Mitel Phone System Integration (PSI) with Zoom Troubleshooting Guide

Service Documentation

07/2025

A31003-H8000-S100-1-7620

Mitel

Notices

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

Trademarks

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

Contents

1 - History of Changes

Issue	Date	Description
1	05/2025	Initial release

2 – Introduction

2.1 Target audience

If you have a direct contract with Zoom, please raise the issue with Zoom if it is not a Zoom PSI issue

3 - Overview

This guide provides basic troubleshooting information for Zoom Workplace but is primarily aimed at Zoom PSI troubleshooting when used in a Mitel environment.

See each section in turn below for details and requirements

4 - Zoom Workplace

4.1 – General

The Zoom deployment guide can be found here - https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0079172

This provides an overview and details for the Zoom deployment\configuration and links to the Call manger specific guides

Link to Zoom troubleshooting – https://support.zoom.com/hc/en

4.1.1 - Data to collect

Zoom Case Submission Minimum Data Set	
The format of the Subject Line should be as follows: *Customer Account Number / Product / Issue (Example: Account 123456789 / Zoom Phone / Call Drops)*	
Product	**Description**
Zoom Meetings (Includes Rooms)	• Meeting ID: • Date & Time: • Audio Issue Reported: • Video Issue Reported: • Issue: • Affected user/device/room details (name):
Zoom Phone Issues	• Name of user with issue: • Date: • Time: • Number Dialed Into: • Number Dialed Out from: • Issue: • Customer Site (if applicable): • Is this issue reproducible? • Are only internal/external calls impacted? • If BYOC - is the customer impacted on Native numbers as well?
Zoom Contact Center Issues	• User and/or queue with issue: • Engagement ID: • Issue: *Problem reports should be submitted when an issue occurs. Include the user email and/or engagement id in the problem report for identification. Note that a problem report does not submit a ticket. *If an engagement ID is not available provide the date and time of issue, and user who experienced problem

SSO	• Description of the issue, including steps taken to replicate.
	• New configuration, or change/update to an existing configuration?
	• How many users are affected? Provide example users.
	• SAML or SCIM API/Automated provisioning issue/question?
	  ○ If SAML authentication
	  ■ Verify SAML Response logs are enabled
	  ■ Provide screenshots of SAML Response logs that correspond with sample users (Logs only last 7 days).
	  ○ If SCIM API
	  ■ Verify whether calls are being made by checking the call logs for integration in the Zoom Marketplace.
	  ■ If there are no logs in the Marketplace showing, or the information being sent isn't what's expected, check provisioning logs with the IdP. If it's something other than Azure/Okta/ADFS, redirect to their provider

Integrations	• Description of the issue, including steps taken to replicate. • The name of the Marketplace Integration • Percentage of user impact (provide example users) • Any relevant error messages/screenshots (Include tracking ID if applicable)

4.1.2 - Identifying the Zoom Account and Owner

Identifying the Zoom Tenant that your user is logged into or collecting data such as Account owner, License in use, etc.

Follow the steps in this link to identify this information

https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0060684

4.2 - Meetings

If you have an issue with Zoom meetings you will need to follow the link to Zoom troubleshooting guide which provides hints and tips on how to investigate the issue and what you are required to collect prior to raising.

https://support.zoom.com/hc/en/category?id=kb_category&kb_category=fdb2be128720391089a37408dabb3589

4.3 - Team Chat

If you have an issue with Zoom meetings you will need to follow the link to Zoom troubleshooting guide which provides hints and tips on how to investigate the issue and what you are required to collect prior to raising.

https://support.zoom.com/hc/en/category?id=kb_category&kb_category=70f6f61a8720391089a37408dabb359a

4.4 - Zoom whiteboard

If you have an issue with Zoom meetings you will need to follow the link to Zoom troubleshooting guide which provides hints and tips on how to investigate the issue and what you are required to collect prior to raising.

https://support.zoom.com/hc/en/category?id=kb_category&kb_category=28687e5a8720391089a37408dabb352d

5 - Zoom PSI

This chapter describes the data that you are required to collect to investigate an issue with Zoom PSI, whilst you will notice there are similarities in the required information the process to collect the data will differ on a per call manager\solution basis.

5.1 - Data to collect

- Impacted users
- Date/time of the incident
- Specifics of the issues
- Can it be reproduced
- Is this a 1 off or has it happened before
- Screenshot or details of any error message displayed

- Detail all troubleshooting steps that have occurred so far.
- Detail all results collected so far
- If the network is believed to be the issue, collect and review a packet capture, if the issue is not resolvable after the review, supply the packet capture complete with a network diagram.

Once the above general Zoom PSI data is collected, gather the CloudLink logs from 5.2.5, then collect the specific data for the call manager\solution found in section 5.2

5.2 - Call Manager\Solution data collection

This section details what and how to collect logs from the specific call manager used in the customers solution.

5.2.1 - MiVB

5.2.1.1 - Registered SIP devices

To see all the registered SIP devices on the system

Log into MiVB

Navigate to Maintenance and Diagnostics → Maintenance commands

Enter the Command - **sip registrar all** press **Enter**

5.2.1.2 - MiVB - CCS Trace

Log into MiVB

Navigate to Maintenance and Diagnostics → Maintenance commands

Enter the Command - **CCS TRACE ENABLE CONTINUOUS** press Enter.

Once testing is complete enter the command **CCS TRACE disable** and press **Enter** to stop the trace.

5.2.1.3 – MiVB SIP Trace

Log into MiVB

Navigate to Maintenance and Diagnostics → Maintenance commands

Start the Trace

Enter the Command - **SIP TCPDUMP ON** press **Enter**

Confirm the start confirmation is displayed

SIP TCPDUMP ON Started...

Reproduce the issue

Stop the Trace

Enter the command - **SIP TCPDUMP OFF** press **Enter** to stop the trace

Confirm the stop confirmation is displayed

SIP TCPDUMP Stopped

Collecting the Trace

There are 2 ways to collect the trace

1. **Download SOS Logs**
    - Log into the MSL of the MiVB [IP Address]/server-manager/
    - Navigate to Administration → View logs files
    - Under the **Collect log files & diagnostic data** section click **Start**
    - The SOS logs will be collected and downloaded to you default download location
2. **SFTP Log Download**
    - Connect to the MiVB using a SFTP client e.g. WinSCP, Enter the IP Address, Username: root and Password: (Same password as Server-Manager admin user account).
    - Navigate to the folder root\vmail copy\download the packet capture that matches the reproduction time.

Note: To connect to MSL using port 22 confirm the allowed networks and secure shell settings are set correctly, to do this navigate to Security → Remote access.

5.2.1.3 - MBG - Packet capture – SIP Signaling

Log into MBG

Navigate to Applications → MiVoice Border Gateway → Troubleshooting Tab → Diagnostics

Select **Load** displayed next to **Packet trace**

Tick the check box next to **Enable signaling capture** it should now display **Running.**

Reproduce the issue

Select the required PCAP file from the **PCAP files for download** box

The file will be downloaded to your PC

Untick the check box next to **Enable signaling capture** to disable the trace it should now Display **Not Running.**

5.2.1.4 - MBG - Packet capture – Full Trace

Log into MBG

Navigate to Applications → MiVoice Border Gateway → Troubleshooting Tab → Diagnostics

Select **Load** displayed next to **Packet trace**

Tick the check box next to **Enable global packet capture** it should now display **Running.**

Reproduce the issue

Select the required PCAP file from the **PCAP files for download** box

The file will be downloaded to your PC

Untick the check box next to **Enable global packet capture** to disable the trace it should now display **Not Running.**

5.2.2 - OpenScape 4000

5.2.2.1 - User Provisioning log collection

User provisioning is managed in OpenScape 4000 Assistant by an OpenScape 4000 administrator. For investigation, Assistant logs related to Zoom PSI Assistant logs should be downloaded from

Diagnostics -> Trace Download -> Zoom PSI profile.

5.2.2.2 - CloudLink and OpenScape 4000 connectivity issue log collection

If there are connectivity issues between CloudLink and OpenScape 4000, platform logs are required for further investigation.

These can be downloaded through OpenScape 4000 Platform Administration by navigating to:

Maintenance > Logs > Export > Export Logs System Webservice (including Kubernetes).

5.2.2.3 - Log Collection for Call Related Issues

For call-related issues (pure SIP signaling like hold, retrieve), please provide:

- RMX traces: From Assistant, navigate to Expert Mode > Permanent Logging > System Status and Mega Traces tab.
- SBC SIP traces see 5.2.4
- CloudLink see 5.2.5

5.2.2.4 - For non-call related issues

For non-call related issues (CSTA-based features like Call Log, DND, CF), please provide the following traces:

- CSTA logs: From Assistant, go to Expert Mode > Permanent Logging > CSTA Tab. Select the CloudLink CSTA connectivity adapter, hover over the button with 3 lines and download the logs.
- CloudLink see 5.2.5

5.2.3 - OpenScape Voice

5.2.3.1 - OpenScape Voice General Log collection

To collect logs from OpenScape Voice type the command:

- *cld-getlogs*

This will create a tarball in the local directory. This tarball contains important logs, configuration files, and a copy of the latest inventory report.

Since the CloudLink Daemon on OpenScape Voice is controlled by the CMP web server, you should also include logs from Common Management Platform (CMP).

5.2.3.2 - Call-related issues

For call related issues, collect the following OpenScape Voice logs:

- RTT (24_7 or 24_7_min)
- SBC SIP traces
- RapidStat level 5 traces

5.2.3.3 - Centralized Call log\history log collection

OpenScape Voice supports a centralized call log service for WebRTC clients.

The call log events for Zoom PSI are routed via the CloudLink Container CSTA Proxy.

The responsible process for sending Call Log Event (CLE) messages is dispProc.

For any call log issues, it is recommended to enable the following flags, as well as 24_7.

- RTT traces for dispProc can be collected using the following commands, as srx user:
  - For node 1: *oprtt_ctl -p `pidof dispProc11` OP_RTT_TRACE_ALL=-1*
  - For node 2: *oprtt_ctl -p `pidof dispProc12` OP_RTT_TRACE_ALL=-1*

In case the Centralized Call Logs are not working for a user, it is necessary to provide the output of cstasmdump, using the following command, as srx user:

- *cstasmdump > cstasmdump.output*

For any call log issues with Zoom PSI client, it is helpful to collect logs from CloudLink Container for CSTA Proxy, using the following commands as root user:

- *docker cp cloudlink:/opt/micloud-link/src/log/. /var/log/ micloud_logs/*
- *docker cp cloudlink:/opt/CstaProxy/log/. /var/log/ cstaproxy_log/*
- All logs can be collected from: /var/log/micloud_logs/ and /var/log/cstaproxy_log/

5.2.3.4 - Non call-related issues

For issues non call related, only Centralized Call Log is supported (see chapter 5.2.3.3 - Centralized Call log\history log collection)

5.2.4 - OS SBC

5.2.4.1 - SBC Log collection

Navigate to Diagnostics & logs → Debugging → Rapid Stat, set to Level 5 and “Get file”

- As root execute the following command in the terminal (ssh connection): *cld-getlogs*

- Logs are collected in *cld-logs-*.tar.xz* file

5.2.5 - CloudLink

5.2.5.1 - CloudLink Gateway Log collection

CloudLink gateway logs are downloaded via MiAccess > Mitel Administration > Select the CloudLink Account.

- Navigate to System Inventory > Applications > Select the CloudLink Gateway from the list > Manage > Download Logs.

Repeat this step if there are multiple gateways involved.

5.2.5.2 - User Comparison Report

The user comparison report is downloaded via MiAccess > Mitel Administration > Select the CloudLink Account.

- Navigate to Support > Zoom > Select the Comparison Report tab > Generate > Download.

For more detail information for the User Comparison Report see here

5.2.5.3 - Checking the CloudLink versions

To check what the latest available CloudLink gateway and associated containers are navigate to https://download.mitel.io/

6 – Troubleshooting

6.1 - MiVB

6.1.1 - Check the CloudLink Daemon Status

Log into MSL for the MiVB or MBG where the CloudLink Daemon is deployed

Navigate to Configuration > CloudLink

Check the versions and Account Number/Account ID is configured correctly.

Check the required Tunnels are running

6.1.2 - Check CloudLink Gateway Status

Log into MSL for the MiVB or MBG where the CloudLink Gateway is deployed

Navigate to Applications > CloudLink Gateway

Check the versions and Account Number/Account ID is configured correctly.

To check if there are connectivity issues, click Run Diagnostics and check the results in the Diagnostics section.

If required, you can restart the CloudLink Gateway by clicking the Restart CloudLink Gateway button.

6.2 - OpenScape 4000

6.2.1 – Is the CloudLink Daemon connected

Log into the OpenScape 4000

Select **CloudLink** from the left-hand menu

Check the **Tunnels** status and confirm they are connected and running.

6.2.2 – Is the CSTAProxy to CloudLink connected

Log in to OpenScape 4000 Assistant

Navigate to **Expert** -> CSTA

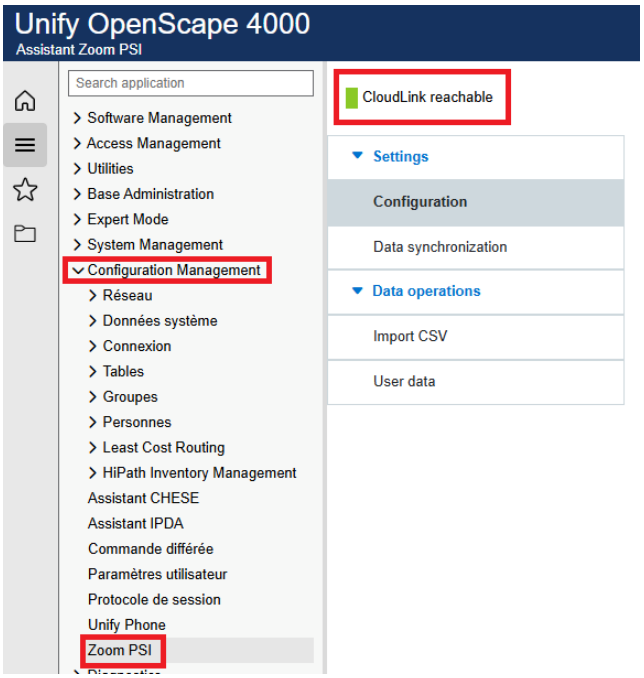
Confirm the **CloudLink_CSTAProxy** is **ConnectedAndActive** and the Profile is set to **CloudLink.**

6.2.3 – Is Zoom PSI configured

Log in to OpenScape 4000 Assistant

Navigate to **Configuration Management** -> **Zoom PSI**

Confirm the icon is **Green** and **CloudLink reachable**



For more on OpenScape 4000 Troubleshooting:
https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/87d2bd91-fcc0-4c92-b2bb-b782de080bea/OpenScape%204000,%20Standard%20Diagnosis%20and%20Troubleshooting%20Procedure,%20Service%20Documentation,%20Issue%201

6.3 - OpenScape Voice

6.3.1 - Check warnings

The CloudLink Daemon (CLD) performs checks to detect common environmental problems (e.g., connectivity, and system time).

Any warning displayed in the CloudLink daemon's user interface should be addressed.

The CloudLink daemon's user interface is accessible via CMP.

6.3.2 - Checking call manager logs errors

The process to collect logs is described here

You can check the CloudLink daemon logs for error messages. If these errors are caused by environmental issues, you may find valuable information. The CloudLink Daemon (CLD) logs can be found under /var/log/cld/* and using the following command:

grep level=ERROR /var/log/cld/*.log

6.3.3 - Networking

The network connection can be checked by running curl command on the daemon's host system.

for example, to check with a PROXY connection on a daemon’s host system.

curl -v --proxy http://: https:// download.mitel.io/cld/linux/amd64/current.json

Also check the proxy configuration file, and that the HTTPS_PROXY and NO_PROXY values are correct.

6.3.4 - System time

Some tokens used by the CLD are only valid for a short time for security reasons. The validation of these tokens may fail if the system time is not correct.

In that case, check your Network Time Protocol (NTP). Using local time zones is supported and should not create any issues.

6.3.5 - Restart the CloudLink Daemon

Restart the CLD using the following command: systemctl restart cld

For more details on OSV Troubleshooting:
https://nuxeo.unify.com/nuxeo/site/proxy/internal/nxdoc/view/raw/181a6d3e-6eae-4277-93c9-61af382c1137

6.4 - OpenScape SBC

6.4.1 - Push notifications

This log is used to investigate **Mobile Push Notifications**

Mobile push notifications are sent to wake up the device when a new call is setup or send a cancel message if the call originator hangs up.

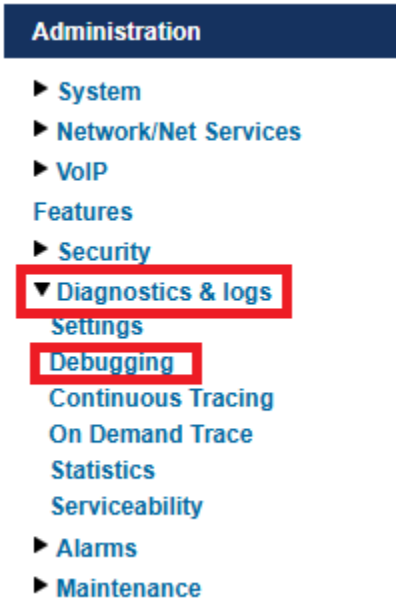
The push notifications are received by CloudLink from either the SBC or MBG, depending on which PBX is involved.

CloudLink notifications then sends the push notification to Zoom, Zoom then sends the message to the mobile device.

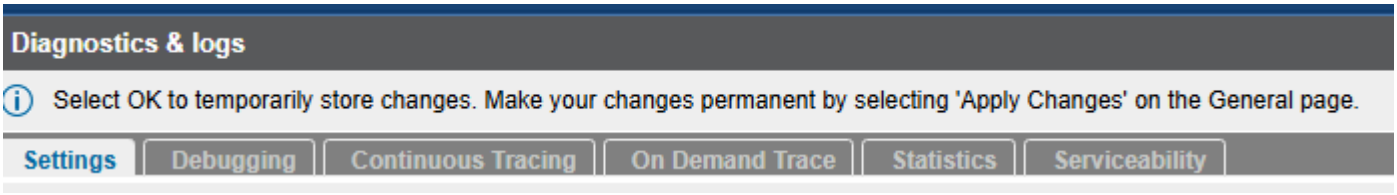
There are multiple things that need to be configured in CloudLink and other parts of the solution for this to work.

The following flow describes the configuration areas and what to look for.

Navigate to Diagnostics & Logs\Debugging



When **Debugging** is selected a new window appears containing multiple tabs

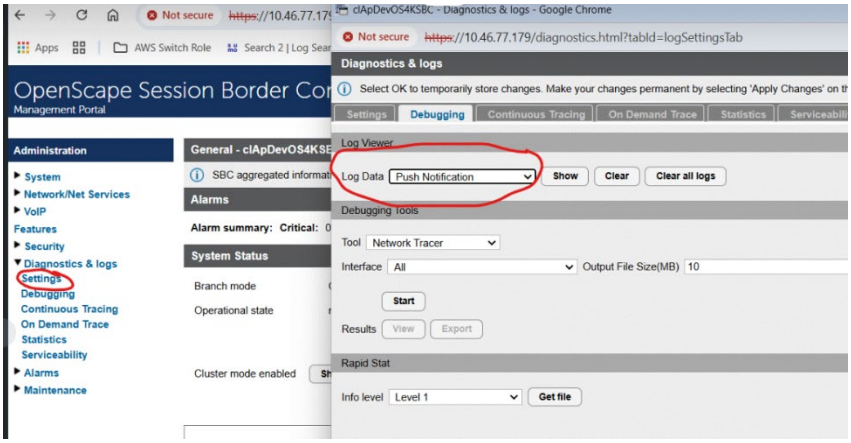


Debugging Tab

Navigate to Diagnostics & Logs\Settings

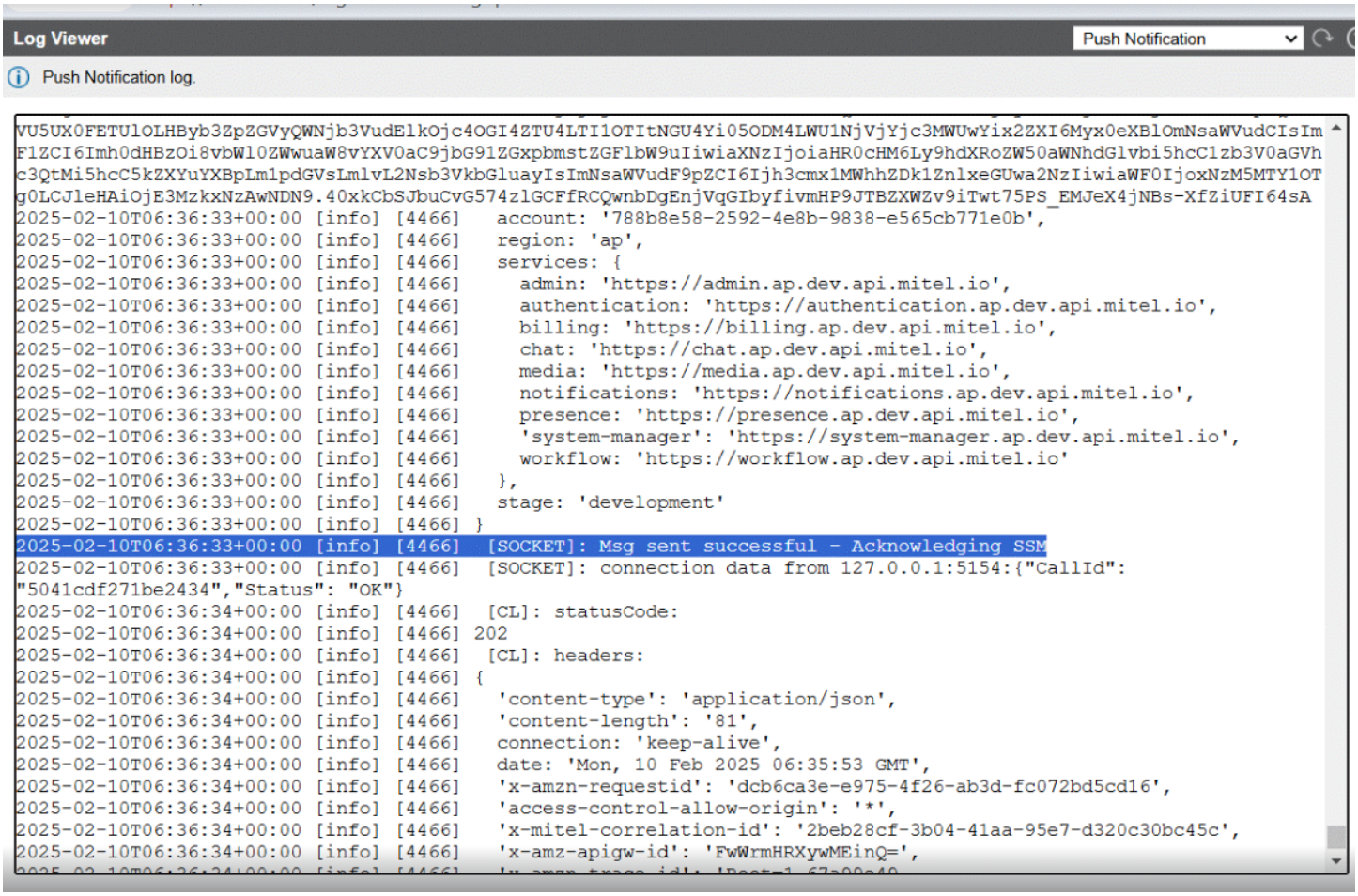
Select the **Debugging** tab

From the **Log Data** drop down select Push Notification



Click **Show**

The log viewer screen will be displayed see below



This will display the push notifications sent from the SBC

In the example above it shows the a message advising the push notification was sent successfully to CloudLink.

** Other error conditions need to worked out and how to debug them

Now we know the SBS successfully sent the push notification we need to look at the next step in the chain which in this case is the CloudLink platform to do this we will need to collect the correlation id from the SBC push notification log.

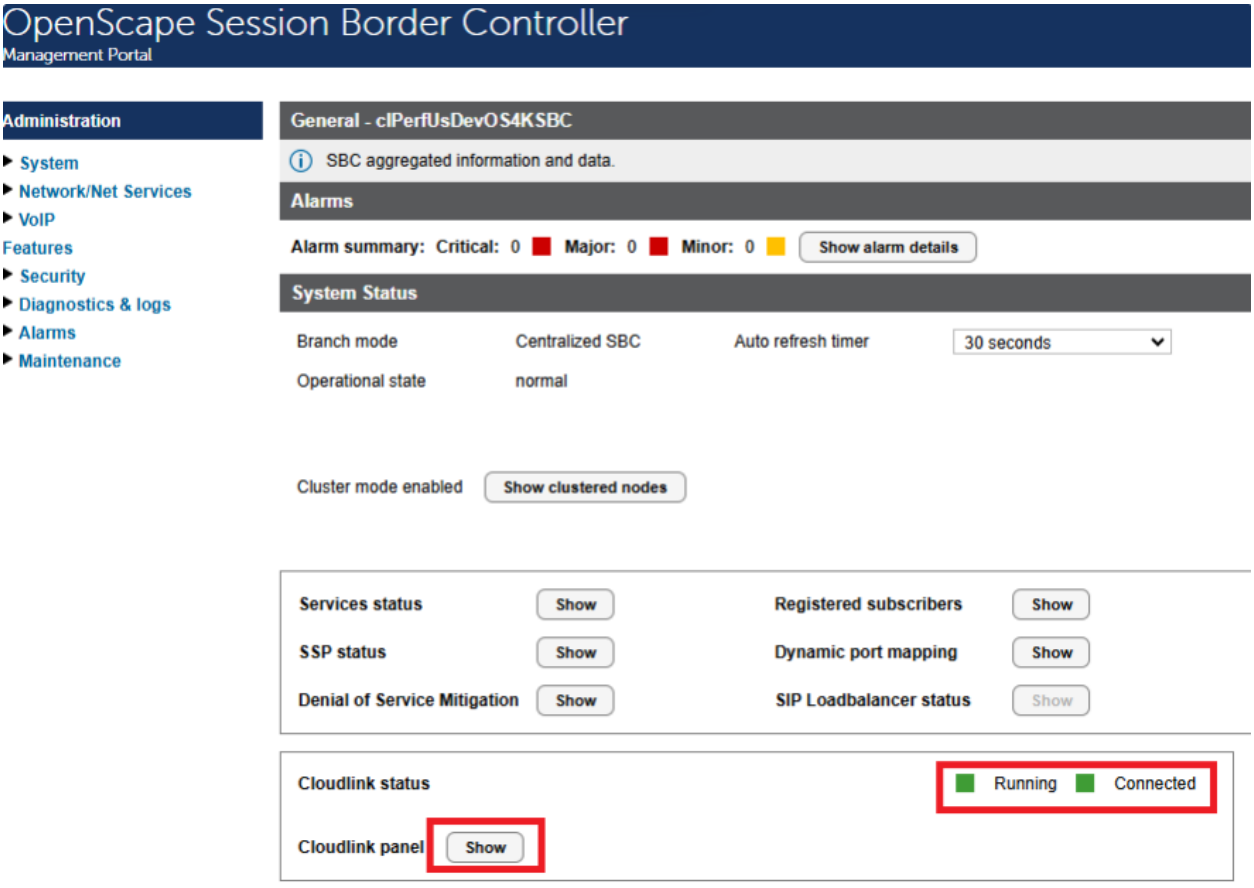
In this example it is 'x-mitel-correlation-id': '2beb28cf-3b04-41aa-95e7-d320c30bc45c'.

The ID '2beb28cf-3b04-41aa-95e7-d320c30bc45c' is unique end to end in the cloud.

6.4.2 - Check the CloudLink Connection Status

The SBC Dashboard contains a CloudLink Status box that shows then the CloudLink Daemon (CLD) is **Connected** and **Running**.

That tile also contains a button call **Show** which displays the CLD page once the CLD is onboarded

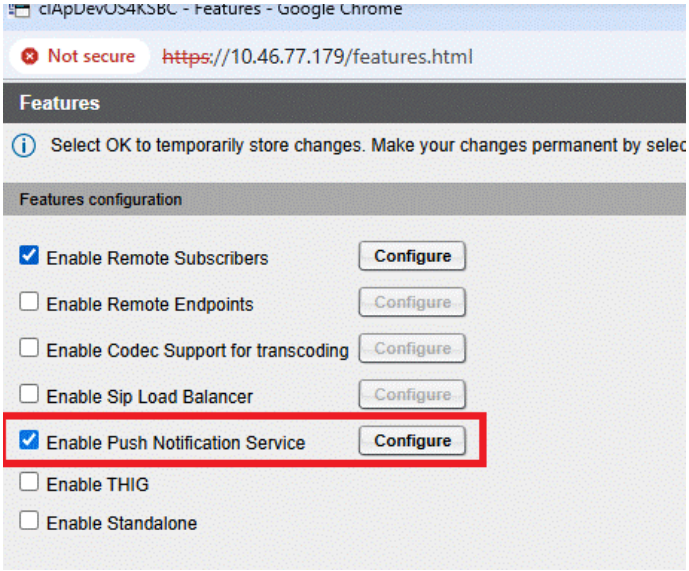


6.4.3 - Is the CloudLink Daemon onboarded and configured?

CloudLink Deamon must be provisioned in the SBC and linked to a CloudLink account with Zoom integration enabled. (See the XYZ integration guide)

6.4.4 - Are push notifications enabled in SBC

You can enable the push notification service under Administration\Features\Enable Push Notification Services see below:

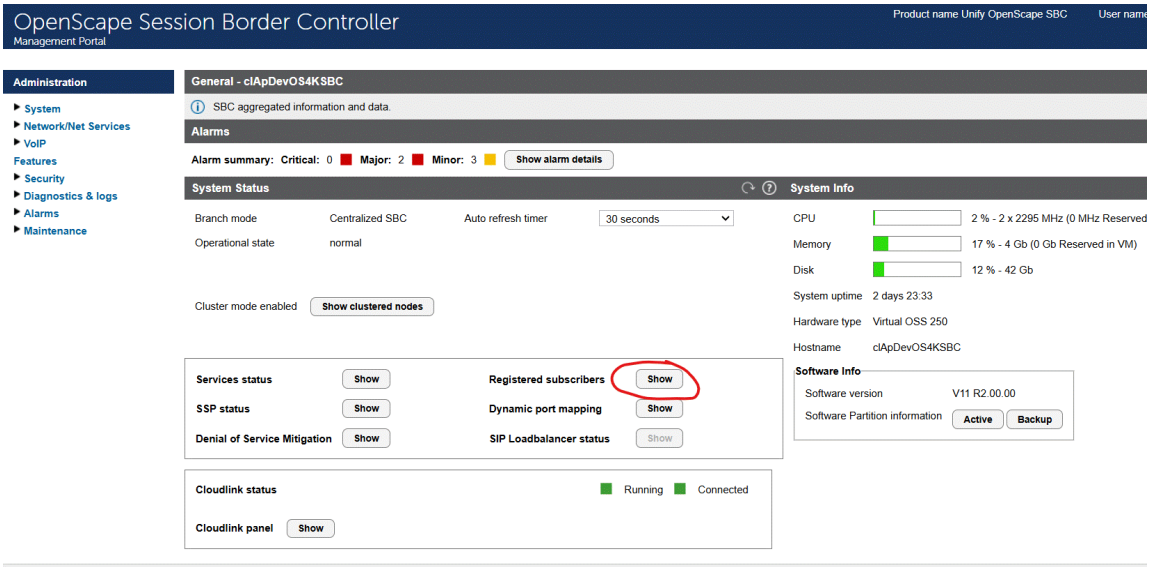


SBC Enable Push Notification Service

- Check the box to Enable Push Notification Services
- Press **OK** to apply and close the features pop up
- Click **Apply Changes** to complete the setup

6.4.5 - Confirm the client is registered

On the OSSBC administration Dashboard page click **Show** next to **Registered subscribers**



A new dialog will be displayed, check for your user in the list, or use the filter option and check the status.

For more details on SBC Troubleshooting:

https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/7e0eded5-0952-4b22-8728-cc072a01eb42/OpenScape%20SBC%20V11%2c%20OpenScape%20Branch%2c%20Troubleshooting%20Guide%2c%20Service%20Documentation%2c%20Issue%203

6.4.5 – CloudLink

6.4.5.1 – 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. 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:

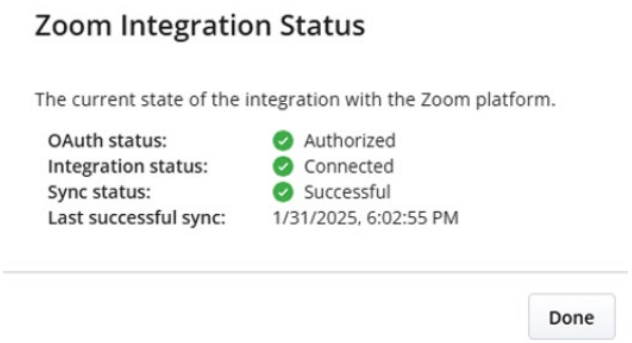
• OAuth status: Displays the OAuth authorization status (Authorized, Failed), indicating whether the Zoom OAuth token is valid, expired, or needs re-authorization. If the OAuth status is Failed, error messages associated with the most recent OAuth failure will also be displayed below the status.

• Integration status: Indicates the current status of the Zoom integration (Connected, Error, or Pending).

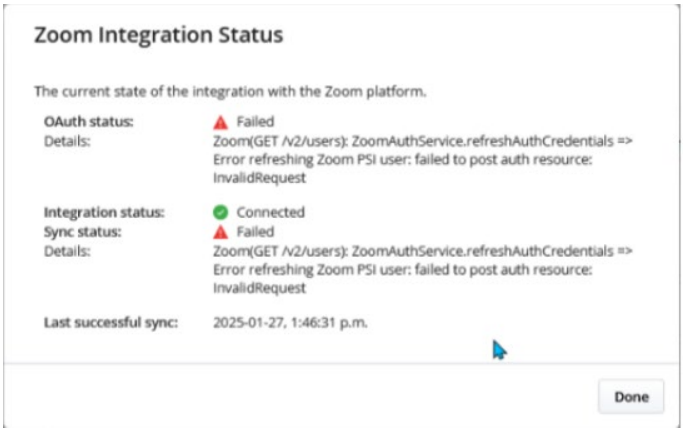
• Sync status: Indicates the synchronization status between CloudLink and Zoom. If the last sync was unsuccessful, error messages associated with the most recent failed sync attempt will also be displayed below the status.

• 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 the Zoom integration status when the integration is incorrectly configured.



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.

6.4.5.2 – User Comparison Report (Detailed)

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.

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

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.

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

Note: Email addresses must match exactly including case across all sources for proper data joining.

6.4.5.3 - Viewing the Event History Table

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

1. Log in to Mitel Administration as an Account Admin.

2. Click Support > Zoom from the left main menu. The Zoom Sync & Provisioning Errors page of the customer account opens.

3. Select the Event History tab.

4. Click on an event in the Event History table to view the event details. The Event Details popup window is displayed.

5. Click Copy to copy the event details of the following tabs:

• Core details

• Properties Changed

• Extra Details

• Log tags

6. Click Export to export all data in a csv format.

Note: Actions performed in Mitel Administration 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.

6.4.5.4 - Performance profile and network requirement prerequisites

https://www.mitel.com/sites/default/files/s3_imports/Technology/CloudLink/All%20Releases/EN/cloudlink-gateway-html/index.html#t=Technology/CloudLink/All_Releases/CloudLink_Gateway/Content/Introduction.html

For more details on CloudLink Gateway Troubleshooting:

https://www.mitel.com/sites/default/files/s3_imports/Technology/CloudLink/All%20Releases/EN/cloudlink-gateway-html/index.html#t=Technology/CloudLink/All_Releases/CloudLink_Gateway/Content/Troubleshooting.html