



A MITEL
PRODUCT
GUIDE

OpenScape Solution Set V11

Zoom Phone System Integration (PSI) with Mitel OpenScape 4000 and
Mitel OpenScape SBC

Solution Guide

05/2026

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 2026, 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.....	8
2.2.2 Network requirements.....	8
3 Overview.....	10
3.1 Key Components.....	10
3.2 Overview of the Phone System Integration (PSI) solution.....	11
3.3 Related Documentation.....	11
4 Integrating Zoom with CloudLink.....	13
4.1 Adding Zoom integration to a customer account.....	13
4.2 Enabling Zoom integration in a customer account.....	14
4.3 Setting up a CloudLink account in Zoom Marketplace.....	16
5 Licensing.....	17
6 Configuring Cloudlink integrations.....	18
6.1 Enabling OS4K - CloudLink to access the Internet.....	18
6.2 Connecting OS4K to CloudLink.....	19
6.3 OpenScape 4000 Assistant connectivity to CloudLink.....	22
6.4 Connecting OpenScape SBC with CloudLink.....	23
6.5 Connecting OpenScape Xpressions with CloudLink.....	26
6.5.1 Prerequisites for connecting OpenScape Xpressions with CloudLink.....	26
6.5.2 Setting a global variable for proxy server use.....	26
6.5.3 Connecting OpenScape Xpressions with CloudLink.....	27
6.5.4 Activating an OpenScape Xpressions user.....	27
6.5.5 Enabling Zoom integration and transcription.....	27
7 Provisioning Users.....	29
7.1 User provisioning in the Zoom tenant.....	29
7.1.1 Adding a new Zoom user.....	29
7.1.2 Setting up the Zoom account from invitation.....	30
7.1.3 Configuring Zoom Phone System Integration.....	31
7.1.3.1 Configuring Phone System Integration settings.....	31
7.1.3.2 Adding Zoom users to the Mitel integration.....	32
7.2 OpenScape 4000 Provisioning: Configuration Guidelines.....	32
7.2.1 Integrating OpenScape 4000 subscribers with Zoom Users.....	34
7.2.1.1 Integrating OpenScape 4000 subscribers with Zoom Users via CSV file import.....	36
8 Monitoring and Troubleshooting Zoom Integration in Mitel CloudLink Admin Portal.....	38
8.1 Viewing the Zoom integration status.....	38
8.2 Generating a user comparison report.....	40
8.3 Troubleshooting common issues identified in the User Comparison Report.....	41
8.4 Viewing the Event History table (Zoom integration).....	42
9 Configuring OpenScape SBC.....	43
9.1 Configuring Network settings.....	43
9.2 Configuring SIP Server.....	45
9.3 Configuring Certificates.....	45

Contents

9.4 Configuring Media Profiles.....	50
9.4.1 Configuring the Codec Manipulation and Remote Subscribers.....	50
9.4.1.1 Configuring Remote Subscribers.....	51
9.4.2 Configuring the Zoom Media Profile.....	52
9.4.3 Configuring the OpenScape 4000 Media Profile.....	54
9.5 Push Notification.....	55
9.5.1 Enabling push notification.....	55
9.5.2 Response Codes for Push timeout.....	55
10 Emergency Configuration.....	57
10.1 Emergency configuration in CloudLink.....	57
10.2 Emergency configuration in OpenScape 4000.....	58
10.3 Emergency Configuration in OpenScape SBC.....	58
10.3.1 Configuring an E911 Media Profile.....	59
10.3.2 Configuring Remote Endpoints for E911.....	59
10.3.2.1 E911 SIP Service Provider Profile Configuration.....	60
10.3.2.2 E911 Remote Endpoint Configuration.....	60
10.4 Adding IP Range Mapping (Redsky).....	61
11 Appendix.....	63
11.1 Appendix A: Restrictions and Known Issues.....	63
11.2 Appendix B: Default User Name and Password.....	63

1 History of Changes

Issue	Date	Summary
1	02/2025	The first issue of the guide
2	03/2025	Updates and enhancements on the Provisioning chapter
3	03/2025	Updated the links Zoom Mitel PSI.
4	04/2025	Updated Prerequisites on page 6 section.
5	06/2025	Updated Prerequisites on page 6 section.
6	06/2025	Added note in Configuring Cloudlink integrations on page 18
7	06/2025	Updated the following chapters: • Adding Zoom integration to a customer account on page 13 • Setting up a CloudLink account in Zoom Marketplace on page 16
8	06/2025	Updated Configuring Remote Subscribers on page 51
9	06/2025	Updated Appendix A: Restrictions and Known Issues on page 63
10	07/2025	Updated OpenScape 4000 Provisioning: Configuration Guidelines on page 32
11	07/2025	Updated Configuring Certificates on page 45
12	08/2025	Added chapter Connecting OpenScape Xpressions with CloudLink on page 26 Updated Appendix A: Restrictions and Known Issues on page 63
13	09/2025	Added chapter Response Codes for Push timeout on page 55

2 Introduction

This document outlines how to connect the OpenScape 4000 (OS4K) 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 4000 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 walks you through 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, managing the Zoom-OS4K-SBC integration, specifically those working with OpenScape 4000 (OS4K) 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 app	6.3.6
OpenScape 4000 with active SSP/SWA (Unify Software Support / Mitel Software Assurance)	V11R0.22 Assistant HF: V11R0.22.5 CSTA HF: V11 R0.22.3 PLT HF V11 R0.22.3 RMX HF V11 R0.22.10 LW HF: V11 R0.22.7
OpenScape SBC	V11 R2.4.0

Product	SW Version (minimum)
OpenScape Xpressions	OpenScape Xpressions V7 R1.5.0 Zoom Package HF1

- **System Requirements and Licenses**

- **SIP configuration:**

- System must have a unique system number (AMO-ANUM, AMO-ANSU)
 - UFIP device must have a configured VM (PMIDX)
 - UFIP device must have digest authentication
 - Zoom PSI as client device of an desk/client configuration is not supported and is not be offered for provisioning but associated devices can be used
 - Should have Call log configured to **All** (AMO-SBCSU - Call log parameter)
 - In standalone operation, a Flex license is required for IP subscribers. If a user utilizes multiple devices or clients, “user-based licensing” also applies.

- **Zoom requirements**

- 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.
 - [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 is completed.
 - It must be ensured that a subscriber license is available for each Zoom subscriber.
 - When logged in to the Zoom web portal as an Admin with the privilege to edit account settings, the **Phone System Integration** tab should be displayed under **Account Management**. If it is not displayed, please contact Zoom.

IMPORTANT: Before proceeding with a planned customer migration to Zoom, ensure that a successful OS4K resource synchronization has been completed and verified. This step is essential to identify any potential issues early in the process.

- **General requirements**

NOTICE: Administrator PC must have access to the internet

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 OS4K configurations interact with each other and other critical components of the solution.

3.1 Key Components

The key components of the Zoom-OS4K 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-OS4K integration, you are granted admin access to the Zoom web portal.
- **OpenScape 4000 (OS4K):** is a hybrid IP/TDM PBX system that supports both legacy TDM telephony and modern IP- based communications. OS4K is designed for medium to large enterprises that need to transition gradually to IP- based telephony while maintaining compatibility with their existing telephony infrastructure.
- **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 OS4K 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 4000) and cloud-based applications. Acting as the intermediary, CloudLink platform bridges the Zoom and OS4K 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 4000 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.

- **OpenScape 4000 Assistant:** This web-based configuration interface supports the OpenScape communications solution. It provides tools for connecting CloudLink, managing Zoom configurations, and integrating Zoom users with OS4K subscribers.

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 4000 (OS4K) and OpenScape Session Border Controller (SBC) work together to enable seamless integration between Zoom clients and external networks.

The OpenScape SBC acts as the secure gateway, managing network boundaries, while OpenScape 4000 handles core telephony functions including SIP message manipulation and call routing. This integration establishes reliable communication paths between Zoom PSI accounts and OS4K subscribers, ensuring smooth call flow in both directions.

The guide begins with the configurations needed for the [Zoom-CloudLink integration](#) configurations, followed by the steps required before setting up and provisioning Zoom-OS4K users.

If your OS4K and SBC are not yet set up, begin with the OpenScape 4000 configuration for SBC connectivity, followed by SBC configurations necessary for Zoom.

Setting Up Users for Zoom-OS4K Integration

The Zoom-OS4K integration involves several key steps:

- 1) Establishing CloudLink connectivity for managing Zoom users associated with OS4K subscribers.
- 2) Connecting the Zoom Account to CloudLink Account.
- 3) Adding users and assigning licenses in your Zoom account.
- 4) Configuring user mapping between Zoom and OS4K through the OpenScape 4000 Assistant.
- 5) 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 Phone clients and the OS4K platform, and a unified user experience across cloud and on-premises systems.

3.3 Related Documentation

Zoom PSI

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

OpenScape 4000

- [OpenScape 4000 V11, Installation Guide](#)
- [OpenScape 4000 V11, Ip Solutions, Service Documentation](#)
- [OpenScape 4000 V11 Assistant, Configuration Management, Administrator Documentation](#)
- [OpenScape 4000 V11, Platform Administration](#)
- [OpenScape 4000 V11, AMO Descriptions](#)

OpenScape SBC

- [OpenScape SBC V11 Administration Guide](#)
- [OpenScape SBC V11 Configuration Guide, Administration Documentation](#)
- [OpenScape SBC V11 Installation Guide](#)
- [OpenScape SBC V11R2/R3 Security Checklist](#)
- [OpenScape SBC Troubleshooting Guide, Service Documentation](#)

CloudLink

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

4 Integrating Zoom with CloudLink

This chapter describes the Zoom and CloudLink integration carried out through the Zoom Web Portal and Mitel Administration.

Before proceeding with the configurations, ensure you have the required user accounts and permissions. For more information, see [User Roles and Permissions](#) on page 8.

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 Zoom account.

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 license.

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 8.

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) Scroll down to locate the Zoom integration and click **Add** next to it.
- 6) The Zoom integration is added to the customer account and it is displayed in the **Integrations** section of the **Account Information** page.
- 7) Go to the newly added Zoom integration and click **Complete Setup**.
- 8) Click **Connect** on the pop-up window.

You will be redirected to accounts.mitel.io to authorize your Zoom Account.

Integrating Zoom with CloudLink

Enabling Zoom integration in a customer account

- 9) Click **Allow** in the authorization window.

NOTICE: Ensure you are logged in with the correct Zoom admin account.

The integration is complete, and you will see it marked as connected on both the CloudLink and Zoom portals.

NOTICE: A Partner Administrator cannot enable integrations in the Partner Prime Account, as the integration with other applications are not supported for Partner Accounts. If a Partner wants to explore or test CloudLink integrations, they must create an End Customer Account within their Partner Portal and enable integrations there. 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 14.

4.2 Enabling Zoom integration in a customer account

After adding the Zoom integration to a customer account, you must provide the required information of the CloudLink account to enable the integration

Prerequisites

You must have a Zoom account enabled for Mitel integrations. Zoom integration must be added in the customer account, as described in [Adding Zoom integration to a customer account](#) on page 13.

You have a **Zoom Business or Enterprise account**.

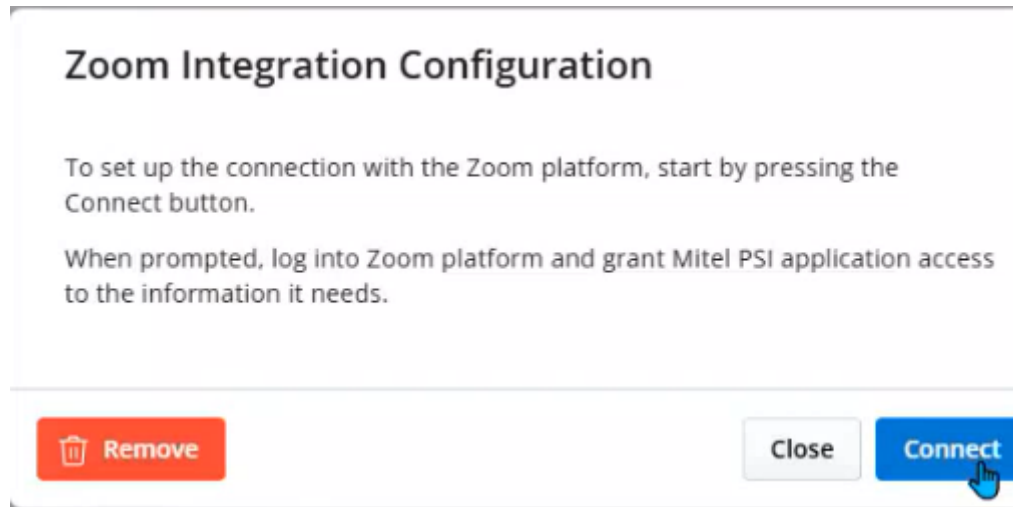
You have obtained the **necessary Zoom PSI licensing**.

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** 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 Zoom platform. 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.
- 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 is automatically displayed in the Zoom Customer's Marketplace under the **Added Apps** section.

To maintain a **stable and functional integration**, follow these best practices:

- **Create and use a dedicated service account** (admin user) with a **unique email address** on your **Zoom account portal**, exclusively for the integration.
- This account must **remain active** and **should not be deactivated**.
- *This is the admin user that will be used to log into the Zoom account in the following steps.*

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 completed the initial Zoom Phone setup.

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.

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 **Add**.
You will be redirected to [accounts.mitel.io](#) to authorize your Zoom Account.
- 4) Click **Allow** authorize the Mitel PSI application to access the necessary account information.

Next steps

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

5 Licensing

OS4K for Zoom Workplace license is required for each user which needs to be enabled with Zoom integration.

IMPORTANT: Initial releases of OpenScape 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.

It must be ensured that a subscriber license is available for each Zoom subscriber.

In standalone operation, a Flex license is required for IP subscribers. If a user utilizes multiple devices or clients, “user-based licensing” also applies. Please refer to the Sales Information document for further details.

6 Configuring Cloudlink integrations

The CloudLink Daemon is a software component embedded in OpenScape 4000 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 4000 tenants, ensuring a secure connection through a proxy server. This chapter describes the CloudLink Daemon configuration for OpenScape 4000 platform and OpenScape SBC.

IMPORTANT: Do not clone any servers where the CloudLink daemon is installed (such as CMP, OSV/OS4K, or SBC). Cloning may cause issues with the interconnection of Cloudlink Daemon with Cloudlink account/tenant and could result in communication or registration failures.

The setup of the CloudLink Daemon is carried out through:

- Administration program of the OpenScape SBC: OpenScape SBC Management Platform.
- OpenScape 4000 Platform Administration.

6.1 Enabling OS4K - CloudLink to access the Internet

This section describes how to enable OpenScape 4000 - 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.

The configuration is managed through OpenScape 4000 Platform Administration.

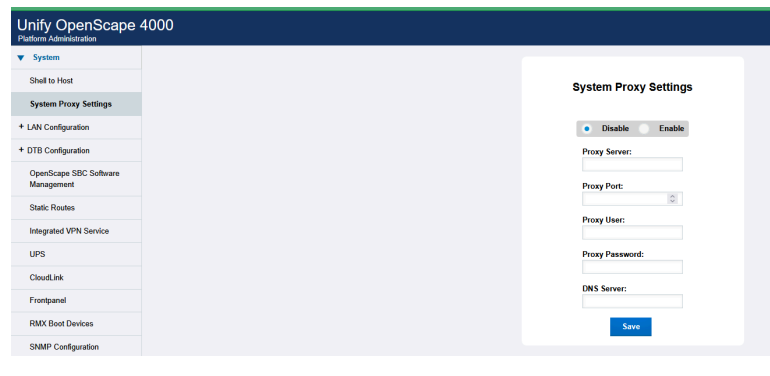
The following options are available under **System**:

- System Proxy Settings
- CloudLink

In case of **direct internet connectivity**, System Proxy Settings should be disabled and only DNS field must be edited.

NOTICE: Since DNS is one of the keys upon which system ALI is based, changing it might render the system license invalid.

Upon saving the configuration, a connectivity check is performed and the message **Cloud connectivity test OK** confirms that the settings are correct and that there is internet connectivity.



In case of internet **connectivity via Proxy**, System Proxy Settings should be enabled and configured:

Proxy server

Proxy Port

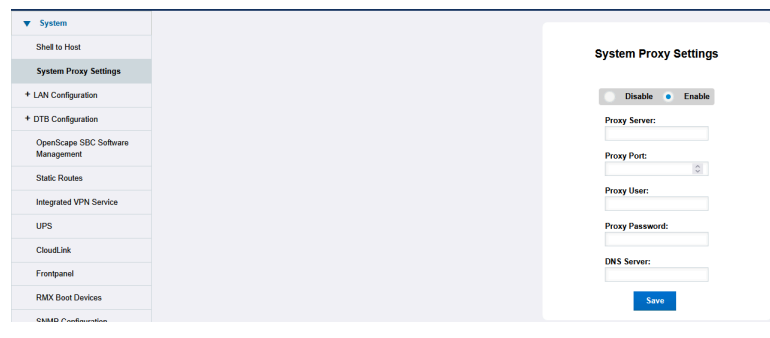
In case the customer has proxy authentication, please fill the following details:

Proxy User

Proxy Password

NOTICE:

In this case DNS field should NOT be edited.



Upon saving the configuration, a connectivity check is performed and the message **Cloud connectivity test OK** confirms that the settings are correct and that there is internet connectivity.

6.2 Connecting OS4K to CloudLink

Prerequisites

Adequate administrative permissions.

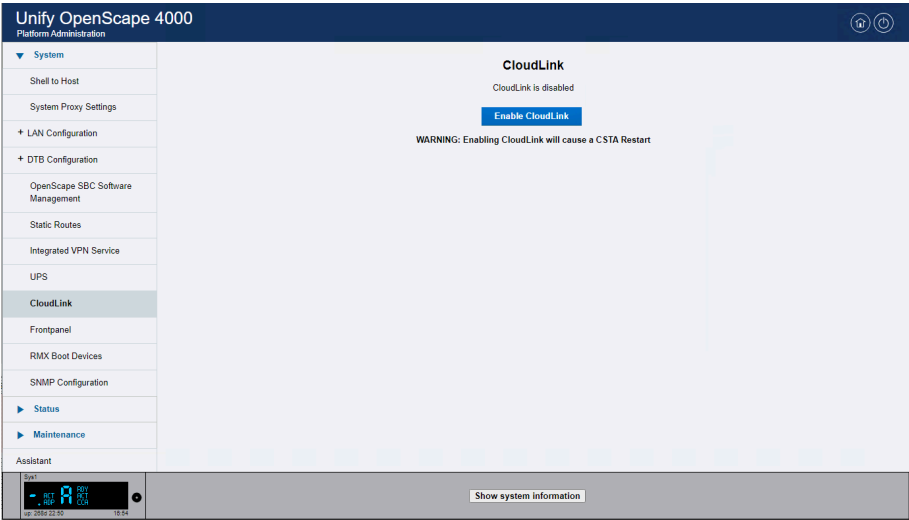
Installation of the minimum versions in [Prerequisites](#) on page 6

You have enabled platform access to internet [Enabling OS4K - CloudLink to access the Internet](#) .

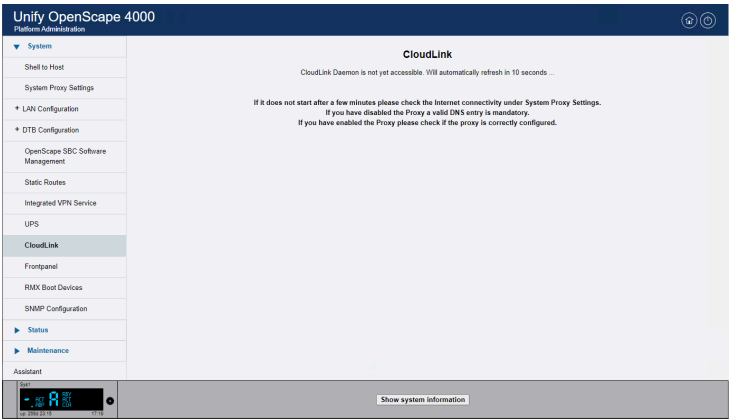
To connect OpenScape OS4K to CloudLink:

Step by Step

- 1) Log in to the OpenScape 4000 Platform Administration.
- 2) Navigate to the **System > CloudLink**
- 3) Click on **Enable CloudLink**.



NOTICE: The following advisories are prompted during CloudLink Daemon activation:



- 4) The following page confirms correct CloudLink Daemon activation:



- 5) Click **Link to Cloudlink**.
A new window is opened with the Cloudlink Portal.
- 6) Sign in to Mitel Cloudlink account with a user with Admin role.
The admin PC must be able to connect to the Internet.
- 7) When the OS4K is successfully connected with CloudLink you will see **Account Information** page:



Configuring Cloudlink integrations
OpenScape 4000 Assistant connectivity to CloudLink

8) Click **Activate container support** in order to enable CSTA Proxy.

Tunnels

Component	Tunnel	Status	Control	Description
CloudLink Gateway	CLGW REST interface	started		Remote access via Mitel Administration
OpenScape 4000 CSTA	CLGW REST interface	started		Remote access via Mitel Administration

Containers

Activate container support

The following page confirms the correct activation of container support:

Tunnels

Component	Tunnel	Status	Control	Description
CloudLink Gateway	CLGW REST interface	started		Remote access via Mitel Administration
OpenScape 4000 CSTA	CLGW REST interface	started		Remote access via Mitel Administration

Containers

Container	Version
cloudlink	1.4.0.01-3665

Restart

Deactivate container support

Performance Profile

small

CPU 8

RAM 15GiB

Next steps

After completing the above-mentioned steps, check in **CloudLink > OpenScape 4K> System Inventory>Platforms** all connected systems.

DO Accounts OS4K ST

os4kadmin

Dashboard

Account

User Management

Integrations & Apps

Billing

Support

OpenScape 4K

System Inventory

Applications

Support Legal EN (US)

Platforms

Q Search Add filter

HOST	PLATFORM TYPE	PLATFORM NAME	APPLICATION TYPES	VERSION	LICENSE	SW STATUS	PORTAL
Tache	os4k	L31988Q0759X	cloudlink-daemon , os4k-assistant , os4k-csta , os4k-rms	V11_R0.22.2	Unlicensed	Not indicated	
Kamala	os4k	L31988Q0758X	cloudlink-daemon , os4k-assistant , os4k-csta , os4k-rms	V11_R0.22.2	Unlicensed	Not indicated	

Mitel

Check in **CloudLink >OpenScape 4K> System Inventory>Applications** the inventory of the needed PBXs required for the integration .

6.3 OpenScape 4000 Assistant connectivity to CloudLink

This integration enables the provisioning of OS4K users in Zoom.

By default Assistant Zoom PSI uses System Proxy Settings. Once Platform System Proxy Settings are properly configured and CloudLink Daemon is activated, Assistant Zoom PSI will be automatically connected to CloudLink. The following settings are necessary only if a different proxy is needed for Assistant Zoom PSI.

Prerequisites

Adequate administrative permissions.

Configuring Cloudlink integrations

Connecting OpenScope SBC with CloudLink

CloudLink requires an internet connection. Set up a proxy for CloudLink only if necessary. By default, platform proxy settings are used.

Cloudlink must be enabled on the OS4K Platform.

For an overview of the CloudLink Daemon and information on its user interface, refer to the [CloudLink Daemon Solution Guide](#).

Step by Step

- 1) Login in to OpenScope 4000 Assistant.
- 2) In the navigation tree, under the **Configurations Management** click **Zoom PSI**
- 3) Click on **Settings** > **Configuration** to set up the proxy settings. If not needed, leave it as default and skip steps 4 and 5.
- 4) Configure the Hostname and port.

In case proxy setup is with authentication, add the relevant information for **proxy username** and **proxy password**.

- 5) Click on **Set proxy**.

The CloudLink connection becomes active (green) when the CloudLink daemon is enabled. And internet connectivity between Assistant and Cloudlink is stable.

NOTICE: Please note that it might take a few seconds for the button to be green after enabling it.

CloudLink reachable

Settings

Configuration

Data synchronization

Data operations

Import CSV

User data

Proxy Settings

Hostname

os4kpit

Port

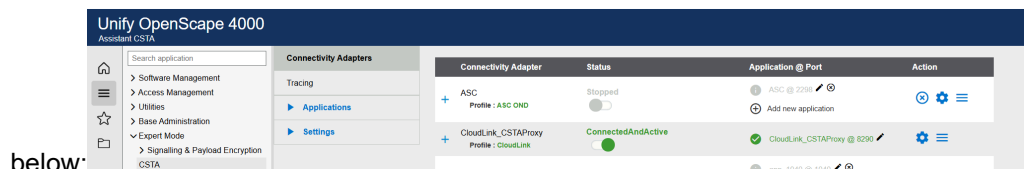
3128

☐ Authenticate

Set proxy

Next steps

The CSTA Proxy must be connected to the **Cloudlink** profile and active and the application link should be connected (green). You can check it from **OpenScope Assistant ->Expert Mode-> CSTA** as shown



6.4 Connecting OpenScope SBC with CloudLink

OpenScope SBC hosts its own instance of CloudLink Daemon which needs to be enabled and connected to CloudLink.

Configuring Cloudlink integrations

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.

To connect OpenScape SBC to CloudLink:

Step by Step

- 1) Log in to the OpenScape SBC Management Platform.
- 2) Navigate to the **System > Settings** tab.
- 3) Locate the **CloudLink** section.
- 4) To enable the SBC-CloudLink connection, check the **Enable CloudLink Service** checkbox.

The screenshot shows a web browser window titled 'sbc01 - System - Google Chrome' with the URL 'https://10.180.0.4/systemConfiguration.html?tabId=systemTab'. The page is titled 'System' and contains a message: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' Below this are three tabs: 'Settings', 'License', and 'Branding'. The 'Settings' tab is active and contains several sections: 'General' (with 'SBC Mode' set to 'Centralized SBC', 'Hostname' as 'sbc01', and 'Domain name' as 'ucaasft.mitel.com'), 'Administration' (with 'Session expiry timer' set to '2 hours' and 'Default language' set to 'English'), 'Watchdog Configuration' (with 'Watchdog expiry timer' set to '1 min'), and 'Cloudlink' (with the 'Enable Cloudlink Service' checkbox checked and a 'Restart Cloudlink Service' button). At the bottom right are 'OK' and 'Cancel' buttons.

- 5) Click **OK**.

On the main page, the SBC Dashboard displays the **CloudLink status**.

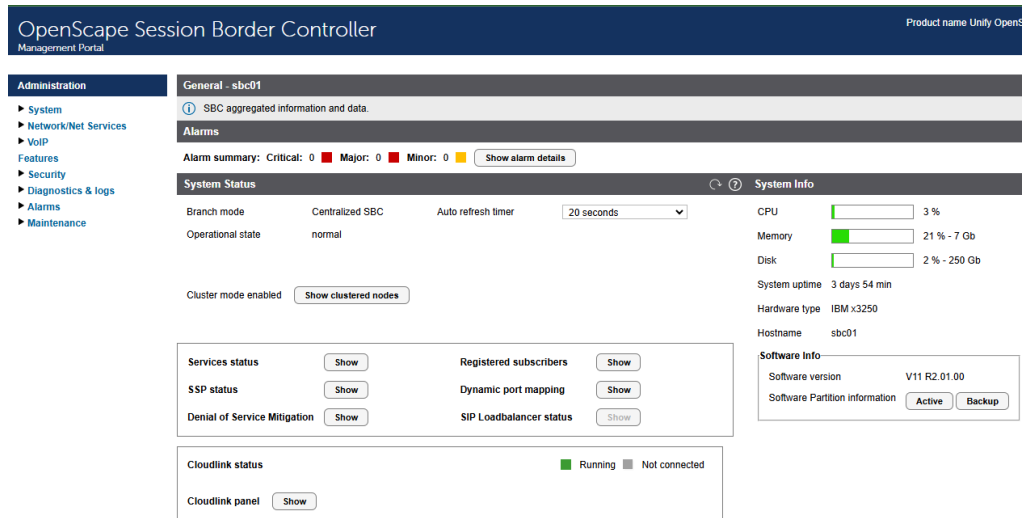


Figure 1:

- 6) To activate 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 connect to the CloudLink server.
- 8) Enter your credentials in the sign-in pop-up window and click **Next**. The CloudLink Daemon window displays the connection details.

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

- 9) Optionally, to configure tunnels and enable the SBC UI within CloudLink:
 - a) In the **Tunnels** section of the CloudLink Daemon, click **Start** next to the OpenScope SBC component.
 - b) Click **Yes** to confirm.
- 10) Optionally, you can view system information and launch a remote SBC configuration:
 - a) From the CloudLink left-hand menu, click the **System Inventory** drop-down to expand it.
 - b) To view the SBC(s) connected to CloudLink, select **Platforms**.
 - c) To perform a remote SBC server configuration, select **Applications**, then 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.

6.5 Connecting OpenScape Xpressions with CloudLink

You can set up the OpenScape Xpressions voicemail system and connect it with CloudLink to allow users to send and receive voicemail messages through their mailbox.

The integration with CloudLink provides a more seamless experience by enabling visual voicemail capabilities. Instead of calling a voicemail number and navigating audio prompts, users can now access and manage their voicemails directly from the Zoom client interface.

6.5.1 Prerequisites for connecting OpenScape Xpressions with CloudLink

This section defines the requirements that must be met to connect OpenScape Xpressions with CloudLink. Review the [Prerequisites](#) on page 6 section to confirm the supported product versions and the following prerequisites to ensure a seamless connection of OpenScape Xpressions with CloudLink.

- 1) You have administrator privileges in Xpression server.
- 2) The date and time in Xpression server are correct.
- 3) The Xpression server has internet access.
- 4) The operating system is **OS Windows Microsoft server 2019 Standard or 2022 Standard**.
- 5) The hotfixes from the latest Zoom Package are installed (**CIAPl**, **CITranscriptApl** and **MTA**).
- 6) You have CloudLink tenant credentials.

6.5.2 Setting a global variable for proxy server use

Prerequisites

Before starting, review the prerequisites in section [Prerequisites for connecting OpenScape Xpressions with CloudLink](#) on page 26.

Step by Step

The following steps are required only if the internet access is routed via a proxy.

- 1) Search for **Edit the system environment variables** in the Windows Start menu and open it.
- 2) In the **System Properties** window, click **Advanced system settings**.
- 3) In the **Advanced** tab, click **Environment Variables**.
The Environment Variables window opens.
- 4) Locate the **System variables** area and click **New** to create the HTTP_PROXY variable:
 - Variable name: HTTP_PROXY
 - Variable value: 192.168.1.1:8080

NOTICE: Use your actual proxy server address.

- 5) Click OK to save the variable.

6) Click **New** again to create the HTTPS_PROXY variable:

- Variable name: HTTPS_PROXY
- Variable value: 192.168.1.1:8080

NOTICE: Use your actual proxy server address.

7) Click OK to save the variable.

8) Ensure both variables appear in the **System variables** list.

9) Restart the Mitel CloudLink Daemon Service for the changes to take effect.

6.5.3 Connecting OpenScape Xpressions with CloudLink

Prerequisites

Before starting, review the prerequisites in section [Prerequisites for connecting OpenScape Xpressions with CloudLink](#) on page 26.

Step by Step

- 1) Open a browser and navigate to: <http://localhost:8288/cld>.
- 2) Click **Connect to CloudLink**.
- 3) Log in using your CloudLink tenant credentials. After successful login, you will be redirected to the **Mitel Administration portal**.
- 4) To manage the Xpression server via the CloudLink portal, start the tunnels.
- 5) Go to **Mitel Administration > System Inventory > Platforms** to verify that the Xpression server is listed in the CloudLink portal.

6.5.4 Activating an OpenScape Xpressions user

You can activate an Xpressions user to receive voicemails, listen to them, and get alerts.

Prerequisites

Before starting, review the prerequisites in section [Prerequisites for connecting OpenScape Xpressions with CloudLink](#) on page 26.

Procedure

- For each user whose primary SMTP address matches, if the CLOUDLINK property is checked, the user will have the new features enabled.

Next steps

Once the CLOUDLINK property is enabled, the user will have access to the new features.

6.5.5 Enabling Zoom integration and transcription

After a user is activated, perform the following steps to allow voicemail access and transcription in Zoom.

Prerequisites

- The user must be activated in Xpressions as described in [Activating an OpenScape Xpressions user](#) on page 27.

Procedure

- User should activate **Always forwarding** to Voicemail number.

- The user must enable the **Voicemail transcript** privilege under **User Administration** menu in WebAssistant.

NOTICE:

Voicemail transcript privilege can be set for an individual user. When configured at the group level, the privilege applies to all users in the group.

- Transcription occurs only when a new message is sent; existing messages cannot be transcribed.
- The transcription language is based on the recipient's language configured in Xpressions. The supported languages are "en-US", "de-DE", "en-GB", "fr-FR", "it-IT", "nl-NL", "es-ES", "pt-PT".

7 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 two accounts are interconnected via a configuration process performed through CloudLink. This chapter outlines the necessary steps for preparing and setting up OpenScape 4000 subscribers, as well as provisioning users, to ensure seamless integration with Zoom.

7.1 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](#)

7.1.1 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. To add multiple users, you can also Import a CSV file, use REST API to provision users, or set up SSO via sML or Identity SP.

Prerequisites

NOTICE:

It is also possible to import and export users as .csv file here. You can use the exported csv file later to import it on OS4K Assistant.

You have a Zoom Business or Enterprise Zoom account.

Provisioning Users

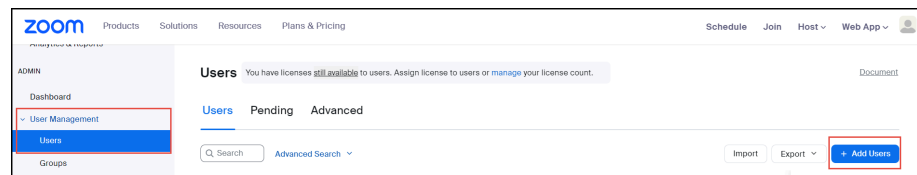
You have obtained the necessary Zoom PSI license.

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

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 8.

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.

After a user has activated the account it is possible to change the role to Admin if needed. It is not possible to create a user with role Admin.

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

7.1.2 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.

7.1.3 Configuring Zoom Phone System Integration

7.1.3.1 Configuring Phone System Integration settings

As an administrator, you can set up users for the Zoom-OS4K 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](#).

7.1.3.2 Adding Zoom users to the Mitel integration

As an administrator, you can set up users for the Zoom-OS4K 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 OS4K 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.

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

7.2 OpenScape 4000 Provisioning: Configuration Guidelines

Before beginning the OpenScape 4000 provisioning process, ensure that the following prerequisites are met.

Prerequisites

- Adequate administrative permissions.
- OpenScape 4000 Assistant is connected to CloudLink Daemon, as described in [OpenScape 4000 Assistant connectivity to CloudLink](#) on page 22.

- Zoom users have been configured in the Zoom tenant, as described in [User provisioning in the Zoom tenant](#) on page 29 and have Phone System Integration enabled.
- The OpenScope 4000 SIP-UFIP phone requires mandatory email configuration, voice mail configuration and authentication.
- The OpenScope 4000 must have configured a valid system number (AMO ANUM and ANSU).
- Ensure that the email address matches the email address that was used while creating the Zoom user and the Cloudlink user and the assigned license. Once configured, you cannot edit the **Email** of a user. Each user is assigned a unique email address that is used as identifier.
- The Email must be assigned to an OS4K subscriber:
 - Via AMO **PERSI : CHANGE - PERSI : EMAIL, <STN0>, "<em@il.address>"**;
 - Via the **OpenScope 4000 Assistant > Configuration Management > Station > Basic 3** tab.

The screenshot displays the 'Unify OpenScope 4000 Configuration Management' window. The 'Station' tab is active, showing configuration details for a station with ID 12799. The 'Basic 3' tab is selected, displaying various configuration fields. Key fields include:

- Station ID:** 12799
- System:** SYST1
- Device:** DOMAIN
- Location Code:** 1-1-422
- Access Code:** 822
- Device Family:** JFJP
- In Service:** Yes
- Status:** TRS
- Connection Type:** IP2
- Preferred Language:** German
- COFID:** [Empty]
- COTED:** [Empty]
- Call Logging:** All
- API Protocol Class:** [Empty]
- ACF State between OPS and Announcement:** [Empty]
- OR-Premise Connection Type:** [Empty]
- Billing Acc:** [Empty]
- Trace malicious call:** [Empty]
- Asynchronous Timer:** 0
- Music on Hold:** [Empty]
- Extended BOS:** [Empty]
- S-Channel Idle Pattern:** [Empty]
- Display Mode:** [Empty]
- MUP Service Domain:** [Empty]
- Cluster ID:** [Empty]
- Code Type:** [Empty]
- NEONMMS:** [Empty]
- Direct Media Connection:** [Empty]
- SMC Allowed:** [Empty]
- Use Secure DMIC:** [Empty]
- Move:** [Empty]
- Temporary Station:** [Empty]
- Redirection Station:** [Empty]
- Temporary Line:** [Empty]
- Local ID Number:** [Empty]
- LIN 1:** [Empty]
- LIN 2:** [Empty]
- Temporary LIN:** [Empty]
- Temporary Emergency Number:** [Empty]
- Charge Pulses:** [Empty]
- Level of Charge Pulses:** [Empty]
- Type of Charge Pulses:** [Empty]
- Primary Rate Interface:** [Empty]
- Public Number:** [Empty]
- Public Name:** [Empty]
- Numbering Plan Identifier:** [Empty]
- Type of Number (TON):** [Empty]
- International Number:** 4036230212799
- Email Address:** cs4k.12799@mitel-test.com
- Smart Card Access Application ID:** [Empty]
- Mobile user feature activation for application:** [Empty]

NOTICE:

The Public SBC IP address (IP advertised to Zoom for SIP client registration) must be assigned under: **CHANGE - ZANDE : TYPE=OSMO, SBCADDR1=<SIP_IP_ADDR>, PORT1=<PORT_NO>;** or

via **Assistant > Configuration Management > Network > System > OSMO**.

Each SIP/UFIP subscriber must have assigned a voicemail (a dummy one in case voicemail feature is not used) and full digest authentication:

CHANGE-

SBCSU:STNO=<STNO>,OPT=OPTI,PMIDX=<PM IDX>,IPPASSW="<IP PW>",USRID="<USR ID>",SECZON="<REALM>"

PMIDX has to point to a corresponding route, even if dummy:ADD-

```
RICHT:MODE=PM,IDX=<PM_IDX>,SAN=<VM_NO>,STYPE=OTHER;
```

Zoom connectivity requires DMC/SMP to be active on SIP gateways:

CHANGE-

CGWB:MTYPE=CGW,LTU=17,SLOT=2,TYPE=DMCDATA,DMCCONN=<DMC CONN NUMBER>,SMP=YES;

and SIP subscribers: CHA-

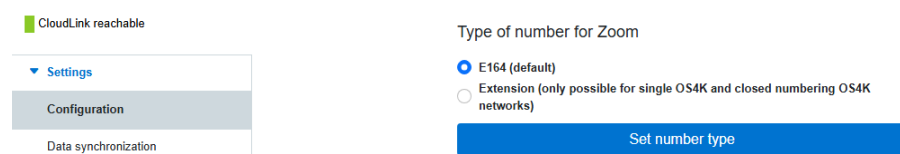
SDAT:<STNO>,ATTRIBUT,DMCALLWD;

Provisioning can be done with E164 or extension number format:

- E164 is the default but requires a proper KXDEF configuration
- Extension can be used when KXDEF is empty but only for single OS4K or closed numbering OS4K networks

In case of extension, OPTFEA 732 must be activated (**CHANGE-ZANDE:OPTFEA,A,732;"**).

The number type is available in OS4K Assistant under **Configuration Management > Zoom PSI**



7.2.1 Integrating OpenScape 4000 subscribers with Zoom Users

Users provisioning is done in OpenScape 4000 Assistant by an OpenScape 4000 administrator.

Prerequisites

General prerequisites regarding subscriber/system configuration mentioned in [OpenScope 4000 Provisioning: Configuration Guidelines](#) on page 32 are met.

To integrate OpenScape 4000 subscribers follow the next steps:

Step by Step

- 1) Log in to the OpenScape 4000 Assistant.
- 2) Click on the **Zoom PSI** navigation tab.
- 3) In the navigation tree, click on **Data operations > User data**.

A list of the existing Cloudlink users is displayed.

- 4) Click **Add user** to provision a new Zoom User.**

The **Add User** window pops up, displaying the following fields:

- **First Name:** Enter the first name of the user.
- **Last Name:** Enter the last name of the user.
- **Email:** Enter a valid email address.

IMPORTANT:

Each user is assigned a unique email address that is used as identifier.

Ensure that the email address matches the email address that was used while creating the Zoom user and the assigned license and also the one configured in AMO PERSI (or Assistant CM) for the corresponding subscriber.

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

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

The OpenScape 4000 subscriber-Zoom user integration is created.

- 6) If the email address for a newly created user matches the email address configured for the OS4K subscriber, the **Update** button will be displayed under the **Action** column for that user. Click the **Update** button to update users one-by-one.

To update multiple users, click the **Update all** button under **Data operations>User data**.

Alternatively, you can synchronize data manually using the **Data synchronization** tab from OS4K to CloudLink or wait for the next scheduled synchronization. You can check and configure synchronization settings in the **Data synchronization** tab.

[illegible]

Next steps

- 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.

IMPORTANT:

Editing or deleting Zoom configurations does not automatically impact the relevant Zoom user data. You must manually re-provision each Zoom user.

You can also import a list of users. For further information, please see: [Integrating OpenScape 4000 subscribers with Zoom Users via CSV file import](#) on page 36

7.2.1.1 Integrating OpenScape 4000 subscribers with Zoom Users via CSV file import

Zoom PSI users must be created on the Zoom admin portal.

You must configure the OS4K subscriber(s) of your choice to enable them for Zoom connection.

Prerequisites

General prerequisites regarding subscriber/system configuration mentioned in [OpenScape 4000 Provisioning: Configuration Guidelines](#) on page 32 are met.

You can export the users from Zoom and importing the list in the OpenScape 4000 Assistant.

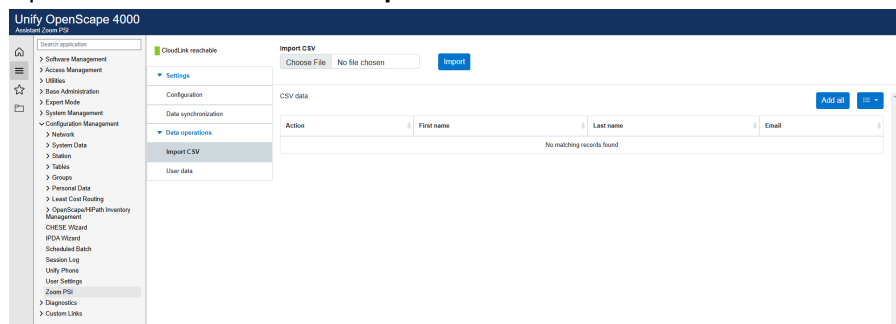
Step by Step

- 1) Log in Zoom.
- 2) Navigate to **User management> Users**.
- 3) Select the users you want to export.
- 4) Click on **Export**.
The users list will be downloaded in a **.csv** format.
- 5) Log in to the OpenScape 4000 Assistant.
- 6) Navigate to **Configuration management> Zoom PSI**.
- 7) Click on **Data Operation > Import CSV** to import the users to CloudLink.

NOTICE:

The export from Zoom contains all Zoom users, i.e. if you want to import only PSI users you have to select them individually.

- 8) Upload the **.csv** file and click **Import**



- 9) Click on **Data operation>User data** to update a new user.
You can also wait until the next data synchronization is scheduled. You can check and set the synchronizations in the **Data synchronization** tab.
- 10) Scroll down to locate the **Zoom user** checkbox and click on it to edit or delete it.

Next steps

NOTICE: Editing or deleting a user from OpenScape 4000 Assistant does not affect the ZoomPSI account. The user will remain active in Zoom until manually removed/edited by an administrator.

8 Monitoring and Troubleshooting Zoom Integration in Mitel CloudLink Admin Portal

8.1 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) Access the **Integrations** panel from the **Accounts Information** page or from the **Integrations & Apps** option.
- 2) 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:

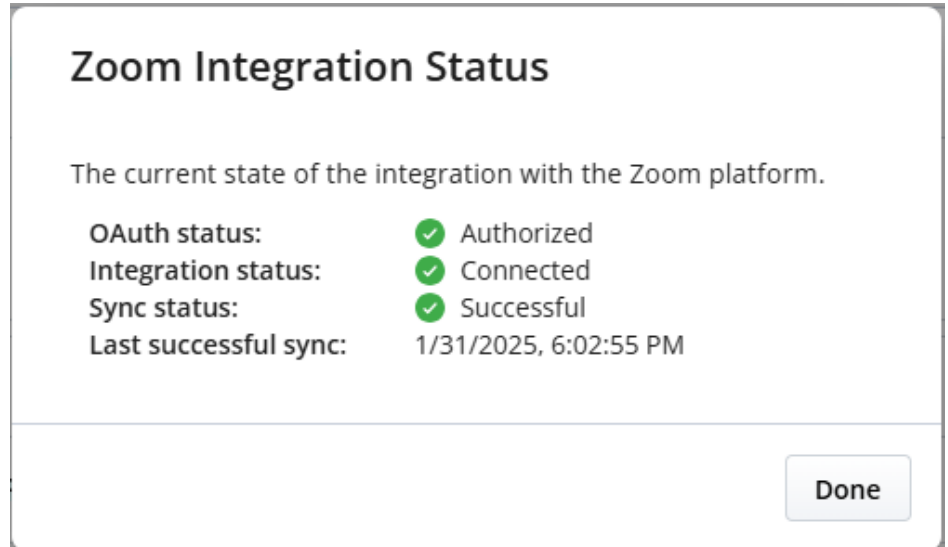
- Click **Status summary** next to the **Zoom** integration in the **Integrations** panel.
- Navigate to **Support > Zoom**.

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

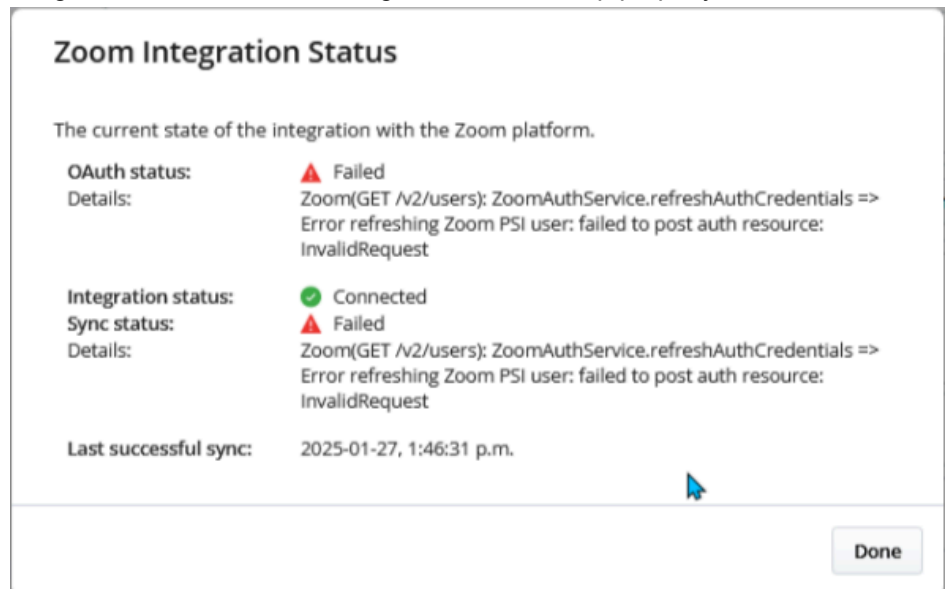
- **OAuth status:** Displays the OAuth authorization status (*Authorized*, *Failed*), indicating whether the Zoom OAuth token is valid, expired, or needs re-authorization. If the OAuth status is *Failed*, error messages associated with the most recent OAuth failure will also be displayed below the status.
- **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.



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



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. To resolve this, a Mitel Partner or Account Admin will need to reauthorize the Zoom integration.

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**.

8.2 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).

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

8.3 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.

8.4 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.

Prerequisites

The Zoom-CloudLink integration is complete.

You have added Zoom PSI users.

Step by Step

- 1) Log in to the **Mitel Administration**.
- 2) Navigate to **Support > Zoom**.
- 3) Select the **Event History** tab.
- 4) Click **Copy** to copy the event details of the following tabs:

The **Event Details** window pops up, displaying Zoom tenant details such as the Event ID number.

You can select any of the following tabs to view the related Zoom tenant information:

- **Core details**
- **Properties Changed**
- **Extra Details**
- **Log tags**

- 5) 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.

9 Configuring OpenScape SBC

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

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.

The OpenScape SBC will be configured with the connection to OpenScape 4000 and Zoom Phone System.

As an example:

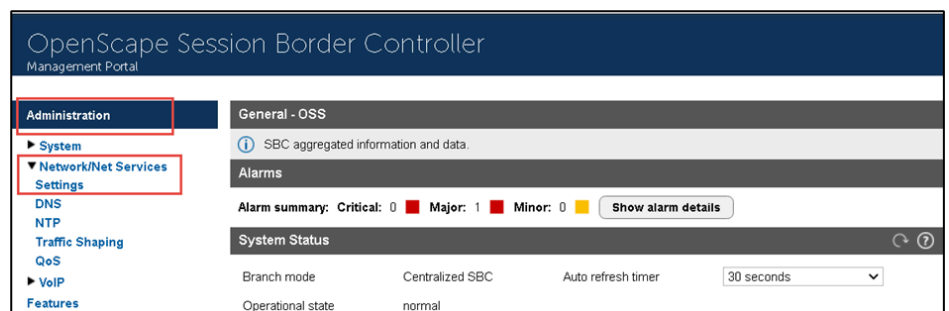
Table 1: Zoom IPs Table

Items	Example
SBC Core (LAN) IP	10.180.0.4
SBC Access (WAN) IP	10.181.181.147
SBC Public FQDN	sbc01.athdlabs.xyz

Mitel OpenScape SBC installation and administration documentation can be found on the [Unify customer documentation site](#).

9.1 Configuring Network settings

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

Type	Network ID	Interface	IP address	Subnet mask	Signaling	Media	SIP-UDP	SIP-TCP
Main IPv4	Main-Core-IPv4	eth0	10.180.0.4	255.255.248.0	☒	☒	5060	5060

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.

Access and Admin realm configuration

Type	Network ID	Interface	IP address	Subnet mask	VLAN tag	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	MDCP	SIP server	Message rate (sec)	Trust level	Signaling restriction
Main IPv4	Main-Access-IPv4	eth1	10.181.181.147	255.255.255.0	0	☒	☒	5060	5060	5061	2727	Any	100	N/A	Unrestricted

Realm Profile

Realm profile	Realm	Signaling network ID	Media network ID	Forward network ID
Main-Core-Realm-ipv4	core	Main-Core-IPv4	Main-Core-IPv4	
Main-Access-Realm-ipv4	access	Main-Access-IPv4	Main-Access-IPv4	

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**).

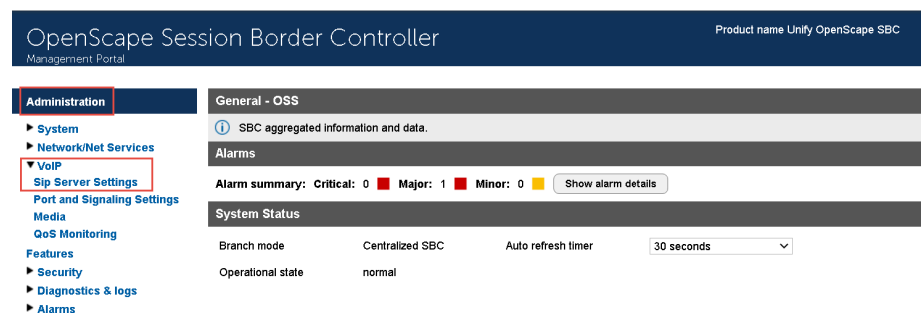
You are redirected back to the **Network/Net Services** window.

- 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**.

9.2 Configuring SIP Server

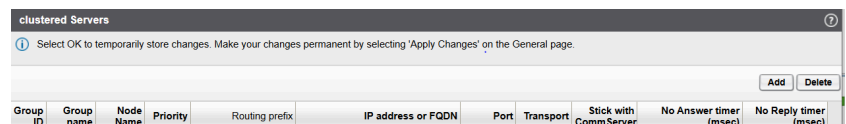
The SIP connectivity to OpenScape 4000 is configured in the **OSSBC Management Portal > VOIP** window.

- 1) Log in to the OpenScape SBC Management Platform.
- 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 **Clustered**.
 - b) Access the **Clustered Node Servers** section, then click **Add** :
 - Add the **Group name**
 - Add the **Node name**
 - Set the **Priority**
 - **IP Address or FQDN**: Enter the OpenScape 4000 IP address.
 - **Stick with CommServer**: enabled
 - From the **Transport** drop-down menu, select **TCP/TLS**.
 - **Port**: Enter **5060/5061**.



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

9.3 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) Navigate to OpenScape SBC **Management Portal** > **Security** > **Denial of Service**.

- 2) In the **Security** pop-up, under the **Dynamic Black List** section, check the **Process initial registration** flag to enable it. If you want to use **User Agent Allowed List** please make sure that **zoompbxphone** is added.

Security

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

General | Firewall | Message Rate Control | RADIUS | Tunnel Connections | Denial of Service Mitigation

Dynamic Black List

☐ Block unauthorized users Unauthorized user quarantine interval (sec) 300

☐ Block unknown users Unknown user quarantine interval (sec) 300

☒ Process initial registration

☐ Enable gateway message rate limit

Trust Level Quarantine Intervals

Minimal (sec) 60

Medium (sec) 10

User Agent Allowed List

User Agent Add

ngtc
microsip
husim openstage simulator
teams
zoompbxphone
mitelcloudlinkt2

Delete

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

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

OpenScape Session Border Controller

Management Portal

Administration

- System
- Network/Net Services
- VoIP
- Features
 - Security**
 - General**
 - Firewall
 - Message Rate Control
 - RADIUS
 - Tunnel Connections
 - Denial of Service
 - Diagnostics & logs
 - Alarms

OS - Security - Google Chrome

Not secure | https://10.70.16.25/security.html?tabId=generalTab

Security

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

General | Firewall | Message Rate Control | RADIUS | Tunnel Connections | Denial of Service Mitigation

Certificates

Certificate management

PKI Configuration

☐ Enable PKI configuration PKI configuration

Configuring OpenScape SBC

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

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

CA Certificates

Upload CA certificate file

Choose File

No file chosen

Upload

CA certificates

CA1.pem
combined-ca-bundle.pem
DigCertGlobalG2TLSPRISQA4H4360200CA1-
DigCertGlobalRootG2.crl.pem
0to_daddy_root_CA.pem
Godaddy_secureCA.pem
serverCA.pem

Delete

X.509 Certificates

Upload X.509 certificate file

Choose File

No file chosen

Upload

X.509 certificates

db4204cc73a95302.pem
servercert.pem

Delete

Key Files

Upload key file

Choose File

No file chosen

Upload

OK

Cancel

- 7) Under the **Key Files** section, click **Choose File** and browse to select the OSSBC server certificate private key. Click **Upload**.
- 8) To create the Zoom certificate profile: In the **Certificate Management** pop-up, under the Certificate profiles area, click **Add**.

Certificate Management

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

System Certificate

System TLS Certificate

OSV Solution

HTTPS certificate profile

HTTPS System Default

Media DTLs certificate profile

iOS Push certificate profile

iOS Push Default

Android Push certificate profile

Android Push Default

Service API certificate profile

Service API Default

Certificate Profiles

Add

Edit

Delete

9) Configure the following parameters:

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

Certificate Profile

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

Certificate Profile configuration

Certificate profile name: Zoom_BYOT

Certificate service: SIP-TLS

Local client certificate file: [Show]

Local server certificate file: ServerCertificate.pem [Show]

Local CA file: ssl_root_with_chain.pem [Show]

Remote CA file: [Show]

Local key file: PrivateKeymit.pem

EC param: secp256r1

Attach to Config file: ☐

Validation

Certificate Verification: None

☐ Revocation status

☐ Identity Check

Renegotiation

☐ Enforce TLS session renegotiation

TLS session renegotiation interval (minutes): 60

TLS version

Minimum TLS version: TLS V1.2

DTLS version

Minimum DTLS version: DTLS V1.0

Cipher Suites

Perfect Forward Secrecy: Preferred PFS

Encryption: Preferred AES-128

Mode of Operation: Preferred GCM

OK Cancel

10) Click **OK**.

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

12) Click **Apply Changes** on the OpenScope SBC main page.

9.4 Configuring Media Profiles

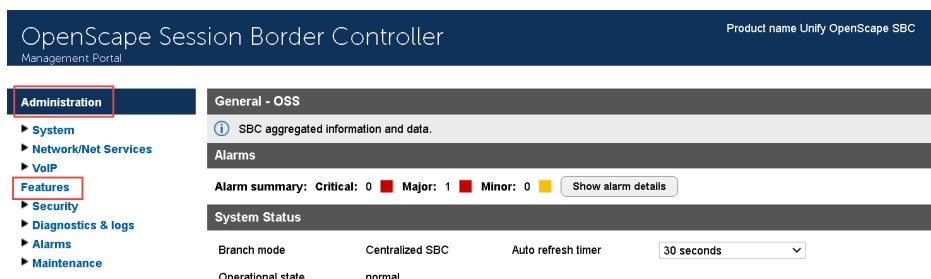
In the **Media Profiles** settings, various SDP messages and audio (RTP) traffic parameters can be configured for the OpenScape SBC SIP endpoints to Zoom PSI and Unify OpenScape 4000.

9.4.1 Configuring the Codec Manipulation and Remote Subscribers

Certain codec configuration for audio is required for the OSSBC – Zoom PSI and OSSBC – SSP media profiles for the corresponding SIP trunks.

It is required to enable the codec configuration options first for the media profile setup.

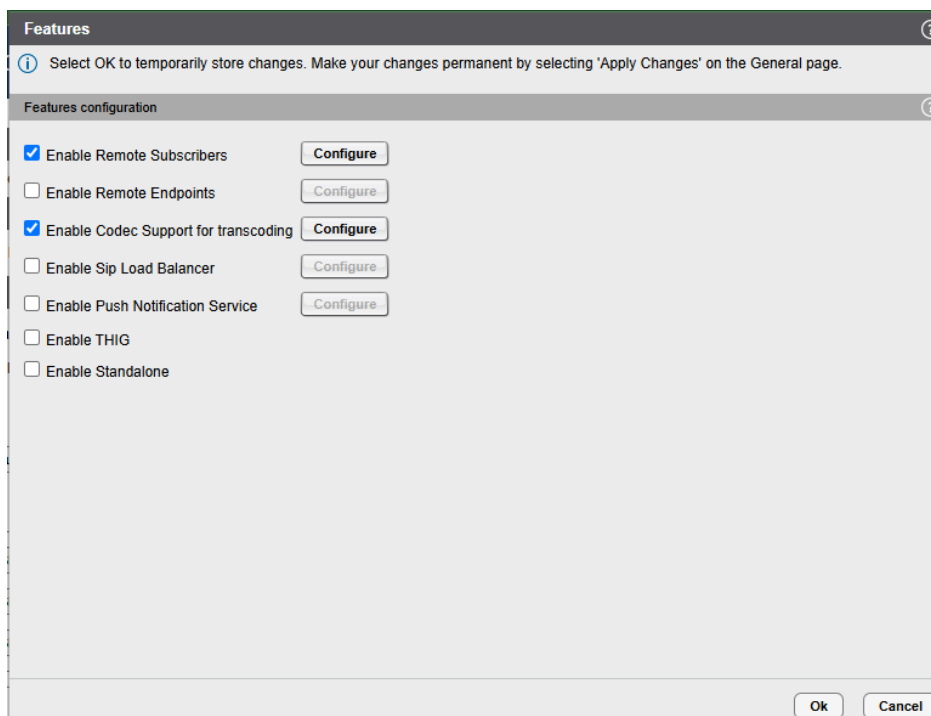
- 1) Navigate to the **OpenScape SBC Management Portal > Features** window.



- 2) Check the following:

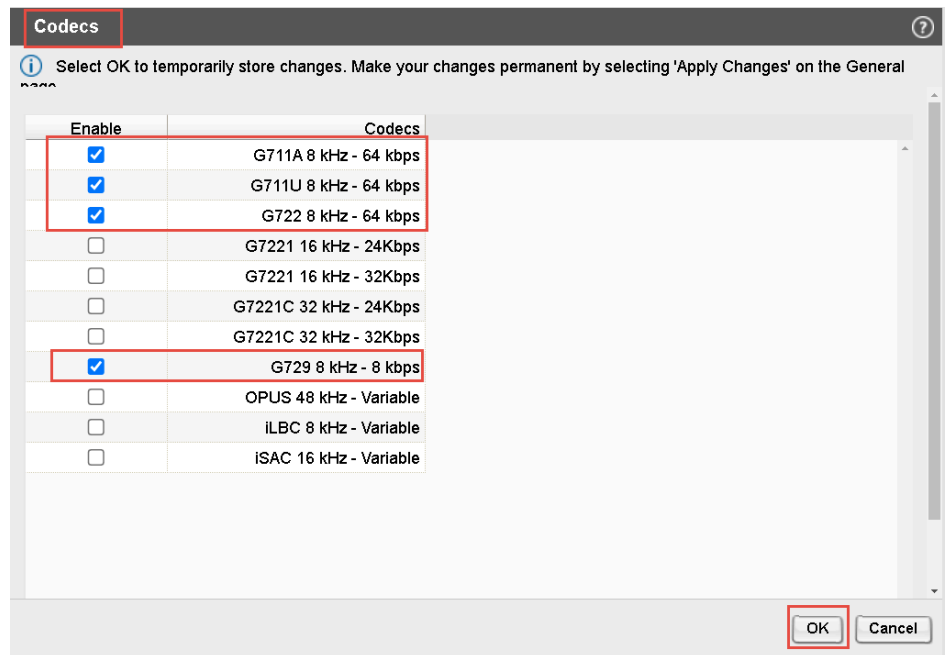
Enable Remote Subscribers checkbox.

Enable Codec Support for transcoding checkbox.



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

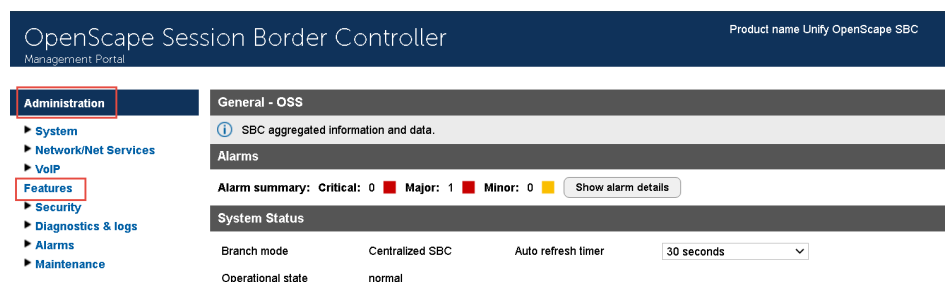
- 4) In the **Codecs** window, you need to select the following codecs to be available for the media profiles (for example, transcoding, prioritization), as shown in the example below:



- 5) Click **OK**.
- 6) Click **Apply Changes**.

9.4.1.1 Configuring Remote Subscribers

- 1) Log in to the OpenScope SBC Management Platform.
- 2) Navigate to the **Administration > Features** window.



- 3) In the **Features > Enable Remote Subscribers** click **Configure**.
- 4) In the **Remote Subscribers** window, check the **Enable register throttling** checkbox to enable it.

5) Check the **Enable register throttling for TLS** checkbox to enable it.

Remote Subscribers

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

General Settings

☒ Enable register throttling

Timer value towards subscriber - UDP (sec) 60

☒ Enable register throttling for TLS

Timer value towards subscriber (sec) TCP/TLS 60

Maximum throttling timer threshold (sec) 1800

Maximum registration expiry time (sec) 2678400

Minimum registration interval (sec) 300

☐ Quarantine registration rate violators

Port Mapping TTL timer (hours) 2

☐ Disable External Port Mapping

Core realm profile Main-Core-Realm - ipv4

Access realm profile Main-Access-Realm - ip

INVITE No Answer timeout (msec) 360000

INVITE No Reply timeout (msec) 3000

☐ Enable remap internal error code 504

☐ Insert Location Header

☐ Open external firewall pinhole

☐ Send RTP dummy packets

☐ Drop received RTP

☐ Dummy RTP to Core side

Stream Delay (ms) 60

OK Cancel

6) Set the **Maximum registration expiry time** to **2678400**, otherwise Zoom mobile clients registration will be rejected. The parameter must be set as shown in the example below:

7) Click **OK**.

8) Click **Apply Changes**.

9.4.2 Configuring the Zoom Media Profile

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

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

OpenScape Session Border Controller

Product name Unify OpenScape SBC

Management Portal

Administration

- System
- Network/Net Services
- VoIP
- SIP Server Settings
- Port and Signaling Settings
- Media
- QoS Monitoring
- Features
- Security

General - OSS

SBC aggregated information and data.

Alarms

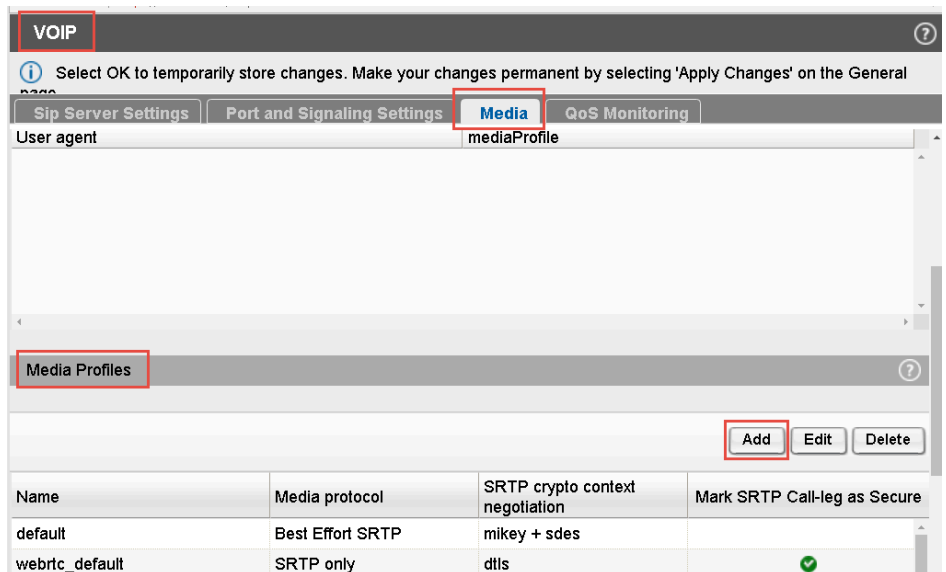
Alarm summary: Critical: 0 Major: 1 Minor: 0 Show alarm details

System Status

Branch mode Centralized SBC Auto refresh timer 30 seconds

Operational state normal

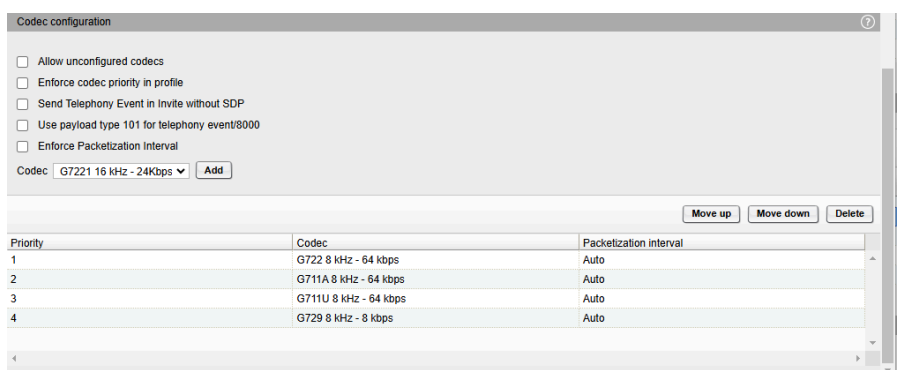
- 3) In the **VOIP** pop-up, go to the **Media** tab.



- 4) Locate the **Media Profiles** area and click **Add**.
The **Media profile** window pops up.
- 5) Under the **General** area, create the media profile for OSSBC - Zoom connections by entering the following:
 - **Name:** Type the media profile name. For example, Zoom.
 - From the **Media protocol** drop-down menu, select **SRTP only**
 - Under the **SRTP configuration** area, check the **SDES** following checkbox.
 - Uncheck the **Keep sendonly attribute on NAT** option.

NOTICE: When this option is enabled, the user will see the Indication Remote Hold, but the Music On Hold (MOH) is not played.

- 6) Under the **RTCP configuration** area, from the **RTCP Mode** drop-down menu, select **Bypass**.
- 7) Under the **Codec configuration** area, uncheck **Allow unconfigured codecs**.
- 8) Add the codecs in the following priority order:



- 9) After the above configurations are finalized, **add the media profile** to the user agent.

In the **User agent** section, click **Add** and configure the following:

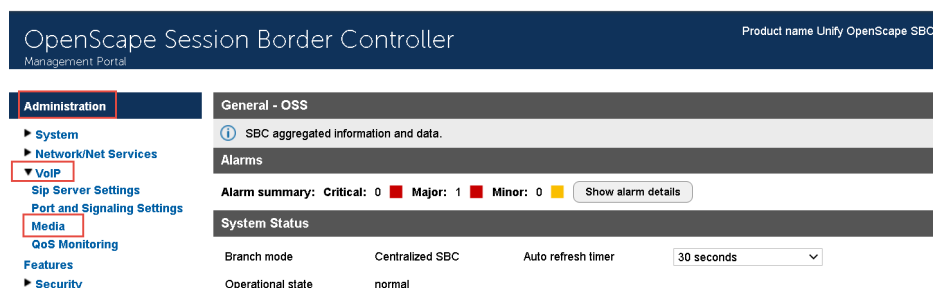
- **User agent: ZoomPbxPhone**
- **mediaProfile**, the one that was previously created. In this example the profile is named: **Zoom**

User agent	mediaProfile
OpenScape Mobile Client - WebRTC NGTC	Unify_Phone_default
Android OpenScape Mobile Client Pro	default
iOS OpenScape Mobile Client Pro	default
Siemens.Sip Engine	OS4K
ZoomPbxPhone	Zoom

- 10) Click **OK** to return to the **Media** window.
- 11) Click **OK** on the **VoIP** window.
- 12) Click **Apply Changes**.

9.4.3 Configuring the OpenScape 4000 Media Profile

- 1) Navigate to the **OSSBC Management Portal > VoIP > Media** window.



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

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

- 1) In the **Media Profiles** area, click **Add** to create the media profile for OSSBC – OS4K connection.
- 2) In the **Media profile** pop-up, locate the **General** section and configure the following:
 - **Name:** Enter the name of the media profile.
 - From the **Media protocol** drop-down menu, select **SRTP only**.
- 3) Under the **SRTP configuration** area, check the **SDES** checkbox.
- 4) In **RTCP configuration**, section, in the **RTCP Modeselect** **Bypass** option.
- 5) Navigate to the **Core Side Media Configuration** section and select the previously configured media profile from the drop-down menu.
- 6) Click **OK** in all open windows.
- 7) Click **Apply Changes** on the SBC main page.

9.5 Push Notification

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

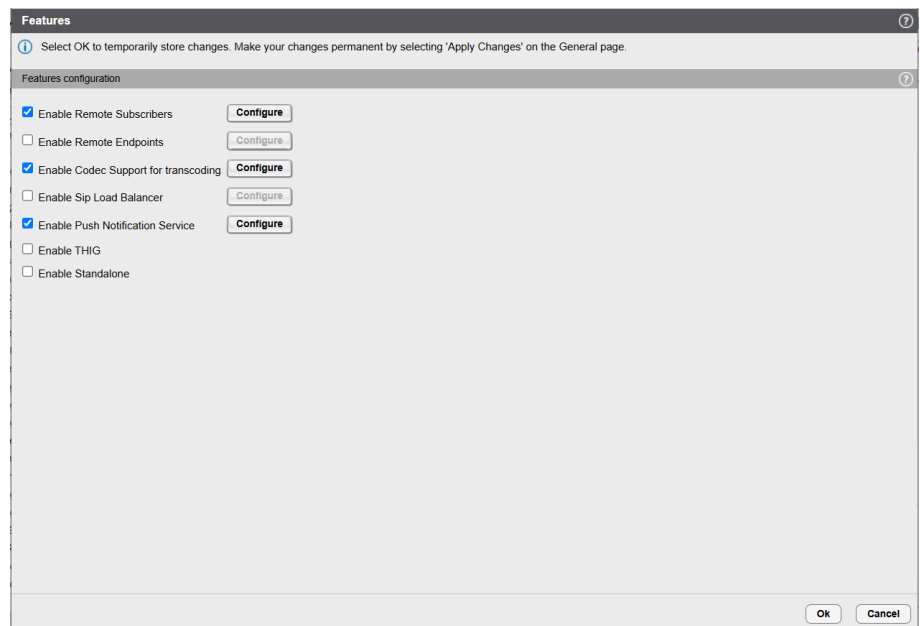
You can set up mobile push notifications by configuring the required settings in the OpenScape SBC and CloudLink.

9.5.1 Enabling push notification

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

Step by Step

- 1) Log in to OpenScape SBC Management Portal.
- 2) Navigate to the **Features** .
The **Features** window pops up.
- 3) Check the **Enable Push Notifications Service** checkbox.



- 4) Click **OK** and **Apply changes**.

9.5.2 Response Codes for Push timeout

If the Zoom mobile app is not reachable by OpenScape SBC (for different reasons, for example due to network issues), the OpenScape SBC will send the 500 SIP error message to calling party, by default. As an administrator, you are able to choose from a list of five error codes. It is recommended to change the **Response Codes/Message for Push timeout** to **480 Temporary Unavailable**.

Configuring OpenScape SBC

Push Notification Service

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

Register expire time (secs)

3600

Register Hold time (days)

1

Outbound calls

Call hold time (secs)

25

☒ Send Session Progress (183) during hold time

Send Session Progress (183) after: (secs)

5

Notification Server (iOS)

Push Certificate Passphrase

Account Team Id

4XGDRF4ETY

Mobile Application Bundle Id

com.unify.iOSMO

Notification Server (Android)

Firebase Database URL

Security

☐ Disable certificate validation

Response Codes for Push timeout

Response Code/Message for Push timeout:

480

Temporarily Unavailable

OK

Cancel

10 Emergency Configuration

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.

OS4K, 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 OS4K, 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, OS4K is integrated with [Redsky](#) in USA and Canada. A valid service agreement with RedSky 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 use SIP trunks to route E911 calls to the appropriate Public Safety Answering Points (PSAPs) based on the civic address.

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 RedSky tenant information, forwards the request to RedSky to retrieve the user's emergency location.

10.1 Emergency configuration in CloudLink

You can configure the emergency configuration for 911 or 112 in Cloudlink.

Prerequisites

Adequate administrative permissions.

Emergency Configuration

Emergency configuration in OpenScape 4000

Installation of the minimum versions in [Prerequisites](#) on page 6

You have enabled platform access to internet [Enabling OS4K - CloudLink to access the Internet](#).

To set the emergency configuration:

Step by Step

- 1) Log in to Mitel Cloudlink.
The admin PC must be able to connect to the Internet.
- 2) Navigate to the **OpenScape 4K > System Settings** and configure the emergency configuration.

Next steps

For CloudLink Emergency configurations, refer also to [Configuring the PBX system settings](#) (steps 5-6).

10.2 Emergency configuration in OpenScape 4000

You can configure the emergency configuration for 911 or 112, depending on your region.

Prerequisites

Adequate administrative permissions.

Installation of the minimum versions in [Prerequisites](#) on page 6

You have enabled platform access to internet [Enabling OS4K - CloudLink to access the Internet](#).

To set the emergency configuration:

Step by Step

- 1) Configure an OS4K SIP native trunk to route the emergency call to SBC.
Please see OpenScape 4000 [Related Documentation](#) on page 11
- 2) To enable the addition of Geolocation information to the outgoing INVITE on the SIP trunk, configure the parameter: "Call Geolocation (RFC 6442)".
This parameter needs to be set to **Send complete Geolocation in XML Geopriv PIDF-LO (emergency call)**

Call Geolocation (RFC 6442):

10.3 Emergency Configuration in OpenScape SBC

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.

10.3.1 Configuring an E911 Media Profile

Follow the steps below to create a new media profile for your E911 Provider.

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 E911 Provider. To ensure compliance with their requirements, please contact your E911 Provider's support.

- 5) If codec configuration is required by your E911 Provider, do the following:

NOTICE: In some cases, codec configuration from an E911 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) Uncheck the **Allow unconfigured codecs** checkbox.
- 6) From the **Codec** drop-down menu, select the codec as specified by your E911 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).
- 7) Click **OK** to save the configuration.
- 8) Click **Apply changes**.

10.3.2 Configuring Remote Endpoints for E911

An endpoint refers to a remote computing device engaged in bidirectional communication with a connected network. In both single-arm and multi-arm

deployment scenarios, you need to first create SIP Service Provider Profiles (SSPs) and then proceed with setting up the remote endpoints configuration settings.

10.3.2.1 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** next to it.
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.

10.3.2.2 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.

10.4 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.

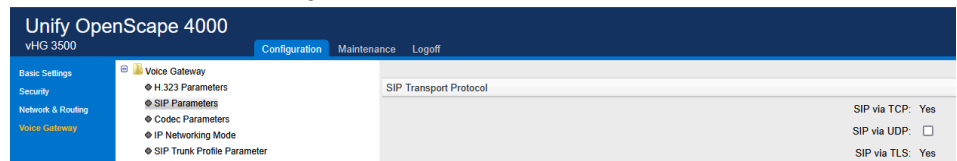
11 Appendix

11.1 Appendix A: Restrictions and Known Issues

OS4K Restriction:

The **SIP via UDP** protocol needs to be unchecked from Gateway:

Log in OpenScape 4000. Under **Configuration > Voice Gateway > SIP Parameters > SIP Transport Protocol** uncheck **SIP via UDP**



The following table lists the tested features when Zoom is integrated with OpenScape 4000 and OpenScape SBC

Feature	Description
Local tones on Zoom PSI client	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> Limitation: This occurs when the PSI client receives a <i>486 Busy Here</i> SIP message from OS4K.
Do Not Disturb (DND)	When the user logs out, DND is automatically deactivated from client side. Upon login, the Zoom PSI Client re-enables Do Not Disturb (DND) if it was active before logout.
Xpressions Voicemail	If the sender is not configured with an Xpressions account, and there is no corresponding Zoom user or Zoom contact for the sender, then the receiver of the Visual Voicemail (VVM) will not be able to see the sender's name, but only the number. This happens since XPR is not currently capable to store the name provided in the PAI header.

11.2 Appendix B: Default User Name and Password

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

Appendix

User Name	Password
administrator	Asd123!.

For information on OpenScape SBC Security Checklist, refer to [OpenScape SBC V11 Security Checklist](#).

