A MITEL
PRODUCT
GUIDE

MiVoice MX-ONE

Zoom with MX-ONE and MBG SBC- Phone System Integration Guide

57/1531-ANF90143 Uen A

Mitel
Powering connections

Notices

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

Trademarks

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

Contents

Introduction 1

This chapter contains the following sections:

This document outlines how to connect the MiVoice MX-ONE and MiVoice Border Gateway SBC (MBG SBC) 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 telecommunication functions with their MiVoice MX-ONE Voice system while extending its functionality with Zoom's cloud-based features.

This integration allows Zoom's Phone tab to become a SIP Softphone that registers to the Mitel Calling Platform, utilizing the MBG SBC. The MBG SBC acts as a secure connection 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 via SIP registration.

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

1.1 Target Audience

This document is intended for professionals involved in configuring and managing the Zoom- MX-ONE -SBC integration, specifically those working with MiVoice MX-ONE and Mitel Border Gateway Session Border Controller (MBG SBC) components. The target audience includes implementation engineers, field technicians, system administrators, business partners, solution providers and customers who are directly involved in the deployment and management of the integration.

1.2 Prerequisites

Supported product versions

Product	SW Version (minimum)
Zoom Workplace Client	V6.3.6
MX-ONE with Active SWA (Mitel Software Assurance)	V8.1

Product	SW Version (minimum)
MX-ONE Provision Manager Portal	V8.1
MBG SBC	V12.3
CMG Voice Mail	NA

System Requirements and Licenses

- **Zoom**
  - Supported License per user which includes Zoom Workplace Business/ Business+, Zoom Workplace Essentials/Enterprise/Enterprise+/ Enterprise Premier, Legacy Meeting Licenses ENH/EAH.
  - Zoom Phone initial setup is completed. See the *How to Complete Initial Setup* section in Zoom Phone initial setup.
  - Automatic Phone assignment for Zoom Workplace Licences is disabled. For more information, refer to Configuring automatic Zoom Phone activation.
  - Zoom Phone *External Contacts setup* for any non-Zoom, Mitel users is completed.
  - When logged in to the Zoom web portal as an Admin with the privilege to edit account settings, the **Phone System Integration** tab should appear under **Account Management**. If it does not, please contact Zoom.
  - For any additional requirements, refer to the Zoom-Mitel Phone System Integration support page

1.2.1 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.

  Note:

  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.

1.2.2 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 MBG SBC, which is located in the DMZ. It should be able to connect to the SIP/TLS port of the access interface of MBG SBC 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 MBG SBC.

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

Overview 2

This chapter contains the following sections:

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 MX-ONE configurations interact with each other and other critical components of the solution.

2.1 Key Components

The key components of the Zoom-MX-ONE-MBG SBC 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-MX-ONE integration, you are granted admin access to the Zoom web portal.
- **MX-ONE**: MiVoice MX-ONE is a scalable SIP-based IP system that provides enterprise-class communications functionality. The MX-ONE platform controls the users' telephony capabilities and manages SIP signaling, call routing, and PSTN and Zoom Phone integration.
- **MiVoice Border Gateway (MBG)**: MiVoice Border Gateway 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 MX-ONE 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 MX-ONE) and cloud-based applications. Acting as the intermediary, CloudLink platform bridges the Zoom and MX-ONE 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 MX-ONE 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.

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.

2.2 Overview of the Phone System Integration (PSI) Solution

MiVoice MX-ONE and MBG work together to enable seamless integration between Zoom clients and external networks, including the Public Switched Telephone Network (PSTN).

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

The following chapters provide detailed configuration instructions for integrating Zoom, MX-ONE, and MBG SBC components into your system.

The guide begins with the configurations needed for the Zoom-CloudLink integration configurations, followed by the steps required before setting up and provisioning Zoom - MX-ONE users.

Setting Up Users for the Zoom-MX-ONE Integration

The Zoom-MX-ONE integration involves several key steps:

1. Configuring Zoom and CloudLink integration.
2. Configuring MiVoice MX-ONE and MBG SBC.
3. Configuring MiVoice MX-ONE in CloudLink.
4. The CloudLink Daemon must be integrated with MiVoice MX-ONE, MBG SBC and MX-ONE Provision manager Platform.
5. Establish CloudLink connectivity for managing Zoom users associated with MX-ONE subscribers.
6. Adding users (if not already added) and assigning licenses in your Zoom account.
7. Configuring user mapping between Zoom and MX-ONE through the MX-ONE Provisioning manager (PM).
8. Completing user provisioning to finalize the integration.

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

The following figure depicts the network topology block diagram.

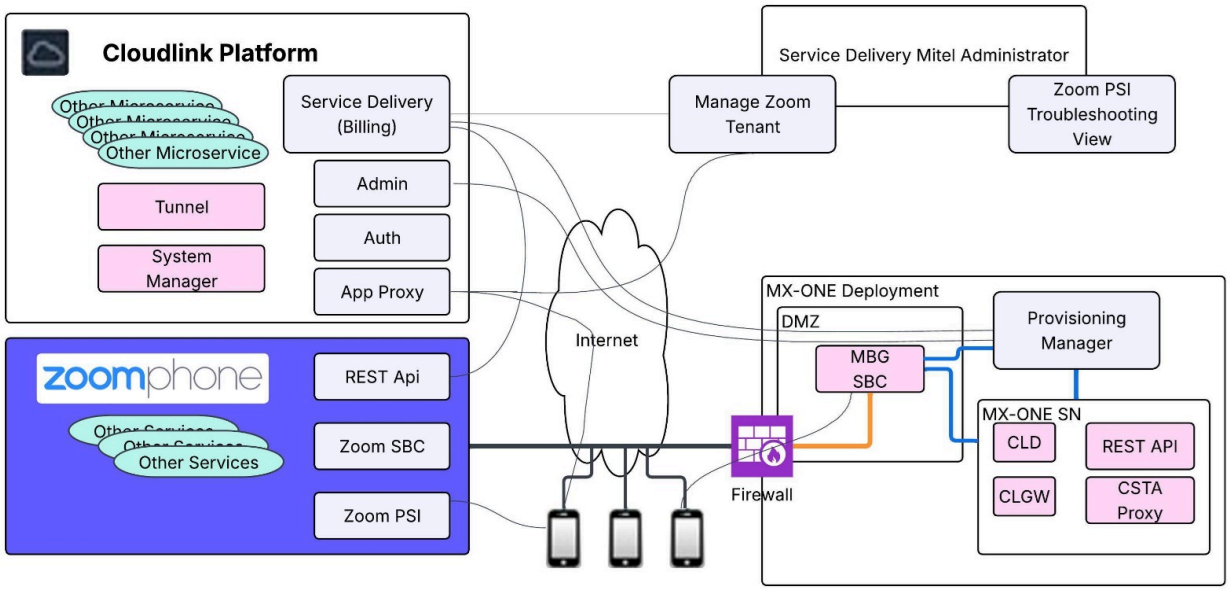


Figure 1: Network Topology Block Diagram

2.3 Related Documentation

- For MiVoice MX-ONE documentation, refer to the MiVoice MX-ONE
- For MBG SBC documentation, refer to the MiVoice Border Gateway
- For CloudLink documentation, refer to the CloudLink
- For Zoom documentation, refer to the Configuring the Zoom-Mitel PSI integration.

Integrating Zoom with CloudLink 3

This chapter contains the following sections:

This chapter describes Zoom and CloudLink integration.

Before proceeding with the configurations, ensure you have the required user accounts and permissions. For more information, see User Roles and Permissions on page 3.

3.1 Adding Zoom Integration to a Customer Account

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

Prerequisites:

- You have a Zoom account, Business or Enterprise.
- You are an Account Owner or Admin with a role for managing Users, Phone System Integration, and Zoom Phone.
- You have obtained the necessary Zoom PSI licensing.
- The Mitel PSI app is published into the Zoom Marketplace. For more information, refer to the Configuring the Zoom-Mitel PSI integration. If you cannot see the app, please contact your Zoom administrator or Mitel support representative.

Note: To maintain a stable and functional integration, you must create and use a dedicated admin user (service account) with a unique email address on your Zoom site specifically for the integration. This account must remain active and should not be deactivated. The provisioning of the Mitel PSI app to your CloudLink Platform (CLP) happens automatically once the proper setup is complete. For more information, see Prerequisites on page 1.

1. Log in to the Zoom App Marketplace.
2. Search for the **Mitel PSI** app using the search bar or filter options.
3. Click **Add** to install the app to your Zoom account.
   You will be redirected to *accounts.mitel.io* to authorize the connection
4. Click **Allow** to authorize the Mitel PSI application to access the necessary account information.

To complete the integration, you must follow the steps described in Configuring Mitel PSI Application in Mitel Admin on page 9.

3.2 Configuring Mitel PSI Application in Mitel Admin

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

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. For more information, see User Roles and Permissions on page 3.
- You have obtained the necessary Zoom PSI licensing.
- The Mitel PSI app is published into the Zoom Marketplace. For more information, refer to the Configuring the Zoom-Mitel PSI integration. If you cannot see the app, please contact your Zoom administrator or Mitel support representative.

To complete the Zoom integration setup via the Mitel Administration.

1. Log in to Mitel Administration as an Account Admin.
2. Click **Account** or **Integrations and Applications** 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, then click **Done**.
6. The Zoom integration is added to the customer account, and it is displayed in the **Integrations** section of the **Account Information** page.
7. Go to the newly added Zoom integration and click **Complete Setup**.
   The **Zoom Integration Configuration** window pops up.
8. Click **Connect**.
   A **Zoom login** window will open in a new browser window.
9. In Zoom login window, sign in using the **Zoom Admin account** designated for this integration with CloudLink.

   Note: It is strongly recommended that this be a **dedicated service account** in Zoom, not a personal or user-based admin login.

   Once signed in, Zoom will redirect the pop-up to the **Mitel PSI authorization page**.
10. Click **Allow** to authorize the Mitel PSI app to access the necessary data for integration.

    After authorization is complete, the pop-up will close, and the main CloudLink Administration console will return to the Zoom integration screen.

    The integration will now show a **Connected** status.

    The **Mitel PSI** application will be automatically added to the Zoom Marketplace account for the customer under **Added Apps**.

11. If you click **Decline**:

    - The integration will not proceed.
    - You will remain on the **Zoom Authorization** page.

    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.

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

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

Licensing 4

To enable integration between the Zoom Workplace client and MiVoice MX-ONE using the MBG SBC, the following items are required per user:

1. Zoom Hybrid License subscription — required to enable Zoom Phone integration with MX-ONE via MBG.
2. MX-ONE system running release 8.1 and covered by an active Software Assurance (SWA).
3. Available MX-ONE User licenses in the MX-ONE system.
4. Available MBG Teleworker licenses.
5. Mitel CMG Voicemail licenses **(optional)**.

If the required licenses are not available, partners can order additional licenses through the Mitel CPQ tool. The Mitel Zoom Hybrid Licenses are located under **Subscription Offers > Mitel Zoom Hybrid Licenses Subscription**.

Limitations for CLD Integration 5

CLD Limitations

- CLD requires connectivity to the CloudLink server hosted on the internet.
- CLD provides a hybrid deployment model, allowing transition from a pure on-premises system to a hybrid environment.
- A CloudLink account and a valid license are required for CLD integration.
- CLD integration is mandatory for customers who want to use Zoom with MX-ONE.
- Customers currently using a CloudLink Gateway server must migrate to a CLD-based deployment if the same services are required in MX-ONE 8.1.
    - Refer to *59/1531-ANF90143_CloudLink Gateway to CloudLink Daemon Migration Guide*.
- CLD deployment is supported only from MX-ONE version 8.1.
- CLD uninstallation is not supported and should not be attempted.
- IPv6-based environments, including dual-stack configurations, are not supported.
- CLD deployment requires approximately 1.4 GB of disk space and 100 MB of RAM for both the Service Node and the Provisioning Manager.
- During installation, CLD connects to cloud-based Mitel servers.
    - Ensure that DNS and network settings on the MX-ONE system are configured correctly.

Zoom Limitations

- For integration with Zoom, MiVoice Border Gateway (MBG) is the certified Session Border Controller (SBC).
- A dedicated MBG must be used for Zoom integration.
    - The connection is authenticated using a username and password.
    - The MiCollab MBG can be reused for this purpose.
    - The MX-ONE Teleworker MBG must not be used for Zoom integration.
- MX-ONE supports MBG cluster deployments.
    - When integrating MBG as a subsystem, use the main MBG or any one of the client MBGs for generating tokens, user provisioning, and related operations.

DND Limitations

- When the Zoom client is integrated with MX-ONE, Do Not Disturb (DND) control is managed by the Zoom backend.
- DND can be set or unset not only by user action but also by client actions such as logout or timeout.
- As a result, DND may be unset automatically when the Zoom client logs out, even if the user has not explicitly changed the status.
- This behavior can also affect the DND state of other forked devices.

Note: This is a Zoom-specific behavior, and MX-ONE has no control over this functionality.

Redundancy Limitations

CLD redundancy is not currently supported. As a result, even in an MX-ONE redundant setup, certain CLD-based features will stop functioning if the server hosting the CLGW process fails and the system switches over to the backup server.

Table 1: Redundancy Support

CloudLink Features	Redundancy Supported	Redundancy Not Supported
Zoom Client - DND and Call F orwarding (CF)	SIP-based features DND/CF using access codes	Call History (UI-based)
MS Teams Presence	None	Teams Presence
Voice Assist	Supported (MBG)	None
Voicemail	Supported	None

CLD Cluster – Node Addition and Removal Limitations

- **Add a new MX-ONE service node to a CLD-integrated MX-ONE system (non-LIM1 server only)**
  - Once CLD is integrated with MX-ONE, all CLD entities across different servers form a single CLD cluster.
  - If a new MX-ONE server needs to be added later, the administrator must first add it to the MX-ONE system.
  - This process automatically installs CLD on the new server and adds it to the existing CLD cluster.
- **Remove an MX-ONE service node from a CLD-integrated MX-ONE system (non-LIM1 server only)**
  - When a LIM is removed from the MX-ONE system, the corresponding CLD instance is also removed and unlinked from the CLD cluster.
  - Removing the LIM1 server breaks the CLD cluster and is therefore not supported.

Configuring CloudLink Integration 6

This chapter contains the following sections:

The CloudLink Daemon is a software component embedded in the MiVoice MX-ONE 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 MiVoice MX-ONE tenants, ensuring a secure connection through a proxy server. This chapter describes the CloudLink Daemon configuration for MiVoice MX-ONE and MBG.

Note:

Do not clone any servers where the CloudLink Daemon is installed (such as PM, MX-ONE SN, or MBG 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 the following software applications:

- Administration program of the MBG SBC: MBG Server manager.
- Administration program of the MX-ONE: Provisioning Manager.

6.1 Integrating CloudLink Daemon with MX-ONE

As an administrator, you can configure the CloudLink Daemon (CLD) to integrate with MX-ONE. This integration allows MX-ONE users to access CloudLink services, and enables CloudLink applications to use MX-ONE telephony features. This document describes the configuration required to support Zoom telephony services for MX-ONE tenants through a secure proxy connection.

The integration process consists of the following configuration steps.

1. Installation of CLD in MX-ONE and CLD registration with CloudLink. See Installation of CLD in MX-ONE.
2. Enable CLD to start CLGW sub service to interface with MX-ONE CSTA proxy. See Enabling (Register) CLD to start CLGW on page 17.
3. Integrate CLD to MX-ONE PM as subsystem for user management and CLD management. See Integrating CloudLink Daemon to MX-ONE PM on page 21.

6.1.1 Installation of CLD in MX-ONE

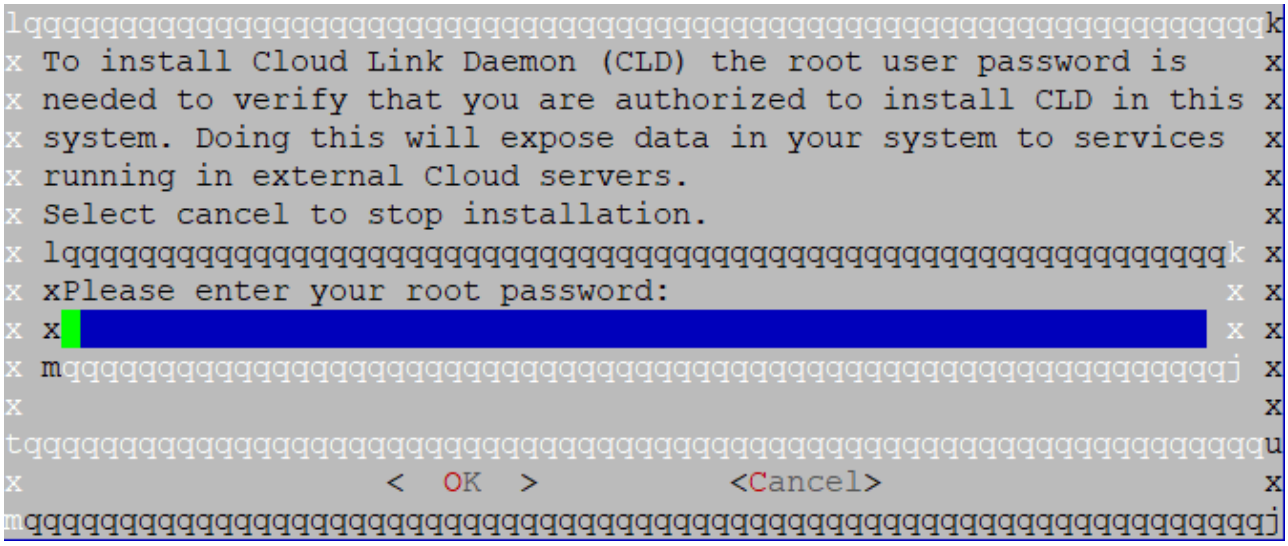
Prerequisites

- Root password is available.
- **mxone_admin** password is available.
- CloudLink login credentials are available:
  - Username
  - Account number
  - Password
- MX-ONE servers must have internet connectivity.
- MX-ONE servers must be deployed behind a firewall.
- MX-ONE DNS must be configured to forward queries to an external DNS server that can resolve the domain *mitel.io*.

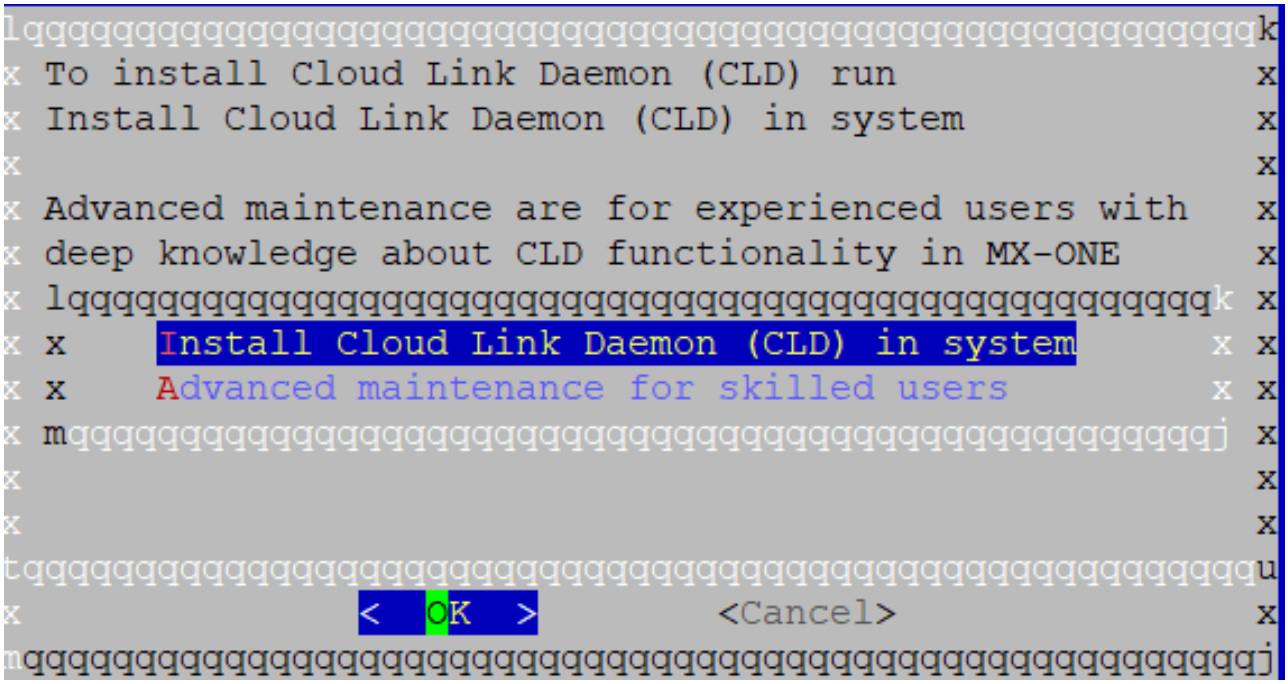
Procedure

To install and enable Cloud Link with MX-ONE:

1. As user mxone_admin run command **sudo -H mxone_maintenance**.
2. Select **cloudLinkDaemon**.
3. Enter root password to verify that you have permissions to install CLD and are aware of that this will connect and expose your system to cloud servers.

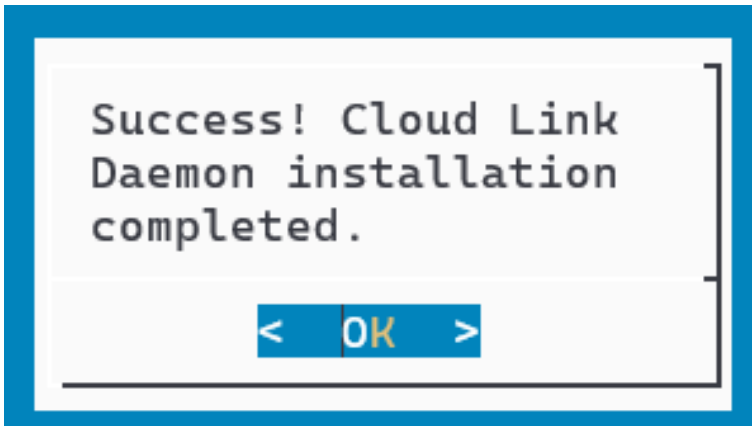


4. Select action **Install Cloud Link Daemon (CLD) in system.**



5. Enter Cloud Link credentials to access CloudLink.

6. Enter password to CloudLink user when requested.
7. System servers are now linked to and have established tunnels to CloudLink.



Once the CLD installation and registration are completed successfully, the Administrator can enable MX-ONE service access to the Zoom user by enabling CLGW subservice as described in the Enabling (Register) CLD to start CLGW on page 17.

6.1.2 Enabling (Register) CLD to start CLGW

This section describes the procedure to enable the Cloudlink Daemon to start CLGW sub service to interface with MX-ONE CSTA proxy.

MX-ONE administrator initiates zero or more CSTA proxies to provide telephony services to clients on one or more MX-ONE Service nodes based on system capacity. Irrespective of the number of CSTA proxies running the services provided by all CSTA proxies will be same. MX-ONE administrator can map/use different CSTA proxy servers for interacting with different applications.

Zoom user access the MX-ONE telephony services using CLGW subservice of the CLD. The CLGW will interact with the MX-ONE CSTA proxy which is CO-LOCATED on the same server to provide services to zoom users. MX-ONE administrator is provided with option to configure which CSTA proxy/proxies will provide services to Zoom.

For Zoom integration purpose, MX-ONE administrator can decide which CSTA proxy will provide services for which set of users based on where corresponding user extensions are located. If there is only one CSTA proxy, then zoom will have to get services for all Zoom users using the CLGW running on the system where the said CSTA proxy is located. If there are say 2 CSTA proxies running on different service nodes, then the administrator can configure zoom to get services for subset of the user from one CSTA proxy and remaining users to get services from other CSTA proxy. The user bifurcation should be done by keeping in mind that CSTA proxy of a service node should serve all co-located user extension. i.e. if the user extension x is in LIM 1 and LIM1 also has CSTA proxy, then it's always suggested to get the services from CSTA proxy running on LIM1. Currently the CSTA proxy must run on default 8882 port without credentials (as they are always co-located) for interacting with CLGW service.

The CLGW will not run by default and administrator has option to start same. MX-ONE Administrator has capability to configure which MX-ONE CSTA proxy interacts with which CLGW.

Prerequisites

- CLD is installed successfully, see Installation of CLD in MX-ONE on page 15.
- CSTA Proxy/Proxies started on default port.
- User root password known.
- User mxone_admin password known.

Procedure

To enable CloudLink Daemon to Start CLGW:

1. Log in as **mxone_admin** and then enter **root** mode.
2. Enter the following command.

   cloud_link_gateway --help-complete

   This command creates a mapping between LIMs where the CSTA server is active (referred to as Gateway LIMs) and LIMs without a CSTA server that depend on those Gateway LIMs for CSTA-based services. Once the mapping is established, the CloudLink Gateway container is started and enabled on the identified Gateway LIMs.

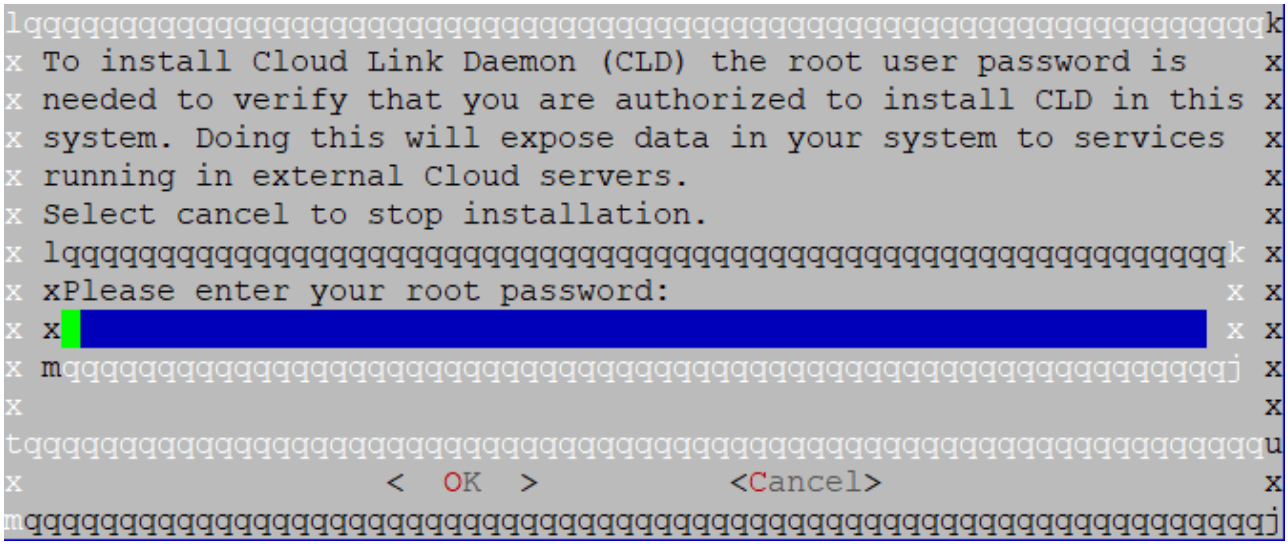
   For more information, enter the **cloud_link_gateway help** command.

6.1.2.1 Advanced CLD Maintenance Actions

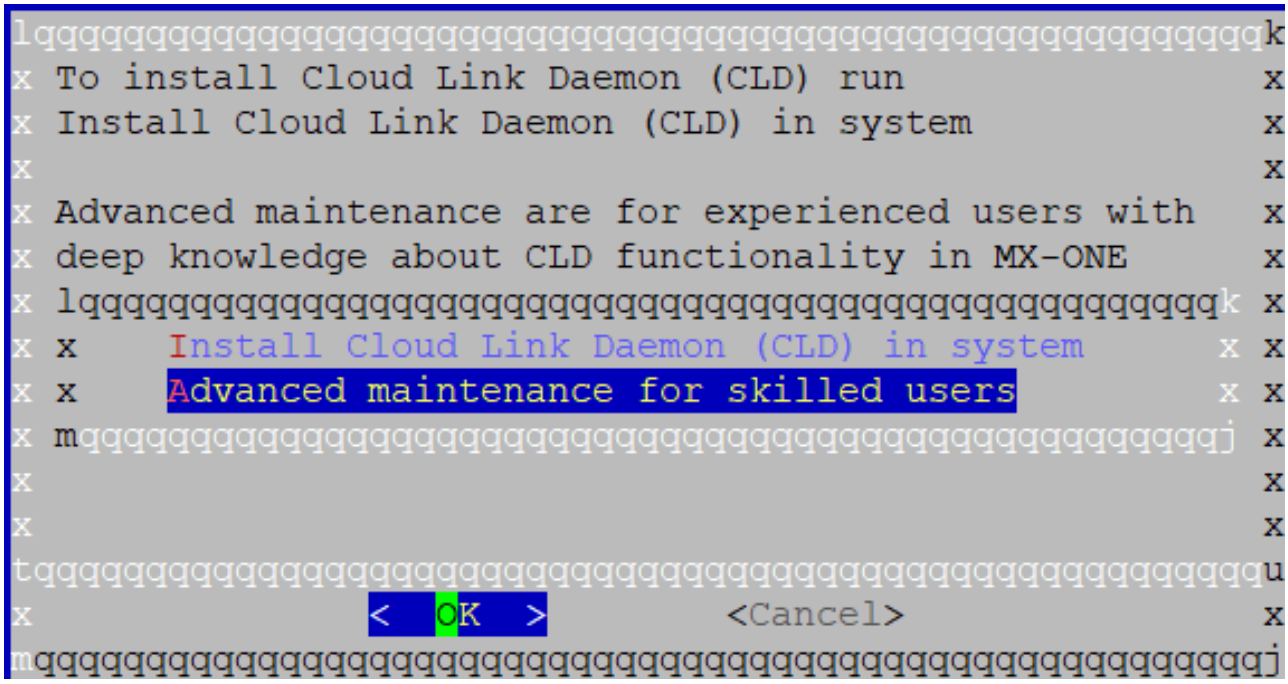
In the **mxone_maintenance** tool, the for ***cloudLinkDaemon*** section has more actions than Installation of CLD in MX-ONE. The advanced CLD maintenance actions are as follows.

Warning: These options are for experienced and advanced users only. To enable the CLGW, the Administrator should use the steps mentioned in the previous section rather than the option mentioned below.

1. As mxone_admin user run command **sudo -H mxone_maintenance**.
2. Select **cloudLinkDaemon**.
3. Enter root password to verify that you have permissions to install CLD and are aware of that this will connect and expose your system to cloud servers.



4. Select **Advanced Maintenance for skilled users**.



5. Select either of the following options:

- Either Select action **Enable all servers via Cloud Link to external Cloud servers**.

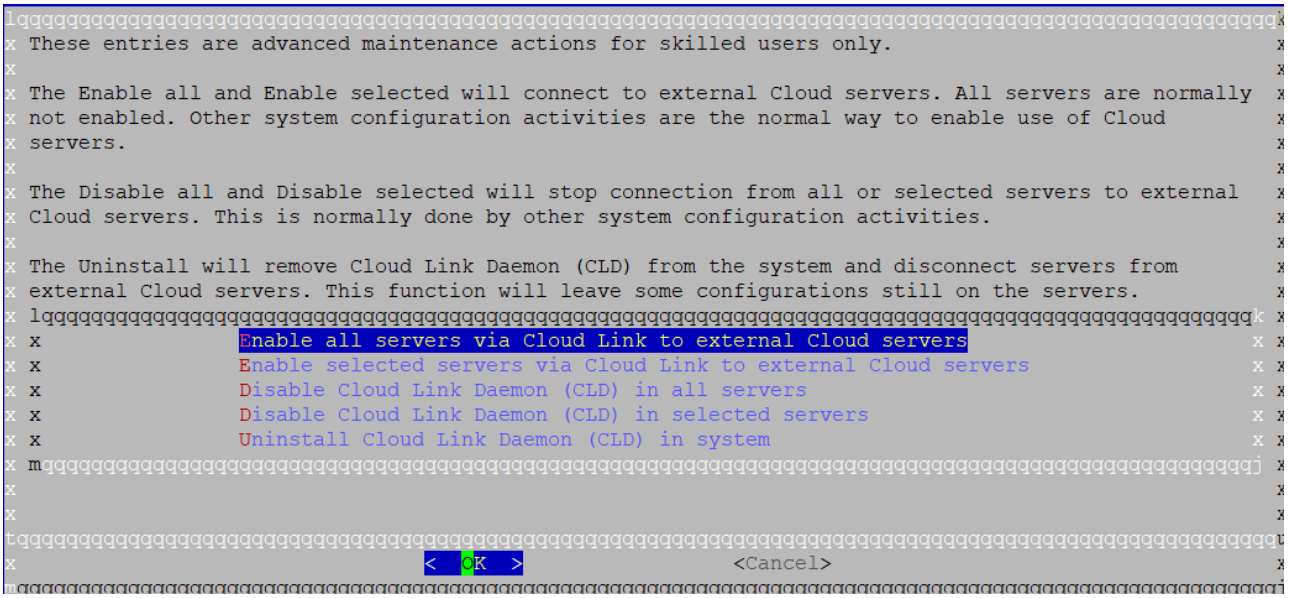
  If all the service nodes have CSTA Proxy running to provide services for Zoom users.

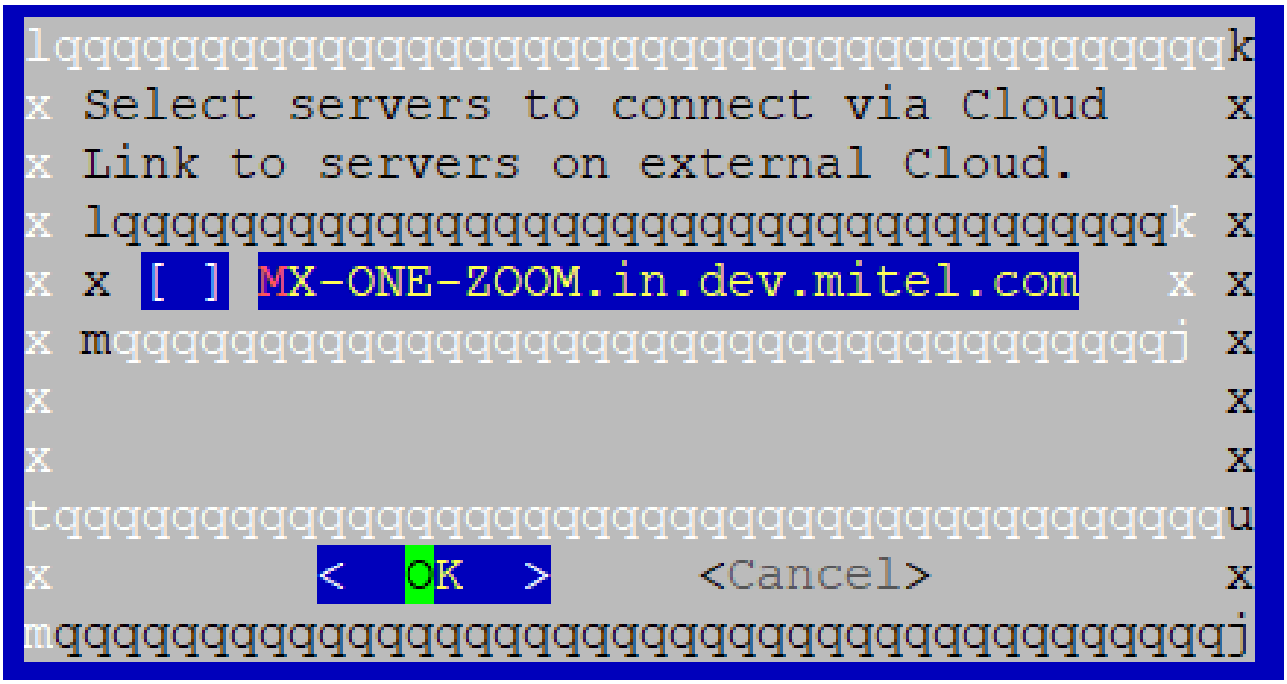
  Or

- Select **Enable selected servers via Cloud Link to external Cloud servers**.

  If subset of service nodes has CSTA proxy running and which can serve the zoom users.

  Here the Administrator must select the service nodes which have CSTA proxy running and intended to provide services to Zoom users. Both these options will trigger the start of the CLGW service in the selected nodes.





6. Exit from MX-ONE maintenance.
7. The above steps will cause CLGW to start and create a connection with the mapped MX-ONE CSTA proxy. Now the administrator must configure which users' extensions are served by which specific CSTA proxy. The Mapping is in terms of LIM to CSTA Gateway. i.e. all the users of LIM X will be served by CSTA GW on LIM Y. The MX-ONE Administrator has to create this mapping using **cloud_link_gateway** command.

> **Note**: In future MX-ONE releases, this will be allowed to be done directly in MX-ONE PM (CSTA proxy page).

8. One successful creation of Mapping the MX-ONE will be ready to serve ZOOM/CloudLink based clients.

- **Disable Cloud Link Daemon (CLD) in all servers.** Cloud link will be disabled in all servers. And related containers deleted. Cloud Link Daemon will still be active and have access to cloud.
- **Disable Cloud Link Daemon (CLD) in selected servers.** Cloud link will be disabled in selected servers, and related containers deleted. A dialog to select servers will be presented. Cloud Link Daemon will still be active and have access to cloud.
- **Uninstall Cloud Link Daemon (CLD) in system.**

  Cloud Link will be disabled and CLD uninstalled in the whole system.

  Some files related to CLD and Cloud Link will remain on the server.

6.1.3 Integrating CloudLink Daemon to MX-ONE PM

After integrating CLD with MX-ONE, all MX-ONE users enabled with CloudLink features—such as Zoom Client, Microsoft Teams Presence, or Voicemail—must be provisioned to the customer's CloudLink account on the CloudLink platform. This provisioning is performed through the MX-ONE Provisioning Manager (PM), which must be linked to the CLD before user provisioning can begin. This is achieved using below mentioned steps.

Prerequisites

- System Administrator user is logged in to PM.
- Service Node Manager URL.
- MX-ONE subsystem name to link this CLD.

Procedure

To set up a connection with CloudLink in the MX-ONE Provisioning Manager:

1. Login to the PM as a **mx-one_admin** user.
2. From the left side navigation tree, select **System > Sub System**.
3. On the main window, Click on **Add**.
4. Configure the parameters as described in the following table.

Note:

- SBC can be configured as a subsystem within PM, which offers two options: 'Other' and 'MBG'. By default, 'MBG' is selected when adding the SBC subsystem.
- Initial Zoom release supports only single tenant deployments.

Table 2: Adding CLD as Subsystem

Parameter	Sample Value	Description
Subsystem Type	CloudLink Daemon	Select the CloudLink Subsystem from the dropdown list.
Subsystem Name	CLD	Provide a name for the CloudLink Subsystem.
Location	Location01	Select the appropriate location.
CloudLink Daemon URL	https://10.211.19.162/cld	Cloudlink Daemon URL should be set to MX-ONE SNM FQDN/ IP. Enter the CLD node manager URL. The format is IP address of LIM1 followed by cld.

Parameter	Sample Value	Description
MiVoice MX-ONE	MX-ONE	Select the MX-ONE system the CLD belongs to as the PM can manage Multiple MX-ONE system.

5. Save the settings using **Apply** button, the CLD will be linked to the MX-ONE.

Once CloudLink Daemon subsystem is added to MX-ONE, Administrator can Click on CloudLink subsystem access the CloudLink UI. The UI can be used for further CLD management.

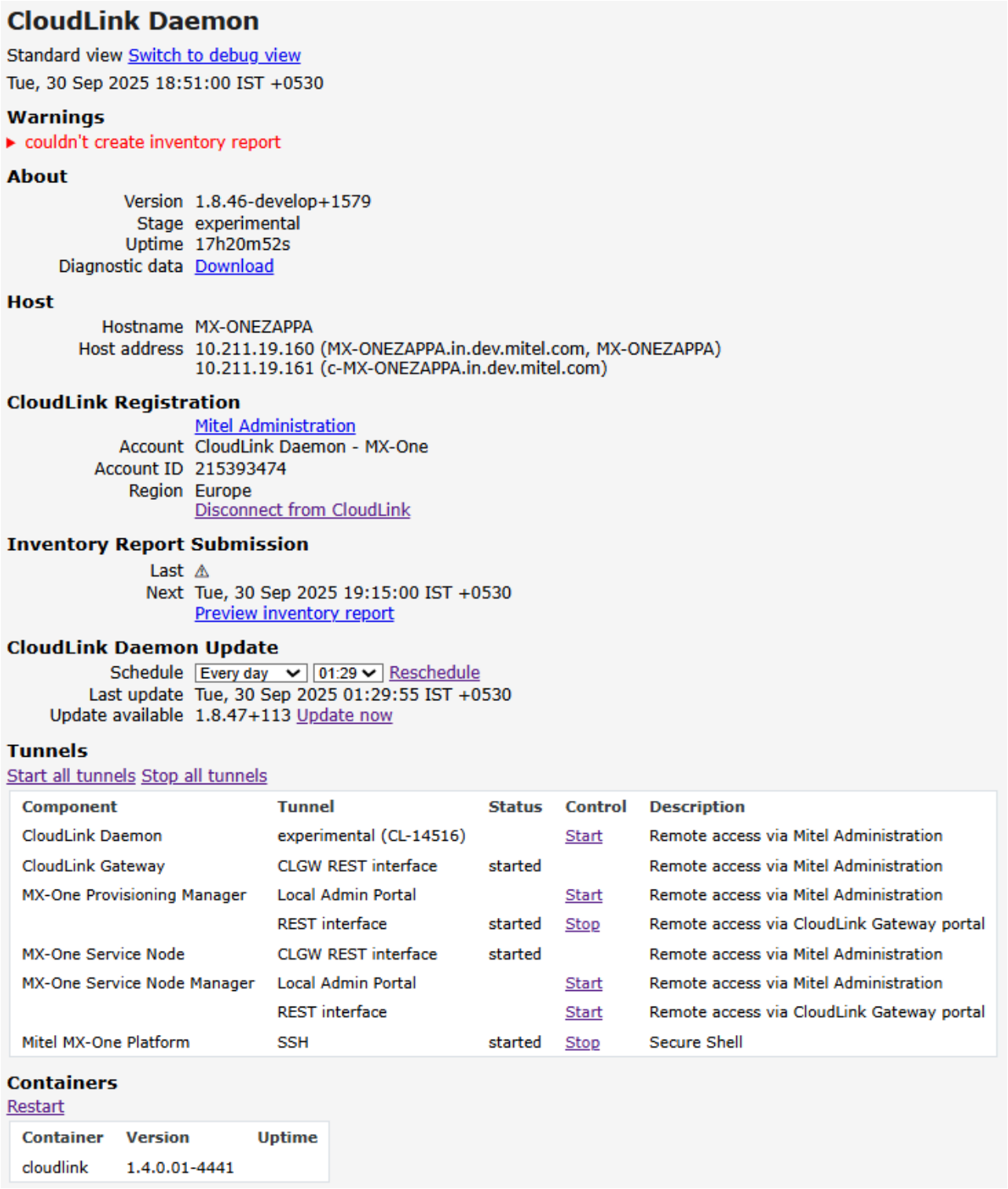


Figure 2: CloudLink Daemon Information

6.2 Integrating MBG SBC with CloudLink

Please refer to MBG documentation for details on how to integrate and start CLD with MBG.

6.3 Configuring PBX System Settings in Mitel Administration

After completing PBX integration with Cloudlink, optionally you can configure the system setting of the PBX. The PBX system settings configured in the CloudLink Account are not directly synced to the PBX. The settings have to be entered manually in the PBX.

Procedure

Note: This configuration is applicable only if you are configuring Emergency calls.

1. Log in to Mitel Administration as an Account Admin.
2. On the left navigation menu click on the name of the PBX. For example, **MiVoice MX-ONE** and select **System Settings**.
3. In the **Voicemail** area add a **Pilot Number** to dial for accessing the voicemail messages.
4. In the **Feature Codes** area, you can configure feature codes for the users.

   To add a feature code:

   a. Select a **Feature** from the drop-down menu.

   - Call Forward
   - Disable Call Forward
   - Do not Disturb
   - Disable Do not Disturb
   - Enable Call Forward
   - Enable Do not Disturb

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

   b. Enter the **Dialing access code**.
   c. To edit a feature code, select the feature code, click on the **Dialing access code** field and edit it as needed.
   d. To delete a feature code, select the feature code and click Delete icon next to the feature code.

5. In the **Emergency Numbers** area you can configure the fallback emergency numbers. To add an emergency number:

   a. Click **Dialables**.
   b. Start typing a number for emergency calls, e.g.: 911, 112.
   c. Press enter, space or add a , (comma) to add the number.
   d. To edit an emergency number, double click on the number and edit it.
   e. To delete an emergency number, click X next to the number.

   You can add multiple emergency numbers.

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

   Key Parameters:

   - **Customer ID**. The unique HELD identifier assigned to your organization by the service provider.
   - **Secret**. The private key or token issued by the service provider to secure communication between Zoom client and the service. This acts as a password and should be treated with high confidentiality.
   - **Extra Headers**. Additional HTTP headers required by the service provider for platform communication. These headers might include custom authentication schemes, API version, or specific configuration options required by the provider. Input must be added in JSON format.

   Note: In some cases, you can retrieve emergency configuration information from your account with your emergency provider. However, it is highly recommended to always verify the settings with your emergency provider.

7. Ensure all the mandatory fields are configured and click **Save**.

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

   You can check and troubleshoot the settings in the **Event History** page.

Configuring MiVoice MX-ONE 7

This chapter contains the following sections:

This chapter describes the Mitel MiVoice MX-ONE configuration for integrating with Zoom clients. The Zoom integration is performed using the following components:

- SBC – MBG is the certified SBC to integrate with Zoom
- CloudLink

Apart from the above components, the MX-ONE also will require specific SRTP settings configuration.

The purpose of MBG SBC connectivity is for Mitel MiVoice MX-ONE to provide the necessary SIP message manipulation and call routing facilities to MBG SBC so that the latter can interconnect to Zoom. The purpose of CloudLink integration is for zoom and MX-ONE ecosystems to interact with each other so it must provide seem less integration with each other.

7.1 Configuring MBG as SBC Subsystem in MX-ONE

Zoom clients use SIP based interface for call-based telephony features. MBG SBC will Provide the SIP based interface for the zoom clients to get MX-ONE services. To achieve this MX-ONE will have to be configured with MBG details. Using these Details MX-ONE configure the MBG to interwork with zoom clients.

Prerequisite

- MBG are created, configured and up. Please refer to MBG guide for details on how to setup and configure MBG.
- MX-ONE system is created and added as subsystem in PM.

Procedure

1. Login to the PM as a **mx-one_admin** user.
2. From the left side navigation tree, select **System > Sub System**.
3. On the main window, Click on **Add**.

4. Configure the parameters as described in the following table.

Note: SBC can be configured as a subsystem within PM, which offers two options: 'Other' and 'MBG'. By default, 'MBG' is selected when adding the SBC subsystem.

Table 3: Adding MBG as Subsystem

Parameter	Sample Value	Description
Subsystem Type	SBC	Select the SBC option from the dropdown list.
SBC Type	MiVoice Border Gateway	Select MBG as the SBC type. For more information, see Key Notes of Parameters on page 31.
MiVoice MX-ONE	MX-ONE	Select the appropriate MX-ONE subsystem.
Use HTTPS	Select Check box	This is selected by Default.
Subsystem Name	OtherSBC	Provide name for MBG subsystem in **Subsystem Name** field .
IP/FQDN Address	10.xxx.x.xx	Enter MBG internal interface IP/ FQDN.
Location	Location01	Select the appropriate location.

Parameter	Sample Value	Description
Consumer Key	mbg	This parameter value must be copied from the MBG server. a. Login to MBG as administrator. b. Navigate to the **MBG >Administrator >Web services**. c. Copy the **Consumer ID** value. d. Paste in this **Consumer Key** field. For more information, see Key Notes of Parameters on page 31.
Consumer Secret	<encryption key value>	This parameter value must be copied from the MBG server. a. Login to MBG as administrator. b. Navigate to the **MBG >Administrator >Web services**. c. Copy the **Shared secret** value. d. Paste in this **Consumer Secret** field. For more information, see Key Notes of Parameters on page 31.

<table>
<tr><th>Parameter</th><th>Sample Value</th><th>Description</th></tr>
<tr><td rowspan="4">Generate Token</td><td colspan="2">Following are the two scenarios to configure this parameter:
• Token is already approved in MBG server:

a. Login to MBG GUI as an administrator.
b. Navigate to the MBG > Administrator > Web Services.
c. Copy the Verifier value from the MBG server to the Verifier field in the PM.

Access Token and Token Secret will get automatically filled and should not be altered.
• Token is not approved in MBG server:

a. Login to MBG GUI as an administrator.
b. Navigate to the MBG > Administrator > Web Services page
c. Click Approve in Temporary Token section.
d. Copy the Verifier value from the MBG server to the Verifer field in the PM.

Access Token and Token Secret will get automatically filled and should not be altered.

For more information, see Key Notes of Parameters on page 31.</td></tr>
<tr><td>Verifier</td><td>Copy the Verifier from MBG server and enter the value in this page.</td></tr>
<tr><td>Access Token</td><td>Ensure that the Token ID from the MBG server is automatically updated in this Access Token field.</td></tr>
<tr><td>Token Secret</td><td>Ensure that theSecret from the M BG server is automatically updated in this Token Secret field.</td></tr>
<tr><td>External Interface</td><td>xx.xx.xx.xxx</td><td>Enter MBG external interface details.</td></tr>
</table>

5. Click on **Apply**.

The MBG integration will be done successfully.

Note: MBG is per MX-ONE system and each individual MX-ONE system can have one or more MBG.

Key Notes of Parameters

SBC Type

If User selects other SBC, Customer can use any other MX-ONE certified SBC for zoom integration, but the SBC must be manually setup and configured by administrator to allow ZOOM client traffic.

IP/FQDN Address and External Interface

MBG will have either single, or 2 interfaces based on the MBG deployment type. In Single interface deployment mode both internal and external interfaces will be same.

Consumer Key and Consumer Secret

MX-ONE will use the MBG Rest interface to configure the MBG. MX-ONE will do this on a secure HTTPS channel and using shared secret. To establish REST based connection with MBG, MX-ONE will initially require Consumer key and Consumer Secret for the specific MBG. Administrators need to copy these values from **Consumer ID** and **Shared secret** fields of **MBG >Administrator >Web services** menu and for MBG specific row. Copy **Consumer ID** and **Shared secret** for MBG and enter these values in **Consumer Key**, **Consumer Secret** field respectively.

Verifier, Access Token, and Token Secret

The following figure depicts the sample MBG Server Information of **Verifier**, **Access Token**, and **Token Secret**.

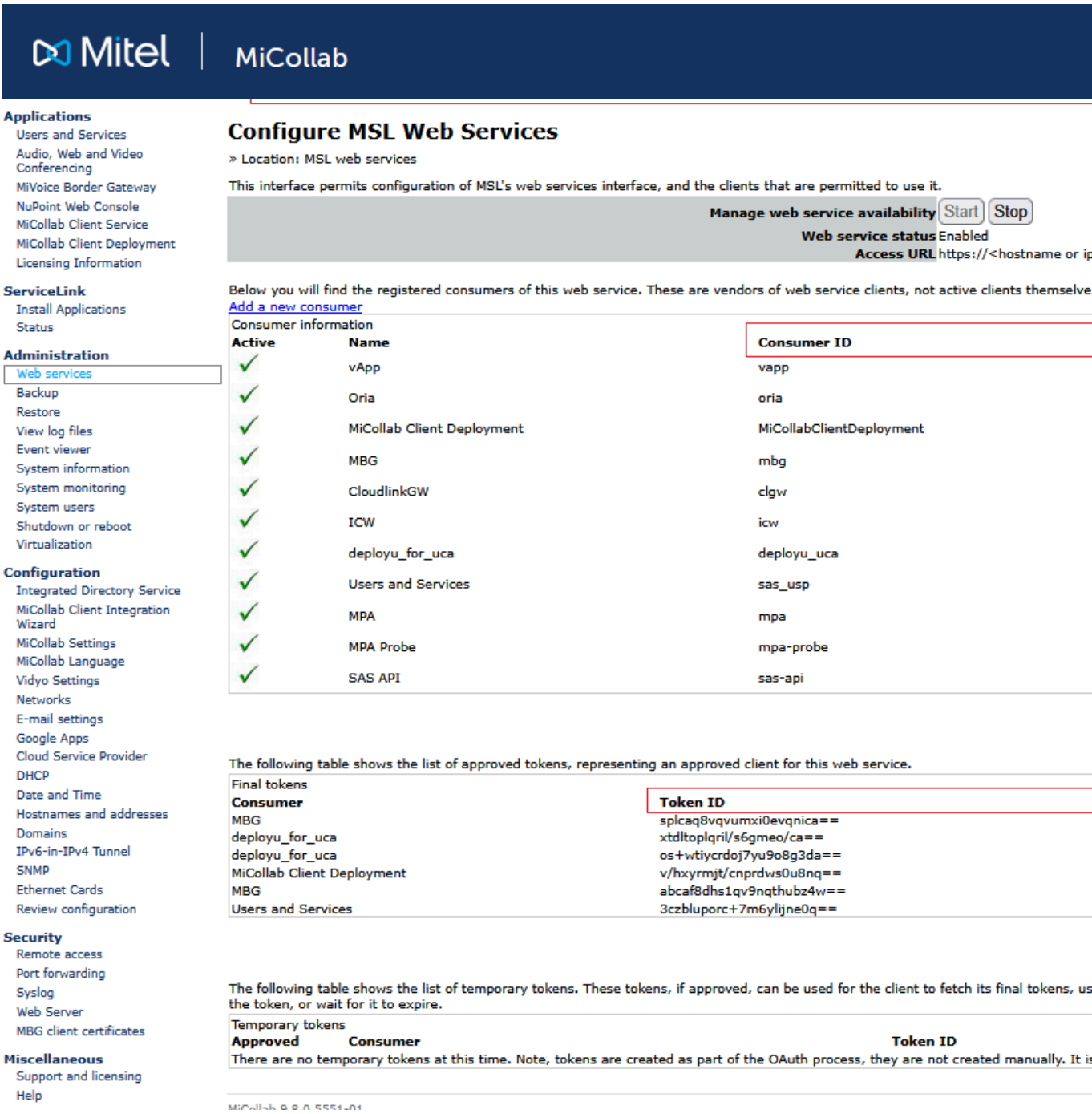


Figure 3: MBG Configuration Information

7.2 Configuring CloudLink Daemon Subsystem

Zoom clients use CloudLink as integration point for integrating with MX-ONE PBX. CloudLink will manage and act as integration point between MX-ONE and ZOOM for provisioning, call-based services, and non-call-based services. CloudLink will interact with MX-ONE using CloudLink Daemons (CLD) running as part of each MX-ONE server. All the CLD servers running in MX-ONE work as a single cluster, with CLD

on SNM as cluster manager. MX-ONE PM must be configured with the cluster manager details for further interaction with CloudLink.

Prerequisite

CLD is installed and registered in MX-ONE, see Configuring CloudLink Integration on page 14.

Procedure

1. Login to the PM as a **mx-one_admin** user.
2. From the left side navigation tree, select **System > Sub System**.
3. On the main window, Click on **Add**.
4. Configure the parameters as described in the following table.

Table 4: Adding CLD as Subsystem

Parameter	Sample Value	Description
Subsystem Type	CloudLink Daemon	Select the CloudLink Subsystem from the dropdown list.
Subsystem Name	CLD	Provide a name for the CloudLink Subsystem.
Location	Location01	Select the appropriate location.
CloudLink Daemon URL	https://10.xxx.xx.xxx/cld	Cloudlink Daemon URL should be set to MX-ONE SNM FQDN/IP. Enter the CLD node manager URL. The format is IP address of LIM1 followed by cld.
MiVoice MX-ONE	MX-ONE	Select the MX-ONE system the CLD belongs to as the PM can manage Multiple MX-ONE system.

5. Click **Apply**.

7.3 Configuring TLS and SRTP Settings

Zoom clients are configured to use TLS and SRTP. To integrate with MX-ONE, the TLS, and STRP should be configured in MBG and MX-ONE. Here are the recommended settings for TLS and STRP.

MBG Settings

SRTP Configuration in MBG GUI:

1. Login to MBG GUI as an administrator.
2. From left side navigation tree select **Applications > MiVoice Border Gateway**.
3. On the main window select **System > Settings**.
4. Scroll to **SIP Options**. In SIP Options, the following configurations are recommended:

> **Note**: For all the other parameters, configure the site specific values.

- Configure **SIP support**:
  - Set **Certificate** as **Web server**.
- Configure **Protocols** and **Access Profile**:
  - In **Protocols** enable **TCP/TLS** and set **Access profile** as **Public**.
- Configure **Set-side RTP security**:
  - Set **Inbound** as **SRTP or RTP**.
  - Set **Outbound** as **SRTP only**.
  - Select **Preferred cipher** as **AES_CM_128_HMAC_SHA1_32**.
- Configure **ICP-side RTP security**:
  - Set **Inbound** as **SRTP or RTP**.
  - Set **Outbound** as **AVP+crypto**.
  - Select **Preferred cipher** as **AES_CM_128_HMAC_SHA1_80**.

5. Click **Apply** to save the configuration.

MX-ONE Settings

SRTP Configuration in MX-ONE:

1. Login to the MX-ONE system as an **mxone_admin** user.
2. Enter the **media_encryption_print** to verify the status. The status should be displayed as follows.

```
Media encryption is enabled for extension
Media encryption is enabled for trunk
```

```
Media encryption is disabled for intermgw
```

To configure (enable/disable) the media encryption, refer to the *201/19082-ANF90114_Technical Reference Guide — Unix Commands*.

7.4 CloudLink Distribute and Sync Options

The MX-ONE Provisioning Manager (PM) provides two key options Distribute and Sync for managing CloudLink configurations.

- The Distribute option reconfigures how PBX services are provided to users from the CloudLink platform, specifically identifying which CSTA server serves each user.
- The Sync option must always be executed after a Distribute operation to complete the reconfiguration successfully.

Use Distribute and Sync when:

- New LIMs are added, requiring updates to which CSTA server provides services to each LIM.
- LIMs are removed, requiring updates to service mappings.
- A CSTA server is added or removed for CloudLink integration.

Use only Sync when:

There is a user data mismatch without any changes to the CSTA server or LIM configuration. In this case, Sync updates user data from the PM database to the CloudLink platform without recalculating CSTA server mappings.

The following figure depicts the CloudLink Distribute and Sync icons in the PM.

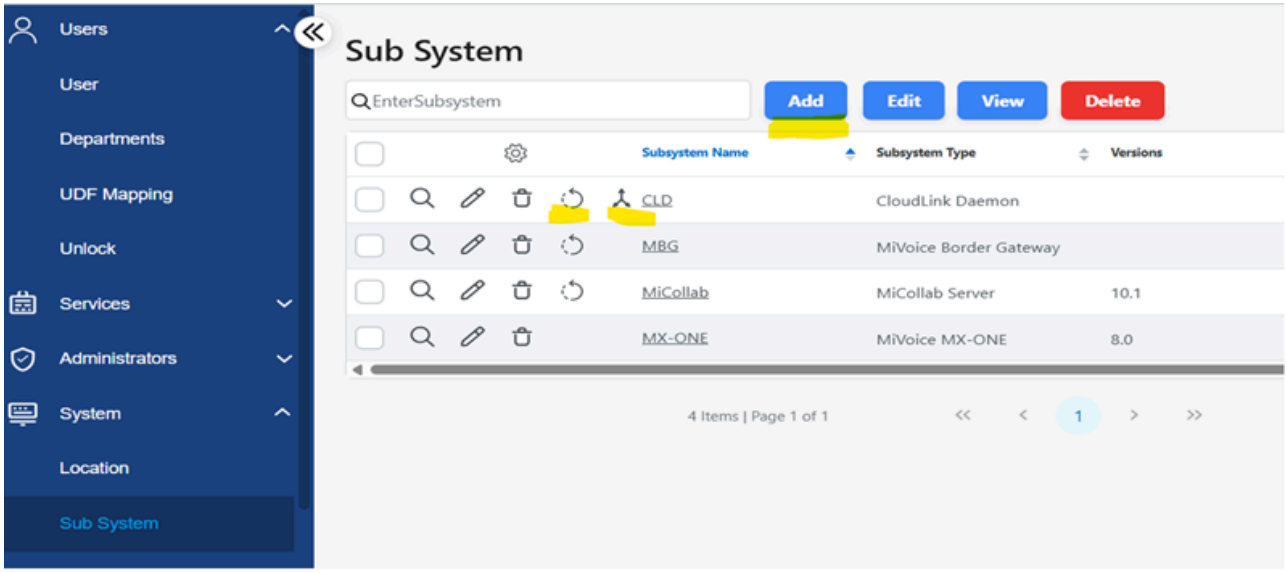


Figure 4: CloudLink Distribute and Sync Icons

Provisioning Users 8

This chapter contains the following sections:

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

8.1 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

8.1.1 Adding a New Zoom User

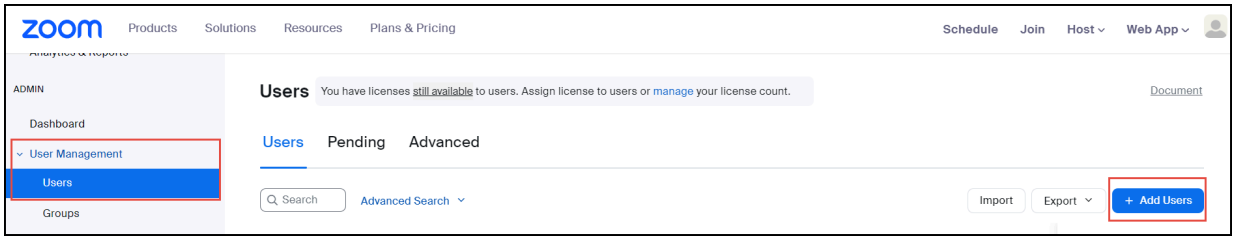
An account owner or admin can add users to their account in several ways. This section describes how to add a single new Zoom User, or multiple users by entering their email addresses.

Important: To successfully enable Zoom PSI user provisioning for a customer who has not previously used Zoom, you must ensure that in the Zoom admin, the settings are adjusted so that users are not required to install the Zoom client before the final provisioning process can be completed.

Prerequisites:

- You have a Zoom account, Business or Enterprise.
- You are an Account Owner or Admin with a Role for managing Users, Phone System Integration, and Zoom Phone.
- You have completed Zoom-CloudLink integration, as described in Integrating Zoom with CloudLink.

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:

Note:

Email address is the unique cross-platform identifier for provisioning Zoom and CloudLink users. i.e. The CloudLink user and zoom user must have same email address configured in the respective system to integrate.

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

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

   New Zoom users will receive an activation email.

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

Next Steps

- Activate the user(s) account.

- Assign licenses to users. Before assigning a license to a phone user, ensure that automatic phone assignment for Zoom One licenses is disabled for your account. For more information, refer to the Assigning Zoom Licenses page.

8.1.2 Setting up the Zoom Account from Invitation

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

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

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.

8.1.3 Configuring Phone System Integration Settings

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

1. Log in to the Zoom Admin Portal.
2. Navigate to **Account Management** > **Phone System Integration**.
3. Go to the **Settings** tab.
4. By default, in the **Integrated calling on Zoom mobile** area, the **Allow use the integrated phone system to phone call on Zoom mobile client** toggle is enabled. If it is not enabled, click to turn it on.

Note:

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

8.1.3.1 Adding Zoom Users to the Mitel Integration

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

Prerequistes:

- 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.

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.

> **Note**:
>
> 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 MX-ONE subscriber-Zoom user integration is completed.

   To add non-Zoom users to Zoom directory, refer to the Creating a shared directory of external contacts page and MX-ONE BYOC documentation.

   To import users with a CSV file, refer to Zoom-Mitel Phone System Integration support page.

8.2 Enabling an MiVoice MX-ONE Subscriber for a Zoom Connection

As a MX-ONE PM administrator, you must manually configure the MX-ONE subscriber(s) to enable their Zoom connection.

8.2.1 Prerequisites

- Adequate administrative permissions.
- PM is connected to CloudLink Daemon, See Configuring CloudLink Integration on page 14.
- MX-ONE is connected to CloudLink, See Configuring CloudLink Integration on page 14.
- You have provisioned users in the Zoom tenant, See User provisioning in the Zoom Tenant on page 36.

8.2.2 Enabling Existing MX-ONE User

To enable an existing MX-ONE user:

1. Log in to the MX-ONE Provisioning Manger Platform.
2. Navigate to **Users > User**.
3. Click on the MX-ONE user you want to enable.

   The **User >Update** window pops up.
4. Go to the **CloudLink Configuration** subsection.
5. Locate the **Zoom Client** checkbox and click on it to enable it.
6. While enabling the user for Zoom client it's a must that user resets the authorization code.

   Set strong alphanumeric authorization code.
7. Click Apply, the existing users will have zoom capability enabled.

8.2.3 Creating New MX-ONE user with Zoom Capability

To create a new MX-ONE user with Zoom Capability:

1. Log in to the MX-ONE Provisioning Manger Platform.
2. Navigate to **Users > User**.
3. Click on the **ADD**.

   The **User >Add** window pops up.
4. Fill all the details required to create MX-ONE user.
5. Go to the **CloudLink Configuration** subsection.
6. Locate the **Zoom Client** checkbox and click on it to enable it.
7. While enabling the user for Zoom client it's a must that user resets the authorization code.

   Set strong alphanumeric authorization code.
8. Click Apply, the existing users will have zoom capability enabled.

Configuring CLD for External Communication via DMZ Proxy

9

This topic describes how to configure the CloudLink Daemon (CLD) in MX-ONE to use an external HTTPS proxy deployed in the DMZ for secure outbound communication with CloudLink services.

Deploying the CLD behind a DMZ HTTPS proxy allows controlled and secure outbound connections from the MX-ONE Service Node to CloudLink public services. When configured, CLD uses the proxy for downloading updates, creating HTTPS tunnels, and accessing CloudLink APIs. The proxy settings are provided to CLD via an environment file so the service runs with the correct proxy context.

Prerequisites

- The network administrator must provision and manage the HTTPS proxy in the DMZ.
- You must have root (or equivalent) access on the Service Node where CLD runs.
- The proxy configuration should only be used in LIM1 (SNM — Service Node Manager) as applicable to your environment.
- The proxy configuration file must follow standard Linux environment variable syntax.
- Add the PM (Provisioning Manager) IP with port `8289` in the `NO_PROXY` list to bypass the proxy for internal communication.
- Ensure proper file ownership and permissions for `/var/lib/cld/proxy-settings.env` to protect credentials.
- If the proxy configuration file does not exist, CLD will run without proxy usage.
- Proxy setup and installation in the DMZ must be handled by the network administrator.

Procedure

1. Login to the MX-ONE system as an Administrator.
2. The CLD proxy configuration file is located at `/var/lib/cld/proxy-settings.env`. If this file does not exist, CLD will not use a proxy.
3. Open `/var/lib/cld/proxy-settings.env` in a text editor (for example `vi` or `nano`).
4. Add the HTTPS proxy environment variable exactly as required. Do not modify the example command text below:

```
https_proxy='https://user:pass@server:port/'
```

Alternatively, supported syntax examples:

```
HTTPS_PROXY="http://<proxy-server>:<port>"
HTTPS_PROXY="http://123.123.123.123:8443"
```

5. Configure `NO_PROXY` to exclude local or internal addresses (include PM IP:8289 if required).

   Examples:

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

> **Note**: The file syntax must follow standard Linux environment variable conventions.

6. Ensure the file is owned and readable by the user running CLD (typically root) and restrict access to protect credentials.

```
chown root:root /var/lib/cld/proxy-settings.env
chmod 600 /var/lib/cld/proxy-settings.env
```

7. The proxy configuration is passed to CLD via environment variables and CLD must be restarted for changes to take effect. Restart using the appropriate service manager.

```
# For systemd
systemctl restart cld

# For SysVinit
service cld restart
```

8. CLD logs the environment variable value during startup, check the CLD logs to confirm the proxy value is picked up.
9. Confirm CLD can download updates, establish HTTPS tunnels, and access CloudLink APIs via the proxy. Check CLD logs for successful startup and proxy configuration, and optionally verify proxy/firewall logs to ensure outbound HTTPS traffic is routed through the DMZ proxy.

Disable Proxy Usage (Optional)

> **Note**: Disabling the proxy is not mandatory. It is only required if the MX-ONE Service Node gains direct internet access, the proxy becomes unavailable, or connectivity troubleshooting is needed.

To disable proxy usage, remove `/var/lib/cld/proxy-settings.env` and restart the CLD. After restart, CLD will no longer use a proxy.

Monitoring and Troubleshooting Zoom Integration in Mitel CloudLink Admin Portal 10

This chapter contains the following sections:

10.1 Viewing the Zoom Integration Status

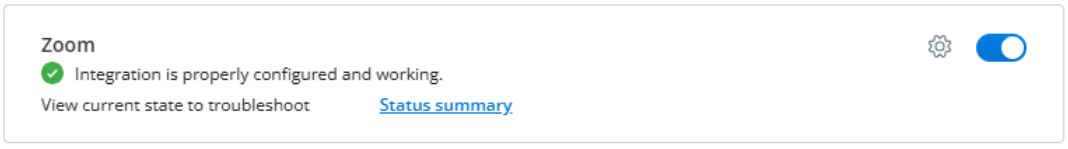
Once the Zoom integration is added to a customer account, you can check its status to ensure it is set up properly. The Zoom integration can have one of the following statuses:

- `Connected`
- `Error`
- `Pending`

Viewing a summary of the Zoom Integration Status

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

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



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

Viewing Detailed Information About the Zoom Integration Status

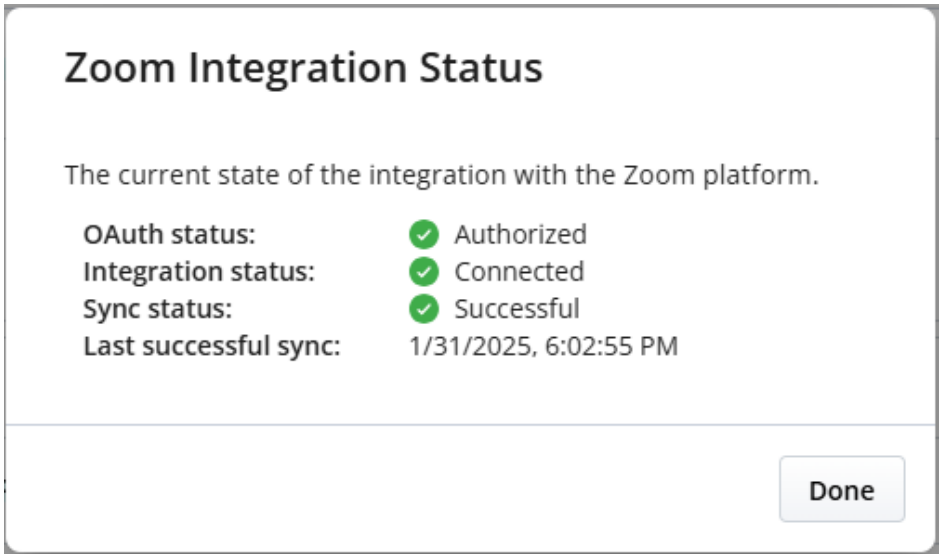
For a more in-depth view of the Zoom integration status, especially for troubleshooting, you can one of the following:

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

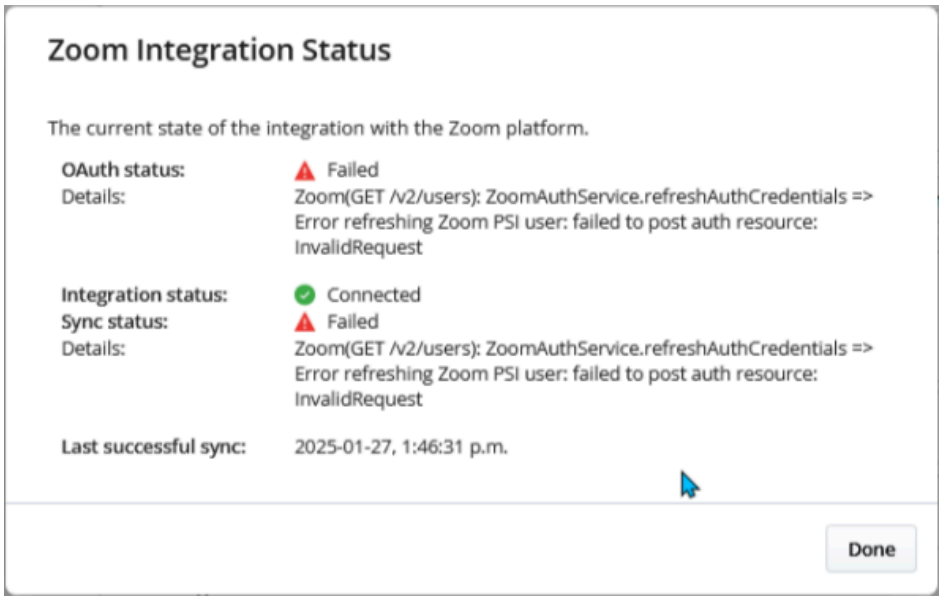
You can then view detailed information about the Zoom integration status, including the following:

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

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



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.

Refreshing the Zoom integration status

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

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

10.2 Generating a User Comparison Report

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

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

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

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

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.

10.3 Troubleshooting Common Issues Identified in the User Comparison Report

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

Below are the potential issues and the recommended resolution:

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

Steps to Validate and Fix Issues

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

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

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

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

10.4 Viewing the Event History Table (Zoom Integration)

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

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.

Configuring E911 Calls 11

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.

MX-ONE, 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 MX-ONE, 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, MX-ONE is integrated with Intrado in USA and with Redsky in USA and Canada. A valid service agreement with either RedSky or Intrado is necessary for the E911 Solution.

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

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

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

Emergency Call Flow

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

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

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

For MX-ONE Voice Emergency Calling information, refer to MX-ONE administrator guide.

For CloudLink Emergency configurations, refer to Configuring the PBX system Settings settings section (Steps 5 to 6).

To complete the Mitel MiVoice MX-ONE and MBG SBC configurations required for an Emergency Solution, please refer the MX-ONE administrator guide.