.
- 3) Locate the Access and Admin realm configuration area and click Add.

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

	Networ	k/Net Services																			0
(Select	OK to temporarily	store changes. Make you	r changes pe	ermanent by selecti	ing 'Apply Chang	es' on the (Seneral pag	pe.												
[Settings		P Traffic Shaping	Q+5																	
	4																				[^]
	Access	ind Admin realm co	orfiguration																		
																				Datata	
	-					_					_								Aut	Denete	
		Type	Network I	D interface	IP address	Subnet mask	VLAN tag	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	SIP-MTLS	MGCP	SIP server	Messa; rate limit (sec)	Trust level	Signaling restriction			
		Main IPv4	Main-Access-IPv	4 eth1	1921 1 2	255 255 255 224	0	2		5060	5060	5061	5161	2727	Node 1	100	NA	Unrestricted		^	1.
													•								- 1
																					- 1
																					- 1
	¢																				- 1
	Restm	votia		_			_	_	_	_		_	_	_	_	_	_	_	_	0	a II
	-																			_	1
																			Add	Delete	
			Realm profile	Realm	Signaling net	work ID	Media n	etwork ID	F.	orward netv	rerk ID										
		Main-Core	s-Realm - ipv4	access	Main-Col Main-Accer	ss-IPv4	Main-Acc	ess-IPv4													
I																					
	4																				
	Doutiero	_	_	_	_	_	-	-		_	_	_	_	_	_	-	-	_	_	0	2
ľ	rouung																		6	Ok Cane	:ei

You are redirected back to the Network/Net Services window.

- 5) Locate the Routing area to configure the default gateway address.
- 6) In the **Routing Configuration** section, click **Add** and add the static routes for core and access interface.
- 7) Click OK.
- 8) Click Apply Changes.

4.2 Configuring SIP Server

The SIP connectivity to OpenScape 4000 is configured in the **OpenScape SBC Management Portal > VOIP** window. 1) Navigate to Administration > VoIP > Sip Server Settings.

OpenScape Sess	sion Border C	Controller		Product name Unify OpenScape SBC				
Administration	General - OSS							
▶ System	() SBC aggregated info	mation and data.						
Network/Net Services	Alarms							
▼ VolP Sip Server Settings	Alarm summary: Critica	al: 0 📕 Major: 1 📕	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						
Diagnostics & logs								
Alarms								

The VOIP window pops up.

- 2) In the Sip Server Settings tab, enter the following:
 - a) Under General, from the Comm System Type drop-down menu, select Clustered.

VOIP									
O Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.									
Sip Server Settings Port and Signaling Settings Error Codes Media QoS Monitoring									
General									
Comm System Type Clustered									
Allow Register from SERVER									
Use RURI to Route to Comm System									
Bond TCP Connection to SLB									
Clustered servers									

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

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

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

cluste	clustered Servers											
 Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page. 												
										Add Delete	J	
- Gro	Group name	Node Name	Priority	Routing prefix	IP address or	Port	Transport	Stick with	No Answer timer	No Reply timer		
11	Zoom	Dino2	2		10.180.2.53	5060	TCP		360000	3000 -		

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

4.3 Configuring Certificates

For secure communication with Zoom, a Trusted Certificate must be installed in OpenScape SBC. Zoom Phone System allows only TLS connections for SIP traffic from SBCs with a certificate signed by one of the Zoom-supported Certification Authorities. The certificate must have the SBC FQDN as the common name (CN) in the subject field. Certificates with a wildcard in the certificate Subject Alternate Name field conforming to RFC2818 are also supported.

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

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

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

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

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

Prerequisites

Adequate administrative permissions.

Adequate knowledge of TLS certificate handling.

At least one OpenScape SBC is configured and in operation.

To configure Certificates:

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

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

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

OpenScape Sessi Management Portal	ion Border Controller	i	Product name I
Administration	OSS - Security - Google Chrome Not recure Helps://10.70.16.25/recurity.html?tabld=generalTab	0	
 System Network/Net Services 	Security	0	
► VolP	Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.		
▼ Security	General Firewall Message Rate Control RADIUS Denial of Service Mitigation		
General Firewall	Certificates	0	
Message Rate Control RADIUS	Certificate management		
Tunnel Connections	PKI Configuration	0	
 Diagnostics & logs 	Enable PKI configuration	_	\$ 6:18
Alarme			1

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

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

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

CA Certificates	
Unload CA cartificate file Choose File No file chosen	
Opload CA Certificate life Choose File No life Chosen	
CA certificates	
DigiCertGlobalRootG2.crt.pem DigiCertILSRSA4096RootG5.crt.pem qd_bundle-g-201.pem LastT-TeleSec_GlobalRoot_Class_2.pem Root_CA.pem SSL_COM_ROOT_CERTIFICATION_AUT ssl_root_with_chain.pem testbscCA.pem	
X.509 Certificates	
Upload X.509 certificate file Choose File No file chosen Upload)
X 509 certificates	
sba01_4ksst_com.pem	
sbacert.pem	
sbc01_4ksst_com.pem	
sbcbyot_4ksst_comm.pem	
SDCDyot_4ksst_com.pem	
ServerCertificate nem	
serversimple.pem 👻	
Key Files	
Upload key file Choose File No file chosen Upload	
Key files	
byotprivatekey pem	
key.pem	
PrivateKeymitel.pem	
PrivateKeymit.pem	
privateKey.pem	
sha01_nrivateKey.nem	
SBA01PrivateKey.pem	
sbakey.pem 👻	
	Ok Cancel

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

Certificate Management			
 Select OK to temporarily st 	tore changes. Make your cl	charges permanent by selecting 'Apply Changes' on the General page.	
System Certificate			0
System TLS Certificate	OSV Solution	v	
HTTPS certificate profile	HTTPS System Default	v	
Media DTLS certificate profile		×	
IOS Push certificate profile	IOS Push Default	×	
Android Push certificate profile	Android Push Default	×	
Service API certificate profile	Service API Default	v	
Certificate Profiles			0
		Ad	d Edit Delete

- 8) Configure the following parameters:
 - a) Certificate profile name: Enter the name of the Zoom certificate profile.
 - b) From the Certificate service drop-down menu, select SIP-TLS.
 - c) From the Local server certificate file drop-down menu, select the certificate file.
 - d) From the Local CA file drop-down menu, select the CA certificate.
 - e) From the Local key file drop-down menu, select the private key file.
 - f) From the Certificate Verification drop-down menu, select None.
 - g) From the Minimum TLS version drop-down menu, select TLS1.2.

Certificate Profile						(?
 Select OK to temporari 	ly store changes. Make yo	our changes	permanent by	selecting 'Appl	y Changes' on	the General page.	
Certificate Profile configura	tion					(?
Certificate profile name	Zoom BYOT						
Certificate service	SIP-TLS	~					
Local client certificate file		~	Show				
Local server certificate file	ServerCertificate nem	~	Show				
Local CA file	cel root with chain non		Show				
Romoto CA filo	[ssi_root_with_chain.pen		Show				
Remote CA life	Drivete Kourrite ever	•	SHOW				
EC param	PrivateKeymit.pem	•					
Attach to Config file	Sech25011						
, and the borning into	-						
Validation						(?)
Certificate Verification No	one 🗸						
Revocation status							
Identity Check							
Renegotiation						(?
Enforce TLS session r	enegotiation						
TLS session renegotia	tion interval (minutes) 60)					
TLS version						(?)
Minimum TLS version TL	S V1.2 👻						
DTLS version						(?)
Minimum DTI Quernien							
Winimum DTLS Version	J1LS V1.0 ♥						
Cipher Suites						(?)
Perfect Forward Secrecy	Preferred PFS	•					
Encryption	Preferred AES-128	•					
Mode of Operation	Preferred GCM	~					
						OK Cancel	

9) Click OK.

tem TLS Certificate Teams_Cert_Profil SerVice API Default ▼ reading and the service API Default * reading and the service API Defau		_	_	_	_		_	_	_
tem TLS Certificate PTFS conflicate profile HTTPS System Default v tod PLus Certificate profile DS Push Default v tod PLus certificate profile Service API Default v tod PLus certificate service Service API Default v tod PLus certificate service Service API Default v Service API Default v tod PLus certificate service Service API Default v Service API Default v Service API Service API Service API Service API Service Certificate file Local CA file Service API Service API Service API Service API Service API Service API Service CA file Service API Service	stem Certificate								
PFS catilicate profile HTTPS System Default in DTS catilicate profile in OF push Default iPack catilicate profile OF push Default iPack catilicate profile Do Push Default iPack catilicate profile Do Push Default iPack catilicate profile Do Push Default iPack catilicate profile Server catilicate profile iPack catilicate profile Server catilicate service IPack catilicate profile Server catilicate file Local CA file Remote CA file Local Key file Attach Key file Category Frofil SIP-TLS Server CALP profil Server CA pean Name Certificate Service API Server CALP profil Server CA pean Nonfortic-Cate Server CA pean Server CALP profil Server CA pean Server CALP profil Server CA pean Server CALP profil Server CALP profil Server Catilicate pean Server CALP pean Server Catilicate pean Server Catilicate pean Server Catilicate pean Server Catilicate pean Server Catilicate pean <th>tem TLS Certificate</th> <th>Zoom_BYOT</th> <th>~</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	tem TLS Certificate	Zoom_BYOT	~						
da D1,S certificate profie ioS Push Default	TPS certificate profile	HTTPS System	Default 🛩						
Public certificate profile OS Public Public Certificate profile Android Public Default Vice API certificate profile Service API Default Vice API certificate profile Service Certificate Bie Local CA Bie Remote CA Bie Local KA Bie Certificate Bie Server Cert	lia DTLS certificate profile		~						
trice API certificate profile wice API certificate profile trice API certificate service Name Certificate service Name Certificate service Certificate service Name Certificate service Service API Service API Certificate service Service API Service API Serv	Push certificate profile	IOS Push Defau	ult 👻						
Name Certificate profile Server Certificate file Server Certificate file Local CA file Local CA file Atlach to Crighte Name Certificate service Client certificate file Server certificate file Local CA file Local CA file Local Key file Teams, Certificate service Client certificate file Server certificate file Local CA file Local Key file Atlach to Crighte Uninofiticace SiP-TLS stool_4kisst_com pen SSL_COM_ROOT_CERTIF privateKey pern NO Service API Service CA pen Root_CA pen gd_bundle-g2-g1 pend NO Service API Service CA pen Service CA pen service Key NO Service API Service CA pen testsbcCA pen get_bundle-g2-g1 pend Service API Service CA pen service CA pen service Key NO Service API Service CA pen testsbcCA pen get_bundle-g2-g1 pend NO Service API Service CA pen testsbcCA pen get_bundle-g2-g1 pend NO Service API Service CA pend testsbcCA pendle-g2-g1 pen	Iroid Push certificate profil	e Android Push D	Jefault 🗸						
tificate Profiles Add Edit r Add Edit r Name Certificate service Client certificate file Service certificate file Local CA file Remote CA file Atlan file Atlan file Certificate file Client certificate file Service CA file Remote CA file Local Key file Atlan file Certificate file Certificate file Local Key file Atlan file	vice API certificate profile	Service API Def	fault 🗸						
Name Certificate service Cient certificate file Server certificate file Local CA file Remote CA file Local Key file Attach to Crigitie Teams_Cert_Profit SIP-TLS stod1_4/asst_com.pem SSL_COM_ROOT_CERTIF ph/nateKey pem NO UnityOfficeCent SIP-TLS Server_CA pem Red_CA pem gd_bundle-g2-g1 pem key pem NO Service API Service API server CAP server CAPI server API server API Service API Service API server CAPI server CAPI server API server API Service API Service API server CAPI server CAPI server API server API SSP_cent SiP-TLS VerticeCentre testbibCApin testbibCApin NO Zoom_BYOT SIP-TLS ServerCertificate pem sst_root_with_chain pem PrivateKeymit pem NO * * * * * * * * CA file Server API * * *	28 D							_	
Name Certificate servic Client certificate file Server certificate file Local CA file Remote CA file Local Key tec Affait he file Teams_Cert_Potil SIP-TLS stedo1_sisst_com.pen SSL_COM_ROD1_CERTF privateKey pem NO UninfOrtice.cert SIP-TLS Server_CA pem Root_CA pem gl_bundle-g2-g1 pem key pem NO SBP_cert SIP-TLS ServerConfficite pem statistic Capem gl_bundle-g2-g1 pem key pem NO SSP_cert SIP-TLS ServerConfficite pem statistic Capem gl_bundle-g2-g1 pem NO SSP_cert SIP-TLS ServerConfficite pem statistic Capem privateKey mite NO SSP_cert SIP-TLS ServerConfficite pem statistic Capem privateKey mite NO * ServerConfficite pem statistic Capem privateKey mite NO	uticate Profiles								
Name University Client certificate file Server certificate file Local CA file Remote CA file Local Key file Atlach to Ctg file Teams_Cert_Profit SIP-TLS sb001_4ksst_com pen SSL_COM_ROOT_CERTIF privaleKey pem NO UnityOffic.Cert SIP-TLS Server_CApert gd_bundle-g2-g pen privaleKey pem NO Service API Service API server.ct server.twy NO SSP_cert SIP-TLS testbbcc4 pen testbbcCA pen priesSec_GlobalRoot_Class; testbbckey pen NO Zoom_BYOT SIP-TLS ServerCertificate pen sst_root_with_chain pen PrivateKeymit pen NO 4tificate Creation struct Creation PrivateKeymit pen NO ServerCertificate									Add Edit De
Name Certificate service Client certificate file Server certificate file Local CA file Remote CA file Local KR file Cighte Teams_CarL_Profit SIP-TLS sbo01_kitst_com.pen SSL_COM_ROOT_CERTIF privaleKeypem NO UnityOfticsCarL SIP-TLS Server CA pen Root_CA.pen gf_bundle-g2-g1.pem Keypem NO Default Service API Server Certificate pen Isstructure server Key NO SSP_cert SIP-TLS ServerCertificate pen testsbcCA.pen gf_bundle-g2-g1.pen Keypem NO Zoom_BYOT SIP-TLS ServerCertificate pen sst_root_with_chain.pen PrivateKeymt pen NO * * * * * * * *								Attach to	
Teams_cnt_Profit SIP-TLS stoO1_46st_com_peni SSL_Cod_ROOT_CERTIF privateKey pemi NO Um/OfficeCert SIP-TLS Server_CA pemi Rod_CA pemi gd_bundle-g2-g1 pemi Key pemi NO Server_CAP Server_CAP Rod_CA pemi gd_bundle-g2-g1 pemi Key pemi NO Server_CAP NO Server_CAP Server_CAP Server_CAP NO Server_CAP NO Server_CAP NO Server_CAP Server_CAP Server_CAP <t< td=""><td>Denaurc</td><td>Sertificate service</td><td>Client certificate file</td><td>Server certificate file</td><td>Local CA file</td><td>Remote CA file</td><td>Local Key file</td><td>Cfg file</td><td>J</td></t<>	Denaurc	Sertificate service	Client certificate file	Server certificate file	Local CA file	Remote CA file	Local Key file	Cfg file	J
UnityOfficaCent SIP-TLS Server_CA pem Root_CA pem gd_bundle-g2-g1 pem key pem NO Service AP1 Service AP1 Service AP1 server rot servero server rot server rot	Teams_Cert_Profil	SIP-TLS		sbc01_4ksst_com.pem	SSL_COM_ROOT_CERTIF		privateKey.pem	NO	
Service API Default Service API server.ort server.en SSP_Detert SIP-TLS testabccert.pem testabcCA.pem LastT- TeleSec_GlobalRod_Class testabckey.pem NO Zoom_BYOT SIP-TLS ServerCertificate.pem sst_root_with_chain.pem PrivateKeymit.pem NO 4 - - - - - -	UnifyOfficeCert	SIP-TLS		Server_CA.pem	Root_CA.pem	gd_bundle-g2-g1.pem	key.pem	NO	
SSP_cent SIP-TLS testsbocker perm testsbocker perm TeedSec_GlobalRoot_Class, testsbocker perm NO Zoom_BYOT SIP-TLS ServerCentificate perm sst_root_with_chain.perm PrivateKeymit perm NO ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' '	Service API Default	Service API		server.crt			server.key	NO	
Zoom_BYOT SIP-TLS ServerCentificate perm sst_root_with_chain.perm PrivateKeymit perm NO	SSP_cert	SIP-TLS		testsbccert.pem	testsbcCA.pem	LastT- TeleSec GlobalRoot Class	testsbckey.pem	NO	
itificate Creation ite New TLS Certificates ie CAtile Self signed v Create	Zoom_BYOT	SIP-TLS		ServerCertificate.pem	ssl_root_with_chain.pem		PrivateKeymit.pem	NO	
tifficate Creation	-								
ate New TLS Certificates ie CA file Salf stoned ✓ Create	tificate Creation								
ate New TLS Certificates								_	
1e CAfile Self signed V Create	ate New TLS Certificates								
	18	CA fil	le Self signed	✓ Create					
i- CCD File	CSD File								
erate C SR File	nerate CSR File		comma separated eq DN	IS:*.ososb.com,DNS:ossbi	.com				
erarte CSR File rt certificate information. Subject alt name is comma separated eg DNS* osob.com.DNS ossbc.com	nerate CSR File	Subject alt name is e				×			
ererte CSR File rt certificate information. Subject alt name is comma separated eg DNS* ososb.com.DNS ossbc.com re for the csr file (8 characters or more) Type RSA	nerate CSR File Int certificate information. : Ine for the csr file (8 char	Subject alt name is a acters or more)		Туре	RSA				
ert cerf.fic8 File ert cerf.fic8 File ert cerf.fic8 File fic haracters or more) Type RSA	nerate CSR File ert certificate information. : ne for the csr file (8 char intry code (C)	Subject alt name is acters or more)		Type State or provinc	e name (ST)				

- **10)** Click **OK** in the **Certificate Management** window and in the **Security** window.
- 11) Click Apply Changes on the OpenScape SBC main page.

4.4 Configuring Media Profiles

In the **Media Profiles** settings, various SDP messages and audio (RTP) traffic parameters can be configured for the OpenScape SBC SIP endpoints to Zoom Phone System, SSP (PSTN provider), and OpenScape 4000.

4.4.1 Configuring the Codec Manipulation Options

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

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

OpenScape Ses Management Portal	Product name Unify OpenScape SBC			
Administration	General - OSS			
System	(i) SBC aggregated int	formation and data.		
Network/Net Services	Alarms			
► VolP Features	Alarm summary: Crit	ical: 0 📕 Major: 1 📕	Minor: 0 Show alarn	n details
 Security Diagnostics & logs 	System Status			
Alarms	Branch mode	Centralized SBC	Auto refresh timer	30 seconds 🗸
- mantenanet	Operational state	normal		

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



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

4.4.2 Configuring the Zoom Media Profile

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

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

OpenScape Ses Management Portal	sion Border C	ontroller		Product name Unify OpenScape SBC
Administration	General - OSS			
System	(i) SBC aggregated inform	nation and data.		
Network/Net Services	Alarms			
Sip Server Settings	Alarm summary: Critica	l: 0 📕 Major: 1 📕	Minor: 0 🧧 Show alarm d	etails
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			0
 Select OK to temporar 	ily store changes. Make your char	nges permanent by selecting 'A	Apply Changes' on the General
Sip Server Settings	Port and Signaling Settings	Media QoS Monitoring	J
User agent		mediaProfile	-
			A
4			• • • • • • • • • • • • • • • • • • •
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	©

3) Locate the Media Profiles area and click Add.

The Media profile window pops up.

- **4)** Under the **General** area, create the media profile for OpenScape SBC Zoom connections by entering the following:
 - Name: Type the media profile name. For example, Zoom_MP.
 - From the Media protocol drop-down menu, select SRTP only
 - Check the RTP/RTCP Multiplex in offer checkbox.
 - Under the **SRTP configuration** area, check the **MIKEY SDES** following checkbox.
- 5) Under the RTCP configuration area, from the RTCP Mode drop-down menu, select Always generate.

Media Profile
() Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.
General
Name Zoom_MP
Media protocol SRTP only Direct Media Support
Support ICE Full
Support NGTC Trickle ICE
Enable NGTC WebRTC Compatibility
Enable TURN Client
RTP/ RTCP Multiplex in offer
SDP Compatibility Mode
Support Mid Attribute
\Box Do not set port to zero on session timer answer SDP
C Keep sendonly attribute on NAT
SRTP configuration
SRTP crypto context negotiation 🛛 MIKEY 🗹 SDES 🗌 DTLS SDES Both 🗸
Mark SRTP Call-leg as Secure
Crypto change mode Default
RTCP configuration
RTCP Mode Always generate
RTCP generation timeout 4

Codec configuration						
Allow unconfigured codecs						
Enforce codec priority in profile						
Send Telephony Event in Invite without SI	DP					
Use payload type 101 for telephony event/8000						
Enforce Packetization Interval						
Codec G7221 16 kHz - 24 khns Y Add	1					
Codec G7221 16 kHz - 24Kbps V Add)					
Codec G7221 16 kHz - 24Kbps Add]		Dele			
Codec G7221 16 kHz - 24Kbps Add]	Move up Move down	1 Dele			
Codec G7221 16 kHz - 24Kbps Add Priority	Codec	Move up Move down Packetization interval	n Dele			
Codec G7221 16 kHz - 24Kbps Add Priority 1	Codec G722 8 kHz - 64 kbps	Move up Move down Packetization interval Auto	Dele			
Codec G7221 16 kHz - 24Kbps Add Priority 1 2	Codec G722 8 kHz - 64 kbps G711A 8 kHz - 64 kbps	Move up Move down Packetization interval Auto Auto	1 Dele			
Codec G7221 16 kHz - 24Kbps Add Priority 1 2 3	Codec G722 8 kHz - 64 kbps G7114 8 kHz - 64 kbps G7110 8 kHz - 64 kbps	Move up Move down Packetization interval Auto Auto Auto	n Dele			

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

4.4.3 Configuring the PSTN Media Profile

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

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

4.4.4 Configuring the OpenScape 4000 Media Profile

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

OpenScape Sess Management Portal	OpenScape Session Border Controller							
Administration System Network/Net Services VoiP Sip Server Settings Port and Singaling Settings	General - OSS (i) SBC aggregated inform Alarms Alarm summary: Critical	ation and data. : 0 📕 Major: 1 📕	Minor: 0 📒 Show alarm deta	alis				
Media	System Status							
QoS Monitoring Features ▶ Security	Branch mode Operational state	Centralized SBC	Auto refresh timer	30 seconds V				

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

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

- In the Media Profiles area, click Add to create the media profile for OpenScape SBC – OS4K connection.
- In the Media profile pop-up, locate the General section and configure the following:
 - Name: Enter the name of the media profile.
 - From the Media protocol drop-down menu, select SRTP only.
- 3) Under the SRTP configuration area, check the SDES checkbox.
- 4) In RTCP configuration, section, in the RTCP Modeselect Bypass option.

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

This is used for OS4K media connection.

- 6) Click OK in all open windows.
- 7) Click Apply Changes on the SBC main page.

4.4.5 General Media Settings

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

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

	VOIP	0
Management Portal	Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the Generation	al
	Sip Server Settings Port and Signaling Settings Error Codes Media QoS Monitoring	
Administration	Media Handling	9
System Network/Net Services VolP Sip Server Settings Port and Signaling Settings Error Codes Media QoS Monitoring	Allow multiple media lines for the same media type Replace the SDP Origin (o) field Reset SRTP context upon key change Use single bridge/port for audio media Core Side Media Configuration	0
Features > Security > Diagnostics & logs > Alarms	Media profile default	
Maintenance		

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

Cloud Support	0
Support OpenScape Cloud	

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

4.5 Configuring Remote Endpoints

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

4.5.1 Configuring the Zoom Remote Endpoints

1) Navigate to the Administration > Features window.

OpenScape Ses Management Portal	ssion Border (Controller			
Administration	General - OSS				
▶ System	 SBC aggregated in 	formation and data.			
Network/Net Services	Alarms				
Sip Server Settings	Alarm summary: Critic	al: 0 📕 Major: 1 📕 Mi	inor: 0 📒 Show alarm de	etails	
Media	System Status				C ()
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
① Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.
Features configuration
Enable Remote Subscribers Configure
Enable Remote Endpoints Configure
Enable Codec Support for transcoding Configure
Enable Sip Load Balancer Configure
Enable Push Notification Service Configure
Enable THIG
Enable Standalone

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

Remote Endpoints			0
() Select OK to temporarily store changes. M	lake your changes p	ermanent by selecting 'Apply Change	s' on the General page.
SIP Service Provider Profile			0
Hostname			
Port			
Remote directory			
User name			
Password			
Download New Profi	le List		
			Add Edit Delete
 Row Name 	Registration required	Registration interval (sec)	

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

SIP Ser	vice Provider Profile				
(i) Sele	ct OK to temporarily store chan	ges. Make your cha	anges permanent by selecting	'Apply Changes' on the General page.	
General					?
Name	Zoom		Default SSP profile	Zoom 🗸	
Enat	ole SSP Privacy and Compleme	ntary Flags			
	ow sending of insecure Referre	d-By header	Send authentication	number in Diversion header	
Se	end P-Preferred-Identity rather t	han P-Asserted-Ide	entity D Send authentication	number in P-Asserted-Identity header	
Do	o not send Diversion header		Send authentication	number in From header	
Se	end URI in telephone-subscriber	format	Include restricted nu	umbers in From header	
SIP Priva	асу				?
Drivoou	upport Full				
Privacy		v			
SIP Serv	ice Address				?
🗹 Use	SIP Service Address for identity	headers			
SIP serv	ice address sbc01.ucaasft.mit	el.com			
🗹 Use	SIP Service Address in Reques	t-URI header	Use SIP Service Address	in From header	
🗹 Use	SIP Service Address in To head	er	Use SIP Service Address	in P-Asserted-Identity header	
🗹 Use	SIP Service Address in Diversion	n header	Use SIP Service Address	in Contact header	
🗹 Use	SIP Service Address in Via hea	der	Use SIP Service Address	in P-Preferred-Identity header	
SIP Use	Agent				?
SIR Lico	Agent towards SSP Pagethru		SIP Liser Agent		
511 036	Agent towards 551 Tassinit	·	on osci Agent		
Registra	tion				?
🗆 Regi	stration required				
Registra	tion interval (sec) 3600				
				Ok	Cance

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

sword				
	Download New Profile	List		
				Add Edit Delet
Row	Name	Registration required	Registration interval (sec)	
1	PSTN1		3600	
2	UnigySSP		60	
3	UnifySPP		3600	
4	Zoom		3600	
3 4	UnifySPP Zoom		3600 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 type drop-down menu, select IP address or FQDN.

Remote endpoint co	nfiguration
() Select OK to tempora	rily store changes. Make your changes permanent by selecting 'Apply Changes' on the Gener
Remote Endpoint Settings	5
Name	ZoomSP1 Edit
Туре	SSP V
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	tion
Support Peer Domain:	s
Support Foreign Peer	Domains White list
Enable access contro	1
Signaling address type	IP address or FQDN

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

- 8) In the **Remote Location Domain** window, configure the following:
 - a) Remote URL: Enter the Zoom IP address (see the Zoom IPs Table under Chapter 3 Configuring OpenScape SBC on page 22).
 - b) Locate the TLS area, and from the TLS mode drop-down menu, select Server authentication.

(or Mutual authentication in case MTLS is required)

- c) From the Remote transport drop-down menu, select TLS.
- d) From the Certificate profile drop-down menu, select Zoom_BYOT.
- e) Locate the Media Configuration area, and from the Media profile drop-down menu, select the Zoom_MPmedia profile.

Remote Location Domain	(2
() Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.	
General	0
Remote URL 69 174 110 247	
Remote port 5061	
Remote transport TLS	
Signaling	$(\overline{\boldsymbol{n}})$
INVITE No Answer timeout (msec) 360000	
INVITE No Reply timeout (msec) 3000	
TLS	0
TLS mode Server authentication 🗸	
Certificate profile Zoom_BYOT V	
TLS keep-alive	
Keep-alive interval (seconds) 120	
Keep-Alive timeout (sec) 10	
Media Configuration	0
Media profile Zoom MP	
Media realm subnet IP address	
Cultound Prov Configuration	\bigcirc
	<u> </u>
Outbound Proxy	
	OK Cancel

- 9) Click OK.
- 10) In the **Remote endpoint configuration** window, locate the **Remote** Location Identification/Routing area.
- 11) In the Core realm port field, enter the core realm value as 50013.

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

4000 Configuration with Zoom Phone System on page 41.

Remote Location Identification/Routing			?
Core FQDN			
Core realm port	50013		
Default core realm location domain name			
Default home DN			
Enable routing based on domain			
FQDN			
Incoming Routing prefix		Add	
	▲	Delete	
	-		

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

NOTICE:

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

Click OK.

Remote endpoint configuration

13) Click Apply changes.

The Remote Endpoints window should look like the figure below:

						Add	Edit Delete E	export Logical IDs
Row	 Name 	Access realm profile	Туре	Profile / Circuit ID	Remote IP address / Logical-Endpoint-ID / Circuit URL	Remote port	Remote transport	Associated E
1	ZoomSP2	Main-Access-Realm - ipv4	SSP	Zoom	69.174.110.247	5061	TLS	A
2	ZoomSP1	Main-Access-Realm - ipv4	SSP	Zoom	162.12.233.60	5061	TLS	

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

4.5.2 Configuring the PSTN Remote Endpoint

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

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

5 OpenScape 4000 Configuration with Zoom Phone System

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

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

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

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

Gateway Configuration in WBM

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

The following settings are configured under the NatTrkEnterprise profile:

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

VHG 3500	Configuration Mainton	nance Logetf	
Basic Settings Security	Genesys GoeTel DEPE Mahle/Commit	SIP Trur	nk Profile
Network & Routing	OHL KOMM	Profile Name:	NatTrkEnterprise
voce careary	B O HTP GmbH	Profile Details:	Recommended Profile for 3rd Party SIP Applications using REFER
	O Huswei	Lines Motors	
	B	USE NORS.	
	🖲 🛛 IP Austia	Activate Trunk Profile:	
		Account/Authentication Required:	
	KPN VoipConnect	Remote Domain Name:	
	8	ID Transact Darkard	TOT
	Magyar Telekom	IP harsport Plotoco.	CP V (doed for Cro cal establishment)
	MCC-B	Default PAI:	(for outgoing "Anonymous" and CLIP "default PAI" profiles)
	Microsoft-Lync	Security	
	B	Released Security Lewel	Signaling and Pavload Security
	MS Teams	TI Surget	No
	NatTrkEnterprise	TTD County Made	The second
	Natificiation Natificiation	RTP bloanty Mode.	secure Payoad (SUES) with labels to insecure V
	• NatTrkWithRegistration	Payload Encr. used:	No
	• NatTrkWithRegistrationMultiNum	Additional Mediasec Parameters Supported:	Not supported
	• NeoTel	Registrar	
	8 OZ Czech	Use Registrar	
	OpenScapeUC		-
	B Orange	IP Address / Host name:	
	B	Specify Port:	
	B	Reregistration Interval (sec)	0
	B Russmedia IT	Press	
	8	Floxy	
	8 Ø SIP Trunk Flexx	IP Address / Host name:	10.180.0.4
	SIPQTrkWithoutRegistration	Specify Port:	
	III I SIPGTrkWithRegistration	TCP/UDP Port:	50013
	B © Skype		
	Segar Distrings Vice Arrays	TLS Port	50013

NOTICE:

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

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

5.1 OpenScape 4000 Routing

For full DN dialing

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

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

For extension dialing

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

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

6 Restrictions

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

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

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

mitel.com

🕅 Miteľ

© 2025 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.