



A MITEL
PRODUCT
GUIDE

OpenScape Solution Set V11

Zoom with Mitel OpenScape Voice and Mitel OpenScape SBC

Phone System Integration (PSI) Solution Guide

04/2025

Notices

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

Trademarks

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

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Contents

1 History of Changes.....	5
2 Introduction.....	6
2.1 Target audience.....	6
2.2 Prerequisites.....	6
2.2.1 User Roles and Permissions.....	7
2.2.2 Network requirements.....	8
3 Overview.....	9
3.1 Key Components.....	9
3.2 Overview of the Phone System Integration (PSI) solution.....	10
3.3 Related Documentation.....	11
4 Integrating Zoom with CloudLink.....	12
4.1 Adding Zoom integration to a customer account.....	12
4.2 Enabling Zoom integration in a customer account.....	13
4.3 Setting up a CloudLink account in Zoom Marketplace.....	14
5 Licensing.....	16
6 Configuring OpenScape Voice.....	17
6.1 Configuring RTP settings.....	17
6.2 Configuring Endpoints.....	18
6.2.1 Configuring the OpenScape SBC Endpoint.....	18
6.2.2 Endpoint Overview.....	22
7 Configuring OpenScape SBC.....	24
7.1 Configuring Network settings.....	24
7.2 Configuring SIP Server.....	26
7.3 Configuring Certificates.....	28
7.4 Configuring Media Profiles.....	31
7.4.1 Configuring the Zoom PSI Media Profile.....	31
7.4.2 Configuring the OpenScape Voice Media Profile.....	33
7.5 Configuring Remote Subscribers.....	33
7.6 Push Notification.....	34
7.6.1 Enabling Push Notification Service.....	34
8 Configuring CloudLink integrations.....	35
8.1 Integrating Common Management Platform with CloudLink.....	35
8.2 Enabling OpenScape Voice and CloudLink to access the Internet via a proxy.....	37
8.3 Integrating OpenScape Voice with CloudLink.....	38
8.4 Integrating OpenScape SBC with CloudLink.....	40
8.5 Configuring the PBX system settings in Mitel administration.....	43
9 Provisioning Users.....	46
9.1 User provisioning in the Zoom tenant.....	46
9.1.1 Adding a new Zoom user.....	46
9.1.2 Setting up the Zoom account from invitation.....	47
9.1.3 Configuring Zoom Phone System Integration.....	48
9.1.3.1 Configuring Phone System Integration settings.....	48
9.1.3.2 Adding Zoom users to the Mitel integration.....	48
9.2 Enabling an OpenScape Voice Subscriber for a Zoom connection.....	49
9.3 Creating a new SBC configuration for Zoom users.....	50

9.4 Integrating OSV subscribers with Zoom users.....	51
10 Monitoring and Troubleshooting Zoom Integration in Mitel CloudLink Admin Portal.....	55
10.1 Viewing the Zoom integration status.....	55
10.2 Generating a User Comparison Report.....	57
10.3 Troubleshooting common issues identified in the User Comparison Report.....	58
10.4 Viewing the Event History table (Zoom integration).....	59
11 Configuring E911 Calls.....	60
11.1 OpenScape SBC E911 Configuration.....	61
11.1.1 Configuring an E911 Media Profile.....	61
11.1.2 Configuring Remote Endpoints.....	62
11.1.2.1 E911 SIP Service Provider Profile Configuration.....	62
11.1.2.2 E911 Remote Endpoint Configuration.....	63
11.2 OpenScape Voice E911 Configuration.....	64
11.2.1 Configuring an E911 Provider Remote Endpoint.....	65
11.2.2 Translation Configuration.....	65
11.2.2.1 Configuring the E911 Call Routing.....	66
11.2.3 Configuring an Access code.....	67
11.2.4 Destinations and Routes Configuration.....	67
11.2.4.1 Configuring the Emergency Destination.....	67
11.2.5 Configuring a new Destination Code.....	68
11.3 CloudLink E911 Configuration.....	69
11.4 Adding IP Range Mapping (Redsky).....	69
12 Appendix.....	71
12.1 Appendix A: Restrictions and Known Issues.....	71
12.2 Appendix B: Default User Name and Password.....	72

1 History of Changes

Issue	Date	Summary
1	02/2025	The first issue of the guide
2	03/2025	Updated and enhanced the following chapters: <ul style="list-style-type: none"> • Configuring RTP settings on page 17 • Endpoint Overview on page 22 • Configuring OpenScape SBC on page 24 • Configuring Media Profiles on page 31 • Enabling an OpenScape Voice Subscriber for a Zoom connection on page 49 • Creating a new SBC configuration for Zoom users on page 50 • Configuring an E911 Solution • Appendix A: Restrictions and Known Issues on page 71
3	03/2025	Updated the following chapters: <ul style="list-style-type: none"> • Configuring Media Profiles on page 31 • Appendix A: Restrictions and Known Issues on page 71
4	03/2025	Updates and enhancements in the entire document.
5	04/2025	Updated the Prerequisites on page 6 section.

2 Introduction

This document outlines how to connect the OpenScape Voice (OSV) and OpenScape SBC (OSSBC) to Zoom.

Zoom is a cloud-based phone system that provides voice communication features such as call management, call forwarding, voicemail, and integration with Zoom Meetings. The Zoom - Mitel Phone System Integration (PSI) solution offers a hybrid communication model that enables users to maintain the telecom functions with their OpenScape Voice system while extending its functionality with Zoom's cloud-based features.

This integration allows Zoom's Phone tab to become a SIP Softphone that registers to the Mitel Calling Platform, utilizing the OpenScape SBC, if accessing over the Internet. The OpenScape SBC acts as the secure registration point between your on-premises Mitel PBX and Zoom Workplace clients. This allows various Zoom PSI endpoints - including desktop clients, mobile devices, and desk phones - to connect directly to your Mitel system through SIP registration.

The Zoom-Mitel PSI integration requires all key components to be properly configured within the user environment. This guide provides the essential setup steps to establish secure, reliable communication paths that will enhance your organization's collaboration capabilities.

2.1 Target audience

This document is intended for professionals involved in configuring and managing the Zoom-OSV-SBC integration, specifically those working with OpenScape Voice (OSV) and OpenScape Session Border Controller (OSSBC) components. The target audience includes implementation engineers, field technicians, system administrators, business partners, solution providers, and customers directly involved in the deployment and management of the integration.

2.2 Prerequisites

Supported product versions

Product	SW Version (minimum)
Zoom Workplace Client	6.3.6
OpenScape Voice with active SSP / SWA (Unify Software Support / Mitel Software Assurance)	V10R3.33.3
OpenScape SBC	V11R2.1.0
OpenScape SBC Management Portal	V10R2.4.0
OpenScape UC ISO files	V10R6 FR7 HF1
OpenScape Common Management Platform	V10R6

System Requirements and Licenses

- **Zoom**

- Supported License per user which includes Zoom Workplace Business/ Business+, Zoom Workplace Essential/sEnterprise/Enterprise+/ Enterprise Premier, Legacy Meeting Licenses ENH/EAH.
- Zoom Phone initial setup is completed. See the *How to Complete Initial Setup* section in [Zoom Phone initial setup](#).
- [Zoom-Mitel Phone System Integration support page](#).
- Automatic Phone assignment for Zoom Workplace Licences is disabled.
- Zoom Phone External Contacts setup for any non-Zoom, Mitel users.

2.2.1 User Roles and Permissions

- **Mitel Administration**

To set up the CloudLink and Zoom integration, you must be a CloudLink account admin. This role is assigned to a user by a Mitel Partner or by an Account Admin.

Account Admins can:

- Add, edit, or delete users (including other Account Admins).
- Enable or disable administrative rights for users.
- Configure the integration and connect the on-premise software to CloudLink.

Regular CloudLink users cannot perform this setup. For more information, refer to the [Mitel Administration User Guide](#).

NOTICE:

A Zoom admin does not need to be a CloudLink admin, unless they also need to manage CloudLink settings.

End users authenticate through Zoom and do not interact with CloudLink directly. They will not see or manage CloudLink settings.

After the initial setup, the integration operates using **service accounts**, ensuring continued functionality without requiring individual admin access.

- **Zoom**

- Zoom Account, Business or Enterprise.
- Account Owner or Admin with a Role for managing Users, Phone System Integration, and Zoom Phone.

To manage users, Phone System integrations and maintain a stable and functional integration, you must create and use a dedicated **Admin user** (service account) with a unique email address on your Zoom site specifically

for the integration. This account must remain active and should not be deactivated.

Do not use a regular user account, as deactivating it (e.g., if the user leaves) will cause connection failure.

For more information, refer to [Managing users](#).

2.2.2 Network requirements

Zoom Workplace

The Zoom Workplace app uses the standard Firewall ports and IP ranges. To add the required Firewall rules, refer to the **Zoom firewall rules** and **Firewall rules for Zoom website** sections in the [Zoom network firewall or proxy server settings](#) page.

Zoom PSI

Firewall rules for incoming traffic:

When the Client is on the Internet, the following incoming traffic must be allowed for the Zoom PSI client:

- SIP over TLS (TCP port 5061): The Zoom PSI client, like any other SIP remote client, must be able to connect to the external firewall of the OSSBC, which is located in the DMZ. It should be able to connect to the SIP/TLS port of the access interface of OSSBC via the external firewall. The default port value is 5061.
- SRTP media traffic (UDP): SRTP packets should be forwarded to the access interface of the SBC, based on the configured port range of the OSSBC.

Firewall rules for outgoing traffic:

When the Client is on-premise, the following outgoing traffic must be allowed for the Zoom PSI client:

- DNS (UDP/TCP port 53): PSI client needs to resolve the FQDN of the external firewall of the OSSBC using DNS.
- SIP over TLS (TCP port 5061): PSI client must be connected to the external firewall of the OSSBC using the SIP/TLS. The default value is 5061.
- SRTP media traffic (UDP) : SRTP must be allowed to reach the external firewall of the OSSBC, based on the configured port range of the OSSBC.

3 Overview

This chapter provides an overview of the integration solution, detailing the key components, actions, and configurations necessary for phone system integration. It also outlines how the Zoom, SBC, and OSV configurations interact with each other and other critical components of the solution.

3.1 Key Components

The key components of the Zoom-OSV-OSSBC phone system integration solution are as follows:

- **Zoom Web Portal:** Allows you to customize your profile and configure your Zoom settings. When setting up your Zoom-OSV integration, you are granted admin access to the Zoom web portal.
- **OpenScape Voice (OSV):** OpenScape Voice is a scalable SIP-based IP system that provides enterprise-class communications functionality. The OSV platform controls the users' telephony capabilities and manages SIP signaling, call routing, and PSTN and Zoom Phone integration.
- **OpenScape SBC (OSSBC):** OpenScape SBC is a software-based network border element designed to deliver superior Voice over IP (VoIP) security and cost savings. It serves as the secure gateway between OSV and external networks, managing SIP traffic flow and ensuring protected communications.
- **CloudLink Platform:** Mitel CloudLink Platform enables communication between the on-premise PBX (such as OpenScape Voice) and cloud-based applications. Acting as the intermediary, CloudLink platform bridges the Zoom and OSV systems, ensuring seamless account integration.

To properly associate a gateway with a new customer account on the CloudLink platform, the Mitel Partner or the Account Admin must access the Mitel Administration.

- **CloudLink Daemon:** CloudLink Daemon is a software component designed for integration with multiple unified communication platforms. It complements the CloudLink gateway, which connects premise-based PBXs to the CloudLink platform and CloudLink applications, by enabling additional features.

The CloudLink Daemon is embedded in the OpenScape Voice platform. Its primary function is to facilitate the connection with Mitel CloudLink enabled applications such as Zoom PSI.

- **Mitel Administration:** Mitel Administration is a web-based application that enables Mitel Partners to create and manage customer accounts. It also allows the Account Administrator of a customer account to manage the account and its users.

Once CloudLink integration is enabled, users within a customer account can access various Mitel applications and third-party CloudLink applications.

- **Unify Common Management Platform:** This web-based configuration interface supports the OpenScape communications solution. It provides tools for connecting CloudLink, managing Zoom configurations, and integrating Zoom users with OSV users (subscribers).

Overview

Overview of the Phone System Integration (PSI) solution

For an overview of the documentation set for each key component and additional configuration details, please refer to the [Related Documentation](#) section and the references throughout this guide.

3.2 Overview of the Phone System Integration (PSI) solution

OpenScape Voice (OSV) and OpenScape Session Border Controller (SBC) work together to enable seamless integration between Zoom clients and external networks, including the Public Switched Telephone Network (PSTN).

The OpenScape SBC acts as a secure gateway, managing network boundaries, while OpenScape Voice handles core telephony functions including SIP message manipulation and call routing. This integration establishes reliable communication paths between Zoom accounts and OSV subscribers, ensuring smooth call flow in both directions.

The following chapters provide detailed configuration instructions for integrating Zoom, OSV, and OSSBC components into your system.

The guide begins with the configurations needed for the [Zoom-CloudLink integration](#) configurations, followed by the steps required before setting up and provisioning Zoom-OSV users.

Setting Up Users for the Zoom-OSV Integration

The Zoom-OSV integration involves several key steps:

- 1) Configuring the Zoom and CloudLink integration.
- 2) Configuring OpenScape Voice and OpenScape SBC.
- 3) The CloudLink Daemon must be integrated with OpenScape Voice, OpenScape SBC and Common Management Platform.
- 4) Establishing CloudLink connectivity for managing Zoom users associated with OSV subscribers.
- 5) Adding users (if not already added) and assigning licenses in your Zoom account.
- 6) Configuring user mapping between Zoom and OSV through the Unify Common Management Platform.
- 7) Completing user provisioning to finalize the integration.

Your system is fully integrated upon completing the configuration steps outlined or referenced in this document. The integration benefits users with seamless call routing, enhanced communication security, efficient traffic management between Zoom clients and the OSV platform, and a unified user experience across cloud and on-premises systems.

Zoom PSI Phone for Mitel OpenScape Voice

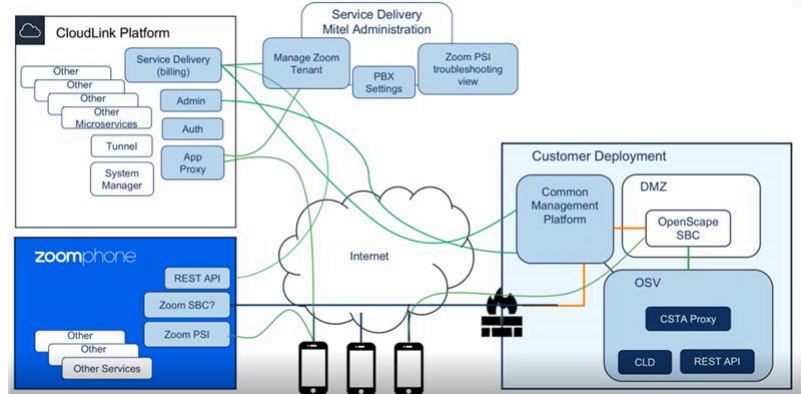


Figure 1: Network Topology Block Diagram

3.3 Related Documentation

Zoom

- [Zoom-Mitel Phone System Integration support page](#)

OpenScape Voice

- [OpenScape Voice V10 Administrator Documentation](#)
- [OpenScape Voice V10 Service Manual, Service Documentation](#)
- [Unify OpenScape Voice Service Manual: Installation and Upgrades](#)
- [Unify OpenScape Voice V10 Interface Manual: Volume 4 CSTA Interface Description](#)
- [OpenScape Solution V11, Zoom with OpenScape Voice and OpenScape SBC BYOC \(Bring Your Own Carrier\).](#)

OpenScape SBC

- [OpenScape SBC V11 Administration Guide](#)
- [OpenScape SBC V11 Configuration Guide, Administration Documentation](#)
- [OpenScape SBC V11 Installation Guide](#)
- [OpenScape SBC V11R2 Security Checklist](#)
- [OpenScape SBC Troubleshooting Guide, Service Documentation](#)

CloudLink

- [CloudLink Daemon Solution Guide](#)
- [CloudLink Gateway User Guide](#)
- [Mitel Administration User Guide](#)

OpenScape Common Management Platform

- [OpenScape Common Management Platform V10 Administrator Documentation](#)

4 Integrating Zoom with CloudLink

This chapter describes the Zoom and CloudLink integration.

Before proceeding with the configurations, ensure you have the required user accounts and permissions. For more information, see [User Roles and Permissions](#) on page 7.

4.1 Adding Zoom integration to a customer account

You can configure integrations with Zoom using Mitel Administration. If Zoom integration is enabled for a customer account, users in that account can integrate their Zoom account with their CloudLink applications.

Prerequisites

You have a Zoom Business or Enterprise account.

You have obtained the necessary Zoom PSI licensing.

You have created a dedicated service account (admin user) with a unique email address on your Zoom account portal, exclusively for the integration. For more information, see [User Roles and Permissions](#) on page 7.

Step by Step

- 1) Log in to Mitel Administration.
- 2) Click **Account** from the left main menu.
The **Account Information** page of the customer account opens.
- 3) In the **Integrations** section, click **+ Add new**.
The **Integrations** pop-up window opens.
- 4) Select the **3rd party** tab.
A pop-up screen displays the available third-party integrations.
- 5) Click **Add** next to the **Zoom** integration and then click **Done**.
- 6) The Zoom integration is added to the customer account and it is displayed in the **Integrations** section of the **Account Information** page.

NOTICE: Mitel Partner cannot enable integrations in the Partner Account as the integration with other applications is not supported for Partner Accounts. To integrate CloudLink with other applications, a Partner must create a customer account and enable integrations in that account. It is recommended to disable any existing integrations in the Partner Account to have the full functionality of CloudLink features. For more information about Partner Accounts, see [Log in as a Mitel Partner](#).

Next steps

Enable Zoom Integration: [Enabling Zoom integration in a customer account](#) on page 13.

4.2 Enabling Zoom integration in a customer account

After adding the Zoom integration to a customer account, you must enable the integration.

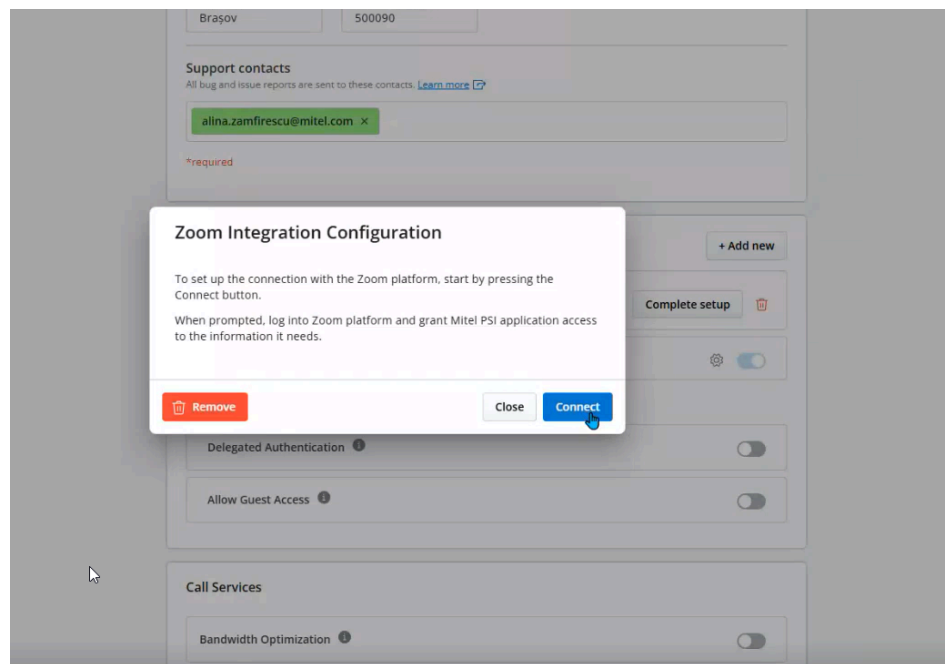
Prerequisites

Zoom integration must be added in the customer account, as described in [Adding Zoom integration to a customer account](#) on page 12.

To complete the Zoom integration via the **Integrations** panel:

Step by Step

- 1) Log in to Mitel Administration as an Account Admin.
- 2) Click **Account** from the left main menu.
The **Account Information** page of the customer account opens.
- 3) Click **Complete Setup** next to the **Zoom** integration in the **Integrations** section.
The **Zoom Integration Configuration** page opens.
- 4) Click **Connect**.



The **Zoom Sign In** window opens.

If you have already signed in, then you will be redirected to the Zoom Authentication window.

- 5) Enter the credentials and click **Sign In**.
The **Zoom Authorization** window opens.

Integrating Zoom with CloudLink

Setting up a CloudLink account in Zoom Marketplace

- 6) Click **Allow** to grant permission for the Zoom application to access and use the CloudLink account information.

If you click **Decline**, the Zoom integration will not be enabled, and the **Zoom Authorization** window will remain open.

To continue, close the Zoom Authorization window, click **Connect** again on the Zoom Integration Configuration page, and then click **Allow** in the Zoom Authorization window.

Next steps

To remove Zoom integration from a customer account, refer to the [Mitel Administration User Guide](#).

Once the Zoom integration is completed in Mitel Administration, the 'Mitel PSI' application automatically appears in the Zoom Customer's Marketplace under the **Added Apps** section.

4.3 Setting up a CloudLink account in Zoom Marketplace

You can configure your Mitel PSI connection via the Zoom web portal.

Prerequisites

You have a Zoom account, Business or Enterprise.

You are an Account Owner or Admin with a role for managing Users, Phone System Integration, and Zoom Phone.

You have obtained the necessary Zoom PSI licensing.

The **Mitel PSI** app is published into the Zoom Marketplace. For more information, refer to [Zoom-Mitel Phone System Integration support page](#). If you cannot see the app, please contact your Zoom administrator or Mitel support representative.

IMPORTANT:

To maintain a stable and functional integration, you must create and use a dedicated admin user (service account) with a unique email address on your Zoom site specifically for the integration. This account must remain active and should not be deactivated. The provisioning of the Mitel PSI app to your CloudLink Platform (CLP) happens automatically once the proper setup is complete.

For more information, see [Prerequisites](#) on page 6.

Step by Step

- 1) Log in to the [Zoom App Marketplace](#).
- 2) Search for the **Mitel PSI** app by using the search bar, selecting a category, or filtering the displayed apps.
- 3) Click **Create Connector**.

- 4) Click **Connect** to confirm you want to connect the third-party Mitel Connector to your Zoom account.

A browser window will open, requesting you to sign in to the Zoom Customer Administrator account.

- 5) Click **Allow** to authorize the Mitel PSI application to access the necessary account information.

Once you are signed in, the communication between Zoom and Mitel's CloudLink will be complete.

5 Licensing

OSV for Zoom Workplace license is required for each user which needs to be enabled with Zoom integration.

IMPORTANT: Initial releases of Open Scape SBC for Zoom DO NOT require a Zoom PSI 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.

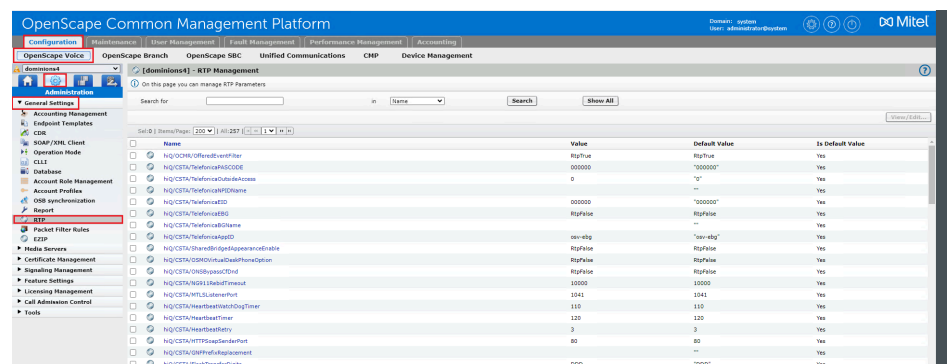
6 Configuring OpenScape Voice

This chapter describes the Mitel OpenScape Voice configuration for connecting to OpenScape SBC. The purpose of this connectivity is for Mitel OpenScape Voice to provide the necessary SIP message manipulation and call routing facilities to OpenScape SBC so that the latter can interconnect to Zoom.

6.1 Configuring RTP settings

Step by Step

- 1) Navigate to **Administration > General Settings > RTP**.



- 2) By default, the **Srx/Main/UseFullDnForZoom** RTP parameter is set to **RtpTrue**. Optionally, confirm that the default value is correctly set.

NOTICE:

This parameter is required to provide the full DN (E164 format) for calls between two Zoom PSI users.

If **Srx/Main/UseFullDnForZoom** is disabled, the number is displayed in a dialable format, such as an extension or any other format configured through Number Display Modification.

- 3) Click on the **hiQ/CCL/TrackingCategory** RTP parameter to edit its value. The **Edit RTP parameter** window pops up.
- 4) In the **Value** field, enter `Non-ONS`.
- 5) Set the **Srx/Sip/UpdateMethodSessionTimingEnable** value to **RtpTrue**.

NOTICE:

If your provider does not properly support the update method for Session Refresh, long calls (over 30 minutes) may drop.

In this case, the administrator should configure the endpoint with the attribute "Do Not Support Update Method for Session Timing".

- 6) Click **Save**.

6.2 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.

6.2.1 Configuring the OpenScape SBC Endpoint

To configure the OpenScape SBC Endpoint Profile:

Step by Step

- 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_PSI.
- 3) In the selected Business Group, navigate to **Profiles > Endpoint** and click **Add**.
- 4) In the **Add Endpoint Profile** window, under the **General** tab, configure the following:
 - a) **Name**: Enter the name of the endpoint profile. For example, EPP_SBC01.
 - b) From the **SIP Privacy Support** drop-down menu, select **Full**.

The screenshot shows the 'Add Endpoint Profile' window in a web browser. The browser address bar shows the URL: <https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessGroup/Profiles/PopUps/modif...>. The window title is '[OSV] - [ZOOM_BG] - Add Endpoint Profile'. The window has three tabs: 'General', 'Endpoints', and 'Services'. The 'General' tab is active. The 'General' tab contains the following fields:

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

Below these fields is a section titled 'Management Information' with the instruction: 'Please enter the data for the following fields in the corresponding screens.' This section contains four rows of fields:

- Class of Service:** (empty text field)
- Routing Area:** (empty text field)
- Calling Location:** (empty text field)
- Time Zone:** (empty text field)

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

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

The screenshot shows the 'Add Endpoint Profile' configuration page in the OpenScape management portal. The 'Services' tab is selected, and a red box highlights the 'Message Waiting' and 'Call Transfer' settings, both set to 'Yes'. Other settings like 'Call Forward Invalid Destination', 'Toll and Call Restrictions', 'Park to Server', and 'CSTA Network Interface Device' are set to 'No'. The 'Save' button is highlighted with a red box at the bottom right.

- 6) Click **Save**.
- 7) To configure the SBC Endpoint, navigate to **Unify OpenScape Common Management Platform > Configuration > Unify OpenScape Voice > Business Group > Members > Endpoints > .**
- 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) **Name:** Enter the name of the SBC endpoint. For example, **EP_SBC01**
 - c) **Profile:** Select the previously created endpoint profile. For example, **EPP_SBC01**.
 - d) **Endpoint Template:** Select **Central SBC** (set of pre-configured endpoint attributes).
 - e) Click **Save**.

The screenshot shows a web browser window with the URL https://10.70.16.6/management/portal/_ns:YWE1NWl3ZWVwLTVlZmItNDg2Ni0.... The page title is "[OSV] - [ZOOM_BG] - [Main Office] - Add Endpoint : EP_SBC01". The "General" tab is selected, and the "Endpoint" section is active. The form contains the following fields and values:

- Name:** EP_SBC01
- Remark:** (empty)
- Registered:** ☒
- Profile:** EPP_SBC01
- Branch Office:** (empty)
- Associated Endpoint:** (empty)
- Default Home DN:** (empty)
- Location Domain:** (empty)
- Endpoint Template:** Central SBC
- Endpoint Type:** Central SBC
- Max number of users:** (empty)

The "Save" button is highlighted in red.

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

The screenshot shows the 'Add Endpoint' configuration page in the OpenScape Voice management portal. The browser address bar shows the URL: <https://10.70.16.6/management/portal/Applications/Operation/OSV/BusinessG...>. The page title is '[OSV] - [ZOOM_BG] - [Main Office] - Add Endpoint'. The 'SIP' tab is selected, and the following settings are visible:

- SIP Private Networking:** ☐
- SIP Trunking:** ☒ (highlighted with a red box)
- SIP-Q Signaling:** ☐

Below these options is a section titled 'SIP Signaling' with a note: '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.'

The following settings are highlighted with a red box:

- Type:** Static
- Signaling Address Type:** IP Address or FQDN
- Endpoint Address:** 10.70.16.6
- Port:** 5060
- Transport protocol:** TCP

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

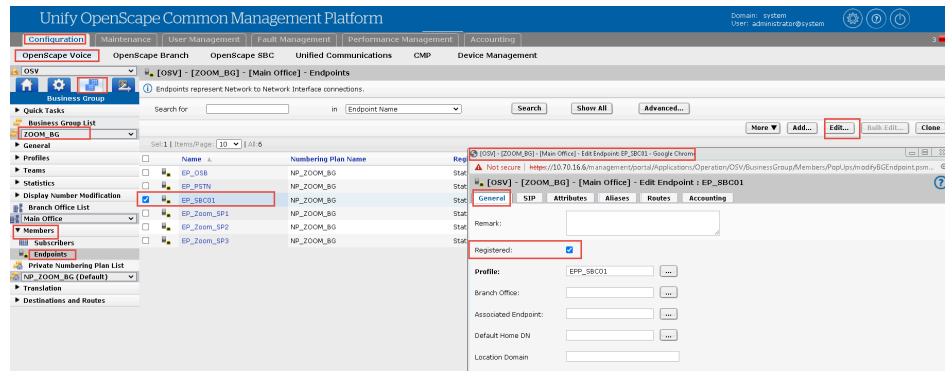
The screenshot shows the 'Edit Endpoint' configuration window for 'SBC_Zoom_PSI'. The 'Attributes' tab is active, displaying various settings. The 'Security' section at the bottom indicates a 'Trusted' status with a green checkmark and the ports '5060-5060'. The 'Save' button is highlighted with a red box.

- 12) Click **Save**.
- 13) The **Attributes** tab is populated automatically since the "Central SBC" template was selected in the General tab. Ensure that the following are selected:
 - a) SIP Proxy
 - b) Central SBC
 - c) Route via Proxy
 - d) Enable Session Timer
- 14) Select the **Aliases** tab and click **Add** to enter the SBC LAN interface for incoming SIP traffic.
- 15) Click **OK** and then click **Save**.

6.2.2 Endpoint Overview

- 1) Navigate to the **Unify OpenScape Common Management Platform > Configuration > Unify OpenScape Voice > Business Group > Members > Endpoints** window.
A list of all the configured endpoints in Unify OpenScape Voice is displayed.
- 2) Select an endpoint and click **Edit**.

- 3) In the **Edit Endpoint** pop-up, under the **General** tab, check the **Registered** checkbox.



- 4) Enable the **Registered** option for all the created endpoints.

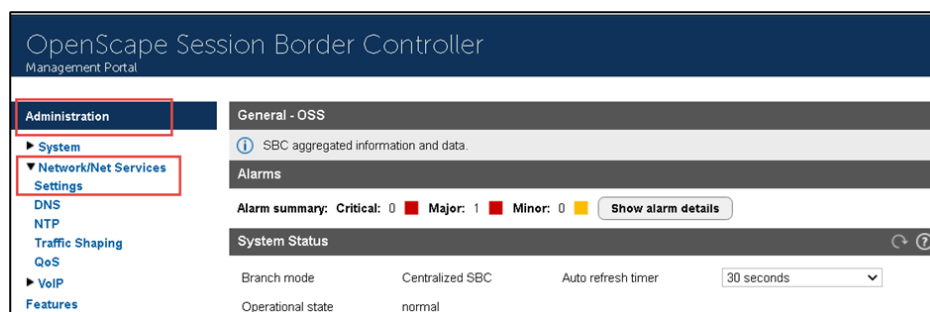
7 Configuring OpenScape SBC

This chapter outlines the configuration of OpenScape SBC for the integration with Zoom, allowing the Zoom PSI to function as a SIP softphone registered to OSV through the SBC over the Internet.

IMPORTANT: Initial releases of Open Scape SBC for Zoom DO NOT require a Zoom PSI 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.

7.1 Configuring Network settings

- 1) Log in to the OpenScape SBC Management Portal.
- 2) Navigate to **Administration > Network/Net Services > Settings**.

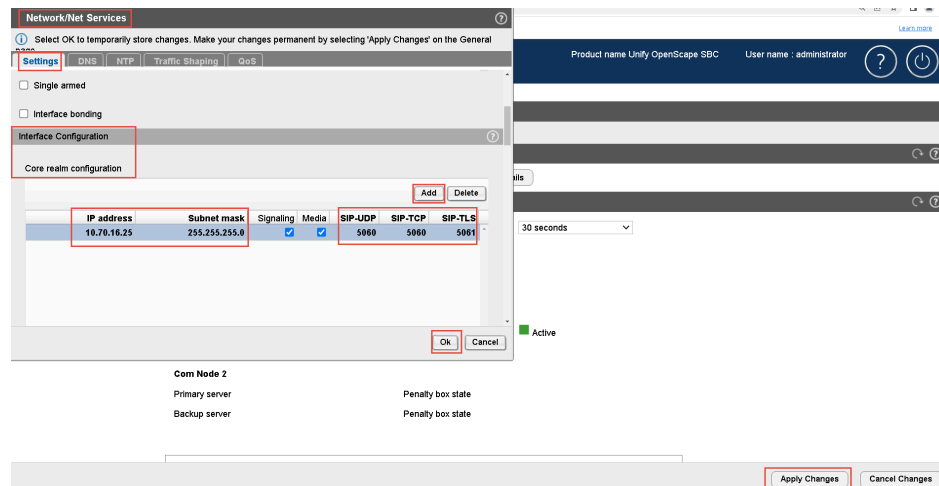


The **Network/Net Services** window pops up. By default, the **Settings** tab is displayed.

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

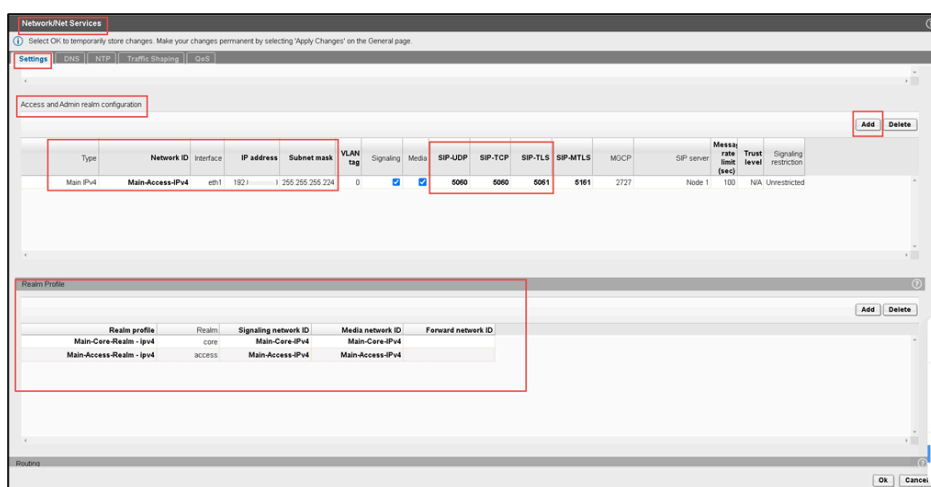
a) Configure the following:

- a) **IP address:** Enter the SBC IP address.
- b) **Subnet mask:** Enter the subnet mask value.
- c) **SIP-UDP:** Configure port number as 5060.
- d) **SIP-TCP:** Configure port number as 5060.
- e) **SIP-TLS:** Configure port number as 5061.
- f) Click **Ok**.
- g) Click **Apply Changes** on the SBC Main page.



4) Locate the **Access and Admin realm configuration** area and click **Add**.

- 5) 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.



NOTICE:

It is recommended to configure the PSI client to use **SIP/TLS**. **UDP** and **TCP** are not recommended for remote subscribers. If **SIP/UDP** and **SIP/TCP** are not needed for other purposes, their values can be set to **0**.

For security reasons, the default **SIP/TLS** port (**5061**) should be changed to a custom port (e.g., **65061**).

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

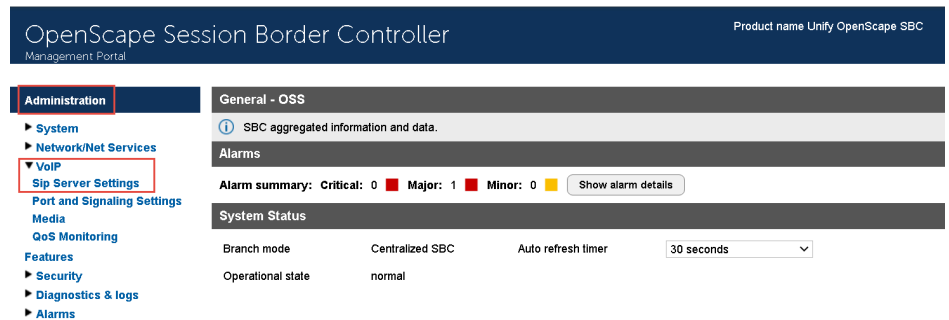
- 6) Locate the **Routing** area to configure the default gateway address.
- 7) In the **Routing Configuration** section, click **Add** and add the static routes for core and access interface.
- 8) Click **OK**.
- 9) Click **Apply Changes**.

7.2 Configuring SIP Server

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

- 1) Log in to the OpenScape SBC Management Portal.

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



The **VOIP** window pops up.

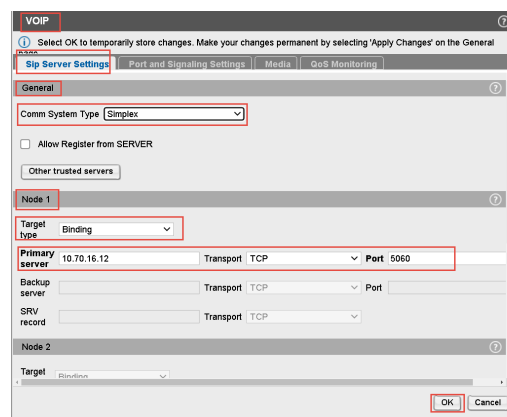
3) In the **Sip Server Settings** tab, enter the following:

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

NOTICE: The **Simplex** option depends on your OSV configuration. For example, if you have 2 OSV nodes, you will have to select the **Active-Standby**, **Collocated** or **Clustered** option.

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

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



4) Click **OK**.

5) Click **Apply Changes**.

NOTICE: The OS Voice SIP Signaling Manager addresses for UDP/TCP/TLS can be found in OS Voice node's **node.cfg** file located in the **/etc/hiq8000** folder (parameters **sipsml_vip** for **OS Voice Node1** and **sipsm2_vip** for **OS Voice**).

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

7.3 Configuring Certificates

For secure communication with Zoom, a Trusted Certificate must be installed in OpenScape SBC.

Zoom Phone System Integration 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 **Security considerations for the Zoom-Mitel integration** and Zoom certificate management, refer to the [Zoom-Mitel PSI integration](#).

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 Zoom, three files in 'pem' format are required from the Certification Authority:

- A certificate authority or certification authority (CA) certificate (for example, "ssl_root_with_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, "ServerCertificate.pem").
- OSSBC server certificate private key used for the CSR to CA (for example, "PrivateKey.pem").

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

Prerequisites

Adequate administrative permissions.

Adequate knowledge of TLS certificate handling.

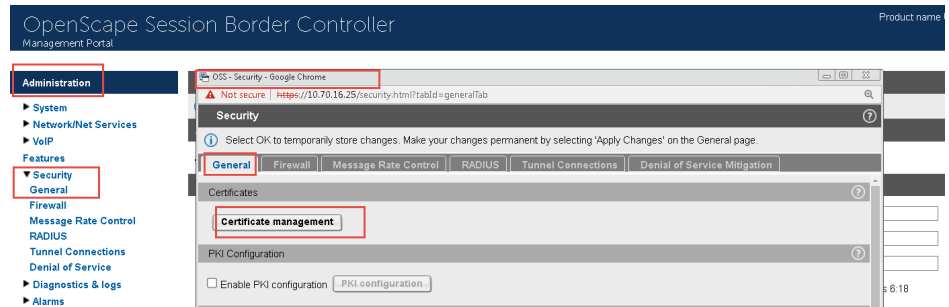
At least one OpenScape SBC is configured and in operation.

To configure Certificates:

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

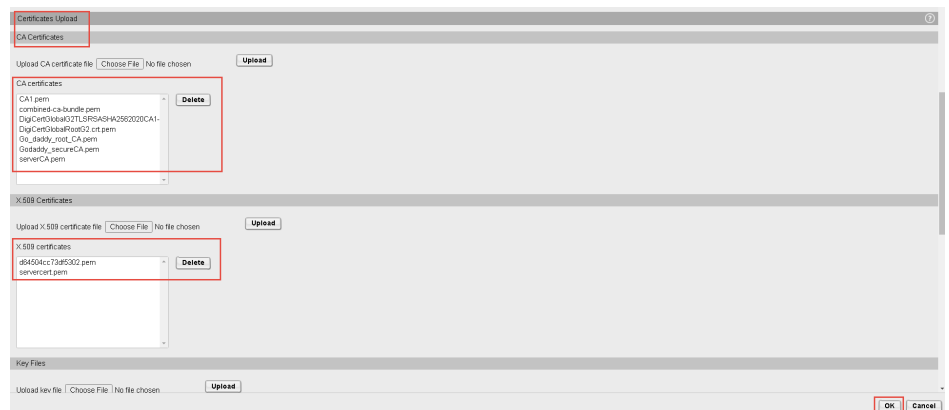
- 4) Click **Ok**.
- 5) Navigate to OpenScape SBC **Management Portal** > **Security** > **General**.
- 6) In the **Security** pop-up, under the **Certificates** section, click **Certificate Management**.

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



- 7) 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**.



- 8) Under the **Key Files** section, click **Choose File** and browse to select the OSSBC server certificate private key. Click **Upload**.
- 9) Edit the existing Certificate profile for OSV Solution: In the **Certificate Management** pop-up, under the **Certificate Profiles** area, select the **OSV Solution** certificate and click **Edit**.

NOTICE: The certificates should be applied to the default OSV certificate profiles that already exist in the SBC, called "OSV Solution". After uploading the certificates, you should edit this profile and select the uploaded certificates.

10) Configure the following parameters:

- a) From the **Local server certificate file** drop-down menu, select the certificate file (e.g., "ServerCertificate.pem").
- b) From the **Local CA file** drop-down menu, select the CA certificate (for example, "ssl_root_with_chain.pem").
- c) From the **Local key file** drop-down menu, select the private key file (for example, "PrivateKey.pem").
- d) From the **TLS version** drop-down menu, select **TLS1.2**.

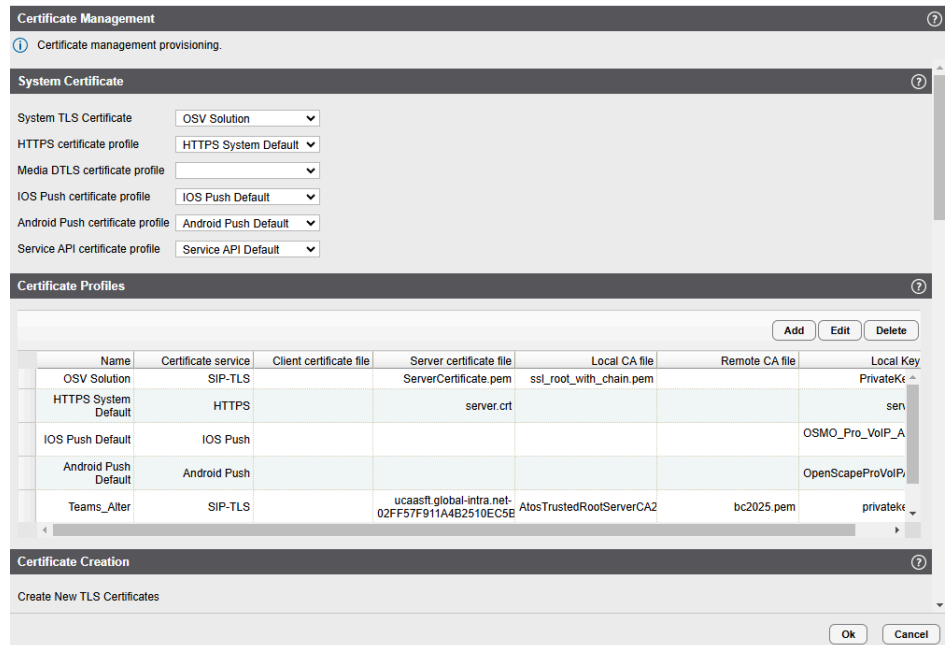
The screenshot shows the 'Certificate Profile' configuration window. At the top, a message states: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' The window is divided into several sections:

- Certificate Profile configuration:** This section contains several fields and dropdown menus. 'Certificate profile name' is set to 'OSV Solution'. 'Certificate service' is set to 'SIP-TLS'. 'Local client certificate file' is empty, with a 'Show...' button. 'Local server certificate file' is set to 'ServerCertificate.pem', with a 'Show...' button. 'Local CA file' is set to 'ssl_root_with_chain.pem', with a 'Show...' button. 'Remote CA file' is empty, with a 'Show...' button. 'Local key file' is set to 'PrivateKey.pem'. 'EC param' is set to 'secp256r1'. 'Attach to Config file' is an unchecked checkbox.
- Validation:** This section has a 'Certificate Verification' dropdown set to 'None'. Below it are two unchecked checkboxes: 'Revocation status' and 'Identity Check'.
- Renegotiation:** This section has an unchecked checkbox 'Enforce TLS session renegotiation'. Below it, 'TLS session renegotiation interval (minutes)' is set to '60'.
- TLS version:** This section has a 'Minimum TLS version' dropdown set to 'TLS V1.2'.

11) Click **OK**.

The **Certificate Profiles** section displays the updated OSV Solution certificate profile:

NOTICE: Please verify that the OSV Solution profile is selected from the **System TLS Certificate** drop-down menu, as shown in the image below.



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

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

7.4 Configuring Media Profiles

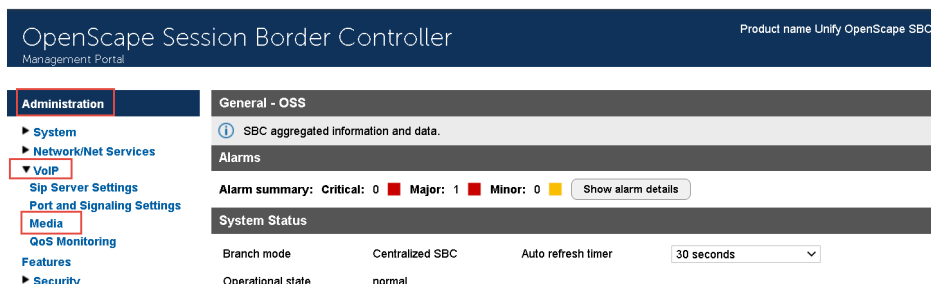
In the **Media Profiles** settings, various SDP messages and audio (RTP) traffic parameters can be configured for the OpenScape SBC SIP endpoints to Zoom PSI client, SSP (PSTN provider), and Unify OpenScape Voice.

7.4.1 Configuring the Zoom PSI Media Profile

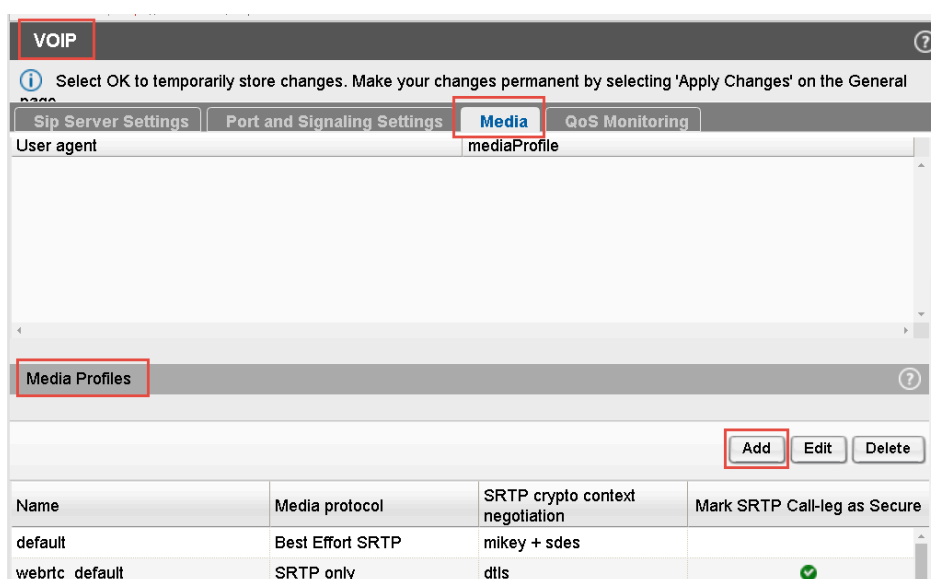
As an administrator, you must create a new user-agent header for Zoom PSI users (ZoomPbxPhone) and assign it a media profile, which supports SRTP only with SDES (cipher supported: AES-128). This media profile will be used by Zoom PSI users.

1) Log in to the OpenScape SBC Management Portal.

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



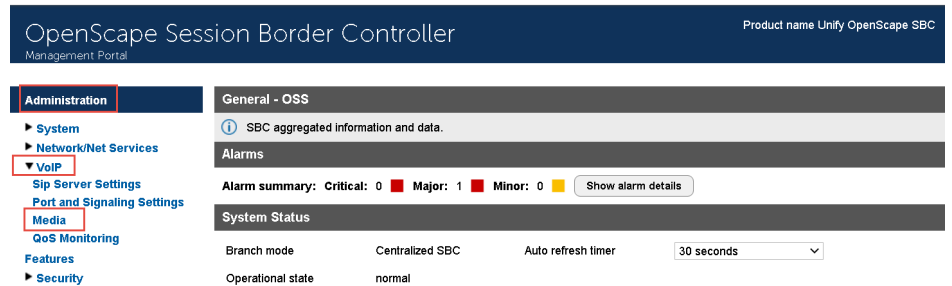
- 3) In the **Media Profiles** area, click **Add** to create the media profile for OpenScape SBC – OpenScape Voice connection.



- 4) In the **Media profile** pop-up, locate the **General** section and configure the following:
 - **Name:** Enter the name of the media profile. For example, Zoom_PSI.
 - From the **Media protocol** drop-down menu, select **SRTP only**
 - Check the **Keep sendonly attribute on NAT** option to allow the user to see the 'Remote Hold' indication.
- 5) Under the **SRTP configuration** area, select the **SDS** option (cipher supported: AES-128) for the **SRTP crypto context negotiation** configuration.
- 6) Under the **RTCP configuration** area, from the **RTCP Mode** drop-down menu, select **Bypass**.
- 7) In the **RTCP generation timeout** field, enter **4**.
- 8) Under the **Codec configuration** area, check the **Allow unconfigured codecs** checkbox.
- 9) Under **User agent**, click **Add** and select the Media profiles created for Zoom PSI.
- 10) Click **OK**.
- 11) Click **Apply Changes** on the SBC main page.

7.4.2 Configuring the OpenScape Voice Media Profile

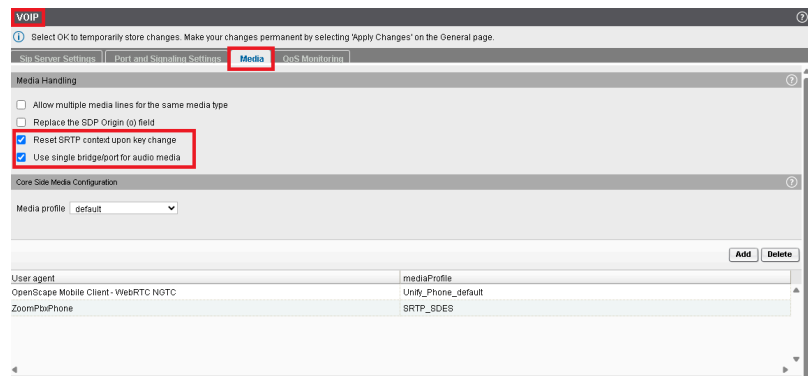
- 1) Log in to the OpenScape SBC Management Portal.
- 2) Navigate to the **Unify OpenScape SBC Management Portal > VOIP > Media** window.



- 3) In the **VOIP** pop-up, go to the **Media** tab.
- 4) Under **Media Handling**, check the following checkboxes:

- **Resend SRTP context upon key change**
- **Use single bridge/port for audio media**

It is recommended to enable the global parameter '**Use single bridge/port for audio media**' to ensure SBC maintains the same audio port with the PSI client during media renegotiation scenarios.

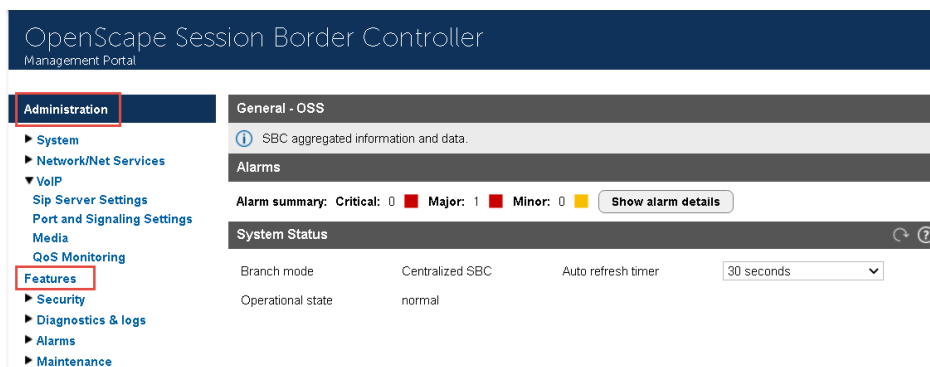


- 5) Click **OK**.
- 6) Click **Apply Changes** on the SBC main page.

7.5 Configuring Remote Subscribers

- 1) Log in to the OpenScape SBC Management Portal.

- 2) Navigate to the **Administration > Features** window.



- 3) In the **Features** pop-up, check the **Enable Remote Subscribers** checkbox and click **Configure**.
- 4) The "Enable register throttling" setting should be disabled to ensure that REGISTER messages from the mobile app are forwarded to OSV, when the app comes to the foreground or restarts.
- 5) In the **Remote Subscribers** window, check the **Enable register throttling for TLS** checkbox.
- 6) Set the **Maximum registration expiry time (sec)** to **2678400** (31 days), to allow the registration from Zoom PSI mobile clients.
- 7) Click **OK**.
- 8) Click **Apply Changes**.

7.6 Push Notification

The mobile push notification service allows users to get notified about an update when they are not actively using their mobile app.

You can set up mobile push notifications by configuring the required settings in the OpenScape SBC and CloudLink.

7.6.1 Enabling Push Notification Service

As an administrator, you can enable the push notifications features required for the Zoom mobile application.

Step by Step

- 1) Log in to the OpenScape SBC Management Portal.
- 2) Navigate to **Features**.
The **Features** window pops up.
- 3) Check the **Enable Push Notification Service** checkbox.
- 4) Click **Ok** and **Apply changes**.

8 Configuring CloudLink integrations

The CloudLink Daemon is a software component embedded in the OpenScape Voice platform. Its primary function is to facilitate the connection with Mitel CloudLink enabled applications such as Zoom PSI. This enables the management of Zoom users associated with the OpenScape Voice tenants, ensuring a secure connection through a proxy server. This chapter describes the CloudLink Daemon configuration for Common Management Platform, OpenScape Voice and OpenScape SBC.

The setup of the CloudLink Daemon is carried out through the following software applications:

- Administration program of the OpenScape SBC: OpenScape SBC Assistant.
- Administration program of the OpenScape Voice: OpenScape Common Management Platform.

For CloudLink troubleshooting information, refer to Chapter 7 of the [OpenScape SBC Troubleshooting Guide, Service Documentation](#).

8.1 Integrating Common Management Platform with CloudLink

As an administrator, you can configure CloudLink to integrate Common Management Platform (CMP) with CloudLink tenants. This integration enables the management of Zoom users associated with those tenants, ensuring a secure connection through a proxy server.

Prerequisites

- 1) Adequate administrative permissions.
- 2) Install the `cld-oscmp` CloudLink Daemon RPM package (UC ISOs of V10 R6 FR6). For more information, refer to the "Searching for RPMs" section, included in the **Using osc-setup for handling Repositories** chapter of the [OpenScape UC Application V10, Installation and Upgrade, Installation Guide](#).
- 3) CloudLink requires an internet connection. Set up a proxy server to gain Internet access for CloudLink only if necessary. For instructions on adding a proxy, refer to 'How to create a proxy server' in the [Common Management Platform V10 Administration Guide](#).
- 4) Acquire account for Mitel Administration portal.
- 5) Provision an NTP server for CMP.

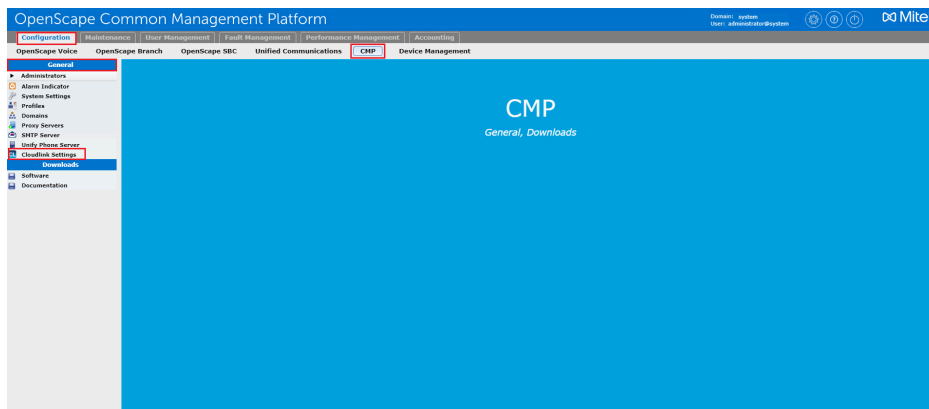
To set up a connection with CloudLink in the Common Management Platform:

Step by Step

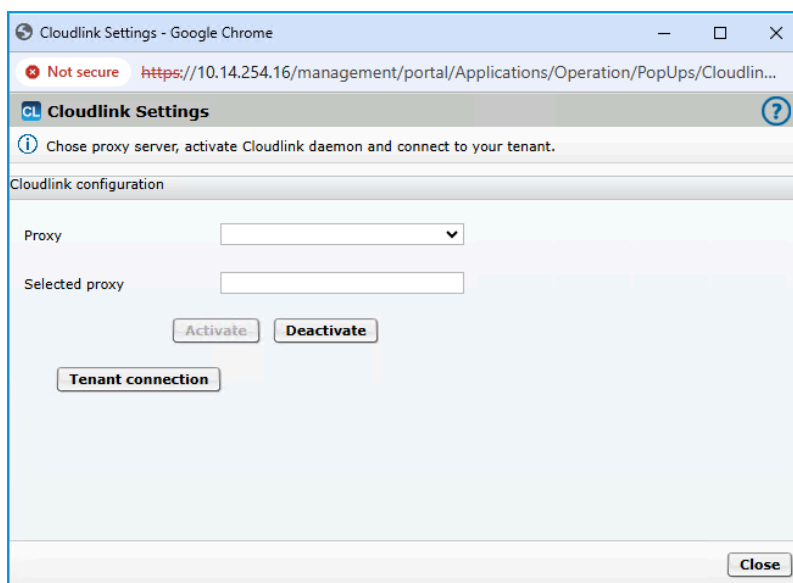
- 1) Log in to the OpenScape Common Management Platform.
- 2) To install the CloudLink Daemon package, execute the following command in cmd: `osc-setup in cld-oscmp`
- 3) Optional: To check the CloudLink Daemon status, execute the following command in cmd: `systemctl status cld`
By default, CloudLink Daemon is deactivated.
- 4) To activate CloudLink Daemon, on the **Configuration** navigation tab, click on the **CMP** navigation menu item.

- 5) In the navigation tree, under the **General** area, click **CloudLink Settings**.

NOTICE: The **CloudLink settings** option is visible only if the CloudLink Daemon package installation is successfully completed.



A **CloudLink Settings** window pops up.



- 6) From the **Proxy** drop-down menu, select a proxy that is configured for CloudLink.

The **Selected Proxy** field (read-only) displays the values that are already stored in CloudLink Daemon.

IMPORTANT: CloudLink requires an internet connection. Set up a proxy for CloudLink only if necessary. For instructions on adding a proxy, refer to 'How to create a proxy server' in the [Common Management Platform V10 Administration Guide](#).

- 7) Click **Activate** to enable CloudLink Daemon. To deactivate it, click **Deactivate**.

IMPORTANT: If you change the proxy selection after clicking the **Activate** button, you will need to click on it again.

- 8) Click **Tenant Connection** to set up a connection with a tenant.

NOTICE: The **Tenant Connection** button becomes active when the CloudLink daemon is enabled. Please note that it might take a few seconds for the button to activate after enabling it.

Upon clicking, you will be directed to the CloudLink Daemon window.

NOTICE:

If your CloudLink account is not linked, you will be prompted to log in with your admin credentials to establish the connection.

If the account is already linked, details of the connected account will be displayed.

- 9) To activate the CMP-CloudLink connection, click **Link to CloudLink**.
- 10) Enter your credentials in the CloudLink sign-in pop-up window and click **Next**.
The CloudLink Daemon window refreshes to display the CloudLink Tenant Information.

NOTICE: If the process is not complete, then please verify that you have configured a valid NTP (Network Time Protocol) server to CMP server. In case of time offset between CMP and CloudLink the creation of the token will fail.

- 11) Click **Close** to save the settings.

8.2 Enabling OpenScape Voice and CloudLink to access the Internet via a proxy

This section describes how to enable OpenScape Voice - CloudLink internet connectivity. System can access the internet via Proxy Server or directly. In case of direct internet connectivity, extra security measures, i.e. DMZ/firewall, are recommended.

IMPORTANT: Before starting this procedure, it is recommended that you back up or save the current `/etc/sysconfig/proxy-osv` to an external server for safekeeping. This ensures the original file can be restored if the OSV behavior following

the update necessitates it. Please review this entire procedure before proceeding with the actual updates.

The proxy settings are managed in the `/etc/sysconfig/proxy-osv` file. This file adheres to the same syntax as the standard `/etc/sysconfig/proxy` file, commonly used in Linux environments. The following variables are supported:

HTTP_PROXY: Specifies the proxy server for HTTP connections.

Examples:

- `HTTP_PROXY="http://<proxy-server>:<port>"`
- `HTTP_PROXY="http://123.123.123.123:8080"`

HTTPS_PROXY: Specifies the proxy server for HTTPS connections.

Examples:

- `HTTPS_PROXY="http://<proxy-server>:<port>"`
- `HTTPS_PROXY="http://123.123.123.123:8080"`

NO_PROXY: Defines a comma-separated list of hosts, IPs, or domains to bypass the proxy.

Examples:

- `NO_PROXY="localhost, 127.0.0.1, example.com"`
- `NO_PROXY="localhost, 127.0.0.1"`
- `NO_PROXY="localhost, 127.0.0.1, 11.12.13.14:8289"`

After the modification, duplex OSV nodes must be configured from state 4 to state 3 and then back to state 4 to ensure the caches are refreshed with the new data. This procedure must be performed on both nodes of the duplex OSV.

NOTICE: On OSV upgrades, the `proxy-osv` file will be migrated. Thus, once configured, the proxy configuration will not be affected by any upgrade or reconfiguration actions performed in the system. For detailed information on OSV installation and upgrades, refer to OpenScape Voice Service Manual: Installation and Upgrades.

8.3 Integrating OpenScape Voice with CloudLink

As an administrator, you can configure OSV connection to CloudLink Daemon via the Common Management Platform.

Prerequisites

Adequate administrative permissions.

CMP is connected to CloudLink.

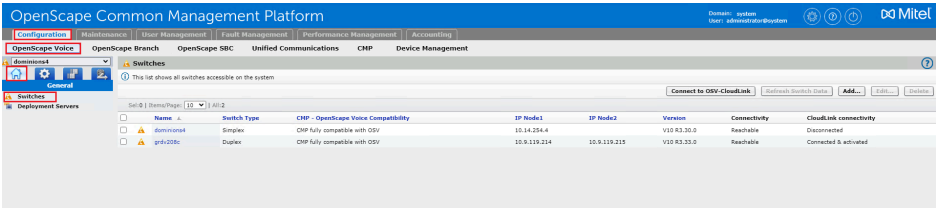
You have enabled [OSV-CloudLink to access the Internet via a proxy](#).

Both CMP and OSV clocks must be synchronized. It is recommended to configure both to use an NTP server for clock synchronization.

To connect OpenScape OSV to CloudLink:

Step by Step

- 1) Log in to the OpenScape Common Management Platform.
- 2) Navigate to the **Configuration > OpenScape Voice** tab and click on the **General** icon.



- 3) Select **Switches**.
The **Switches** dialog opens listing the switches accessible on the system.
- 4) Optional: Select a switch from the list of available switches. If no switch is selected, all listed switches will be included in the OSV-to-CloudLink connection.

NOTICE: The process may take several minutes if one of the switches does not have the Cloudlink Daemon installed.

- 5) Click **Connect to OSV/Cloudlink**.
CMP connects to Cloudlink Daemon on OSV nodes.
The **CloudLink connectivity** column displays the status of each system.
For more information, please refer to the **Status of the OSV system** table below.
- 6) To enable CloudLink features for Zoom on a switch, select the connected switch of your choice and click **Edit**.
The **Edit switch** window pops up.
- 7) Locate the **CloudLink Configuration** area and click **Enable container**.

NOTICE: The **Enable container** button is active only when the OSV status is **Connected** or **Connected and deactivated**, but NOT **Connected and activated**.

Please refer to the **Status of the OSV system** table below.


- 8) Click **Save** to save the settings.
The switch status is **Connected and activated**.

Table 1: Status of the OSV system

Status	Description
Disconnected	The OSV system is not connected to CloudLink.
Connected and deactivated	The CloudLink is successfully connected. CloudLink features for Zoom are <u>not</u> enabled.

Configuring CloudLink integrations

Integrating OpenScape SBC with CloudLink

Status	Description
Connected and activated	<p>The CloudLink is successfully connected and CloudLink features for Zoom are enabled.</p> <hr/> <p>NOTICE: To enable CloudLink features for Zoom, see step 7.</p> <hr/>
Connected and activated 	<p>One of the OSV nodes is not connected to CloudLink, or there has been an OSV failover.</p> <hr/> <p>NOTICE: To fix this manually, click the Enable container button.</p> <hr/>

Upon a successful connection, you can open the CloudLink Daemon window and configure the allocated tunnels.

8.4 Integrating OpenScape SBC with CloudLink

OpenScape SBC hosts its own instance of CloudLink Daemon which needs to be enabled and connected to CloudLink. For OpenScape SBC, CloudLink also serves as the platform for transmitting mobile push notification requests to the Zoom Service.

Prerequisites

Adequate administrative permissions.

SBC has internet connectivity.

Acquire credentials for a valid Cloudlink tenant.

To connect OpenScape SBC to CloudLink:

Step by Step

- 1) Log in to the OpenScape SBC Management Portal.

- 2) Navigate to the **System > Settings** tab.

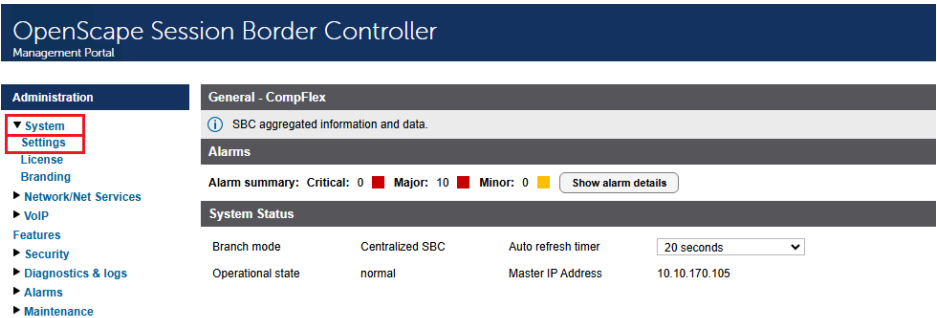
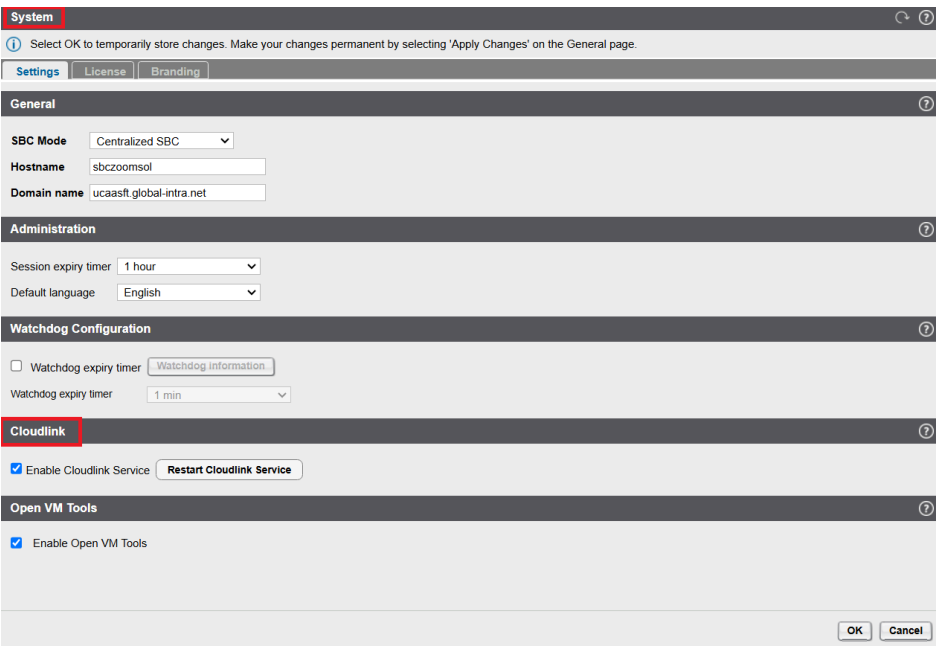


Figure 2:

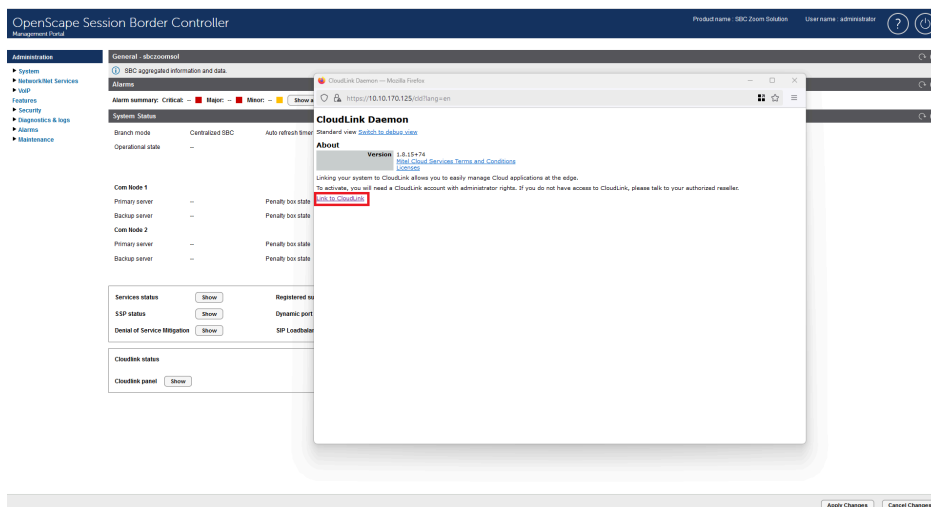
The **System** window pops up.

- 3) Locate the **CloudLink** section.
- 4) To enable the SBC-CloudLink connection, check the **Enable CloudLink Service** checkbox.



- 5) Click **OK**.
- You are redirected to the main page.
- 6) To display the SBC-CloudLink connection information, click **Show** next to the **CloudLink panel** item.
- The CloudLink Daemon window pops up. By default, CloudLink is disconnected.

- 7) Click **Link to CloudLink** to link CloudLink Daemon to CloudLink.



- 8) Enter your admin credentials in the CloudLink sign-in pop-up window and click **Next**.

After the CloudLink Daemon is enabled and linked to the CloudLink platform, the CloudLink status on the SBC Dashboard updates, and a green indicator shows that CloudLink Daemon is running and connected.

The CloudLink Daemon dashboard displays the following details:

- About
- CloudLink Registration
- Inventory Report Submission
- CloudLink Daemon Update
- Tunnels

NOTICE:

Upon a successful connection, an inventory report is generated and refreshed approximately every 30 minutes.

For the details on each of these functionalities, see the [CloudLink Daemon Solution Guide](#).

- 9) Optionally, to connect the CloudLink Daemon for each component or to enable the tunnel:
- a) In the standard view of the CloudLink Daemon dashboard, under **Tunnels**, select a component, e.g. SBC, to connect or link to, and then click **Start**.
 - b) Click **Yes** to confirm.
 - c) Log in to CloudLink as an administrator.

- 10) Optionally, you can view system information and launch a remote SBC configuration:

- a) Log in to Mitel Administration and navigate to **System Inventory > Platforms**.

The list of Platforms and Applications that are connected from the Tunnel in Server Manager are now populated under the Mitel Administration System Inventory page.

- b) To remotely access the CloudLink Daemon for SBC, click **Launch**.

NOTICE: The **Launch** button becomes active only after the tunnel has been successfully established.

- 11) To disconnect from CloudLink, click **Disconnect from CloudLink** in the main CloudLink window.

8.5 Configuring the PBX system settings in Mitel administration

After completing PBX integration with Cloudlink, optionally you can configure the system setting of the PBX.

The PBX system settings configured in CloudLink Account are not directly synced to the PBX. The settings have to be entered manually in the PBX.

NOTICE: The steps below are mandatory only if you are configuring Emergency calls.

Step by Step

- 1) Log in to Mitel Administration as an Account Admin.
- 2) On the left navigation menu click on the name of the PBX e.g. **OpenScape Voice** and select **System Settings**.
- 3) In the **Voicemail** area add a **Pilot Number** to dial for accessing the voicemail messages.

NOTICE: If using local voicemail, ensure you enter the pilot number of the Expressions voicemail system in the system settings.

4) In the **Feature Codes area you can configure feature codes for the users.**

a) To add a feature code:

- Select a **Feature** from the drop-down menu. The following features are available:
 - **Call Forward**
 - **Disable Call Forward**
 - **Do not Disturb**
 - **Disable Do not Disturb**
 - **Enable Call Forward**
 - **Enable Do not Disturb**

NOTICE: The same access codes can be configured in the PBX.

- Enter the **Dialing access code**.
- Click  **Add**.

b) To edit a feature code:

Select the feature code, click on the **Dialing access code** field and change the feature code.

c) To delete a feature code:

Select the feature code and click  next to the feature code.

5) In the **Emergency Numbers area you can configure the fallback emergency numbers.**

a) To add an emergency number:

- Click **Dialables**.
- Start typing a number for emergency calls, e.g.: 911, 112.
- Press enter, space or add a , (comma) to add the number.

b) To edit an emergency number:

Double click on the number and edit it.

c) To delete an emergency number:

Click X next to the number.

You can add multiple emergency numbers.

6) In the **Dynamic Location provider area configure a dynamic location provider for the emergency calls.**

Enter the following information:

- **Name**
- **Type**
- **Primary Server**
- **Secondary Server**
- **Customer ID:** the unique HELD identifier assigned to your organization by the service provider.
- **Secret:** the private key or token issued by the service provider to secure communication between Zoom client and the service. This acts as a password and should be treated with high confidentiality.
- **Extra Headers:** additional HTTP headers required by the service provider for platform communication. These headers might include custom

authentication schemes, API version, or specific configuration options required by the provider. Input must be added in JSON format.

NOTICE:

In some cases, you can retrieve emergency configuration information from your account with your emergency provider.

However, it is highly recommended to always verify the settings with your emergency provider.

7) Click **Save.**

All mandatory fields must be completed before clicking save.

If the Zoom client has an emergency configuration enabled, the user will receive the message **Emergency location detected** upon login.

You can check and troubleshoot the settings in the [Event History](#) page.

9 Provisioning Users

Integration between the CloudLink tenant and the Zoom tenant is established through a process that links the two accounts. On one side, there is the CloudLink tenant or account, and on the other, a corresponding Zoom tenant or account. These are interconnected via a configuration process performed through CloudLink. This chapter outlines the necessary steps for preparing and setting up OpenScape Voice subscribers, as well as provisioning users, to ensure seamless integration with Zoom.

9.1 User provisioning in the Zoom tenant

This chapter describes how to add a new Zoom user, set up a new Zoom account, and configure the Zoom-Mitel Phone System Integration.

For more detailed information on managing Zoom users, including deactivating, unlinking, or deleting users from your account, as well as performing actions such as batch importing and user auto-activation, refer to the links below.

-
- [Zoom-Mitel Phone System Integration support page](#)
 - [Managing users](#)
 - [Deactivating, unlinking, or deleting users from your account](#)
 - [Batch importing, exporting, or updating users on your Zoom account](#)
 - [Auto activating added users](#)
 - [User Management API's](#)

Zoom single sign-on configuration allows your Zoom users to log in to Zoom using their company credentials.

To configure Zoom single sign-on (SSO), refer to the links below:

- [Quick start guide for single sign-on \(SSO\)](#)
- [SSO with Active Directory](#)
- [Settings and Configuration for SSO](#)

9.1.1 Adding a new Zoom user

An account owner or admin can add users to their account in several ways. This section describes how to add a single new Zoom User, or multiple users by entering their email addresses.

Prerequisites

You have a Zoom account, Business or Enterprise.

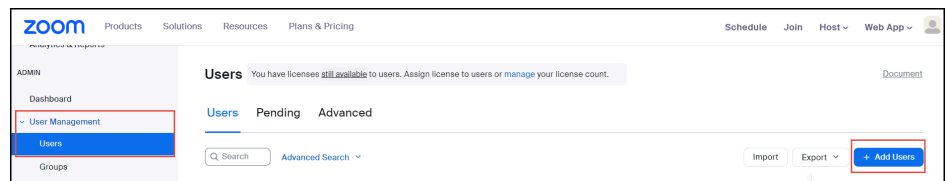
You are an Account Owner or Admin with a Role for managing Users, Phone System Integration, and Zoom Phone.

You have completed Zoom-CloudLink integration, as described in [Configuring CloudLink integrations](#) on page 35.

Step by Step

- 1) Log in to the Zoom web portal.

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



3) In the **Add Users** pop-up window, enter the user's email address.

To add multiple users with the same settings, enter multiple email addresses separated by commas: , .

NOTICE:

Email address is the unique cross-platform identifier for provisioning Zoom and CloudLink users.

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

5) Click **Add**.

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

New Zoom users will receive an activation email.

If a user already exists in Zoom, you will be prompted to accept the transfer of their account and be assigned to the new Zoom account owner.

Next steps

Activate the user(s) account.

Assign licenses to 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 [Assigning Zoom licenses](#) page.

9.1.2 Setting up the Zoom account from invitation

Prerequisites

You have received an email invitation from **no-reply@zoom.us** to set up your Zoom account.

NOTICE: Remember to check your junk or spam folder if you can't find the invitation email in your inbox.

Step by Step

- 1) Open the email and click **Activate your Zoom Account**.
- 2) On the **Activate Your Account** screen, enter the following details:
 - a) First Name
 - b) Last Name
 - c) Password

3) Click **Continue**.

The Zoom user account is activated. In the Zoom Web Portal, the new user(s) will now appear under the **Users** tab of the **User Management** section.

To recover a disabled, inactive or locked account, refer to the official [Zoom support](#) page.

9.1.3 Configuring Zoom Phone System Integration

9.1.3.1 Configuring Phone System Integration settings

As an administrator, you can set up users for the Zoom-OSV integration.

Prerequisites

You have a Zoom account, Business or Enterprise.

You are an Account Owner or Admin with a Role for managing Users, Phone System Integration, and Zoom Phone.

You have added Zoom users and assigned licenses to them.

Step by Step

- 1) Log in to the Zoom Admin Portal.
- 2) Navigate to **Account Management** > **Phone System Integration**.
- 3) Go to the **Settings** tab.
- 4) In the **Integrated calling on Zoom mobile** area, click the **Allow use the integrated phone system to phone call on Zoom mobile client** toggle to enable it.

NOTICE:

Ensure that this setting is always enabled. For more information, refer to [Configuring the Zoom-Mitel PSI integration](#).

9.1.3.2 Adding Zoom users to the Mitel integration

As an administrator, you can set up users for the Zoom-OSV integration.

Prerequisites

You have a Zoom account, Business or Enterprise.

You are an Account Owner or Admin with a Role for managing Users, Phone System Integration, and Zoom Phone.

You have added Zoom users and assigned licenses to them. Zoom user accounts are activated.

Step by Step

- 1) Log in to the Zoom Admin Portal.
- 2) Navigate to **Account Management** > **Phone System Integration**.
The **Integrated users** tab is displayed.
- 3) Click **Add users**.
The **Add users** window pops up.
- 4) Select the user(s) you want to activate.

NOTICE:

You can add a maximum of 50 users at a time.

Ensure that the email address of the user(s) you add matches the email address that was used while creating the Zoom user and the assigned license.

- 5) Click **Add**.

The new user(s) will be added under the **Integrated Users** tab with the status **Pending SIP credential**.

This status will be updated once the OSV subscriber-Zoom user integration is completed.

To add non-Zoom users to Zoom directory, refer to the [Creating a shared directory of external contacts](#) page and [OpenScape Solution V11, Zoom with OpenScape Voice and OpenScape SBC BYOC \(Bring Your Own Carrier\)](#).

To import users with a CSV file, refer to [Zoom-Mitel Phone System Integration support page](#).

9.2 Enabling an OpenScape Voice Subscriber for a Zoom connection

As a CMP administrator, you must manually configure the OSV subscriber(s) to enable their Zoom connection.

Prerequisites

Adequate administrative permissions.

CMP is connected to CloudLink Daemon, as described in [Integrating Common Management Platform with CloudLink](#) on page 35.

OSV is connected to CloudLink, as described in [Connecting OSV to CloudLink Daemon](#).

You have provisioned users in the Zoom tenant.

To enable an OSV subscriber:

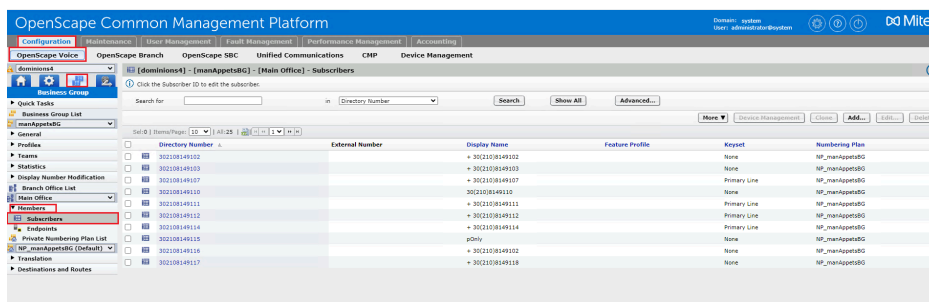
Step by Step

- 1) Log in to the OpenScape Common Management Platform.

Provisioning Users

Creating a new SBC configuration for Zoom users

- 2) Navigate to **Configuration > OpenScope Voice > Business Group > Members > Subscribers**.



- 3) Click on the OSV subscriber you want to enable.
The **Edit subscriber** window pops up.
- 4) Go to the **Routing** tab.
- 5) Scroll down to locate the **Zoom user** checkbox and click on it to enable it.

NOTICE: This attribute controls whether the specific user can accept a CallLogSnapshot. If enabled, OSV will respond with a CallLogEvent. Otherwise, it will return an `InternalServerErrorCode`.

If both parties in a call have this attribute enabled, the full number (E164 format) is used instead of the dialable format, such as an extension.

- 6) Go to the **Connection** tab and check the **Registration via Central SBC Allowed** checkbox.
- 7) Go to the **Security** tab and enter the **SIP Authentication** credentials:
 - a) Realm
 - b) User Name
 - c) Password
 - d) Confirm Password
- 8) Go to the **Features** tab and locate the **Subscriber Features** section.
- 9) For the **CSTA Access** item, select **Assigned** from the **Assignment** drop-down menu.
- 10) Click **Save** to save the settings.
You are redirected back to the main **OpenScope Voice** page.
- 11) Repeat the steps for all subscribers that will be integrated with Zoom users.

9.3 Creating a new SBC configuration for Zoom users

You can create a new Zoom Configuration in OpenScope Common Management Platform.

Prerequisites

Adequate administrative permissions.

CloudLink Daemon configurations are completed.

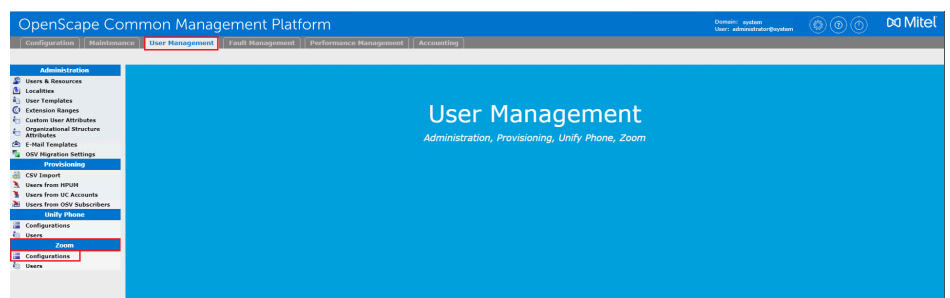
OSV subscribers are enabled for Zoom connection. For more information, refer to [Enabling an OpenScape Voice Subscriber for a Zoom connection](#) on page 49.

Zoom users have been configured in the Zoom tenant, as described in [User provisioning in the Zoom tenant](#) on page 46.

To create a new Zoom configuration:

Step by Step

- 1) Log in to the OpenScape Common Management Platform.
- 2) Click on the **User Management** navigation tab.
- 3) In the navigation tree, click on **Zoom > Configurations**.



A list of the existing SBC configurations is displayed.

- 4) Click **Add** to create a new Zoom configuration.
A new **Add configuration** window appears containing the following fields:

- **Name**
Name of the SBC configuration.
- **IP/FQDN address**
IP or FQDN of the SBC access interface that has a public address, or the external firewall of the SBC if it is located in the DMZ.
- **Port**
Specify the SIP over TLS port, which is used to the SBC access interface, which has internet access.
- **Protocol**
Specify the used protocol (**TLS**, **TCP** or **UDP**).

NOTICE: The PSI client is recommended to be configured to use SIP/TLS. UDP and TCP are not recommended for remote subscribers.

- 5) Click **Save** to save the settings.
The newly created SBC configuration is displayed in the list.

9.4 Integrating OSV subscribers with Zoom users

As an administrator, you can provision one-by-one Zoom users in OpenScape Voice in the OpenScape Common Management Platform.

Prerequisites

Adequate administrative permissions.

CloudLink configurations are completed.

Zoom users have been configured in the Zoom tenant, as described in [User provisioning in the Zoom tenant](#) on page 46.

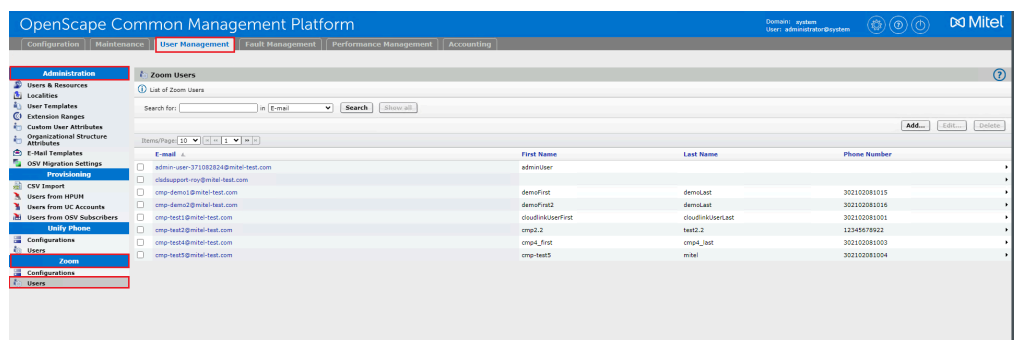
Zoom configurations are completed, as described in [Creating a new SBC configuration for Zoom users](#) on page 50.

General prerequisites regarding subscriber/system configuration from previous chapters are met.

To integrate OSV subscribers with Zoom users:

Step by Step

- 1) Log in to the OpenScope Common Management Platform.
- 2) Click on the **User Management** navigation tab.
- 3) In the navigation tree, click on **Zoom > Users**.



4) Click **Add...** to create a new Zoom User.

A new **Add Zoom User** window pops up containing the following fields:

- **Email:** Enter a valid email address.

IMPORTANT:

The email address is the unique identifier that associates a user with a single Zoom tenant and must be unique.

Ensure that the email address matches the email address that was used while creating the Zoom user and the assigned license.

Once configured, you cannot edit the **Email** of a user.

-
- **First Name:** Enter the first name of the user.
 - **Last Name:** Enter the last name of the user.
 - **Configuration:** Select the SBC configuration you want from the dropdown list, as created in [Creating a new SBC configuration for Zoom users](#) on page 50.
 - **Phone number:** Click the three-dot icon to add a pre-configured phone number.

The **Select OpenScape Voice resource** window pops up, containing a list of the available phone numbers.

Check the box in front of the phone number you want to select and click **OK**.

IMPORTANT:

When selecting a phone number, all OSV subscribers are visible, not just those with the Zoom user flag enabled. However, when searching, if the Zoom user flag is not enabled, the subscriber will not be shown.

The administrator must be aware of which OSV subscribers are configured for the Zoom connection. For easier lookup, it is recommended to use search operators such as `*your_subscriber*` to locate your subscriber.

-
- **VoiceMail:** Callback number of XPR Voicemail server.

- 5) Click **Save** to save the settings.

NOTICE: If the selected OSV subscriber is not a Zoom User, an error message, `The action has failed`, is displayed, indicating that the connection has failed.

The OSV subscriber-Zoom user integration is completed:

- In CMP, the new user is added in the **Zoom Users** list.
- In the Mitel Admin **User Management** menu area, the new users is added under the **Users** list.

NOTICE:

The administration of users should not be performed from Mitel Admin. The provisioning of users should be performed from the PBX's management platform.

- In the Zoom **System Integration** menu area, under the **Integrated Users** list, the status and the information of the newly created Zoom user is updated.

To edit or delete a user, refer to [OpenScape Common Management Platform V10 Administrator Documentation](#).




IMPORTANT:

Editing the first name and/or last name of the user and deleting a Zoom PSI user is not reflected in the Zoom tenant.

10 Monitoring and Troubleshooting Zoom Integration in Mitel CloudLink Admin Portal

10.1 Viewing the Zoom integration status

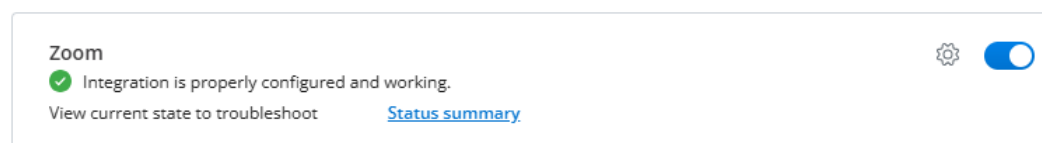
Once the Zoom integration is added to a customer account, you can check its status to ensure it is set up properly. The Zoom integration can have one of the following statuses:

-  Connected
-  Error
-  Pending

Viewing a summary of the Zoom integration status

To view a summary of the Zoom integration status, follow the steps below:

- 1) Log in to Mitel Administration as an Account Admin.
- 2) Access the **Integrations** panel from the **Accounts Information** page or from the **Integrations & Apps** option.
- 3) In the **Integrations** panel, locate the **Zoom** integration. Check the status icon and message next to it.



The icon indicates the current status of the integration, while the status message provides additional information about the overall status.

Viewing detailed information about the Zoom integration status

For a more in-depth view of the Zoom integration status, especially for troubleshooting, you can one of the following:

- Click **Status summary** next to the **Zoom** integration in the **Integrations** panel.
- Navigate to **Support > Zoom**.

You can then view detailed information about the Zoom integration status, including the following:

- **OAuth status:** Displays the OAuth authorization status (*Authorized*, *Failed*), indicating whether the Zoom OAuth token is valid, expired, or needs re-authorization. If the OAuth status is *Failed*, error messages associated with the most recent OAuth failure will also be displayed below the status.
- **Integration status:** Indicates the current status of the Zoom integration (*Connected*, *Error*, or *Pending*).
- **Sync status:** Indicates the synchronization status between CloudLink and Zoom. If the last sync was unsuccessful, error messages associated with the most recent failed sync attempt will also be displayed below the status.
- **Last successful sync:** Date and time of the last successful synchronization between CloudLink and Zoom.

The following image shows an example of detailed information about the Zoom integration status when the integration is set up properly.

Zoom Integration Status

The current state of the integration with the Zoom platform.

OAuth status:	✓ Authorized
Integration status:	✓ Connected
Sync status:	✓ Successful
Last successful sync:	1/31/2025, 6:02:55 PM

Done

The following image shows an example of detailed information about the Zoom integration status when the integration is not set up properly.

Zoom Integration Status

The current state of the integration with the Zoom platform.

OAuth status:	▲ Failed
Details:	Zoom(GET /v2/users): ZoomAuthService.refreshAuthCredentials => Error refreshing Zoom PSI user: failed to post auth resource: InvalidRequest
Integration status:	✓ Connected
Sync status:	▲ Failed
Details:	Zoom(GET /v2/users): ZoomAuthService.refreshAuthCredentials => Error refreshing Zoom PSI user: failed to post auth resource: InvalidRequest
Last successful sync:	2025-01-27, 1:46:31 p.m.

Done

In the second example, as shown in the details section below the failed **OAuth status** and **Sync status**, an error occurred while attempting to obtain a new refresh token from Zoom.

Refreshing the Zoom integration status

To refresh the Zoom integration status, follow the steps below:

- 1) Navigate to **Support > Zoom**.
- 2) In the **Status** tab, click **Refresh**.

10.2 Generating a User Comparison Report

The User Comparison Report analyzes user data across multiple systems to identify inconsistencies. It consolidates user information from four sources, using the email address as the unique identifier:

- CloudLink User Database (CL User DB)
- Service Delivery License Database
- Zoom User List
- Zoom Phone List

The User Comparison Report helps identify mismatches and missing data that may impact the proper provisioning of services.

You can generate and download a report comparing users' information between Zoom and CloudLink.

Step by Step

- 1) Log in to Mitel Administration as an Account Admin.
- 2) Click **Support > Zoom** from the left main menu.
The **Zoom Sync & Provisioning Errors** page of the customer account opens.
- 3) Select the **User Comparison Report** tab.
- 4) Click **Generate** to compare users' information between Zoom and CloudLink.
The system initiates an asynchronous request for generating the report.
A report is generated in a csv format.
- 5) Click **Download** next to the csv file.

The User Comparison Report contains the following information:

Field	Description
email	The primary identifier.
name	User's display name.
clUserId	The user's ID in CloudLink (if found).
licenses	Assigned licenses (e.g., ["ZoomPSI"]).
zmUserId	The user's ID in Zoom (if found).
zmUserStatus	The current status of the user in Zoom (active, inactive, pending).
zmSipPhoneId	The ID of the user's assigned Zoom desktop client SIP phone (if found).
zmSipPhoneNumber	The assigned Zoom desktop client SIP phone number.
zmSipPhoneMobileId	The ID of the user's assigned Zoom mobile SIP phone (if found).

Monitoring and Troubleshooting Zoom Integration in Mitel CloudLink Admin Portal

Troubleshooting common issues identified in the User Comparison Report

Field	Description
zmSipPhoneMobileNumber	The assigned Zoom mobile phone number.
issues	A list of identified inconsistencies.

10.3 Troubleshooting common issues identified in the User Comparison Report

If any issue is identified in the User Comparison Report, it is recorded in the issue column of the User Comparison Report.

Below are the potential issues and the recommended resolution:

Issue	Cause	Resolution
CloudLinkUserNotFound	The user is not found in the CloudLink User Database.	Ensure the user is provisioned in CloudLink. Verify that their email address is correct.
ZoomUserNotFound	The user does not exist in Zoom.	Confirm that the user has been added to the Zoom tenant. Verify the email address that is used.
ZoomSipPhoneNotFound	The user does not have a Zoom SIP phone assigned.	Assign a SIP phone to the user in the Zoom Admin Portal.
ZoomUserStatusInactive	The user's Zoom status is inactive.	Reactivate the user in the Zoom Admin Portal.
ZoomUserStatusPending	The user's Zoom status is pending activation.	Ensure the user completes the activation process by following the Zoom invite email.
NoClZoomPsiLicense	The user does not have the required "ZoomPSI" license in CloudLink.	Assign the "ZoomPSI" license to the user in the management Portal. If this issue is detected, no further checks are performed.

Steps to Validate and Fix Issues

- 1) Open the User Comparison Report.
- 2) Locate users with issues in the issues column.
- 3) Identify the corresponding inconsistency from the list above.
- 4) Follow the resolution steps for each detected issue.
- 5) After making corrections, regenerate the report to verify the fixes.

If the issues persist after resolving them, contact the appropriate system administrator for further investigation.

NOTICE: If a user does not have a "ZoomPSI" license, no further checks are performed.

NOTICE: Email addresses must match exactly across all sources for proper data joining.

10.4 Viewing the Event History table (Zoom integration)

The Event History provides insight to Mitel Partners and Account Admins regarding events that occurred within an account with Zoom integration.

Step by Step

- 1) Log in to Mitel Administration as an Account Admin.
- 2) Click **Support > Zoom** from the left main menu.
The **Zoom Sync & Provisioning Errors** page of the customer account opens.
- 3) Select the **Event History** tab.
- 4) Click on an event in the Event History table to view the event details.
The **Event Details** popup window is displayed.
- 5) Click **Copy** to copy the event details of the following tabs:
 - **Core details**
 - **Properties Changed**
 - **Extra Details**
 - **Log tags**
- 6) Click **Export** to export all data in a csv format.

NOTICE:

Actions performed in Mitel Administration (MA) will only appear in the **Event History** after a 24-hour delay. This delay is expected and does not indicate a failure or issue with the action itself.

11 Configuring E911 Calls

This chapter provides information on the necessary configurations to ensure that the E911 solution can successfully determine the physical location of a registered user during an emergency call. Once the exact location is identified, the E911 solution routes the E911 call to the appropriate Public Safety Answering Point (PSAP) and notifies security personnel.

E911 Solutions must comply with E911 legislation. The Federal Communications Commission (FCC) developed [Kari's Law and the RAY BAUM's Act](#), which comprise a set of rules and regulations that specify direct dialing, notification, and dispatchable location minimum requirements for all Multi-line Telephone System (MLTS) platforms. All organizations across the US must comply with both Kari's Law and the RAY BAUM's Act.

OSV, as a Multi-line Telephone System (MLTS), implements Section 506 of RAY BAUM Act and Kari's Law support in conjunction with third-party Next Generation of 911 emergency services providers in the USA.

For OSV, we have the following device categories:

- Fixed MLTS Devices. For example, Analog Devices TDM devices (Analog Devices, Digital Devices, and Integrated DECT).
- Non-Fixed MLTS devices. For example, IP Devices, SIP Devices, softphones, all teleworkers, and so on.

To fully support the requirements above, OSV is integrated with [Intrado](#) in USA and with [Redsky](#) in USA and Canada. A valid service agreement with either RedSky or Intrado is necessary for the E911 Solution.

NOTICE: Mitel does not provide this service agreement directly. To support local notifications compliant with Kari's law compliant, the solution will use the E911 Provider's notification application.

RedSky and Intrado use SIP trunks to route E911 calls to the appropriate Public Safety Answering Points (PSAPs) based on the civic address. Both providers pass callback information from the call-server to enable the PSTN to route the call back from the PSAP to the specified callback number.

NOTICE: Intrado also offers a function called Extension bind for non-DID numbers. This function, when enabled, assigns a temporary valid Direct Inward Dialing (DID) callback number for the extension number (non 10-digits number) that made the 911 call. In this case, if the call gets disconnected the Emergency Response Team can call back the person that called the Emergency Service.

Emergency Call Flow

Emergency calls are **only supported** from the **Zoom desktop client**. If you attempt to place an emergency call from the **Zoom mobile client**, the call will automatically be redirected to the mobile cellular network.

Additionally, the emergency location is provided by RedSky. The process for retrieving the emergency location is as follows:

- When a user logs into the Zoom desktop client, Zoom sends a request to CloudLink.
- CloudLink, using the Emergency Provider tenant information, forwards the request to Emergency Provider to retrieve the user's emergency location.

For OpenScape Voice Emergency Calling information, refer to chapter 4.9 *Emergency Calling* of the [OpenScape Voice V10 Administrator Documentation](#).

For CloudLink Emergency configurations, refer to [Configuring the PBX system settings in Mitel administration](#) on page 43 (steps 5-6).

To complete the Mitel OpenScape Voice and Mitel OpenScape SBC configurations required for an Emergency Solution, follow the instructions provided in the following chapters.

11.1 OpenScape SBC E911 Configuration

This section describes how to configure Mitel OpenScape SBC for emergency calls used by Zoom users.

Prerequisites

- 1) You must request an account from your Emergency provider (Redsky or Intrado).
- 2) You must have a **CloudLink account** with **CloudLink account admin** privileges.
- 3) The IP address from which the SBC will send traffic must be added to the provider's whitelist. Please contact your emergency provider.
- 4) Proper firewall rules must be created to allow traffic for signaling and RTP ports configured for emergency calls.
- 5) You must enable the NG911 service in Mitel OpenScape Voice. To do this, refer to chapters 4.9.5 *How to Route Emergency Calls to NG911 Service Providers* and 4.9 *Emergency Calling* in the [OpenScape Voice V10 Administrator Documentation](#).

11.1.1 Configuring an E911 Media Profile

Follow the steps below to create a new media profile for your Emergency Provider (Intrado or Redsky).

Step by Step

- 1) Log in to the SBC management portal.
- 2) Navigate to **VoIP > Media** in the navigation tree under Administration.
- 3) Under **Media Profiles**, click **Add**.

The **Media Profiles** window pops up.

4) Under the **General** section:

- a) Enter an E911 Media Profile name. For example, RedSky.
- b) From the **Media protocol** drop-down menu, select **RTP only**.

NOTICE:

The **Media Protocol** is specified by your Emergency Provider. To ensure compliance with their requirements, please contact your Emergency Provider's support.

5) If codec configuration is required by your Emergency Provider, do the following:

NOTICE: In some cases, codec configuration from an Emergency Provider (such as Redsky) is necessary to align technical specifications and ensure that emergency calls can be handled efficiently within the organization's communication infrastructure.

- a) Locate the **Codec Configuration** area.
- b) Check the **Allow unconfigured codecs** checkbox.
- c) From the **Codec** drop-down menu, select the codec as specified by your Emergency Provider, according to the region where they are located. For example, select G711U 8kHz - 64 kbps (for US-NA) or G711A 8kHz - 64 kbps (for Europe).

NOTICE: Redsky accepts only US & Canada locations. In addition, it prefers G711U codec.

6) Click **OK** to save the configuration.

7) Click **Apply changes**.

11.1.2 Configuring Remote Endpoints

To configure Emergency remote endpoints, you must first create SIP Service Provider Profiles (SSPs) and then proceed with configuring the remote endpoints.

11.1.2.1 E911 SIP Service Provider Profile Configuration

The following configuration must be applied to the E911 Remote Endpoint Profile to handle Zoom > E911 calls.

Step by Step

- 1) Log in to the SBC management portal.
- 2) Navigate to **Features** in the navigation tree under Administration.

The **Features** window pops up.

- 3) Check the **Enable Remote Endpoints** checkbox and click **Configure**.

The **Remote endpoints** window pops up.

- 4) Under the **SIP Service Provider Profile** area, click **Add**

NOTICE: The **SIP Service Provider Profiles** window pops up.

- 5) In the **Name** field, enter the name of your E911 Provider. For example, RedSky.
- 6) Check the **Enable SSP Privacy and Complementary Flags** checkbox.
- 7) Click **OK** to save the configuration.
- 8) Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

11.1.2.2 E911 Remote Endpoint Configuration

Follow the steps below to configure an E911 Provider remote endpoint.

Prerequisites

You have created a E911 SIP Service Provider Profile.

Step by Step

- 1) Log in to the SBC management portal.
- 2) Navigate to **Features** in the navigation tree under Administration.
The **Features** window pops up.
- 3) Check the **Enable Remote Endpoints** checkbox and click **Configure** next to it.
The **Remote endpoints** window pops up.
- 4) Scroll down to locate the **Remote endpoint configuration** area and click **Add**.
The **Remote Endpoint configuration** window pops up.
- 5) Under the **Remote Endpoint Settings** area:
 - a) In the **Name** field, enter a unique name for the E911 Provider remote endpoint. For example, RedSky.
 - b) From the **Type** drop-down menu, select **SSP**.
 - c) From the **Profile** drop-down menu, select the E911 SIP Service Provider Profile you created in E911 SIP Service Provider Profile configuration.
 - d) From the **Access realm profile** drop-down menu, select the network ID that has access to Internet. For example, **Main-access-Realm-ipv**.

IMPORTANT:

For security purposes, IP whitelisting is used by E911 Providers to block network access to all IPs except those in the whitelist. To ensure the public Firewall IP

you are using will be whitelisted, share it with your E911 Provider.

- e) From the **Core realm profile** drop-down menu, select the core realm profile. For example, **Main-core-realm-ipv4**.

6) Under the Remote Location domain list area, click Add

The **Remote Location Domain** window pops up.

NOTICE: The settings presented below are provided by your E911 Provider.

- a) In the **Remote URL** field, enter the URL of the remote endpoint for E911.
 - b) In the **Remote port** field, enter the remote port for communication between E911 and OSSBC.
 - c) From the **Remote transport** drop-down menu, select the remote transport protocol provided by your E911 Provider (TCP, UDP, or TLS).
- 7) Under the Media Configuration area, from the Media Profile drop-down menu, select the Media profile of your E911 Provider created in *Configuring an E911 Media Profile*.**
- 8) Click OK.**

You are directed back to the **Remote Endpoint Configuration** window.

- 9) Locate the Remote Location Identification Routing area.**
- 10) In the Core realm port, enter a unique value.**
- 11) Click OK.**
- 12) Click Apply changes.**

You are directed back to the **Remote Endpoints** window. The E911 Provider Remote endpoint is shown under the **Remote endpoint configuration** table.

11.2 OpenScape Voice E911 Configuration

This section describes how to configure Mitel OpenScape Voice for emergency calls used by Zoom users.

Prerequisites

- 1) You must request an account from your Emergency provider (Redsky or Intrado).**
- 2) You must have a CloudLink account with CloudLink account admin privileges.**
- 3) The IP address from which the SBC will send traffic must be added to the provider's whitelist. Please contact your emergency provider.**
- 4) Proper firewall rules must be created to allow traffic for signaling and RTP ports configured for emergency calls.**
- 5) You must enable the NG911 service in Mitel OpenScape Voice. To do this, refer to chapters *4.9.5 How to Route Emergency Calls to NG911 Service Providers* and *4.9 Emergency Calling* in the [OpenScape Voice V10 Administrator Documentation](#).**

11.2.1 Configuring an E911 Provider Remote Endpoint

To create a new Endpoint Profile for your Emergency Provider:

Step by Step

- 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, Redsky.
 - b) Select the **Profile** for Zoom PSI.
- 5) Click **Save**.
- 6) 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, as configured in OpenScape SBC [E911 Remote Endpoint Configuration](#) on page 63 (step 10).
 - f) From the **Transport protocol** drop-down menu, select **TCP**.
- 7) Click **Save**.
- 8) Go to the **Attributes** tab and select the following attributes to enable them:
 - a) Public/Offnet Traffic
 - b) Enable Session Timer
- 9) Go to the **Aliases** tab and click **Add** to add an Aliase with the format SBC IP : port.
- 10) Click **OK** and then click **Save**.

11.2.2 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.

11.2.2.1 Configuring the E911 Call Routing

This section describes how to create a prefix to route the call to Emergency service.

- 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 prefix. For example, 933.
 - b) **Minimum length**: Enter the minimum expected length of the Emergency number.
 - c) **Maximum length**: Enter the maximum expected length of the Emergency number.
 - d) **Digit Position**: Configure 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 **Unknown**.
 - 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) To create a Destination code for 911:

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) Click the **Select Traffic Type** button and then click the three-dot icon (only enabled if the option is selected) to open the traffic type selection window.

Select the **Emergency** traffic type.

Click **OK**.
 - c) From the **Destination Type** drop-down menu, select **Service**.
 - d) Click the three-dot icon next to **Service** and select **Emergency** from the Service List pop-up.

Click **OK**.
 - e) Click **Save**.

11.2.3 Configuring an Access code

As an administrator, you can create an Access code to route the emergency call to a Destination.

Step by Step

- 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** to edit it. For example, Zoom_PSI.

The **Edit Business Group** window pops up. The General tab is displayed by default.

- 3) Go to the **Services** tab.
- 4) Under the **Next Generation 911** area, check the **Activate** option.
- 5) Enter an access code in the **Access Code** text field. For example, 333.
- 6) Click **Save**.

11.2.4 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.

11.2.4.1 Configuring the Emergency Destination

To add a Destination that will be used to route the emergency calls to SBC:

- 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, DEST_NG911.
- 4) Click **Save**.
- 5) Select the destination you created in the previous step and click **Edit**.
- 6) In the **Edit Destination** pop-up, select the **Routes** tab and click **Add**.
- 7) In the **Add Route** pop-up, configure the following:
 - a) **ID**: Enter the priority level of this route ID as 1 (if there are multiple routes to a destination and route prioritization is selected, the route with the lowest numbered route ID has the highest priority and will be selected first).
 - b) From the **Type** drop-down menu, select **SIP Endpoint**.

- c) Click the three-dot icon at the right side of the **SIP Endpoint** and select the Emergency Endpoint (for example, Redsky) created in [Configuring an E911 Provider Remote Endpoint](#) on page 65.

NOTICE: The emergency provider requires three digits, thus the route should remove all digits and send a three-digit number (e.g., 933).

- 8) Configure the Destination Directory Number settings as below:
 - a) From the **Modification Type** drop-down menu, select **Number Manipulation**.
 - b) In the **Number of digits** field, enter the number of digits to cut off from the directory number. For the Redsky configuration, enter **6**.
 - c) In the **Digits to insert** field, enter the digit string which gets added to the beginning of the remaining digits. For the Redsky configuration, enter, for example, **933**.
 - d) From the **Nature of Address** drop-down menu, select **Unknown**.
 - e) Click **Save**.

11.2.5 Configuring a new Destination Code

As an administrator, you can create a new Destination Code, based on the configurations described in [Configuring the Emergency Destination](#) on page 67.

Example

In case you have created a prefix for emergency calls (933) and an access code (333) in [Configuring the Emergency Destination](#) on page 67, you will need to create a new destination code: 933333.

The first 3 digits (933) will route the call to Emergency Service of **OSV**.

The next three digits (333) will route the call to the **SBC**.

Finally, you can manipulate the number (displayed when selecting to edit the pre-configured emergency destination under the **Routes** tab) so that only **933** is sent to the SBC, ensuring the correct number is sent to the SIP Endpoint created for the Emergency Endpoint, which is actually the SBC, since the emergency call will be routed to Emergency provider via SBC.

- 1) To create a new Destination code:
 - Navigate to **OpenScape Common Management Platform > Configuration > Unify OpenScape Voice > Business Group > Translation > Destination Codes**.
- 2) Click **Add**.

- 3) In the **Add Destination Code** pop-up, configure the following:
- a) **Destination Code:** Enter the destination code. For example, 933333.
 - b) Click the **Select Traffic Type** button and then click the three-dot icon (only enabled if the option is selected) to open the traffic type selection window.

Select the **Emergency** traffic type.

Click **OK**.
 - c) From the **Destination Type** drop-down menu, select **Destination**.
 - d) Click the three-dot icon next to **Destination** and select the destination configured in [Configuring the Emergency Destination](#) on page 67. For example, **DEST_NG911**.

Click **OK**.
 - e) Click **Save**.

11.3 CloudLink E911 Configuration

For CloudLink Emergency configurations, refer to [Configuring the PBX system settings in Mitel administration](#) on page 43 (steps 5-6).

11.4 Adding IP Range Mapping (Redsky)

Prerequisites

You have an administrator account from your Emergency provider (Redsky).

Step by Step

- 1) Log in to your Redsky account.
- 2) Select **Network Discovery** from the left-side Configuration menu.

The **Network Discovery** page is displayed.
- 3) Go to the **IP Ranges** tab.
- 4) Click **Add IP Range Mapping** at the top right of the **Network Discovery** page to add the IP Range mapping configurations.
- 5) Configure the following fields as required:
 - Range Start
 - Range End
 - Building
 - Location
 - Description

NOTICE:

If the Building or Location you want to select does not appear in the dropdown, you must add it as a new Building or Location entry.

6) Click **Save.**

For more information, refer to the [Redsky Online Help](#) page.

NOTICE:

The IP range created should be mapped with an E911 location created in the Redsky portal.

12 Appendix

12.1 Appendix A: Restrictions and Known Issues

The following table lists the tested features when Zoom is integrated with OpenScape Voice and OpenScape SBC.

Feature	Description
Local tones on Zoom PSI client	<p>The Zoom PSI client does not play a busy tone when the called party is busy. Instead, it only displays the message: <i>"The number you are calling is currently busy, please try again later."</i></p> <p>Limitation: This occurs when the PSI client receives a <i>486 Busy Here</i> SIP message from OSV.</p>
Prevent Forking to the Transferring Device in Flip Scenario	<p>When the PSI client performs a blind transfer to its own number (flip scenario) to redirect the call to another device or client of the same user, OpenScape Voice (OSV) sends an INVITE to all registered contacts of the transferred-to destination number (DN), including the device that initiated the transfer.</p> <p>As a result, the transferring device receives the call, which may confuse the user into thinking it is a recall.</p> <p>Limitation: This issue occurs when Call Waiting is enabled on the transferring device.</p>
Managing Zoom PSI Users via CMP	<p>Zoom PSI user deletion or name modification via CMP is not synchronized with the Zoom tenant.</p> <p>Limitation: When a Zoom PSI user is deleted from CMP, the user remains in the Zoom tenant and continues to consume a PSI license. Similarly, if an administrator modifies a user's first or last name in CMP, the changes are not propagated to the Zoom tenant.</p>
Hold Retrieve with OPUS Codec	<p>Hold retrieve fails if the OPUS codec is not available.</p>

Appendix

Appendix B: Default User Name and Password

Feature	Description
Session timers	<p>Zoom PSI client does not fully support SIP session refresh using the INVITE method (RFC 4028), which may lead to unexpected SDP renegotiation and audio issues. To address this limitation, OSV is configured to use the UPDATE method for session refresh by changing <code>Srx/Sip/UpdateMethodSessionTimingEnable</code> to true.</p> <p>Administrators should verify whether the SIP service provider or any other third-party endpoint supports the UPDATE method for session refresh.</p> <p>If the UPDATE method is not supported but is included in the Allow header, the endpoint should be configured with the attribute Do Not Support Update Method for Session Timing.</p>
Support for Storing Message Waiting Indicator (MWI) Message Counters from Xpressions Voicemail Server	<p>OSV does not support storing the Message Waiting Indicator (MWI) message counters sent by the Xpressions voicemail server.</p> <p>Zoom PSI users cannot see the number of waiting voicemail messages upon login or registration.</p> <p>MWI notifications do not reflect the actual number of unread voicemail messages.</p>
Local Conference	<p>A local conference is limited to 3 members (including the initiator).</p>
SIP error message (487)	<p>The SIP error message (487) appears in the Zoom client when the user dials a service code to activate or deactivate a service. Despite the error code, the user's action is successfully applied.</p>

12.2 Appendix B: Default User Name and Password

The following table lists the default user name and password for the OpenScape SBC Management Portal.

User Name	Password
administrator	Asd123!.

For information on OpenScape SBC Security Checklist, refer to [OpenScape SBC V11R2 Security Checklist](#).

